Windows Authentication on Microsoft SQL Server

Introduction

Microsoft SQL Server offers two types of security authentication: *SQL Server authentication* and *Windows authentication*. SQL Server authentication authenticates the user to the database using a database user name and password. Windows authentication is also referred to as "Windows Integrated Security" or a "trusted connection" because it relies on the user being authenticated, or “trusted,” by the operating system. Windows authentication is the authentication mode recommended by Microsoft.

Windows authentication takes advantage of Windows user security and account mechanisms. By allowing Microsoft SQL Server to share the user name and password used for Windows, users with a valid Windows account can log into Microsoft SQL Server without supplying a user name and password. In addition to a single login within a Windows domain, Windows authentication provides a more secure mechanism for logging into Microsoft SQL Server. Standard Windows security mechanisms also provide the added advantages of auditing, password aging, minimum password length, and account lockout after multiple invalid login requests.

The DataDirect Connect® *for* JDBC® SQL Server driver is the only JDBC driver for Microsoft SQL Server that provides two methods for supporting Windows authentication, a Pure Java (Type 4) implementation and a Windows-specific (Type 2) implementation. The Windows-specific implementation requires minimal configuration to enable Windows authentication; however, it can only be used when the driver is running on a Windows platform. The Pure Java implementation is not restricted to Windows platforms, but requires configuration of your Kerberos environment.

This document describes both types of Windows authentication methods supported by the DataDirect Connect *for* JDBC SQL Server driver and provides an overview of the configuration required to use each method. Finally, it describes the current limitations and future enhancements planned for this functionality.

Choosing a Windows Authentication Mechanism

The DataDirect Connect *for* JDBC SQL Server driver provides the following methods for supporting Windows authentication:

- **Pure Java (Type 4) authentication** supports connections in a Windows domain running Windows Active Directory. The DataDirect Connect *for* JDBC SQL Server driver is the only JDBC driver on the market that supports Windows authentication while remaining a pure Type 4 JDBC driver. DataDirect Technologies has a patent pending on this innovative technology. This authentication method supports Kerberos authentication, an authentication protocol that is an integral component of Windows Active Directory.

- **Windows-specific (Type 2) authentication** requires that the DataDirect Connect *for* JDBC SQL Server driver be installed on a Windows client; however, it supports both NT LAN Manager (NTLM) and Kerberos authentication.

The Pure Java authentication method is important to many Java developers because it eliminates the need to install database-specific client libraries or additional shared libraries. It requires J2SE 1.4 or higher and knowledge of how to configure Windows Active Directory and Kerberos to support this functionality.

The Windows-specific method requires J2SE 1.2 or higher and requires minimal configuration. In addition, it can be used in both Windows Active Directory and NTLM domains.

Configuring for Pure Java Windows Authentication

Pure Java Windows authentication supports connections to Microsoft SQL Server 2000 and Microsoft SQL Server 2000 Enterprise Edition (64-bit) SP2 or higher in a Windows domain running Windows Active Directory. This authentication method supports Kerberos authentication, an authentication protocol that is an integral component of Windows Active Directory.

Setting the AuthenticationMethod Property

You set the DataDirect Connect *for* JDBC SQL Server driver's AuthenticationMethod connection property to control which authentication method is used by the driver. For example, the following connection URL specifies that Pure Java Windows authentication will be used for the connection if a user name is not specified:

```
jdbc:datadirect:sqlserver://server1:1433;AuthenticationMethod=type4
```

Alternatively, you can configure the driver to automatically select the appropriate Windows authentication method to use for the connection based on a combination of criteria, such as whether the application provides a user ID, the driver is running on a Windows platform, and the driver can load the DLL required for Windows-specific Windows authentication. For example:

```
jdbc:datadirect:sqlserver://server1:1433;AuthenticationMethod=auto
```

For more information about setting the AuthenticationMethod connection property, refer to the *DataDirect Connect for JDBC User's Guide and Reference*.

Configuring Your Kerberos Environment

To use Pure Java Windows authentication with the DataDirect Connect *for* JDBC SQL Server driver, configuration is required on the Microsoft SQL Server database server, the domain controller, and the client machine as summarized in Table 1. DataDirect Connect *for* JDBC performs some of this configuration for you during installation.

Table 1: Configuring Your Kerberos Environment for Pure Java Windows Authentication

Component	Configuration
Domain controller	• Make sure that the Active Directory encryption property is set to use DES encryption in the Microsoft SQL Server Service Startup Account. • Make sure that a Service Principal Name (SPN) has been created for each Microsoft SQL Server instance to allow the Kerberos Key Distribution Center (KDC) to provide authentication to your Microsoft SQL Server database.
Microsoft SQL Server database server	• Set the authentication mode to Windows Only or Mixed authentication. • Configure the login properties of the user IDs and passwords used to log on the database server and for the Service Startup Account used to start the Microsoft SQL Server instance.
Client	• Modify the Kerberos configuration file to reference your environment. • A login configuration file is automatically installed and configured when you install DataDirect Connect *for* JDBC.

For more information about configuring your environment for Pure Java Windows authentication, including detailed instructions for each of these configuration steps, refer to the *DataDirect Connect for JDBC User's Guide and Reference*.

Configuring for Windows-Specific Authentication

Windows-specific authentication requires that the DataDirect Connect *for* JDBC SQL Server driver be installed on a Windows client; however, it supports both NTLM and Kerberos authentication for Microsoft SQL Server 2000 SP3 or higher and Microsoft SQL Server 2000 Enterprise Edition (64-bit) SP2 or higher.

Setting the AuthenticationMethod Property

You set the DataDirect Connect *for* JDBC SQL Server driver's AuthenticationMethod connection property to control which authentication method is used by the driver. For example, the following connection URL specifies that Windows-specific Windows authentication will be used for the connection if a user name is not specified:

```
jdbc:datadirect:sqlserver://server1:1433;AuthenticationMethod=type2
```

Alternatively, you can configure the driver to automatically select the appropriate Windows authentication method to use for the connection based on a combination of criteria, such as whether the application provides a user ID, the driver is running on a Windows platform, and the driver can load the DLL required for Windows-specific Windows authentication. For example:

```
jdbc:datadirect:sqlserver://server1:1433;AuthenticationMethod=auto
```

For more information about setting the AuthenticationMethod connection property, refer to the *DataDirect Connect for JDBC User's Guide and Reference*.

Using the Windows-Specific Authentication DLL

To use Windows-specific authentication with the DataDirect Connect *for* JDBC SQL Server driver, copy the appropriate Windows-specific authentication DLL to a directory on the Windows system path on the machine where you have installed the driver. DataDirect Connect *for* JDBC provides two Windows-specific authentication DLLs, a 32-bit and a 64-bit version. If the application using Windows-specific Windows authentication is running in a 32-bit Java Virtual Machine (JVM), the driver uses the 32-bit version of the DLL. Similarly, if the application is running in a 64-bit JVM, the driver uses the 64-bit version.

Alternatively, you can set the java.libary.path system property to specify the directory of the Windows-specific authentication DLL. For example, if the DataDirect Connect *for* JDBC SQL Server driver is installed in a directory named "DataDirect," you can specify the location of the DLL by using the following Virtual Machine argument when the Java application is started:

```
-Djava.library.path=C:\DataDirect\lib
```

For more information about configuring your environment for Windows-specific authentication, refer to the *DataDirect Connect for JDBC User's Guide and Reference*.

Using Windows Authentication with a Security Manager

If the DataDirect Connect *for* JDBC SQL Server driver is used on a Java 2 Platform with a Security Manager, you must grant certain permissions to the DataDirect Connect *for* JDBC SQL Server driver in the security policy file of the Java 2 Platform. The security policy file is located in the jre/lib/security subdirectory of the Java 2 Platform installation directory. The permissions that must be granted depend on whether the driver is using Pure Java or Windows-specific Windows authentication.

Pure Java Windows Authentication

For Pure Java authentication, security permissions must be granted to the application and the driver. For example:

```
grant codeBase "file:/Program Files/DataDirect/Connect for JDBC/lib/-" {
   permission javax.security.auth.AuthPermission
      "createLoginContext.DDTEK-JDBC";
   permission javax.security.auth.AuthPermission "doAs";
   permission javax.security.auth.kerberos.ServicePermission
      "krbtgt/Kerb_realm1@Kerb_realm1", "initiate";
   permission javax.security.auth.kerberos.ServicePermission
      "MSSQLSvc/SQLServer_server1:1433@Kerb_realm1", "initiate";
};
```

Windows-Specific Windows Authentication

For Windows-specific authentication, the only permission that must be granted is one to allow the driver to establish connections. For example:

```
grant codeBase "file:/Program Files/DataDirect/Connect for JDBC/lib/-" {
   permission java.net.SocketPermission "*", "connect";
};
```

In addition, if Microsoft SQL Server named instances are used, permission must be granted for the listen and accept actions as shown in the following example:

```
grant codeBase "file:/Program Files/DataDirect/Connect for JDBC/lib/-" {
   permission java.net.SocketPermission "*", "listen, connect, accept";
};
```

Future Enhancements

Currently, DataDirect Connect *for* JDBC supports Windows authenticated connections to Microsoft SQL Server 2000 or Microsoft SQL Server 2000 Enterprise Edition (64-bit) from a Windows client.

For future versions of the DataDirect Connect *for* JDBC drivers, the current Windows Authentication functionality will be enhanced to support:

- Pure Java authentication from UNIX clients
- MIT Kerberos KDC support
- Pure Java authentication for DB2, Oracle, and Sybase

Conclusion

The DataDirect DataDirect Connect *for* JDBC SQL Server driver is the only JDBC driver for Microsoft SQL Server that provides two methods for supporting Windows authentication, a Pure Java (Type 4) implementation and a Windows-specific (Type 2) implementation. Both methods of Windows authentication supported by the DataDirect Connect *for* JDBC driver provide secure connections for your applications to Microsoft SQL Server.

We welcome your feedback! Please send any comments concerning documentation, including suggestions for other topics that you would like to see, to:

docgroup@datadirect.com

FOR MORE INFORMATION

800-876-3101

Worldwide Sales

Belgium (French).....0800 12 045
Belgium (Dutch).....0800 12 046
France.....0800 911 454
Germany.....0800 181 78 76
Japan.....0120.20.9613
Netherlands.....0800 022 0524
United Kingdom.....0800 169 19 07
United States.....800 876 3101

DataDirect TECHNOLOGIES

DataDirect Technologies is focused on standards-based data connectivity, enabling software developers to quickly develop and deploy business applications across all major databases and platforms. DataDirect Technologies offers the most comprehensive, proven line of data connectivity components available anywhere. Developers worldwide at more than 250 leading independent software vendors and thousands of corporate IT departments rely on DataDirect® products to connect their applications to an unparalleled range of data sources using standards-based interfaces such as ODBC, JDBC™ and ADO.NET. Developers also depend on DataDirect to radically simplify complex data integration projects using XML products based on the emerging XQuery and XQJ standards. DataDirect Technologies is an operating company of Progress Software Corporation (Nasdaq: PRGS), a US$300+ million global software industry leader. Headquartered in Bedford, Mass., DataDirect Technologies can be reached on the Web at http://www.datadirect.com or by phone at +1-800-876-3101.