Release Notes

IBM® Tivoli® Identity Manager

SQL Server 2000 Adapter

Version 4.6.6

Tenth Edition (September 3, 2010)

This edition applies to version 4.6 of this Adapter and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Preface

Welcome to the IBM Tivoli Identity Manager SQL Server Adapter.

These Release Notes contain information for the following products that was not available when the IBM Tivoli Identity Manager manuals were printed:

- IBM Tivoli Identity Manager SQL Server Adapter Configuration and Installation Guide

Adapter Features and Purpose

The SQL Server Adapter is designed to create and manage SQL Server accounts. IBM recommends the installation of this Adapter on a Windows 2000, Windows 2003 or XP workstation. Typically, one adapter is installed to manage multiple SQL Server databases. The optimum deployment configuration is based, in part, on the configuration of your SQL Server databases, but the primary factor is the planned structure of your Identity Manager Provisioning Policies and Approval Workflow process. Please refer to the Identity Manager Policy, Organization & Administration Guide for a discussion of these topics.

The SQL Server Adapter is a powerful tool that requires Administrator Level authority. The Adapter operates much like a human system administrator, creating accounts and assigning privileges. Operations requested from the Identity Manager server will fail if the Adapter is not given sufficient authority to perform the requested task. IBM recommends that this Adapter run with administrative permissions.

Contents of this Release

Adapter Version

Component	Version
Release Date	September 3, 2010
Adapter Version	4.6.6 (build 4.6.1008)
Comm. Libraries	ADK v4.805
Documentation	SQL Server 2000 Adapter Installation and Configuration Guide v4.6.0 SC32-1230-03

New Features

Enhancement # (FITS)	Description
	Items included in current release
MR0326106750	SQL Server adapter: unlock account at password change See Configuration Notes for more information.
	Items included in release 4.6.5
MR0824095956	Need secure connection from SQL adapter to SQL server. Please refer your SQL Server product documentation to setup secure communication (SSL) between SQL Client and SQL Server.
MR1202085222	Support all admin login options for SQL Server adapter
	Items included in release 4.6.4
N/A	This version of adapter is certified for Windows 2008 32 bit and Windows 2008 64 bit.
	Items included in release 4.6.3
OR0214067055	Support for SQL Server 2005 o supports Sql Server 2000 and 2005 o supports ADO. DBlibrary support has been removed. o supports unicode. Previous agent used to support char only. o xforms.xml has been removed from this version of the adapter o database access attribute from old version of the agent is now split into 4 attributes - database roles, user alias, database user and user schema (only for Sql Server 2005) o new support data - server roles, database roles, user schema

Enhancement # (FITS)	Description
	Items included in release 4.6.1
MR0823054737	SQL Server: support multiple SQL Servers from a single instance of the adapter. CAUTION: This multi-instance feature requires the SQL Server Admin Account and Password on the Service Form. IBM recommends enabling the encryption of the SQL Admin Password attribute (ersql2000adminPassword) before importing the profile (provided with this release) and creating any services. Please see "Configuring SQL Administrator Password Encryption" (below) for additional information.
	Items included in release 4.6.0
	Updated Adapter to support ITIM 4.6

Closed Issues

DevTrack	APAR#	PMR# / Description
		Items closed in current version
	IZ78139	02876,001,666 Warning returned by SQL adapter if default DB and DBUser for default database are both defined with the same value. Functionality change! Please see Configuration Notes for more information.
	IZ78158	02923,001,666 Transaction failure returned when using PreExec with SQL Adapter if no other attributes are passed in the request.
	IZ80899	02940,001,666 MSSQL Adapter 5.0.5 Password Change broken
	IZ58983	N/A Certtool unable to list certificate Verisign Class 3
36607		N/A Incorrect return status for multi-valued attribute with special characters.
		Items closed in version 4.6.5
		None
		Items closed in version 4.6.4
32915 32993 32994	N/A	N/A (internal defects) ○ SQL Adapter fails to set password related attributes. ○ SQL Server adapter crash. ○ SQL server Adapter not able to restore account.
		Items closed in version 4.6.3
N/A	N/A	N/A Replaced Attribute "erSQL2000AdminPassword" with erServicePwd1" to ensure encryption of the Service Form passwords.
		Items closed in version 4.6.1
S17252	IY82756	76159,344,000 Password change fails if the first character is numeric.

Known Issues

DevTrack	APAR#	PMR# / Description
		Class 3 Certificates Class 3 Certificates (class 3 secure server CA-G2) are not written properly to "DamlCACerts.pem" file through CertTool.exe Utility. The certificate data is written twice between BEGIN CERTIFICATE and END CERTIFICATE. Work around: To correct this issue, please follow the below steps and edit "DamlCACerts.pem" file present in "<Adapter installation path>\data" folder. Step 1. Start the CertTool utility Step 2. Import the class 3 CA certificate by using "F" option from the main menu of CertTool Utility. Step 3. Once the class 3 CA certificate is successfully installed, open "DamlCACerts.pem" file stored in the "<Adapter installed path>\data" folder using text editor. Step 4. Delete the class 3 CA certificate data (i.e. content between BEGIN CERTIFICATE and END CERTIFICATE) from "DamlCACerts.pem". Step 5. Open class 3 CA certificate file using text editor and copy the certificate data (between the BEGIN CERTIFICATE and END CERTIFICATE) Step 6. Paste the certificate data to "DamlCACerts.pem" file between the BEGIN CERTIFICATE and END CERTIFICATE lines of same class 3 CA Certificate. If more than one class 3 certificates are installed then you can identify the certificate using issuer and subject data. Step 7. Save "DamlCACerts.pem" file. Step 8. To verify the "DamlCACerts.pem" file is edited properly, display certificate information by using option "E" from the main menu of CertTool Utility. Note: Please note that this issue is seen after installing class 3 CA certificate. If you correct the DamlCACerts.pem and then install another class 3 CA certificate, the newly installed class 3 CA certificate will show same issue. This issue is also seen when you delete any certificate using option "G" from the main menu of CertTool utility. The delete option will affect all remaining class 3 CA certificate and you have to follow step 1 to 8 to correct the DamlCACerts.pem file.

Installation and Configuration Notes

See the IBM Tivoli Identity Manager SQL Server Adapter Installation Guide for detailed instructions.

Corrections to Installation Guide

The following corrections to the Installation Guide apply to this release:

None.

Configuration Notes

The following additions to the Installation Guide apply to this release:

General Configuration Notes

NOTE: "BUILTIN\ADMINISTRATORS" and "sa" are returned in a RECON; however, they cannot be deleted. These accounts should not be suspended or managed through the IBM Tivoli Identity Manager system.

Syntax for specifying user's access and roles on the Database Access tab:

Database Role	dbname:dbroleName	i.e master:db_owner
Database User	dbname:dbuser	i.e pubs:vijay
Database Alias	dbname:aliasName	i.e pubs:myalias
Database Schema	dbname:schemaName	i.e pubs:administerSchema

Enabling Encryption of the SQL Administrator Password

The multi-instance enhancement allows a single adapter process to service requests from multiple ITIM Services. The adapter now requires the SQL Server Name, Administrator Account and Administrator Password on the Service form. This information is sent on each adapter request so that the adapter can connect and process the transaction. This version of the adapter now encrypts these attributes by default. Please note that the name of this attribute has changed from ersql200adminPassword to erServicePwd1.

New Features in Version 4.6.5 of this Adapter

Earlier version of adapter was using only "SQL Server Authentication" for connecting to SQL Server. From this version "Windows Authentication" can be used for SQL server adapter admin account. Adapter is also enhanced to use SSL communication between adapter and SQL Server.

To support this enhancement schema of SQL Server Adapter is extended.

Following attributes are defined in schema.dsml and are added to "erSQL2000DAMLService" class

i. Integer attribute "erSQL2000AuthMethod(OID: 1.3.6.1.4.1.6054.3.61.2.24)"
ii. Boolean attribute "erSQL2000SSL(OID: 1.3.6.1.4.1.6054.3.61.2.25)"

Following New labels are added in Customlabel.properties file

i. **Authentication** for attribute **ersql2000authmethod**
ii. **Use SSL for Adapter to SQL Server Connection** for attribute **ersql2000ssl**
iii. **SQL Server Authentication** for dropdown item **tag.sqlauthmethod.sql**
iv. **Windows Authentication** for dropdown item **tag.sqlauthmethod.windows**

If one wants to use same adapter instance to manage multiple SQL servers then all must support SSL and the adapter service must run under a windows account (Active Directory domain account). This account must have required permission on all these instances of SQL server. If any SQL server instance is in different domain then trust between Windows domain must exists. If domain setup does not exist and these are individual servers (e.g. SQL server running on standalone Windows OS say Windows 2003) then you must install one adapter per SQL server.

SQL Admin Account and *SQL Admin Password* service form attribute values are not required if "Windows Authentication" option is selected for *Authentication* service form attribute.
By default SQL Authentication is used for connection and SSL communication is false.

Note:

1. *SQL Admin Account* and *SQL Admin Password* attributes are ignored if provided with "Windows Authentication".
2. Only Windows Authentication can be used with SSL. SSL Communication with SQL authentication is not supported.
3. SSL is not supported with all versions of SQL server. Please refer your SQL server product documentation before configuring adapter to use SSL with SQL server.

New Features in Version 4.6.6 of this Adapter

MR0326106750 - SQL Server adapter: unlock account at password change
Earlier version of adapter was not supporting UNLOCK option on a SQL user account. From this version SQL Server adapter can be used to unlock SQL user account directly from account form or during password change operation.

To configure this feature, a new registry key “UnlockOnPasswordChange” is added; by default value of this registry key is set to FALSE.

Find below table for the functionality of this key:

Value of “UnlockOnPasswordChange”	**Adapter Behavior**
TRUE	***Password Change Operation on a locked account:*** Adapter changes password and unlocks the account. **Restore with Password on a locked account:** Adapter Restores the account, changes password and unlocks the account.
FALSE	***Password Change Operation on a locked account:*** Adapter changes password and account is not unlocked. **Restore with Password on a locked account:** Adapter restores the account, changes password and account in not unlocked

To support this enhancement schema of SQL Server Adapter is extended.
Following attributes are defined in schema.dsml and are added to “erSQL2000DAMLService” class

i. Boolean Attribute “erSQLisaccountlocked(OID: 1.3.6.1.4.1.6054.3.61.2.26)”

Following New labels are added in Customlabel.properties file

i. **Account is Locked** for attribute **erSQLisaccountlocked**

ii. **True** for attribute **tag.option.True**

iii. **False** for attribute **tag.option.False**

Note:

1. **Account is Locked** attribute is set to TRUE in add operation, adapter returns warning "WARNING : Account cannot be locked by agent, only unlocked."

2. **Account is Locked** attribute is set to TRUE in Modify operation there are two different behaviors by adapter on locked and unlocked account

   Account is Locked on resource:
   Adapter returns SUCCESS if the account is locked on the resource
   Account is not Locked on resource:
   Adapter returns Warning "WARNING : Account cannot be locked by agent, only unlocked." If the account is not locked on resource.

3. **Account is Locked** attribute is set to FALSE, account gets unlocked.

IZ78139 - WARNING RETURNED BY SQLADAPTER IF DEFAULTDB DEFINED AND DBUSER FOR DEFAULT DATABASE ALSO DEFINED FOR COMPLIANCE

From this version of adapter, functionality of adding user into SQL Server is changed. In previous version (Before Build Number: 4.6.1008) of SQL Server Adapter, adapter is adding user in the "Default Database" (by default in master database) when adding login in MS SQL Server. In current version of adapter, adapter does not create user in the default database. If you want to add the user in default database then specify it in the attribute Database User.

Example: If you want to add login "ABC" with default database "model", you must specify "Default Database" as "model". If you want to add user in the database also, you have to specify attribute "Database User" as "model:ABC"

Corrections to Installation Guide

The following corrections to the Installation Guide apply to this release:

Creating a SQL server service

The SQL server service form contains these additional fields:

Authentication: Specify the authentication method to be used for SQL Server adapter administrator account.

Use SSL for Adapter to SQL Server Connection: Enable this checkbox if you want to use SSL communication between SQL Server adapter and SQL Server.

Configuring event notification

Modifying Event Notification Context

The following attributes are required to be specified for each event notification context along with the value specified for that attribute on the service form:

1. If SQL Authentication is used for SQL Server adapter administrator account,
    - erSQL2000ServerName : SQL Server Name value
    - erSQL2000AdminAccount : SQL Admin Account value
    - erServicePwd1 : SQL Admin Password value
    - ersql2000authmethod : 0 (for SQL authentication)
    - ersql2000ssl : false (SQL authentication doesn't support SSL Communication)
2. If Windows Authentication is used for SQL Server adapter administrator account,
    - erSQL2000ServerName : SQL Server Name value
    - ersql2000authmethod : 1 (for Windows authentication)
    - ersql2000ssl : true if SSL required, false if non SSL communication

    Note: erSQL2000ServerName and erSQL2000AdminAccount are mandatory attributes only if used with SQL authentication for SQL Server adapter administrator account

Supported Configurations

Installation Platform

The IBM Tivoli Identity Manager Adapter was built and tested on the following product versions.

Adapter Installation Platform:
- Windows 2003 Server Enterprise Edition
- Windows 2008 Server Enterprise Edition (32 or 64 bit)

Managed Resource:
- SQL Server 2000
- SQL Server 2005

IBM Tivoli Identity Manager:
- ITIM 4.6.0 or later

IMPORTANT NOTE:
- This Adapter is now multi-instance capable and will process requests for multiple SQL Servers.

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

```
IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY  10504-1785
U.S.A.
```

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

```
IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan
```

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.
IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged should contact:

```
IBM Corporation
2ZA4/101
11400 Burnet Road
Austin, TX 78758 U.S.A.
```

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Trademarks

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

AIX
DB2
IBM
IBM logo
SecureWay
Tivoli
Tivoli logo
Universal Database
WebSphere

Lotus is a registered trademark of Lotus Development Corporation and/or IBM Corporation.
Domino is a trademark of International Business Machines Corporation and Lotus Development Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

End of Release Notes