Release Notes

IBM® Tivoli® Identity Manager

Oracle Database Adapter

Version 5.0.11

First Edition (December 24, 2011)

This edition applies to version 5.0 of Tivoli Identity Manager and to all subsequent releases and modifications until otherwise indicated in new editions.

Copyright International Business Machines Corporation 2003, 2011. All rights reserved.
US Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Preface

Welcome to the IBM Tivoli Identity Manager Oracle Database 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 Oracle Database Adapter Installation and Configuration Guide

Adapter Features and Purpose

The Oracle DB Adapter is designed to create and manage accounts on an Oracle database. The adapter runs in “agentless” mode and communicates using JDBC to the systems being managed.

IBM recommends the installation of this adapter (and the prerequisite Tivoli Directory Integrator) on each node of an Identity Manager WAS cluster. A single copy of the adapter can handle multiple Identity Manager Services. The optimum deployment configuration is based, in part, on the topology of your network domain, but the primary factor is the planned structure of your Identity Manager Provisioning Policies and Approval Workflow process. Please refer to the Identity Manager Information Center for a discussion of these topics.

The Identity Manager Adapters are powerful tools that require administrator level authority. Adapters operate much like a human system administrator, creating accounts, permissions and home directories. 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 (root) permissions.

Contents of this Release

Adapter Version

Component	Version
Release Date	December 24, 2011
Adapter Version	5.0.11
Component Versions	Adapter Build: 5.0.11.6 Profile: 5.0.11.6 Connector: None (uses TDI JDBC connector) Dispatcher; 5.125 or higher
Documentation	Directory Integrator- Based Oracle Database Adapter Installation and Configuration Guide SC23-6157-00

New Features

Enhancement # (FITS)	Description
	Items included in current release
MR110910208	Oracle Transparent Application Failover (TAF). See "Configuration Notes" for additional information.
	Items included in 5.0.10 release
MR1111103725 MR0716094732	Oracle: Add ability to require SSL connection from Oracle adapter to Oracle. Oracle: Need secure connection from Oracle adapter to Oracle database. See "Configuration Notes" for additional information.
	Items included in 5.0.9 release
MR070810203	Oracle database adapter needs to support proxy-from and proxy-to provisioning functionality. See "Configuration Notes" for additional information.
OSDB	This version of adapter is certified for Oracle Database version 11*g*R2. See "Configuration Notes" for additional information.
	Items included in 5.0.8 release
MR091010394	Oracle database adapter did not handle tablespace quota properly when tablespace is dropped. Added support for "dropped" flag in the adapter. See "Configuration Notes" for additional information.
	Items included in 5.0.6 and 5.0.7 releases
	None
	Items included in 5.0.5 release
MR0605095719 MR0605094210	Enhance the Oracle adapter to manage non-default roles. See "Configuration Notes" for additional information.
	Items included in 5.0.4 release
	None

Enhancement # (FITS)	Description
	Items included in 5.0.3 release
MR1125084337	Added support for Oracle 11*g*
MR111708284	Allow the optional installation of view DBA_WM_SYS_PRIVS. The table DBA_WM_SYS_PRIVS is available in Oracle version 9 and onwards. However it is setup specific and some customers do not set options during installation. The result is the failure in executing query and so no user privileges are returned during recon.
N/A	Changes to Oracle Profile for new Dispatcher features 1. Changes in profile for Disabling AL caching. A new attribute erOraDisableALCache (OID: 1.3.6.1.4.1.6054.3.138.2.20) is defined and added in the erOraRMIService class. A new label (eroradisablealcache = Disable AL Caching) is added to the `CustomLabels.properties` file. This attribute helps to configure the AL cache size. 2. Changes in profile for AL file system Path. A new attribute erOraALFileSystemPath (OID: 1.3.6.1.4.1.6054.3.138.2.21) is defined and added in the erOraRMIService class. A new label (eroraalfilesystempath = AL File System Path) is added to the `CustomLabels.properties` file. This attribute is used to set the path of file system. If we want to Load AL from the file system instead of from ITIM then this property is useful. 3. Changes in profile for Maximum connection count. A new attribute erOraMaxConnectionCnt OID: 1.3.6.1.4.1.6054.3.138.2.22) is defined and added in the erOraRMIService class. A new label (eroramaxconnectioncnt = Max Connection Count) is added to the `CustomLabels.properties` file. This attribute is used to control the maximum connections to the resource per service. From now onwards the service form is changed to a tabbed format: The newly added attributes are visible on the service form under the tab "Dispatcher Attributes". All other attributes are on the default tab "Oracle Connection".

Enhancement # (FITS)	Description
	Items included in 5.0.2 release
MR0624082821	PMR 46887,999,744 - Oracle adapter, Oracle database throws an error of unable to extend the temp segment.
	Items included in 5.0.1 release
	Initial release for ITIM v5.0

Closed Issues

Internal#	APAR#	PMR# / Description
		Items closed in current version
	IV04068	Oracle adapter not setting default roles. See “Configuration Notes” for more information.
	IV12085	In the "Managing passwords when restoring accounts" section of the "Directory Integrator-Based Oracle Database Adapter Installation and Configuration Guide" document, the Property Name (mixed case) should be property name (lower case). There is also a missing ">" at the end of RESTORE".
		Items closed in 5.0.10 version
38718		Test connection function in service form does not attempt to connect to Oracle server after a first successful connection. As a result, test connection reports a successful connection to Oracle server even when Oracle server is down.
		Items closed in 5.0.9 version
	IZ89618	31212,122,000 Error during add account for Oracle, if password contains special character, curly brackets {}.
37696		Restore operation gives warning even if account type is "Local".
37698		Restore sets password as "null" even if password is not changed. If a restore operation does not contain password attribute (erPassword) then adapter was setting the password as "null" string. The adapter is updated.
		Items closed in 5.0.8 version
	IZ81058	63319,668.668 Oracle adapter modify tablespace quota not working.
	IZ81480	90554,999,760 Script error occurs when changing password to Oracle account where authentication type is EXTERNAL.
		Items closed in 5.0.7 version
	IZ74714	66853,122,000 Account under which the Oracle adapter is running must have Create Table and Drop Table permission. (release note update only)
		Items closed in 5.0.6 version
	IZ67181	08436,228,631 Oracle adapter always returns attribute erOraExpirePwd as failed.

		Items closed in 5.0.5 version
	IZ55533	14373,487,000 Oracle adapter shows the Oracle connection password in clear text in the `ibmdi.log` file.

Internal#	APAR#	PMR# / Description
		Items closed in 5.0.4 version
	IZ51277	PMR 37877,999,624 Oracle adapter is converting the username to uppercase during provisioning. A new configuration option has been added to control this behavior. See “Configuration Notes” for more information.
		Items closed in 5.0.3 version
		None
		Items closed in 5.0.2 version
	IZ14723	34101,668,668. Problems setting Oracle passwords containing special characters.
	IZ23733	72043,379,000 Error exporting Oracle profile using the TIM Export page.
	IZ28676	34874,668,668 On account creation multivalued attribute (e.g. Oracle Tablespace quota) being stored in ITIM with only a single value.
		Items closed in 5.0.1 version
		None

Known Issues

Internal#	APAR#	PMR# / Description
N/A	N/A	**Editing adapter profiles on UNIX or Linux** The adapter profile JAR file may contain ASCII files that were created with a MS-DOS ASCII format. For example `schema.dsml`, `CustomLabels.properties`, and `service.def`. If you edit a MS-DOS ASCII file in Unix you will often see the characters ^M at the end of each line. This is the extra character 0x0d that is used to indicate a new line of text in MS-DOS. There are tools, such as dos2unix, that can be used to strip out the ^M character. In addition, there are text editors that will ignore the ^M character. If you are using the vi editor, you can strip out the ^M character as follow: From the vi's command mode: :%s/^M//g followed by pressing Enter. The ^M (or Ctrl-M) typed to show it here should actually be entered by pressing ^v^M in sequence. (The ^v preface tells vi to use the next keystroke literally instead of taking it as a command.)
N/A	N/A	IMPORTANT NOTE: Oracle SYSDBA privilege is not managed by this adapter. Although the following Oracle System Privileges appear on the IBM Tivoli Identity Manager Account Form, they are only valid on "Trusted Oracle" (a multi-level secure version of Oracle) WRITEDOWN DBLOW READUP DBHIGH WRITEUP DBHIGH WRITEDOWN READUP WRITEUP
		Converting between Default and Non-default Roles It is a two-step process to make a role as a non-default role. a) Assign a role to a user by the "GRANT" statement. b) Assign the role as non-default by "ALTER USER". If the "ALTER USER" command fails, then that role will become the default role on the resource. However it will not reflect on the TIM side in any of the role lists. You are required to submit the recon operation, so it will appear in the default list or you can submit the request again.

		Restoring Local Authenticated Accounts Restoring an account for local authentication is a two-step process. a) Change the password for the user. b) Restore the account on the resource. If the step 1 executes successfully and step 2 fails then the password is changed on the resource without the account being restored. Workaround: the user remains suspended and the account can be restored with a new password.

Installation and Configuration Notes

See the “IBM Tivoli Identity Manager Adapter Installation Guide” for detailed instructions.

Corrections to Installation Guide

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

Required Account Permissions

The account under which the adapter runs must have Create Table and Drop Table permissions. This information is omitted from the installation guide.

Configuration Notes

The following configuration notes apply to this release:

Updating Adapters from Version 4.6

Tivoli Directory Integrator version 6.1.1 is a prerequisite to run the 5.0 adapters. To upgrade the adapter from a Tivoli Identity Manager 4.6 installation, perform the following:

1. If the Tivoli Directory Integrator is not version 6.1.1, take the appropriate actions to upgrade it.

2. Install all the adapter's components, as described in the installation guide, on the Tivoli Directory Integrator version 6.1.1. The installer will replace any previous installation.

3. Import the adapter profile into the Tivoli Identity Manager 5.0.

Convert User Name to Upper Case Option

Configuration Attribute "ConvertUserNameToUpperCase" has been added to the Profile. If the customer does not wish to convert the username to uppercase when provisioning accounts on the resource, they can select ConvertUserNameToUpperCase = FALSE.

Summary of Changes:

- A new attribute erOraConvertUserNameToUpperCase (OID: 1.3.6.1.4.1.6054.3.138.2.23) is defined and added in the erOraRMIService class.
- A new label (eroraconvertusernametouppercase = Convert Username to Uppercase) is added to the `CustomLabels.properties` file.

Limitations:

- If the attribute "ConvertUserNameToUpperCase" value is "FALSE", then the following attributes are not set:
    - Resource Consumer Group
    - Default Consumer Group
    - Workspace related System Privileges

  This is due to the fact that the above attributes are set using the Oracle-supplied stored procedures. These stored procedures convert the username to Uppercase.

- The TIM server does not support differentiation of usernames based only on case. If there are multiple users on a resource with the same username & different case, then during recon the TIM server generates a warning and only one user out of the multiple users is reconciled.

- Please refer the IBM Tivoli Identity Manager Messages Guide (Version 5.0).
- Please refer the IBM Tivoli Identity Manager Messages Guide (Version 5.1).

Support for Non-Default Roles

Oracle adapter is enhanced to manage Non-Default roles through ITIM adapter for Oracle resource. To support this enhancement profile of Oracle adapter is extended.

The following two new String attributes are defined in the `schema.dsml` file:

i) "erOraNonDefRole (OID: 1.3.6.1.4.1.6054.3.138.2.24)" added in the "erOraAccount" class.
ii) "erOraPassRequired (OID: 1.3.6.1.4.1.6054.3.138.2.25)" added in the "erOraRoles" class.

A new label (eroranondefrole = Database Non Default Roles) is added for the "erOraNonDefRole" attribute in the `CustomLabels.properties` file.

This attribute is visible on the account form, and only password protected and external roles will be displayed in the search widget of this attribute. If you want to display the all roles in the non-default list then you will need to modify the search filter on account from as,

Existing filter:
<filter>(&amp;(objectclass&#61;erOraRoles)(!(erOraPassRequired&#61;No)))</filter>

Modify the filter as:
<filter>(objectclass&#61;erOraRoles)</filter>

A role can be converted from a Non-Default role to a Default role in one TIM operation using the following process:

a) First remove the role from Non-default role list and assign same role as a default role in same operation.

Prior to adapter version 5.0.11, converting a role from a Default role to Non-default required two TIM operations using the following process:

a) First revoke(delete) the role from the default role list from TIM in one operation,
b) Modify the account and add the role as a non-default role from TIM in second operation.

From adapter version 5.0.11 onwards, a role can be converted from a Default role to a Non-Default role in one TIM operation using the following process:

a) First remove the role from the default role list and assign the same role as a Non-default role in the same operation.

MR091010394 – Dropped Tablespace

Oracle adapter is enhanced so that if a tablespace is dropped from the system table "DBA_TS_QUOTAS", then during the reconcile operation, tablespace quota will not be returned to the ITIM.

Note that this feature will be supported on those versions of Oracle on which the column "DROPPED" is available in system table "DBA_TS_QUOTAS".

For example in Oracle versions 8i and 9i, the column "DROPPED" is not available in the system table "DBA_TS_QUOTAS", so, this feature (enhancement) will not be supported on these versions and the adapter will recon all the tablespace quotas as earlier versions were doing.

Support for Oracle 11*g*R2

Oracle adapter is certified for Oracle Database 11*g*R2.

The following item needs to be added under sub section the "Managed Resource" in the "Installation Platform" under the section "Supported Configuration"

a) Managed resource: Oracle Database - 11*g*R2

The type 4 drivers for 11*g*R2 should be copied to one of the following locations.

i) `TDI_HOME\jars\3rdparty\others`
ii) `TDI_HOME\jvm\jre\lib\ext`

where `TDI_HOME` is the directory where the Tivoli Directory Integrator is installed. For example, on a *Windows* platform this directory would be "`C:\Program Files\IBM\TDI\V6.1.1`"

MR070810203 - Proxy Provisioning

Adapter is enhanced to manage proxy-to provisioning functionality. To support this enhancement profile of Oracle adapter is extended.

The following new String attribute is defined in schema.dsml:

i) "erOraProxyToUsers (OID:1.3.6.1.4.1.6054.3.138.2.26)" is added in the "erOraAccount" class.

   a. A new label (eroraproxytousers = Proxy to Users) is added for this attribute in the `CustomLabels.properties` file.
   b. This attribute is visible on the Account form.

The label for the string attribute "erOraProxyUsers" is replaced with "Proxy from Users" in the `CustomLabels.properties` file. This attribute is also visible on the Account form.

Notes:
=====

i) Account form is enhanced to incorporate a new attribute "Proxy to Users". The user being added from the account form will act as a proxy user for all the valid specified values in this attribute.

ii) “Proxy to Users” attribute is a multivalued attribute.

MR1111103725 - Secure Connection Option

Adapter is enhanced to allow a secure connection from the adapter to the Oracle database.

The following new Boolean and Distinguished Name (DN) attributes are defined in the `schema.dsml` file:

i) "erOraUseSSL (OID:1.3.6.1.4.1.6054.3.138.2.27)" is added for the “erOraRMIService” class.

   a. A new label (erorausessl = Use SSL communication with Oracle?) is added for this attribute in the `CustomLabels.properties` file.
   b. This attribute is visible on the Service form.

ii) “erOraServerDN (OID:1.3.6.1.4.1.6054.3.138.2.28)" is added for the “erOraRMIService” class.

   a. A new label (eroraserverdn = Oracle Server Distinguished Name) is added for this attribute in the `CustomLabels.properties` file.
   b. This attribute is visible on the Service form.

JDBC driver location for SSL

SSL support in the JDBC Thin driver was first included in the 10*g* Release 2 of the driver. Thus the driver is obtained from Oracle Database 10*g*R2, 11*g*, or 11*g*R2. One can obtain the driver from:

- The `ORACLE_HOME\jdbc\lib` directory of an Oracle database (client or server) installation.
- The JDBC Driver Downloads page on the Oracle Technology Network (OTN) website.

The driver for use with JDK 1.5 and thus TDI 6.1.1 is `ojdbc5.jar`. The `ojdbc5.jar` file should be copied to one of the following locations on the Tivoli Directory Integrator (TDI) machine:

i) *`TDI_HOME`*`\jars\3rdparty\others`
ii) *`TDI_HOME`*`\jvm\jre\lib\ext`

where *`TDI_HOME`* is the directory where the TDI is installed. For example, on a window platform this directory would be "`C:\Program Files\IBM\TDI\V6.1.1`".

Furthermore previous versions of the JDBC Thin driver should be removed from the two above *`TDI_HOME`* locations. The previous versions of the driver are one or more of the following:

- `ojdbc14.jar`
- `classes12.zip`
- `nls_charset12.zip`
- `classes111.zip`
- `nls_charset11.zip`

Note that the zip files listed above may alternatively have been named as jar files, e.g. `classes12.jar`.

Configure the SSL Connection

To enable SSL communication between the Oracle adapter and the Oracle database, a truststore and optionally a keystore need to be configured for the RMI dispatcher. A keystore will have to be configured if the Oracle database requires SSL client authentication.

To configure the truststore for the RMI dispatcher, you must minimally import the Certification Authority (CA) certificate that is used to sign the certificate for the Oracle database.

TDI Configuration Server Authentication

The command to import a CA certificate into the truststore is as follows:

```
keytool -import -v -alias OACA -file CA.cer -keystore truststore.jks -storetype JKS
-storepass "ThePwd12"
```

The location for the `truststore.jks` and the `solutions.properties` files are in the *`TDI_HOME`*`\timsol` directory.

In the `solutions.properties` file, the following properties need to be set:

```
## server authentication
javax.net.ssl.trustStore=truststore.jks
javax.net.ssl.trustStorePassword=ThePwd12
javax.net.ssl.trustStoreType=jks
```

If the `javax.net.ssl.trustStore` property is already set to a truststore other than `truststore.jks`, then the keytool command must import the CA certificate into the file specified in the property.

Note that the store password, `ThePwd12`, is for test purposes only.

If a keystore is not required for the Oracle adapter and the keystore properties haven't been set in the `solution.properties` file, then you must set the properties to the same values as the truststore properties:

```
## client authentication
javax.net.ssl.keyStore=truststore.jks
javax.net.ssl.keyStorePassword=ThePwd12
javax.net.ssl.keyStoreType=jks
```

TDI Configuration Client Authentication

If the Oracle database requires SSL client authentication, then a keystore will have to be configured. For test purposes you can use the following commands to setup a JKS type keystore:

```
cd c:\temp
mkdir clientjks

keytool -genkey -alias OADB -dname "CN=client,C=US" -storetype JKS -keystore
clientjks\client.jks -keyalg RSA -storepass "ThePwd12"

keytool -certreq -alias OADB -file clientjks\creq.cer -keystore clientjks\client.jks
-storepass "ThePwd12"

orapki cert create -wallet ./authority -request clientjks\creq.cer -cert
clientjks\signed.cer -validity 3650 -pwd=ThePwd12

keytool -import -v -alias OACA -file authority\CA.cer -keystore clientjks\client.jks
-storepass "ThePwd12"

keytool -import -v -alias OADB -file clientjks\signed.cer -keystore
clientjks\client.jks -storepass "ThePwd12"
```

The above commands assume that you've created a self-signed certification authority as described in the *Oracle Database Server Configuration* section later in this document.

If a keystore is required for the Oracle adapter and the keystore properties haven't been set in the `solution.properties` file, then set the following properties accordingly:

```
## client authentication
javax.net.ssl.keyStore=client.jks
javax.net.ssl.keyStorePassword=ThePwd12
javax.net.ssl.keyStoreType=jks
```

Note that the store password, `ThePwd12`, is for test purposes only.

To determine whether the Oracle database requires SSL client authentication, check the `sqlnet.ora` file on the target Oracle database server (the managed resource) for the following line:

```
SSL_CLIENT_AUTHENTICATION = FALSE
```

The FALSE value means that the Oracle database server does NOT require SSL client authentication. The TRUE value means that the Oracle database server DOES require SSL client authentication.

Oracle Database Server Configuration

To configure both the truststore and the keystore on the Oracle database server, Oracle tools, such as the Oracle Wallet Manager and the `orapki` command, are used. For test purposes you can use the following commands to setup a self-signed certification authority, truststore, and keystore:

```
cd c:\temp
mkdir authority
mkdir server
mkdir client
```

Self-signed Certification Authority

```
orapki wallet create -wallet ./authority -pwd=ThePwd12

orapki wallet add -wallet ./authority -dn "CN=authority, C=US" -keysize 2048
-self_signed -validity 3650 -pwd=ThePwd12

orapki wallet export -wallet ./authority -dn "CN=authority, C=US" -cert
./authority/CA.cer -pwd=ThePwd12
```

The `CA.cer` file in the authority directory is the trusted certificate that is used in the `keytool` command to import a CA certificate into the truststore for the RMI dispatcher.

Stores for Server Authentication

```
orapki wallet create -wallet ./server -auto_login -pwd=ThePwd12

orapki wallet add -wallet ./server -dn "CN=server, C=US" -keysize 2048 -pwd=ThePwd12

orapki wallet export -wallet ./server -dn "CN=server, C=US" -request ./server/creq.cer
-pwd=ThePwd12

orapki cert create -wallet ./authority -request ./server/creq.cer -cert
./server/signed.cer -validity 3650 -pwd=ThePwd12

orapki wallet add -wallet ./server -trusted_cert -cert ./authority/CA.cer
-pwd=ThePwd12

orapki wallet add -wallet ./server -user_cert -cert ./server/signed.cer -pwd=ThePwd12
```

Stores for Client Authentication

```
orapki wallet create -wallet ./client -auto_login -pwd=ThePwd12

orapki wallet add -wallet ./client -dn "CN=client, C=US" -keysize 2048 -pwd=ThePwd12

orapki wallet export -wallet ./client -dn "CN=client, C=US" -request ./client/creq.cer
-pwd=ThePwd12

orapki cert create -wallet ./authority -request ./client/creq.cer -cert
./client/signed.cer -validity 3650 -pwd=ThePwd12

orapki wallet add -wallet ./client -trusted_cert -cert ./authority/CA.cer
-pwd=ThePwd12

orapki wallet add -wallet ./client -user_cert -cert ./client/signed.cer -pwd=ThePwd12
```

Oracle Network Configuration

The following two files need to be configured on the Oracle database server to enable SSL:

- `listener.ora`
- `sqlnet.ora`

These files are located in the `network\admin` directory of the Oracle home directory. These files are often edited through the Oracle Net Manager, but they can be edited through a text editor.

`listener.ora`:

```
SSL_VERSION = 3.0
SSL_CLIENT_AUTHENTICATION = FALSE

WALLET_LOCATION =
  (SOURCE =
    (METHOD = FILE)
    (METHOD_DATA =
      (DIRECTORY = C:\temp\server)
    )
  )

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)(HOST = YourHost)(PORT = 1521))
    )
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCPS)(HOST = YourHost)(PORT = 2484))
    )
  )
```

Make sure that you substitute the directory location, `C:\temp\server`, with the directory where the trusted certificate store is on your Oracle Database Server target. Substitute `YourHost` above with your hostname. Port 1521 is often the port used for non-SSL communication (protocol TCP). Port 2484 is often the port used for SSL communication (protocol TCPS).

`sqlnet.ora`:

```
SQLNET.AUTHENTICATION_SERVICES= (TCPS, NTS)
NAMES.DIRECTORY_PATH= (TNSNAMES)

SSL_VERSION = 3.0
SSL_CLIENT_AUTHENTICATION = FALSE

WALLET_LOCATION =
  (SOURCE =
    (METHOD = FILE)
    (METHOD_DATA =
      (DIRECTORY = C:\temp\client)
    )
  )
```

Make sure that you substitute the directory location, `C:\temp\client`, with the directory where the trusted certificate store is on your Oracle Database Server target.

Oracle Adapter Service Form

To enable SSL communication between the Oracle adapter and the Oracle database, the following changes are needed on the Oracle adapter service form:

- Check the checkbox labeled **Use SSL communication with Oracle?**
- Update the value of **Oracle Service Port** field to the TCPS port, for example 2484, listed in the `listener.ora` file.
- Optionally provide a value for the **Oracle Server Distinguished Name** field.

When a value is entered for the **Oracle Server Distinguished Name** field, the entry will be verified against the Oracle database server certificate.

Notes:

i) Start both the listener and database services with the same user who has created the wallet, so they're both able to access the wallet successfully. On *Windows*, change the Log On As account for the listener and database services from the default Local System account to the user who created the wallet.

ii) The wallet location is provided in both the `sqlnet.ora` and the `listener.ora` files. In the most common case, both files contain the same wallet location, but this is not necessarily the case, the listener could use its own wallet.

   a. The distinguished name of the certificate pointed by the wallet in the `sqlnet.ora` file is the name to which the Oracle Adapter must verify (when we include a distinguished name in the service form).

   b. It is recommended that you include a distinguished name in the service form as an extra measure of security, so that you avoid the risk of a server to potentially fake its identity.

iii) For more details about how to configure SSL with the Oracle driver, refer to the Oracle Technical White Paper *SSL with Oracle JDBC Thin Driver* on Oracle's website (www.oracle.com).

MR110910208 – Oracle Transparent Application Failover (TAF)

Adapter is enhanced to allow a failover connection from the adapter to the Oracle database.

The following new Boolean and String attributes are defined in the `schema.dsml` file:

i) "erOraUseOCI (OID:1.3.6.1.4.1.6054.3.138.2.29)" is added for the "erOraRMIService" class.

   a. A new label (erorauseoci = Use OCI communication with Oracle?) is added for this attribute in the `CustomLabels.properties` file.

   b. This attribute is visible on the Service form.

ii) "erOraServiceAlias (OID:1.3.6.1.4.1.6054.3.138.2.30)" is added for the "erOraRMIService" class.

   a. A new label (eroraservicealias = Oracle Service Alias) is added for this attribute in the `CustomLabels.properties` file.

   b. This attribute is visible on the Service form.

JDBC driver location for OCI

Transparent Application Failover (TAF) is a feature of the Java Database Connectivity (JDBC) Oracle Call Interface (OCI) driver. Thus Oracle Database Client software must be installed on the TDI target.

One can obtain the Oracle Database Client software from the Downloads page on the Oracle Technology Network (OTN) website. For example, one can download the `win32_11gR2_client.zip` file for the *Oracle Database 11g Release 2 Client (11.2.0.1.0) for Microsoft Windows (32-bit)* software.

When installing the client software, select the installation type that installs tools for developing applications, networking services and basic client software. For example, with the *Oracle Database 11gR2 Client* installation, select the *Runtime* installation type.

Alternatively select the installation type that installs the instant client software. For example, with the *Oracle Database 11gR2 Client* installation select the *InstantClient* installation type. The instant client installation requires less disk space to the runtime installation.

On the Oracle Support website, article *[207303.1] Client/Server Interoperability Support* indicates that the Oracle Client 11g (11.1) works with Oracle Server 10gR2 (10.2). Other articles further suggest that one should use Oracle Client 11gR2 (11.2.0.2.0 or higher) to connect to Oracle Server 10gR2 (10.2.0.2.0 or higher). For example, to enable SSL communication using the OCI JDBC driver to connect from a 11gR2 client to a 10gR2 server requires a 11.2.0.2.0 or higher client and a 10.2.0.2.0 or higher server.

Configure the OCI Connection

To enable OCI communication between the Oracle adapter and the Oracle database, Oracle Net Services (ONS) must be configured on the TDI target – where the Oracle Client software is installed.

To configure Oracle Net Services one must edit the following ONS configuration files:

- `tnsnames.ora`
- `sqlnet.ora`

TDI must be configured to locate these Oracle Net Services files along with locating the JDBC OCI driver.

In a Database Client installation, the *`ORACLE_HOME`* environment variable is defined, thus enabling TDI to locate the Oracle Net Services files. On *Windows*, *`ORACLE_HOME`* is often defined in the registry.

In an Instant Client installation, one must define the *`TNS_ADMIN`* environment variable, which is an Oracle Client variable, to point to the location (directory) of the ONS configuration files.

Configuring TDI to locate the JDBC OCI driver is described in the Oracle Adapter Configuration section later in this document.

Oracle Network Configuration

The following two files need to be configured on the Oracle database client to enable TAF:

- `tnsnames.ora`
- `sqlnet.ora`

These files are located in the `network\admin` directory of the Oracle home directory. These files are often edited through the Oracle Net Manager, but must be edited through a text editor for purposes of TAF configuration. Editing both these files effectively configures Oracle Net Services.

In an Instant Client installation these files do not exist. Once created, they must co-exist in the same directory. For example, these files can be saved in the Instant Client directory, an apt destination.

The information in the following files serves as an example on how TAF can be configured:

`sqlnet.ora`:

```
SQLNET.AUTHENTICATION_SERVICES= (NONE)
NAMES.DIRECTORY_PATH= (TNSNAMES)
```

`tnsnames.ora`:

```
PRODONE =
(DESCRIPTION_LIST =
  (FAILOVER = true)
  (LOAD_BALANCE = false)
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = YourFirstHost)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVER = dedicated)
        (FAILOVER_MODE =
           (BACKUP = PRODTWO)
           (TYPE = select)
           (METHOD = basic)
           (RETRIES = 20)
           (DELAY = 3)
        )
      (SERVICE_NAME = ORCL)
    )
  )
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = YourSecondHost)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = ORCL)
    )
  )
)

PRODTWO =
(DESCRIPTION_LIST =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = YourSecondHost)(PORT = 1521))
    )
    (CONNECT_DATA =
        (SERVICE_NAME = ORCL)
      )
    )
)
```

With TAF the adapter can automatically reconnect to a database when the instance to which the connection is made fails or is shutdown. TAF enables the application to transparently reconnect to a preconfigured secondary instance creating a fresh connection, but identical to the connection that was established on the first original instance.

In the `tnsnames.ora` file listed above, `PRODONE` is the net service alias that defines (as an example) both TAF and Connect Time Failover (CTF). The first description in the description list defines TAF. The second description in the description list defines CTF.

The TAF description indicates that once a connection to `YourFirstHost` is established and then subsequently the connection fails, then the connection fails over to `YourSecondHost` via the `PRODTWO` net service alias. The CTF description indicates that when `YourFirstHost` is down prior to the initial connection, then the connection fails over to `YourSecondHost.`

One feature of TAF is to configure a failover `TYPE` of `select` which indicates that after the first connection fails and the second connection succeeds and the first connection was in the middle of a SELECT statement, the statement will re-execute on the second connection, repositioning the cursor so the client can continue fetching rows as if nothing has happened.

Oracle Adapter Configuration

TDI must be configured to locate the JDBC OCI driver and Oracle Net Services. To locate the JDBC OCI driver, the *`path`* variable must be amended to include the Oracle home `bin` directory or the Instant Client directory. To locate Oracle Net Services, the *`ORACLE_HOME`* environment variable must be defined for a Database Client installation or the *`TNS_ADMIN`* environment variable for an Instant Client installation.

Depending on the TDI service, the *`path`* variable is configured slightly different in TDI.

There are two TDI services that can exist or co-exist on your TDI target.

- The "IBM Tivoli Identity Manager Adapter" aka *`ITDIAsService.exe`*
- The "IBM Tivoli Directory Integrator" service aka *`ibmdiservice.exe`*

For the *`ITDIAsService`* service, we configure the path in the *Windows* registry. For the *`ibmdiservice`* service, configure the path in the `ibmdiservice.props` properties file.

For both TDI services, check to see that the *`ORACLE_HOME`* environment variable is defined in the *Windows* registry in a Database Client installation, or alternatively define the *`ORACLE_HOME`* environment variable as a System variable in *Windows*.

For an Instant Client installation, define the *`TNS_ADMIN`* environment variable as a System variable in *Windows*.

An example *`ORACLE_HOME`* environment value is:

```
ORACLE_HOME=C:\app\administrator\product\11.2.0\client_1
```

An example *`TNS_ADMIN`* environment value is:

```
TNS_ADMIN=C:\app\administrator\product\11.2.0\client_1
```

With *`ORACLE_HOME`* defined, the JDBC OCI driver knows to locate the Oracle Net Services files in the `network\admin` directory of the Oracle home directory. With *`TNS_ADMIN`* defined, the JDBC OCI driver knows to locate the Oracle Net Services files in the specified directory.

Path for ibmdiservice in Properties File

Edit the path variable in the `ibmdiservice.props` file, which can be found in the following directory:

```
C:\Program Files\IBM\TDI\V6.1.1\timsol
```

Edit the `path` variable to include the Oracle home `bin` as follows:

```
path=C:\Program Files\IBM\TDI\V6.1.1\jvm\jre\bin;C:\Program Files\IBM\TDI\V6.1.1\libs;
C:\app\administrator\product\11.2.0\client_1\bin;
```

For an Instant Client installation edit the `path` variable as follows:

```
path=C:\Program Files\IBM\TDI\V6.1.1\jvm\jre\bin;C:\Program Files\IBM\TDI\V6.1.1\libs;
C:\app\administrator\product\11.2.0\client_1;
```

Path for ITDIAsService in Registry

Edit the `ImagePath` registry variable, which can be found in the following location:

```
HKLM\SYSTEM\ControlSet001\Service\IBM Tivoli Identity Manager Adapter
```

Note: The value of `ImagePath` is an expandable String Value aka a *REG_EXPAND_SZ* Type.

Edit the `ImagePath` variable to include `%ORACLE_HOME%\bin` as follows:

```
"C:\Program Files\IBM\TDI\V6.1.1\timsol\ITDIAsService.exe" … -Djava.library.path
="C:\Program Files\IBM\TDI\V6.1.1\libs;%ORACLE_HOME%\bin;%PATH%" …
```

Note: Use `%ORACLE_HOME%` in the `ImagePath` variable only when the `ORACLE_HOME` variable is defined as a System variable on *Windows*, otherwise explicitly include the Oracle home `bin` directory as follows:

```
"C:\Program Files\IBM\TDI\V6.1.1\timsol\ITDIAsService.exe" …
-Djava.library.path ="C:\Program Files\IBM\TDI\V6.1.1\libs;
C:\app\administrator\product\11.2.0\client_1\bin;%PATH%" …
```

For an Instant Client installation, edit the `ImagePath` variable to include the directory of the Instant Client files as follows:

```
"C:\Program Files\IBM\TDI\V6.1.1\timsol\ITDIAsService.exe" …
-Djava.library.path ="C:\Program Files\IBM\TDI\V6.1.1\libs;
C:\app\administrator\product\11.2.0\client_1;%PATH%" …
```

Oracle Adapter Service Form

To enable OCI communication between the Oracle adapter and the Oracle database, the following changes are needed on the Oracle adapter service form:

- Check the checkbox labeled **Use OCI communication with Oracle?**
- Enter a value for the **Oracle Service Alias** field that corresponds to the net service alias listed in the `tnsnames.ora` file.

Once the *Use OCI communication with Oracle* checkbox is checked, then the JDBC OCI driver will be used to communicate with the Oracle database server. When unchecked then the JDBC Thin driver will be used to communicate with the Oracle database server.

Net service aliases defined in the `tnsnames.ora` file are names on the left hand side of the equal sign. For example, in the `tnsnames.ora` file listed above, `PRODONE` is the net service name defined for TAF and thus the value to be entered in the **Oracle Service Alias** field.

Note that the checkbox labeled **Use SSL communication with Oracle** is for only the JDBC Thin driver. To enable SSL communication between the Oracle adapter and the Oracle database on behalf of the JDBC OCI driver requires additional configuration.

The information in the following files serves as an example on how TAF with SSL can be configured:

`sqlnet.ora`:

```
SQLNET.AUTHENTICATION_SERVICES= (TCPS)
NAMES.DIRECTORY_PATH= (TNSNAMES)

SSL_VERSION = 3.0
SSL_CLIENT_AUTHENTICATION = FALSE
SSL_SERVER_DN_MATCH = YES

WALLET_LOCATION =
  (SOURCE =
    (METHOD = FILE)
    (METHOD_DATA =
      (DIRECTORY = C:\temp\client)
    )
  )
```

tnsnames.ora:

```
PRODONESSL =
(DESCRIPTION_LIST =
  (FAILOVER = true)
  (LOAD_BALANCE = false)
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCPS)(HOST = YourFirstHost)(PORT = 2484))
    )
    (CONNECT_DATA =
      (SERVER = dedicated)
        (FAILOVER_MODE =
           (BACKUP = PRODTWOSSL)
           (TYPE = select)
           (METHOD = basic)
           (RETRIES = 20)
           (DELAY = 3)
        )
      (SERVICE_NAME = ORCL)
    )
    (SECURITY =
      (SSL_SERVER_CERT_DN = "CN=client, C=US")
    )
  )
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCPS)(HOST = YourSecondHost)(PORT = 2484))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = ORCL)
    )
    (SECURITY =
      (SSL_SERVER_CERT_DN = "CN=client, C=US")
    )
  )
)

PRODTWOSSL =
(DESCRIPTION_LIST =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCPS)(HOST = YourSecondHost)(PORT = 2484))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = ORCL)
    )
    (SECURITY =
      (SSL_SERVER_CERT_DN = "CN=client, C=US")
    )
  )
)
```

Configuring SSL for the JDBC OCI driver is described in the *Stores for Client Authentication* subsection of the *Oracle Database Server Configuration* section earlier in this document.

Customizing or Extending Adapter Features

The Identity Manager adapters can be customized and/or extended. The type and method of this customization may vary from adapter to adapter.

Getting Started

Customizing and extending adapters requires a number of additional skills. The developer must be familiar with the following concepts and skills prior to beginning the modifications:

- Tivoli Identity Manager administration
- Tivoli Directory Integrator management
- Tivoli Directory Integrations assemblyline development
- LDAP schema management
- Working knowledge of Java scripting language
- Working knowledge of LDAP object classes and attributes
- Working knowledge of XML document structure

Note: If the customization requires a new Tivoli Directory Integrator connector, the developer must also be familiar with Tivoli Directory Integrator connector development and working knowledge of Java programming language.

Tivoli Identity Manager Resources:

Check the “Learn” section of the Tivoli Identity Manager Support web site for links to training, publications, and demos.

Tivoli Directory Integrator Resources:

Check the “Learn” section of the Tivoli Directory Integrator Support web site for links to training, publications, and demos.

Support for Customized Adapters

The integration to the Identity Manager server – the adapter framework – is supported. However, IBM does not support the customizations, scripts, or other modifications. If you experience a problem with a customized adapter, IBM Support may require the problem to be demonstrated on the GA version of the adapter before a PMR is opened.

Supported Configurations

Installation Platform

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

Adapter Installation Platform:

> This adapter installs into Tivoli Directory Integrator (TDI) and may be installed on any platform supported by the TDI product. IBM recommends installing TDI on each node of the ITIM WAS Cluster and then installing this adapter on each instance of TDI.
>
> Supported TDI versions include:
>
> TDI 6.1.1 Fix Pack 3 or later

Managed Resource:

> Oracle Database 8i, 9i, 10*g*, 10*g*R2, 11*g*, 11*g*R2

IBM Tivoli Identity Manager:

> Identity Manager v5.0

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:

IBM
IBM logo
Tivoli
WebSphere.

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

Intel, Intel Inside (logos), MMX and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

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

Linux is a trademark of Linus Torvalds in the U.S., other countries, or both.

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

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

End of Release Notes