TIM – TAM Integration

For TIM – TAM Integration, TAM Combo Adapter is required. The installation and configuration details of TAM Combo Adapter is described below.

Planning to install the Tivoli Access Manager Combo Adapter

Installing and configuring the Tivoli Access Manager Combo Adapter involves several steps that you must complete in the appropriate sequence. Review the prerequisites before you begin the installation process.

Prerequisites

Table identifies hardware, software, and authorization prerequisites to install the Tivoli Access Manager Combo Adapter. Verify that all of the prerequisites have been met before installing the Tivoli Access Manager Combo Adapter.

Table: Prerequisites to install the adapter

Prerequisite	Description
Operating System	The Tivoli Access Manager Combo Adapter can be used on any operating system that is supported by Tivoli Directory Integrator.
Network Connectivity	TCP/IP network
Tivoli Directory Integrator Server	6.1.1 Fixpack 9 7.0.0 Fixpack 3
Tivoli Identity Manager Server	Version 5.1
IBM Tivoli Identity Manager Adapter (also known as the RMI Dispatcher)	For Tivoli Directory Integrator Server 6.1.1, use RMI Dispatcher version 5.013 and above. For Tivoli Directory Integrator Server 7.0, use RMI Dispatcher version supplied in the installation package or later.
IBM Tivoli Access Manager Java Run-Time	Corresponding version to IBM Tivoli Access Manager Server. The Tivoli Access Manager Combo Adapter supports Tivoli Access Manager Server version 6.0, 6.1 and 6.1.1.
Tivoli Directory Integrator	

Tivoli Access Manager Connector (supplied with Tivoli Access Manager Combo Adapter)	Version supplied in installation package or later.

Installation of Tivoli Directory Integrator 6.1.1 Fix Pack 9 on TAM Machine

Steps to install Tivoli Directory Integrator Fixpack for all Platforms, Except z/OS.

1. Download the Fixpack.zip and save the content in any preferred folder

2. To install this fixpack you need to launch update installer using GMI tool, Default location for GMI tools is like this:

   For Windows GMI tool is available in **C:\Program Files\IBM\Common\ci\gmi\bin**

3. Start GMI tool from applicable location, using "gmi" command.

4. Click next on "Welcome to the Update Installer" screen.

5. Select "Install maintenance packages such as fixes, fix packs or refresh packs" and press next.

6. Then it will perform Offering query, let it go, it may take some time.

7. Select TDI 6.1.1 on the next screen and click next, you may have multiple instances of TDI 6.1.1 on same machine, select the one you want to apply the fixpack to. You can click on the Offering record in the list to check the details like installation directory etc.

8. You need to select the path where you have unzipped the Fixpack content. Press "edit" and add that path here. Also check the "include subdirectory" checkbox. This is the folder where GMI will be searching for applicable Fix or fixpack for selected Offering in earlier screen. Then press Next on this screen.

9. Next screen will be querying for the applicable fixpack in the search directory, and will list the applicable fixpack. Select Fixpack-9 on that screen and click Next.

10. Select "Install Maintenance on this computer" and click Next.

11. Next screen will show the summary, verify that everything looks ok and Click "Install" Button.

12. This should install the fixpack successfully.

Directory Integrator RMI Dispatcher Installation and Configuration

Required information	**Value**
Tivoli Directory Integrator Home Directory	If Tivoli Directory Integrator is automatically installed with your Tivoli Identity Manager product, the default directory path for Tivoli Directory Integrator is as follows: **Windows:** v for version 6.1.1: *drive*\ IBM\TDI\V6.1.1
Solution Directory	**Windows:** v for version 6.1.1: *drive*\ IBM\TDI\V6.1.1\timsol

Installing the RMI Dispatcher

The RMI Dispatcher has several different types of installer binaries. Select the one appropriate for your operating system

For Windows operating systems only - DispatcherInstall_win.exe

1. Start the installation program using the DispatcherInstall file in the temporary directory. For example on a Windows operating system, select **Run...** from the Start menu and type C:\Temp\DispatcherInstall_win.exe in the **Open** field.

2. Click **Next** on the Welcome window.

3. Do the following at the License Agreement window:

   Review the license agreement and select **Accept** .

   Click **Next**.

4. Specify the location of the TDI_HOME directory at the prompt.

5. If this is the first Tivoli Directory Integrator-based adapter installation, you are prompted in the Adapter Solution Directory panel to specify the adapters solution directory to be used for the Tivoli Directory Integrator-based Tivoli Identity Manager adapters. If the adapters solution directory has been specified during a previous Tivoli Directory Integrator-based adapter installation, the prompt is not displayed.

6. Review the installation settings in the Install Summary window and do one of the following:

   Click **Back** and return to a previous window to change any of these settings.

   Click **Next** when you are ready to begin the installation.

7. Click **Finish** when the software displays the Install Completed window.

Verifying the installation

If the dispatcher is installed correctly, these components exist on the Tivoli Directory Integrator server.

Dispatcher components

Directory Dispatcher	component
ITDI_HOME\jars\3rdparty\IBM	rmi-dispatcher.jar rmi-dispatcher-client.jar itdiAgents-common.jar itdiAgents.jar
ITDI_HOME\jars\3rdparty\others	antlr-2.7.2.jar jakarta-regexp-1.4.jar
adapter_solution_directory	ITIM_RMI.xml log4j.properties ibmdiservice.props ibmdiservice.exe
ITDI_HOME	itim_listener.properties

Starting and stopping the RMI Dispatcher

Windows operating systems

From the Control Panel, select **Administrative Tools -> Services**. From the Services menu, you can start and stop the dispatcher service. The service name is IBM Tivoli Directory Integrator (TIM Adapters).

Configuration properties of the RMI Dispatcher

Changing the port number for the RMI Dispatcher

If the Remote Method Invocation (RMI) Dispatcher is run as a service, by default, the port number is 16231. The installer automatically sets this parameter in the global.properties file.

If the IBM Tivoli Directory Integrator home directory is the same directory as the IBM Solutions directory, change the port number in the global.properties file. Otherwise, change the port number in the solutions.properties file in the IBM Solutions directory. To change the port number for the dispatcher, complete these steps.

1. Stop the service that is used to run the adapter.

2. Change the solutions.properties file to use the correct port number.
com.ibm.di.dispatcher.registryPort=16232

3. Start the service again.

Configuring the RMI Dispatcher JVM properties

You can set the UTF-8 support on Windows operating systems. Perform the following steps to force the dispatcher into UTF-8 compatibility mode at the startup:

On the Windows operating system:

1. Stop the IBM Tivoli Directory Integrator (TIM Adapters) service.

2. Navigate to the adapter timsol directory.

3. Open the ibmdiservice.props file in the notepad.

4. Set the value of the jvmcmdoptions property to the Java property that you want to change. For example, if you want the RMI Dispatcher jvm to run with UTF-8 encoding, then set

    jvmcmdoptions=-Dfile.encoding=UTF-8.

Note: Separate more than one property with a space.

5. Save and close the ibmdiservice.props file.

6. Restart the IBM Tivoli Directory Integrator (TIM Adapters) service.

Task performed on the SSL server (Tivoli Directory Integrator server workstation)

The Tivoli Directory Integrator acts as the SSL server. All of these tasks are performed on the Tivoli Directory Integrator server.

Note: The file names and locations such as tdikeys.jks and *ITDI_HOME*\keys used in these tasks are examples and used for consistency. Your actual file names and locations might be different.

Creating a keystore for the Tivoli Directory Integrator server

Note: The keystore can be the same physical file as the truststore.

1. Navigate to the *ITDI_HOME*\jvm\jre\bin directory.

2. Launch the ikeyman.exe file (Windows operating systems).

3. Select **Key Database File > New**.

4. Select key database type of **JKS**.

5. Type the keystore file name: tdikeys.jks.

6. Type the location: *ITDI_HOME*\keys.

Note: This directory must already exist, otherwise the step fails.

7. Click **OK** .

8. Type the keystore a password, for example, cyber2003.

9. Click **OK** to continue.

Creating a truststore for the Tivoli Directory Integrator server

Note: The truststore can be the same physical file as the keystore.

1. Navigate to the *ITDI_HOME*\jvm\jre\bin directory.

2. Launch the ikeyman.exe file (Windows operating systems).

3. Select **Key Database File > New**.

4. Select key database type of **JKS**.

5. Type the keystore file name: tditrust.jks.

6. Type the location: *ITDI_HOME*\keys.

Note: This directory must already exist, otherwise the step fails.

7. Click **OK**.

8. Type the keystore a password, for example, cyber2003.

9. Click **OK** to continue.

Creating a server-signed certificate for the Tivoli Directory Integrator server

To create the self-signed certificate:

1. Navigate to the *ITDI_HOME*\jvm\jre\bin directory.

2. Launch the ikeyman.exe file (Windows operating systems)

3. Select **Key Database File > Open**.

4. Browse to the keystore file created previously: *ITDI_HOME*\keys\tdikeys.jks

5. Enter the keystore password: cyber2003.

6. Select **Create > New Self Signed certificate**.

7. Set the Key Label to tdiserver.

8. Use your system name (DNS name) as the Common Name (workstation name).

9. Enter your Organization, for example IBM.

10. Click **OK**.

Creating a CA certificate for Tivoli Directory Integrator

1. Extract the Server certificate for client use by selecting **Extract Certificate**.

2. Select **Binary DER data** as the data type.

3. Enter the certificate file name: idiserver.der.

4. Enter the location as *ITDI_HOME*\keys.

5. Click **OK**.

6. Copy the idiserver.der certificate file to the workstation on which Tivoli

Identity Manager is installed.

Importing the WebSphere CA certificate into the Tivoli Directory Integrator truststore

1. Copy the SSL Client CA certificate file created in “Creating a WebSphere Application Server CA certificate for Tivoli Identity Manager” on page 10, timclient.der, to the *ITDI_HOME*\keys directory on the workstation on which Tivoli Directory Integrator is installed.

2. Navigate to the *ITDI_HOME*\jvm\jre\bin directory.

3. Launch the ikeyman.exe file (Windows operating systems).

4. Select **Key Database File > Open**.

5. Select key database type of **JKS**.

6. Type the keystore file name: tditrust.jks.

7. Type the location: *ITDI_HOME*\keys.

8. Click **OK**.

9. Click **Signer Certificates** in the dropdown menu.

10. Click **Add**.

11. Select **Binary DER data** as the data type.

12. Use **Browse** to select the timclient.der file stored in *ITDI_HOME*\keys.

13. Use timclient as the label.

14. Click **OK** to continue.

Configure Tivoli Directory Integrator to use the keystores

1. Navigate to the Tivoli Directory Integrator *adapters solution* directory (*ITDI_HOME*\timsol).

2. Open the Tivoli Directory Integrator solution.properties file in an editor.

3. Edit the following lines under client authentication, uncomment them if necessary, and set the location, password and type of keystore to match the keystore you created in "Creating a keystore for the Tivoli Directory Integrator server"

javax.net.ssl.keyStore=*ITDI_HOME*\keys\tdikeys.jks
{protect}-javax.net.ssl.keyStorePassword=cyber2003
javax.net.ssl.keyStoreType=JKS

4. Save your changes.

5. Stop and restart the adapter service.

Configure Tivoli Directory Integrator to use the truststores

1. Navigate to the Tivoli Directory Integrator *adapters solution* directory (*ITDI_HOME*\timsol).

2. Open the Tivoli Directory Integrator solution.properties file in an editor.

3. Edit the following lines under client authentication, uncomment them if necessary, and set the location, password and type of truststore to match the truststore you created in "Creating a truststore for the Tivoli Directory Integrator server"

javax.net.ssl.trustStore=*ITDI_HOME*\keys\tditrust.jks
{protect}-javax.net.ssl.trustStorePassword=cyber2003
javax.net.ssl.trustStoreType=JKS

4. Save your changes.

5. Stop and restart the adapter service.

Enabling the adapter service to use SSL

1. Navigate to the Tivoli Directory Integrator *adapters solution* directory (*ITDI_HOME*\timsol).

2. Open the Tivoli Directory Integrator solution.properties file in an editor.

3. Edit the following two lines depending on the type of secure communications you want to use.

For two-way SSL:
com.ibm.di.dispatcher.ssl=true
com.ibm.di.dispatcher.ssl.clientAuth=true

4. Save your changes.

5. Stop and restart the adapter service.

Tasks performed on the SSL client (Tivoli Identity Manager and WebSphere Application Server workstation)

All the tasks are performed on the server workstation on which Tivoli Identity Manager and WebSphere Application Server are installed.

Note: The file names and locations such as timclient.der and c:\keys used in these tasks are examples and used for consistency. Your actual file names and locations might be different.

Creating a signed certificate for the Tivoli Identity Manager server

1. Connect to the WebSphere Application Server Administrative Console.

2. Navigate to **Security > SSL certificate and key management > Keystores and certificates**.

3. Select **NodeDefaultKeyStore**.

4. Select **Personal certificates**.

5. Select **Create a self-signed certificate**.

6. Enter appropriate values for the certificate fields:

- Set the Alias to timclient.
- Use your system name (DNS name) as the Common Name (workstation name).
- Enter your Organization, for example IBM.

7. Click **OK** and save.

8. Extract the CA certificate from the self-signed certificate.

Creating a WebSphere Application Server CA certificate for Tivoli Identity Manager

1. Check the checkbox for the created certificate, and select **Extract**.

2. Enter a file name: c:\keys\timclient.der.

3. Select **Binary DER data** as the data type.

4. Click **OK**.

Importing the Tivoli Identity Manager CA certificate into the WebSphere Application Server truststore

1. Copy the SSL server CA certificate file created in "Creating a CA certificate for Tivoli Directory Integrator" on page 7, idiserver.der, to the c:\keys directory on the workstation on which Tivoli Identity Manager is installed.

2. Connect to the WebSphere Application Server Administrative Console.

3. Navigate to **Security > SSL certificate and key management > Keystores and certificates**.

4. Select **NodeDefaultTrustStore**.

5. Select **Signer certificates**.

6. Click **Add**.

- Set the Alias to idiserver.

- Specify the file name of the exported Tivoli Directory Integrator server certificate: c:\ keys\idiserver.der.
- Select **Binary DER data** as the data type.

7. Click **OK** to continue and save.

Installing the Tivoli Access Manager Combo Adapter

To install the adapter, follow these steps:

1. Configure JRTE against Tivoli Directory Integrator Java Runtime Environment (JRE).

2. Configure Tivoli Directory Integrator JRE into the Tivoli Access Manager secure domain.

3. Extract the Tivoli Access Manager Combo zip file (Adapter51_TamCombo_5.1.x.zip) from the distribution package.

4. Install the IBM Tivoli Access Manager Combo Adapter Utilities Package.

5. Importing the adapter profile into the Tivoli Identity Manager Server.

Configuring the Tivoli Access Manager Runtime for Java System

JRTE must be installed on the same system where Tivoli Directory Integrator Server and Tivoli Identity Manager Adapter are installed. To configure JRTE against Tivoli Directory Integrator Server JRE, follow these configuration steps:

1. Start the Tivoli Access Manager configuration utility (pdconfig).

2. Select **Access Manager Runtime for Java** from the list of installed packages.

3. Click **Configure**.

4. Select **Full** for configuration type and then click **Next**.

5. Specify the JRE path, for example C: \ibm\TDI\V6.1.1\jvm\jre. Then click **Next**.

6. Specify **Host name**, **Port** and **Domain**. Then click **Next**.

7. Optionally enable Tivoli Common logging. Then click **Finish**. A message saying that JRTE is successfully configured is shown on the screen.

8. Click **Close** to exit the utility.

Configuring the Tivoli Directory Integrator Java Run-Time

Environment into the Tivoli Access Manager secure domain

To make use of Tivoli Access Manager security, Tivoli Identity Manager Adapter must be configured into your Tivoli Access Manager secure domain. Tivoli Access Manager provides a utility class called **com.tivoli.pd.jcfg.SvrSslCfg** that can be used to accomplish the necessary configuration and unconfiguration tasks.

To run the utility, Tivoli Directory Integrator JRE must be used.

For example, the following command could be used to configure IBM Tivoli Directory Integrator to use the IBM Tivoli Access Manager policy server on **amserver.example.com,** using standard ports and default install paths:

```
C:\IBM\TDI\V6.1.1\jvm\jre\bin>java com.tivoli.pd.jcfg.SvrSslCfg
-action config
-admin_id sec_master
-admin_pwd cyber2003
-appsvr_id itdi_tam
-port 1234
-mode remote
-policysvr tampoc.rc.com:7135:1
-authzsvr tampoc.rc.com:7136:1
-cfg_file C:\IBM\TDI\V6.1.1\timsol\tam.conf
-key_file C:\IBM\TDI\V6.1.1\timsol\tam.ks
```

Note that the **tam.conf** file generated in this step will be used in later configuration process.

Installing the Tivoli Access Manager Combo Adapter Utilities Package

To install the utilities package:

1. Copy TAMComboUtils.jar from the installation package to an appropriate Tivoli Directory Integrator location:

Windows

Tivoli Directory Integrator version 6.1.1 or 7.0:

ITDI_HOME\jars\3rdparty\IBM

2. Restart the IBM Tivoli Identity Adapter (RMI Dispatcher) service.

Importing the adapter profile into the Tivoli Identity Manager Server

You must import the adapter profile into the Tivoli Identity Manager Server before using the Tivoli Access Manager Combo Adapter.

Before you import the adapter profile, verify that the following conditions are met:

- The Tivoli Identity Manager Server is installed and running.
- You have root or Administrator authority on the Tivoli Identity Manager Server.

The Tivoli Access Manager Combo adapter distribution package contains two versions of the adapter profile. You should use only one of them:

itamprofile.jar

The itamprofile.jar profile is intended for use when Tivoli Access Manager is configured against supported non Active Directory user registries.

Importing the itamprofile.jar after having imported an itamprofileAD.jar profile is unsupported, and will cause directory server schema violation errors.

itamprofileAD.jar

The itamprofileAD.jar profile is intended for use when Tivoli Access Manager is configured against Active Directory, including Active Directory Application Mode (ADAM) or other supported user registries.

To import the adapter profile, complete the following steps:

1. Log in to the Tivoli Identity Manager Server using an account that has the authority to perform administrative tasks.

2. Import the adapter profile using the **import** feature for your IBM Tivoli Identity Manager product.

3. Restart the IBM Tivoli Identity Manager Adapter (Dispatcher) service.

If you receive an error related to the schema when you import the adapter profile, refer to the trace.log file for information about the error. The trace.log file location is specified using the handler.file.fileDir property defined in the IBM Tivoli Identity Manager enRoleLogging.properties file. The enRoleLogging.properties file is installed in the *ITIM_HOME*\data directory.

Creating a Tivoli Access Manager Combo service

You must create a service for the Tivoli Access Manager Combo Adapter before the Tivoli Identity Manager Server can use the adapter to communicate with the managed resource. To create a service, complete these steps:

1. Log in to the Tivoli Identity Manager Server using an account that has the authority to perform administrative tasks.

2. Create the service using the information for your IBM Tivoli Identity Manager product. Refer to the information center or the online help for specific instructions about creating a service.

To create or change a service, you must use the service form to provide information for the service. Service forms might vary depending on the adapter. The Tivoli Access Manager Combo Adapter service form contains the following fields:

SERVICE SETUP Tab

Service name

Specify a name that defines this Tivoli Access Manager Combo Adapter service on the Tivoli Identity Manager Server.

Description

Optional: Specify a description for this service.

Tivoli Directory Integrator location

Optional: Specify the URL for the Tivoli Directory Integrator instance. Valid syntax is rmi://*ip-address*:*port*/ITDIDispatcher, where *ip-address* is the Tivoli Directory Integrator host and *port* is the port number for the RMI Dispatcher. For example, you might specify the URL as rmi://tampoc.rc.com:16232/ITDIDispatcher.

Owner

Optional: Service owner

Service prerequisite

Optional: Service prerequisite

TAM SETUP Tab

Reconciliation Method

The Tivoli Access Manager Combo adapter has two methods of reconciling Tivoli Access Manager user accounts and their associated user registry attributes:

TAM API

This method is designed to use the Tivoli Access Manager administration Java API.

LDAP - TAM v6.x

Applicable only when Tivoli Access Manager version is 6.0 or 6.1 and when directory server type is non Active Directory.

This method is designed to reconcile Tivoli Access Manager user accounts and their associated user registry attributes directly from the directory server.

Do not reconcile SSO credentials

Enabling this option will exclude SSO credentials from the retrieval of accounts information during reconciliation operation.

LDAP Reconciliation Page Size

Optional: Applicable only when using LDAP reconciliation.

If a page size other than 0 is specified, the Tivoli Access Manager Combo adapter will try to use **page mode** search when obtaining user accounts information.

TAM Admin User

Specify the Tivoli Access Manager administrator account name (for example, sec_master). This account must have enough access rights to manage accounts.

TAM Admin User Password

Specify the password for the Tivoli Access Manager administrator account.

TAM Config File

Specify the file name and path for the configuration file that was created using **SvrSslCfg** with the –cfg_file option during step "Configuring the Tivoli Directory Integrator Java Run-Time Environment into the Tivoli Access Manager secure domain". In the provided example, the file path is: C:\IBM\TDI\V6.1.1\timsol\tam.conf

Add Account

Specify the following options for adding IBM Tivoli Access Manager user account:

Create user entry in registry.

Causes the adapter to create a new user entry in the directory server registry with a specific DN. If the entry already exists, requests for account provisioning will fail.

Import user entry from registry.

Causes the adapter to re-use an existing user entry from the directory server registry. If an entry with a specified DN doesn't exist, the request will fail.

Import or create user entry.

Causes the adapter to check if a user entry with a specific DN exists, and if so, this user entry is used. Otherwise a new registry entry for the Tivoli Access Manager account is created.

Delete user entry from Registry

If this check box is checked, during the deletion of the Tivoli Access Manager account, the user entry is removed from the directory server registry. If the check box is left unchecked, the user entry remains in the registry.

Add group

Specify one of the following options for adding IBM Tivoli Access Manager groups:

Create group entry

Causes the adapter to create a new group in the directory server registry with a specific DN. If the entry already exists, the group cannot be created.

Import group entry

Causes the adapter to import an existing group entry from the directory server registry. Import will fail if the entry with the DN specified does not exist.

Delete group entry from registry

If this check box is checked, during the deletion of the Tivoli Access Manager group, the group entry is removed from the directory server registry. If the check box is left unchecked, the group entry remains in the registry.

Synchronize TAM password in SSO Lockbox

If this check box is checked, during the password change operation, all of the account's SSO credentials passwords will be synchronized with the new account password.

TAM Domain Name

Optional: Specify the Tivoli Access Manager Domain Name. If this field is left blank, the default Tivoli Access Manager run-time domain will be used.

TAM Management Domain Name

Optional: Applicable only when using LDAP reconciliation for Tivoli Access Manager version 6.1 and above.

Specify the management domain that was used when the Tivoli Access Manager policy server was configured.

TAM Management Domain Location DN

Optional: Applicable only when using LDAP reconciliation for Tivoli Access Manager version 6.1 and above.

Specify the distinguished name of Tivoli Access Manager server management domain location on directory server which was used during Tivoli Access Manager installation. If not specified, it is assumed to be a standalone suffix on the directory server.

Object Class(es) for TAM User Entry

Optional: List of object class names used for user entry in the registry, it must be provided in the form of a comma-separated list.

These classes must already be defined in the directory schema. If not specified, user entries will be instances of object classes defined in Tivoli Access Manager Server configuration. This value is ignored if the adapter is configured to "**Import user entry from registry**".

REGISTRY SETUP Tab

TAM Directory Server Admin ID

Specify the directory server administrator's Distinguish Name (such as cn=root).

TAM Directory Server Admin Password

Specify the directory server administrator's password.

TAM Directory Server URL

Specify the location and port number of the directory server configured against Tivoli Access Manager. The valid syntax is ldap://*ip-address*:*port*, where *ip-address* is the directory server host and *port* is the port number. For example, you might specify the URL as ldap://9.38.215.218:389.

TAM Directory Server Type

Specify the type of directory server that Tivoli Access Manager is configured against:

- *LDAP-based* should be used for directory server other than Active Directory or Active Directory Application Mode.
- *Active Directory* should be used for Active Directory.
- *ADAM* should be used for Active Directory Application Mode.

TAM Directory Server SSL Connection

Check this option if Secure Sockets Layer is used by the Tivoli Directory Integrator LDAP Connector for communication with the directory server. Note that SSL is mandatory in case of Active Directory type registries.

Once the service has been created, click **Test** to ensure that the connection to both the directory server and to the Tivoli Access Manager Policy Server can be established.

Configuration information for the adapter should be reported in the Tivoli Directory Integrator log file (ibmdi.log) as a result of a successful test.

References:

- Tivoli Access Manager Combo Adapter Installation and Configuration Guide http://www.redbooks.ibm.com/redbooks/pdfs/sg246477.pdf

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.
Produced in the United States of America
08-10