IBM Security Directory Integrator
Version 7.2

Problem Determination Guide

GC27-2709-02

IBM Security Directory Integrator
Version 7.2

Problem Determination Guide

GC27-2709-02

Note

Before using this information and the product it supports, read the general information under Appendix B, “Notices,” on page 55.

Edition notice

Note: This edition applies to version 7.2 of IBM Security Directory Integrator licensed program (5724-K74) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this publication

This publication contains the information that you require to develop solutions by using components that are part of IBM® Security Directory Integrator.

IBM Security Directory Integrator components are designed for network administrators who are responsible for maintaining user directories and other resources. It is assumed that you have practical experience with installation and usage of both IBM Security Directory Integrator and IBM Security Directory Server.

The information is also intended for users who are responsible for the development, installation, and administration of solutions by using IBM Security Directory Integrator. The reader must familiar with the concepts and the administration of the systems that the developed solution would connect to. Depending on the solution, these systems might include, but are not limited to, one or more of the following products, systems, and concepts:

- IBM Security Directory Server
- IBM Security Identity Manager
- IBM Java™ runtime environment (JRE) or Oracle Java runtime environment
- Microsoft Active Directory
- Windows and UNIX operating systems
- Security management
- Internet protocols, including Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS) and Transmission Control Protocol/Internet Protocol (TCP/IP)
- Lightweight Directory Access Protocol (LDAP) and directory services
- A supported user registry
- Authentication and authorization concepts
- SAP ABAP Application Server

Access to publications and terminology

Read the descriptions of the IBM Security Directory Integrator Version 7.2 library and the related publications that you can access online.

This section provides:

- A list of publications in the "IBM Security Directory Integrator library."
- Links to "Online publications" on page viii.
- A link to the "IBM Terminology website" on page ix.

IBM Security Directory Integrator library

The following documents are available in the IBM Security Directory Integrator library:

- *IBM Security Directory Integrator Version 7.2 Federated Directory Server Administration Guide*

  Contains information about using the Federated Directory Server console to design, implement, and administer data integration solutions. Also contains information about using the System for Cross-Domain Identity Management (SCIM) protocol and interface for identity management.
- *IBM Security Directory Integrator Version 7.2 Getting Started Guide*

  Contains a brief tutorial and introduction to IBM Security Directory Integrator. Includes examples to create interaction and hands-on learning of IBM Security Directory Integrator.

- *IBM Security Directory Integrator Version 7.2 Users Guide*

  Contains information about using IBM Security Directory Integrator. Contains instructions for designing solutions using the IBM Security Directory Integrator designer tool (the Configuration Editor) or running the ready-made solutions from the command line. Also provides information about interfaces, concepts and AssemblyLine creation.
- *IBM Security Directory Integrator Version 7.2 Installation and Administrator Guide*

  Includes complete information about installing, migrating from a previous version, configuring the logging functionality, and the security model underlying the Remote Server API of IBM Security Directory Integrator. Contains information on how to deploy and manage solutions.
- *IBM Security Directory Integrator Version 7.2 Reference Guide*

  Contains detailed information about the individual components of IBM Security Directory Integrator: Connectors, Function Components, Parsers, Objects and so forth – the building blocks of the AssemblyLine.
- *IBM Security Directory Integrator Version 7.2 Problem Determination Guide*

  Provides information about IBM Security Directory Integrator tools, resources, and techniques that can aid in the identification and resolution of problems.
- *IBM Security Directory Integrator Version 7.2 Message Guide*

  Provides a list of all informational, warning and error messages associated with the IBM Security Directory Integrator.
- *IBM Security Directory Integrator Version 7.2 Password Synchronization Plug-ins Guide*

  Includes complete information for installing and configuring each of the five IBM Password Synchronization Plug-ins: Windows Password Synchronizer, Sun Directory Server Password Synchronizer, IBM Security Directory Server Password Synchronizer, Domino® Password Synchronizer and Password Synchronizer for UNIX and Linux. Also provides configuration instructions for the LDAP Password Store and JMS Password Store.
- *IBM Security Directory Integrator Version 7.2 Release Notes®*

  Describes new features and late-breaking information about IBM Security Directory Integrator that did not get included in the documentation.

Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

Information related to the IBM Security Directory Integrator is available in the following publications:

IBM Security Directory Integrator Library

The product documentation site (http://http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDI.doc_7.2/welcome.html) displays the welcome page and navigation for this library.

IBM Security Systems Documentation Central

IBM Security Systems Documentation Central provides an alphabetical list of all IBM Security Systems product documentation and links to the online documentation for specific versions of each product.

IBM Publications Center

The IBM Publications Center site (http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss) offers customized search functions to help you find all the IBM publications you need.

Related information

Information related to IBM Security Directory Integrator is available at the following locations:

- IBM Security Directory Integrator Version 7.2 uses the JNDI client from Oracle. For information about the JNDI client, see the *Java Naming and Directory Interface™ Specification* at http://download.oracle.com/javase/7/docs/technotes/guides/jndi/index.html.
- Information that might help to answer your questions related to IBM Security Directory Integrator can be found at https://www-947.ibm.com/support/entry/myportal/overview/software/security_systems/tivoli_directory_integrator.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at http://www.ibm.com/software/globalization/terminology.

Accessibility

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use information technology products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You also can use the keyboard instead of the mouse to operate all features of the graphical user interface.

For additional information, see the Accessibility Appendix in *IBM Security Directory Integrator Version 7.2 Users Guide*.

Technical training

For technical training information, see the following IBM Education website at http://www.ibm.com/software/tivoli/education.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at http://www.ibm.com/software/support/probsub.html.

IBM Security Directory Integrator Version 7.2 Problem Determination Guide provides details about:

- What information to collect before contacting IBM Support.
- The various methods for contacting IBM Support.
- How to use IBM Support Assistant.
- Instructions and problem-determination resources to isolate and fix the problem yourself.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Chapter 1. Introduction to problem determination

This guide provides information about IBM Security Directory Integrator Version 7.2 tools, resources, and techniques that can aid in the identification and resolution of problems.

IBM Security Directory Integrator Version 7.2 overview

IBM Security Directory Integrator (IBM Security Directory Integrator) manages the technicalities of connecting to and interacting with the various data sources that you want to integrate, abstracting away the details of their APIs, transports, protocols and formats. Instead of focusing on data, IBM Security Directory Integrator lifts your view to the information level, enabling you to concentrate on the transformation, filtering and other business logic required to perform each exchange.

The architecture of IBM Security Directory Integrator is divided into two parts:

- The kernel, where most of the system's functionality is provided, and which you leverage to quickly build the framework of your solution.
- The components, which abstract away the technical details of the data systems, platforms and formats that you want to work with. IBM Security Directory Integrator provides you with a number of component types, such as: connectors, parsers and Function Components.

When faults and errors occur, several built-in diagnostic tools are used to collect information and determine the exact cause of the problem.

Troubleshooting topics

This guide contains troubleshooting information for the following topics:

- Installation: See Chapter 3, “Installation and uninstallation,” on page 7 for more information.
- Configuration Editor: See Chapter 4, “Configuration Editor,” on page 15 for more information.
- Administration and Monitoring Console: See “Administration and Monitoring Console Problem Determination” on page 21 for more information.
- Components: See Chapter 7, “Components,” on page 25 for more information.
- Known limitations and general troubleshooting: See Chapter 9, “Known limitations and general troubleshooting,” on page 37 for more information.
- Scenarios: See Chapter 10, “Troubleshooting scenarios,” on page 45 for more information.

Built-in troubleshooting features

Note: Many of the built-in troubleshooting features are documented elsewhere in the IBM Security Directory Integrator Version 7.2 documentation library. The following sections tell you where to look for information about these features.

Logging

IBM Security Directory Integrator relies on log4j as a logging engine. It is a very flexible framework that lets you log to file, NT eventlog, Unix syslog and more, and can be tuned so it suits most needs. It can be a great help when you want to troubleshoot or debug your solution.

For information about IBM Security Directory Integrator logging, see the "Logging and debugging" chapter in the *IBM Security Directory Integrator Version 7.2 Installation and Administrator Guide*.

To see examples of the logging windows of the Configuration Editor see the "Configuration Editor" chapter in the *IBM Security Directory Integrator Version 7.2 Users Guide*

AssemblyLine Auto Dump

The property `com.ibm.tdi.autodump.directory` is a property you can set in `global.properties` or `solution.properties`. It enables AssemblyLine state dumps to be performed automatically when an AssemblyLine terminates abnormally. The state dump contains valuable information about the state of the AssemblyLine at the time of termination such as JavaScript variables and other useful information. The value of this property should be a relative or absolute path to an existing directory. For default installations it is useful to specify "`logs`" so that the dumps end up in the same directory as the other logs. The log for each AssemblyLine is named after the AssemblyLine itself. The dump is appended to existing files.

Debugging

IBM Security Directory Integrator Version 7.2 offers an AssemblyLine debugging tool called the AssemblyLine Stepper. The AssemblyLine Stepper allows you to:

1. Define breakpoints for AssemblyLines.
2. Pause AssemblyLine processing at the defined breakpoints to examine the AssemblyLine for errors.

The AssemblyLine Stepper is part of the Configuration Editor. For more information about how to use the AssemblyLine Stepper, refer to the "Configuration Editor" chapter of the *IBM Security Directory Integrator Version 7.2 Users Guide*.

Tracing and First Failure Data Capture (FFDC)

IBM Security Directory Integrator is instrumented throughout its code with tracing statements, using the JLOG framework, a logging library similar to log4j, but which is used inside IBM Security Directory Integrator specifically for tracing and First Failure Data Capture (FFDC).

For information about IBM Security Directory Integrator logging, see the "Tracing and FFDC" chapter in the *IBM Security Directory Integrator Version 7.2 Installation and Administrator Guide*.

Sandbox

IBM Security Directory Integrator includes a Sandbox feature that enables you to record the operation of one or more Connectors in an AssemblyLine for later replay without the necessary data sources being available. This feature uses the System Store.

This feature can be very useful when providing support materials. Often, the time to reproduce the environment for an AssemblyLine and the state of data sources to reproduce a condition can be quite comprehensive. With a sandbox database with a recorded session, a support person can run the AssemblyLine without having access to all data stores the AssemblyLine requires. In addition, the AssemblyLine configuration can be modified to print out more information if that is necessary. The only change that cannot be done to the AssemblyLine configuration is to make additional calls or reorder the calls to recorded components. This would cause an error during playback as calls to the connector would not match the next expected call to the connector.

For more information, see the section called "Debugging features in IBM Security Directory Integrator" in *IBM Security Directory Integrator Version 7.2 Users Guide*.

Action Manager

The Action Manager is an error management mechanism that allows you to create Action Manager rules for your AssemblyLines.

An Action Manager rule consists of two parts:

1. The condition under which the rule is to be invoked, called a "trigger." Some examples of triggers are Server API failure, AssemblyLine failure, or failure of the AssemblyLine to run at specified intervals.
2. A set of alternate actions to perform when the trigger is encountered.

The Action Manager is part of the Administration and Monitoring Console (Administration and Monitoring Console). For instructions on how to use the Action Manager, consult the Administration and Monitoring Console chapter in the *IBM Security Directory Integrator Version 7.2 Installation and Administrator Guide*

Performance Test and Debug Utilities

IBM Security Directory Integrator Version 7.2 includes Performance Test and Debug Utilities tools. The Performance Test Tool monitors the system-level parameters and the server, records and logs information for the system and server at specified intervals of time. Performance test parameters are then used for throughput measurement and capacity planning.

The Debug Utilities tool identifies memory usage and memory leaks in specific IBM Security Directory Integrator components by collecting information at specific intervals and upon certain actions.

See Chapter 2, “Performance Test Utilities and Debugging,” on page 5 for more information about IBM Security Directory Integrator's benchmarking tools.

Using the Messages Guide to resolve errors

See the *IBM Security Directory Integrator Version 7.2 Message Guide* for information about why the error occurred and how to resolve it.

Chapter 2. Performance Test Utilities and Debugging

There are two performance tools included with IBM Security Directory Integrator Version 7.2: a Performance Test Utilities tool and a Performance Debugging tool. These tools monitor and log system and server information at specified intervals of time. The information gathered can then be used for throughput measurement and capacity planning.

This chapter describes these tools and explains how to configure and gather information from them.

Performance Test Utilities

The Performance test utilities are shell scripts that launch a server instance for a particular configuration and log system-level (Input/Output (IO), Central Processing Unit (CPU), network) and Java Virtual Machine (JVM) level information. The test utilities can be used to benchmark macro parameters such as throughput, application memory and CPU usage. Data is logged into the performance logs at user specified intervals.

Running the Performance Test Utilities scripts

There are two shell scripts: The ibmdisrvtp.sh utility and the ibmdibenchmark.sh utility. The ibmdisrvtp.sh utility measures server throughput. The ibmdibenchmark.sh utility logs system-level information. The utilities must be executed separately.

Note: The Performance Test Utilities shell scripts are not supported on Windows operating systems.

Running the ibmdisrvtp.sh utility

1. Copy the ibmdisrvtp.sh and benchmark.properties files from the `<itdi_install_dir>/performance` directory to the `solution` directory.
2. Open the benchmark.properties file, and specify the following settings:
   - ibmdiroot: Specify the IBM Security Directory Integrator install directory
   - solutiondir: Specify IBM Security Directory Integrator solution directory
   - configfile: The name of the Config file to be loaded
   - assemblyline: The AssemblyLine to be started
   - cmdoptions: The ibmdisrv command line options. By default, the value for cmdoptions is None.
   - jvmcmdoptions: The JVM command line options. By default, the value for jvmcmdoptions is `None`.
3. At a command prompt, execute the following command from the command line:

   ```
   ./ibmdisrvtp.sh –f benchmark.properties
   ```

Running the ibmdibenchmark.sh utility

1. Copy the ibmdibenchmark.sh and benchmark.properties files from `<`*`itdi_install_dir`*`>/performance` directory to `solution` directory.
2. Open the benchmark.properties file, and specify the following properties:
   - duration: Duration time in seconds, set it to`-1` to run it for an infinite time period.
   - interval: Interval time in seconds to collect system-level information. If duration is not set to `-1` then interval should be less than the duration.
   - ios: enable or disable input-output information recording (`y` to enable, `n` to disable)
   - vms: enable or disable memory usage/information recording (`y` to enable, `n` to disable)
   - nets: enable or disable network information recording (`y` to enable, `n` to disable)
3. From the command line, execute the following command:

```
./ibmdibenchmark.sh –f benchmark.properties
```

Performance debugging

The Performance Debugging tool identifies memory usage and memory leaks in specific IBM Security Directory Integrator components by collecting information at specific intervals and upon certain actions.

Data collected by the Performance Debugging tool

This feature logs the following information:

- Component name
- Time (in milliseconds)
- Memory usage

Component names are prefixed with the name of the AssemblyLine instance that uniquely identifies each component.

Memory usage is the difference between total memory available (JVM) at start and total memory available at end for each component during its execution.

Before AssemblyLine terminates, the performance entry that contains performance statistics is logged. This is then followed by logging of the overall AssemblyLine performance statistics.

Running the Performance Debugging tool

To run the Performance Debugging tool, use one of the following methods:

- Start the server using the -T parameter
  ```
  ibmdisrv -T
  ```
- Start the server by setting the following property in the global.properties or solution.properties file:
  ```
  ## Enable\Disable performance logging
  com.ibm.di.server.perfStats=true
  ```

Note: The -T parameter takes precedence over the solution.properties file setting. If the com.ibm.di.server.perfStats value is set to `false`, you can still obtain performance statistics by starting the server using the -T parameter.

Chapter 3. Installation and uninstallation

Troubleshooting installation

Installation and uninstallation of IBM Security Directory Integrator is scripted and implemented using InstallAnywhere 2012 SP1 installer technology.

Gathering installation information

Gathering information about your installation can help IBM Support determine the source of your problem.

For any problems with the user interface, the install process or post-install process collects the `sdiv72install.log` and `sdiv72debug.log` found in the system's temp directory.

During an upgrade from IBM Security Directory Integrator 7.0 , 7.1 or 7.1.1 to IBM Security Directory Integrator 7.2, if there is a problem with uninstalling IBM Security Directory Integrator 7.0 , 7.1 or 7.1.1, collect the following files:

- The `tdiv7*uninstall.log`, `tdiv7*debug.log`, and `sdiv72install.log` found in the system's temp directory.
- Any logs found in the `<`*`SDI_Install_dir`*`>\logs`directory.

In addition, collect any of the following files, if they exist, from the system's temp directory:

- amcInstall.log
- amcInstallErr.log
- amcRoles.log
- amcRolesErr.log
- StdErr.log
- StdOut.log
- sdiv72uninstall.log
- tdiSoldir.log
- tdiSoldirErr.log
- lum.out
- lumerr.out
- ITLM.xx

The InstallAnywhere debug logs, `sdiv72debug.log`, and `sdiv72install.log`, which are generated in the system’s temp directory, contain more debug information than the regular install log.

Performing a manual uninstallation

When uninstallation of IBM Security Directory Integrator, using uninstaller, fails due to unexpected errors, manually restore the target system to a state without IBM Security Directory Integrator. Refer to the InstallAnywhere installation registry location for details on Zero G Registry file.

Removing IBM Security Directory Integrator on Windows

1. Run the *`TDI_install_dir`*`\bin\amc\stopAM.bat` utility to stop the Action Manager (AM), if it is running.
2. If the AMC was installed as service, execute the following commands:
   - sc stop <amcservice_name>

- sc delete <amcservice_name>

Else, use the `stop_tdiamc.bat` utility in the *TDI_install_dir*`\bin\amc` folder.

3. If the AMC was deployed on IBM WebSphere® Application Server, use *TDI_install_dir*`\bin\amc\uninstall.bat` utility to undeploy it from IBM WebSphere Application Server.
4. Run `ibmditk –tdishutdown`. This stops any other TDI server instances that might have left running.
5. If you have installed the password plug-ins, go back through the install steps and unregister native plugin, if any, that you have registered.
6. Use the `pwd_plugins/bin/stopProxy.bat` script to stop the running Java Proxy.
7. Remove the IBM Security Directory Integrator install directory.
8. Optional: Remove the IBM Security Directory Integrator Solutions Directory.
9. Remove the Windows shortcuts from the Start Menu.
10. Remove TDI's Add/Remove Program entries and the AMC service from the Windows Registry.
11. Locate the InstallAnywhere installation registry file `.com.zerog.registry.xml`, which is found at the following location: `C:\Program Files\Zero G Registry\.com.zerog.registry.xml`

    Perform the following steps:

    a. Open the `.com.zerog.registry.xml` file in a text editor.
    b. Within the <products> element, remove the <product> element and all its descendant elements.
    c. Within the <components> element, remove the <component> element and all its descendant elements.
    d. Save and close the file.

Removing IBM Security Directory Integrator on Unix and Linux

1. Run the *TDI_install_dir*`/bin/amc/stopAM.sh` script to stop AM.
2. Call the `stop_tdiamc.sh` script. If the AMC was deployed on IBM WebSphere Application Server, use the *TDI_install_dir*`/bin/amc/uninstall.sh` script to undeploy it from IBM WebSphere Application Server.
3. If you have installed the password plug-ins, go back through the install steps and unregister the native plugin, if any, that you have registered.
4. Use the `pwd_plugins/bin/stopProxy.sh` script to stop the running Java Proxy.
5. Remove the IBM Security Directory Integrator install directory.
6. Optional: Remove the IBM Security Directory Integrator Solutions Directory.
7. Edit the `/etc/inittab` file and remove the `amc::once:/opt/IBM/Security Directory Integrator/V7.2/lwi/bin/lwistart.sh > /dev/console 2>&1` line that is associated with the IBM Security Directory Integrator instance you are removing. The install location should match the location you are removing.
8. Locate the InstallAnywhereinstallation registry file `.com.zerog.registry.xml` on your system. This registry file is found at:
    - `/var/.com.zerog.registry.xml` directory if logged in as root during install.
    - `<user_home_dir>/.com.zerog.registry.xml` directory if logged in as user during install.

    Perform the following steps:

    a. Open the `.com.zerog.registry.xml` file in a text editor.
    b. Within the <products> element, remove the <product> element and all its descendant elements.
    c. Within the <components> element, remove the <component> element and all its descendant elements.

d. Save and close the file.

Troubleshooting installation problems

This section explains troubleshooting problems and explains any workarounds you can use.

For a more detailed Installation procedure, see *IBM Security Directory Integrator Version 7.2 Installation and Administrator Guide*.

IBM Security Directory Integrator Version 7.2 installer does not appear to honor -D$INSTALLER_TEMP_DIR$ option

Symptom:

On Windows, this option appears to be silently ignored, and temporary installer data still is stored in the system's temp directory. On Linux/UNIX, specifying the option results in an exception being thrown.

Resolution:

To use a custom temporary files directory for Version 7.2 of the IBM Security Directory Integrator installer, you need to specify the InstallAnywhere temp variable as a system environment variable.

For Windows: Setting `IATEMPDIR` as an environment variable prior to launching the installer does not work. Instead, empty the system's temp directory and ensure you have enough space available there to continue with the installation, or set the environment variable %TEMP% to point to a directory with sufficient space.

Note: Take a backup of the current temp directory before emptying it.

For Linux/UNIX: Set the environment variable for InstallAnywhere to use as a temp directory in the console window, for example:

```
IATEMPDIR=/opt/IBM/TDI/temp

export IATEMPDIR
```

IBM Security Directory Integrator Version 7.2 installer fails to detect previously installed v6.1 or v6.1.1 instances

Symptom 1:

The IBM Security Directory Integrator Version 7.2 installer will catch an exception from the Solution Installation other than `SINotInstalledException`. Although the v6.1 and the v6.1.1 versions of IBM Security Directory Integrator are installed, the IBM Security Directory Integrator Version 7.2 installer is unable to detect them. The installer displays the following message:

```
A Solution Installation exception was encountered. There may be undetected versions of Security Directory Integrator
installed. If an installation directory of a previously installed version of Security Directory Integrator is chosen
as the new installation location, the previously installed version of Security Directory Integrator will be overwritten.
When the previously installed version of Security Directory Integrator is overwritten, this may cause a loss of user data.
```

Resolution:

If you choose to continue, you must manually verify whether the install directory contains a 6.1 or 6.1.1 installation of IBM Security Directory Integrator. If the selected install directory contains a 6.1 or 6.1.1 installation, IBM Security Directory Integrator Version 7.2 will be installed on that directory, but a migration will not take place. The old user data may be lost, and the previous IBM Security Directory Integrator version is unusable.

Also, you can restart the ACSI service on the system and run the installer again to detect previous versions of IBM Security Directory Integrator.

Symptom 2:

The IBM Security Directory Integrator Version 7.2 64-bit installer will catch the `SINotInstalledException` exception from the Solution Installation. Although the v6.1.1 version of IBM Security Directory Integrator is installed and Solution Install service is running, the IBM Security Directory Integrator Version 7.2 64-bit installer is unable to detect it. The installer displays following message in the debug.log file:

```
SI not installed.
```

Resolution:

Restart the ACSI service on the system and run the installer again to detect previous versions of IBM Security Directory Integrator. Also, you can manually migrate the files from IBM Security Directory Integrator 6.1.1 to Version 7.1.1 and then install IBM Security Directory Integrator Version 7.2. For more information on manual migration, see the “Migrate files to a newer version” section in the *IBM Security Directory Integrator Version 7.2 Installation and Administrator Guide*.

On RHEL 5.0 (or any other system with SELinux enabled), IBM Security Directory Integrator Version 7.2 installer fails to launch with error "No Java Runtime Environment (JRE) was found on this system"

The RHEL 5.0 default settings for SELinux prevents Java 6 from running properly. IBM Security Directory Integrator Version 7.2 bundles Java 7 and uses it to launch the installer.

The following steps produce the error:

1. The user launches the IBM Security Directory Integrator installer

   ```
   # ./install_sdiv72_linux_x86_64.bin
   ```

2. Message will appear stating:

   Initializing Wizard.....
   Extracting Bundled JRE.
   Verifying JVM

   No Java Runtime Environment (JRE) was found on this system.

The following solutions are available:

- Temporarily disable SELinux by using the **setenforce 0** command, run the install , and enable SELinux by using the **setenforce 1** command. or.
- Edit the `/etc/selinux/config` file and set SELINUX to either permissive or disabled. This solution, however, affects the level of security for the entire system.

"No Java Runtime Environment (JRE) was found on this system": JVM verification fails while installing IBM Security Directory Integrator on some slower platforms

Note: On RHEL 5.0, there can be another reason for this error situation.
Verification of the JVM sometimes fails during installation on slower platforms. Failure usually results because the verification takes more time than the installer expects it to take.

The following steps produce the error:

1. The user launches the IBM Security Directory Integrator installer.

   Linux example:

   ```
   # ./install_sdiv72_linux_x86_64.bin
   ```

2. The following message appears:

```
Initializing Wizard.....
Extracting Bundled JRE.
Verifying JVM

No Java Runtime Environment (JRE) was found on this system.
```

The solution is to run the installer from the command line and specify a longer time to wait before verifying the JRE:

```
... -is:jvmtimer
```

Use a longer time span to give the verification step more time on slower platforms. Specify the time span in seconds. The syntax of this parameter is (this parameter is valid on non-Windows platforms only):

`-is:jvmtimer <`*`seconds`*`>`

Linux example:

```
# ./install_sdiv72_linux_x86_64.bin -is:jvmtimer 15
```

For HP-IA64 11iV2, this value needs to be 60 seconds. Use a command as follows:

```
./install_sdiv72_hpux_ia64.bin -console -is:log log.txt -is:jvmtimer 60 -is:tempdir ./tmp
```

The value 15 may be altered as needed.

AIX 5.3: No Java Runtime Environment (JRE) was found on this system.

On AIX 5.3, if may receive the following error message when trying to run the installer:

```
No Java Runtime Environment (JRE) was found on this system.
```

This may indicate that AIX is not at the appropriate level. You may check this with the oslevel -r command:

```
# oslevel -r
5300-00
```

The digits after the dash indicate the maintenance level, and at least ML03 is required. Apply this maintenance level if it is not installed and attempt to run the installer again.

Ikeyman file needs executable permissions on Solaris operating systems

On Solaris operating systems, the Ikeyman file requires executable file permissions; for example, 555. The Ikeyman file is located in the jre/bin directory.

Unable to migrate Cloudscape System Store of IBM Security Directory Integrator 7.0 to IBM Security Directory Integrator 7.x

These conditions are symptoms of a failed migration from Cloudscape System Store 6.0 to Derby System Store 7.0, 7.1, 7.1.1, or 7.2.

- The IBM Security Directory Integrator SysStore folder is empty.
- Unable to access IBM Security Directory Integrator 6.0 System Store data.
- Installer failed with message: Unable to migrate Cloudscape Database.

The migration failed because the Cloudscape Database could not be migrated by the installer.

IBM Security Directory Integrator Version 7.2 uses Derby v10.x drivers that are not compatible with previous versions of Cloudscape. Because IBM Security Directory Integrator 6.0 uses Cloudscape version 5.1 as its System Store, Cloudscape must be first migrated to a Derby v10.x database in 7.0, 7.1, 7.1.1, or 7.2.

To migrate to Derby version 10, you need the `migrateCS` script shipped with IBM Security Directory Integrator 7.0 and later. This script is located in the following directory:

`TDI_install_dir``/tools/CSMigration`

To migrate your older Cloudscape database, invoke the migrateCS script as follows:

```
migrateCS <oldCSdirectoryDB> <newCSdirectoryDB>
```

For example, if your old Cloudscape DB is in the E:\MyDB directory, and you wish to create a new one in the E:\Security Directory Integrator61\MyDB_10 directory, run the following command:

```
migrateCS E:\MyDB E:\Security Directory Integrator61\MyDB_10
```

Note:

- The MyDB_10 folder will be automatically created by the script. It must not exist before invoking the script.
- This migration utility can be used for migrating only from Cloudscape 5.1 to Derby Version 10. Hence, the *TDI_install_dir*/tools/CSMigration/migratCS.bat(sh) file can be used for migrating system store database from IBM Security Directory Integrator Version 6.0 to Versions 6.1.1 and later. However, for migrating system store database from IBM Security Directory Integrator Version 6.1.1 to later versions, you must simply copy the old TDISysStore from the Version 6.1.1 installation directory to the new installation of the new version.

Silent installation/uninstallation of IBM Security Directory Integrator Version 7.2 fails if double quotes are used to specify InstallAnywhere variable values

Symptom:

Silent installation of IBM Security Directory Integrator 7.2 fails when the USER_INSTALL_DIR path is specified in the response file using double quotes, for example, USER_INSTALL_DIR = "/opt/IBM/TDI/V7.2", and displays the following error message:

```
The chosen directory is not with absolute path in sdiv72debug.log.
```

Solution:

Do not use double quotes (“ ”) for InstallAnywhere variable values in the response file. The InstallAnywhere takes care of the spaces and treats that value as a String. The best practice is to use the response file for silent installation and uninstallation, which is generated using GUI or Console mode of installer/uninstaller.

@LongLink error when extracting the release image

Symptom:

When you extract release image using the native AIX or Solaris tar command, you might get the following @LongLink error:

```
Preparing to install...
./install_sdiv72_solaris_x86_64.bin: !: not found
Extracting the JRE from the installer archive...
Unpacking the JRE...
tar: ././@LongLink: typeflag 'L' not recognized, converting to regular file
tar: ././@LongLink: typeflag 'L' not recognized, converting to regular file
tar: ././@LongLink: typeflag 'L' not recognized, converting to regular file
.....
The included VM could not be unarchived (TAR). Please try to download
the installer again and make sure that you download using 'binary'
mode. Please do not attempt to install this currently downloaded copy.
```

When IBM Security Directory Integrator installation kits in the product DVD media, use a directory structure, which is too deep for UNIX platforms, such as AIX and Solaris, you get this error message. This error is due to the lengthy file name. The file name includes full path of the file, which is too long for the native operating system commands.

Solution:

Use the GNU tar, available at http://www.gnu.org, when you extract the release tar image on AIX and Solaris platforms. Before you extract the release tar image on AIX or Solaris platform, ensure that GNU tar is the default native tar on the operating system.

Known limitations

The following statements represent known issues with the IBM Security Directory Integrator installation process. Workarounds are provided where available.

Multiple installations not registered correctly in Windows Add/Remove Programs

The InstallAnywhere 2012 SP1 used by IBM Security Directory Integrator Version 7.2 allows you to install multiple versions of IBM Security Directory Integrator. However, these installations are not tracked properly in the Windows Add/Remove Programs control panel.

In fact, only the last installation you performed is visible there. If you use the control panel to uninstall IBM Security Directory Integrator, it is indeed the last installation you remove. Any remaining installations will not be visible.

The recommended and safer way to uninstall a particular version is to go to the *`TDI_install_dir`*`/_uninst` folder of a particular installation, and run the uninstaller executable from there.

Glibc package 2.3 or higher required for installation on Linux operating systems

When installing IBM Security Directory Integrator on a Linux operating system, the *glibc* package must be at level 2.3 or higher.

To determine the level of the glibc package, run the following command:

```
rpm -qa|grep glibc
```

Maintenance Level 3 required for installation on an AIX 5.3 operating system

Make sure that Maintenance Level 3 has been applied before installing IBM Security Directory Integrator Version 7.2 on an AIX® 5.3 operating system.

Incorrect text emphasis when installing IBM Security Directory Integrator on a Windows operating system in Simplified Chinese

During IBM Security Directory Integrator installation on a Windows operating system in Simplified Chinese, some text strings in normal text should be in bold text.

Monitor the installation or uninstallation log during silent installation execution

A silent installation or uninstallation runs in the background. The only way to tell when the silent process has completed, or if an error has occurred, is to follow the installation or uninstallation log while the silent process executes. If you do not monitor the log during installation or uninstallation, you are unable to determine if the silent process completes.

Problems with setting up the IATEMPDIR environment variable

Setting up the environment variable `IATEMPDIR` is not redirecting the debug log file to the custom temp directory on Linux/Unix platform. The file is created in the default temp directory of the system.

Chapter 4. Configuration Editor

Troubleshooting the Configuration Editor

This section explains how to troubleshoot problems and describes any workarounds you can use.

Verify that the server associated with your project has been started

If you receive connection errors when you try to run an AssemblyLine, verify that you have started the server associated with the project. This is usually the *Default* server unless it has been reconfigured to a different server. Also check the logs/ibmdi.log file in your server's working directory. This log file shows indications of server errors that prevent the Configuration Editor from running an AssemblyLine on that server.

Consult the Error View when using the Configuration Editor

Check the Error View in the Configuration Editor for error messages when your actions do not produce the expected results. Select **Window** in the main window toolbar, then select **Show View > Error Log**.

If the Configuration Editor by itself does not start, you may be able to pinpoint problems by looking at the very file this view represents; this file can be found in `workspace/.metadata/.log`, where *workspace* is the path to the workspace directory you have instructed IBM Security Directory Integrator to use.

Unwanted perspective changes

If you for some reason see the "Resource" perspective when you start the Configuration Editor, you should probably switch to the Security Directory Integrator perspective that shows the proper IBM Security Directory Integrator views and functions. Use the **Window -> Open Perspective -> Other...** menu option and choose **Security Directory Integrator** from the list of perspectives.

Problems during installation of the CE into Eclipse

If you experience problems installing the IBM Security Directory Integrator CE into a non-IBM Security Directory Integrator Eclipse environment, you may have to add an additional update site where software update can access plugins for Eclipse Version 4.2.2 prior to installing the IBM Security Directory Integrator feature.

Eclipse Editor is not using the defined solution directory path

Problem

The path defined for the solution directory in the Servers view of CE is not used by the Eclipse Editor.

Solution

When the CE is installed as a plug-in in Eclipse, you need to define the solution directory path before starting Eclipse using the following steps:

1. Right click on the Eclipse icon.
2. Click **Properties**.
3. Type the solution directory path for IBM Security Directory Integrator in the **Start in** field.

Note: Start the Eclipse from the defined solution directory.

Problems when an invalid character is used for delta store name

The name used for a delta store must be a valid table name in the system store database. The exact rules depend on the database. Use only ASCII letters, numbers, or underscore for the delta store name.

Known limitations

The following issue statements represent known issues with the IBM Security Directory Integrator Configuration Editor. Workaround are provided where available.

Solution directory does not always resolve to expected path

The default working directory for the Configuration Editor is your solution directory. However, you can have many projects associated with different servers, each server having a different solution directory path. The relative path for the solution directory in each of your project components may not resolve to the path you expect.

Upper part of characters truncated in Javascript panel

When tabs in a tabbed control have English text as the first label in the list and other tabs have Chinese labels, the Chinese labels will be cut off at the top by a few pixels when they are not selected. Clicking on a tab with Chinese text will properly make the full text visible.

CE hangs after seeing the splash screen or choosing the workspace on AIX

The CE may hang after seeing the splash screen or choosing the workspace on AIX. This has been seen happening when there are many firewalls/routers/bridges between the client and the AIX machine on which the CE is started. Getting closer to the AIX in networks terms can possibly solve the issue. Also try a different window manager.

Logging difference between IBM Security Directory Integrator 6.1.1 and 7.x.x version when startAL() script is run from CE

Problem

In IBM Security Directory Integrator 6.1.1, when you run an AssemblyLine from CE, a new server is started to run the AssemblyLine. This server is set up to make all logging to go a standard output, instead of a log file. The CE displays output in the console, which includes all logging from the AssemblyLine being run and also from the child AssemblyLines that are being started, directly or indirectly, from the parent AssemblyLine. The output also includes logging from main.logmsg() method, messages written to standard out, and standard error.

In IBM Security Directory Integrator 7.x.x, the CE connects and starts the server before starting an AssemblyLine. This server uses the normal logging defined in the etc/log4j.properites file and all events are logged to the logs/ibmdi.log file. The log file includes everything logged from all AssemblyLines that are started in that server, and also logging by main.logmsg() method. You can see the standard output or standard error of the server in the Console tabbed window, which is located at the bottom of the CE.

When CE starts an AssemblyLine, it uses the already started server, and starts the AssemblyLine with a logger attached to it, in addition to the normal loggers. This attached logger catches all log messages logged by the AssemblyLine and are displayed in the Run AssemblyLine window.

If this AssemblyLine starts the child AssemblyLines, the log messages are not shown in the Run AssemblyLine window. To view the log messages of the other AssemblyLines in the window, pass the logger of the initially started AssemblyLine to them, when started.

The Servers view, located on the lower left corner of the CE, shows a tree view of running servers and AssemblyLines. To view the log messages of other running AssemblyLines:

1. In the Servers view, located on the lower left corner of the CE, select a running AssemblyLine from the tree structure.
2. Click **View Log**.

The log messages of the selected AssemblyLine are displayed in the ibmdi.log file, in a text editor.

Solution

To view log messages of all the running AssemblyLines in the Run AssemblyLine window, pass the logger of the initially started AssemblyLine to the other running child AssemblyLines as shown:

```
var al=main.startAL("ALNAME", task.getLog());
```

Or

```
var taskcallblock = task.getTCB();
taskcallblock.setALSetting("debug", "true");
var vector = new java.util.Vector();
vector.add(taskcallblock);
vector.add(task.getLog());
var al = main.startAL("ALNAME", vector, null);
```

Chapter 5. IBM JavaScript limitations

The following sections describe limitations you might encounter when using IBM JavaScript.

java.lang.OutOfMemoryError: Failed to fork OS thread

This section explains the following error:

```
java.lang.OutOfMemoryError: Failed to fork OS thread
```

This error occurs when thousands of threads are started in very quick succession (almost simultaneously). The error indicates that the upper limit on the number of concurrent threads for the JVM has been reached.

Normally this error occurs when a Javascript loop starts thousands of threads in a very short period of time. This error should not occur in normal conditions in which IBM Security Directory Integrator solutions usually operate.

You can avoid this error by inserting a very small delay between starting successive threads (even as small as 1 millisecond). This delay can cause performance to decrease a little, but the error would disappear.

String representations of numbers not represented in exponential format

String representations of numbers do not use exponential format. For example, the following string:

```
String( -1000000000000000000000 )
```

yields the following results:

```
"-10000000000000000000000"
```

Package and class references do not return string values

Package and class references do not return string values. For example, the following reference:

```
main.logmsg ("String: " + java.lang.String);
```

results in an exception.

Date constructors cannot take values higher than the maximum integer value

Date constructors that use numeric values higher than 2.32 wrap and return the wrong date value.

All comparisons of prototypes return false

Comparisons of prototypes return false; for example:

```
Math.__proto__ == Object.prototype --> false
```

Arrays with high numeric values truncate

Creating an array with a numeric value higher than 2*32 results in a truncated value and a smaller array than requested.

Variable override of standard types allowed

IBM JavaScript allows variables to override standard types; for example, the following string:

```
STRING = ""; new STRING())
```

does not result in an exception.

Declaring two or more functions on same line allowed

IBM JavaScript allows you to declare more than one function on the same line.

Chapter 6. Troubleshooting the Administration and Monitoring Console

Administration and Monitoring Console Problem Determination

This section explains problems found in the Administration and Monitoring Console, and provides workarounds, where available.

Note: The AMC feature is deprecated and will be removed in a future version of IBM Security Directory Integrator.

Problems with localized messages in the console

The embedded Web server (LWI) web container used by AMC relies on UTF-8 for encoding its messages. This encoding is capable to represent every character in the Unicode standard but causes problems when messages are logged in the Windows command prompt. The reason is that the prompt uses the default code page (encoding) of the machine, specified by the language for non-Unicode applications configured in '**Control Panel > Regional and Language Options**' (Advanced tab). Thus, for example, when a Japanese message is logged it is encoded by LWI using UTF-8 and transferred to the console which displays it using the default Japanese encoding (code page 930). This causes the message to appear incorrectly. For IBM Security Directory Integrator messages we have overridden the LWI behavior to use the default encoding of the machine, so there should be no problem to display, for instance, Japanese messages on a Japanese machine. Please note that, if the option for non-Unicode programs in the Control Panel differs from the language used by IBM Security Directory Integrator, it must be modified accordingly.

When AMC is started, several LWI and ISC messages can be seen in the console. They are not under the control of IBM Security Directory Integrator, so if users need to see them properly, they must comment the following line in file *TDI_install_dir*/lwi/conf/logging.properties:

```
java.util.logging.ConsoleHandler.encoding=UTF-8
```

This way, the default encoding of the machine will be used instead of UTF-8, so all message should appear normally.

Another option is to change the code page used by the console to UTF-8 by entering command 'chcp 65001' in the console. Please note, though, that this may cause problems when executing the AMC bat scripts.

Action Manager and Administration and Monitoring Console on different machines

If Action Manager is running on a machine other than the machine where Administration and Monitoring Console is running (for example, Action Manager on zOS), then you should either the use IP Address or the Domain Name Server name

while registering IBM Security Directory Integrator servers. Administration and Monitoring Console is shipped with a default local IBM Security Directory Integrator Server registered using 'localhost'. You should re-register this server using either the IP Address or the DNS name.

Unable to delete IBM Security Directory Integrator Server and Solution Views

You can configure Action Manager rules for a Solution View, so that one rule references some other rule. If one rule references another rule in the Solution View, then you cannot delete either the Solution View or the server that is running the Solution View. To avoid this problem, you can reference one rule to another rule if you associate either of the following with the rule:

- An Execute Action Manager Rule action
- An Enable or Disable Action Manager rule action

Deleting a Server

To delete an IBM Security Directory Integrator server where one rule references another in the Solution View:

1. Select **Servers** in the left navigation area under the AMC grouping. The Servers window appears.
2. In the Servers table, select the **Server** that you want to delete.
3. Click **Delete**.
4. When the confirmation message appears, click **OK** to delete the Server, and click **Cancel** to cancel the deletion.

Deleting a Solution View

To delete the IBM Security Directory Integrator Solution Views where one rule references another in the Solution View:

1. Select **Solution Views** in the left navigation area under the AMC grouping. The Solution Views window appears.
2. In the Solution Views table, select the **Solution View** you want to delete.
3. Click **Delete**.
4. When the confirmation message appears, click **OK** to delete the Solution View and click **Cancel** to cancel the deletion.

String is truncated on the Start AssemblyLine window

The following string is truncated in the Start AssemblyLine window: `The attributes exposed for the selected operation`.

This problem occurs only in Internet Explorer, and only in Korean.

The background of the text in Filter field overlaps the field

When using Simplified Chinese locale in AMC and working with Internet Explorer some text fields might overlap the near images. This is not observed with Mozilla Firefox.

SSL communications problems with AMC in ISC AE

AMC can communicate with the IBM Security Directory Integrator server over SSL. This is the default mode of communication between AMC and an IBM Security Directory Integrator Server. For SSL communication the certificates have to be added in the trust store of IBM WebSphere Application Server to enable it to trust the certificates. If this is not done, Websphere throws the following exception:

```
[5/8/08 14:39:39:984 IST] 00000021 SystemOut     O CWPKI0022E: SSL HANDSHAKE FAILURE:  A signer
 with SubjectDN "CN=host IP, O=IBM, C=US" was sent from target host:port "*:9043".  The signer may
 need to be added to local trust store "${WAS_HOME}\systemApps\isclite.ear\tdiamc.war\testadmin.jks"
 located in SSL configuration alias "DefaultSystemProperties" loaded from SSL configuration file
 "System Properties".  The extended error message from the SSL handshake exception is:
 "No trusted certificate found".
```

In order to resolve the above mentioned error you have to follow the steps mentioned below:

1. Create a new Key store and certificate entry using the **SSL certificate and key management > Key stores and certificates** panel.
2. In the New Panel fill in the necessary details, that is the SSL Configuration name and select the required alias.
3. Add a new entry for the SSL configurations. Map the key store and certificates entry added in step one to the new SSL Configuration.
4. Map the newly added SSL Configuration to the Inbound and Outbound endpoints of the Local Topology.

Note: The AMC feature is deprecated and will be removed in a future version of IBM Security Directory Integrator.

Authentication failure on UNIX when LWI runs as non-root user

On some UNIX platforms (for example, SLES 10) AMC in ISE SE fails consistently to authenticate users, even when correct credentials are specified. Such behavior is observed when AMC is run as a non-root user and the operating system uses a password database (for example, a /etc/shadow file).

To work around this problem, run AMC as a user that has read permissions to the password database. For example, on systems that use shadow passwords you should try adding the user to the shadow group.

Here is an explanation:

By default on UNIX platforms LWI uses a JAAS module that authenticates users through the PAM stack on the machine (see `*TDI_install_dir*/lwi/security/jaas/jaas.config`). PAM is not normally a part of the operating system kernel, so it runs with the permissions of the calling process. To authenticate a user on a system that uses a password database, PAM has to verify the specified password against the password database. This task requires read access to the password database. To work around this restriction, some PAM modules use a special utility which is able to run with root permissions regardless of the caller (an executable whose setuid bit is set and whose owner is root). For example the "pam_unix.so" module available in RHEL 5 uses the "unix_chkpwd" tool to access the password database. Yet there exist PAM modules that do not employ such a mechanism and therefore require the calling process to have read access to the password database.

On systems that use so called "shadow passwords", passwords are stored in hashed form in the /etc/shadow file. To verify a password one needs read access to that file. Usually /etc/shadow is associated with a group named "shadow", whose members are given read access to the file.

Note: The AMC feature is deprecated and will be removed in a future version of IBM Security Directory Integrator.

Chapter 7. Components

This chapter contains troubleshooting information about IBM Security Directory Integrator (IBM Security Directory Integrator) components.

Components overview

Components abstract away the technical details of the data systems, platforms and formats that you want to work with, allowing you to integrate your information across various data sources.

IBM Security Directory Integrator provides you with a number of components types:

- Connectors
- Function Components
- Parsers

Note: The concept of EventHandlers is no longer available in IBM Security Directory Integrator Version 7.2. Use AssemblyLines with Server Mode connectors instead.

The following sections contain troubleshooting information for each type of component.

Connectors

Connectors help you to build your AssemblyLine. Each one is designed to tie a specific data source to your data flow.

Note: The following connectors are deprecated and will be removed in a future version of IBM Security Directory Integrator: Generic Log Adapter (GLA) Connector, Remote Agent Controller (RAC) Connector, CCMDB Connector, Deployed Assets Connector (DPA), DIS (IT Registry) Connector.

File Management Connector

Problem::

When using the File Management Connector to access file system data, symbolic links ("shortcuts") are detected as folders and *isSymbolicLink* Input parameter is false.

Resolution::

The Connector does not detect symbolic links in Windows OS. This is a limitation in the Java 1.6 virtual machine and Windows OS. This problem will be solved with new Java 7.0.4 API.

Remote Agent Controller (RAC) Connector

The following four sections explain issues with the RAC Connector.

Note: This connector is deprecated and will be removed in a future version of IBM Security Directory Integrator.

Agent controller on a non-Windows platform

Currently, the Remote Agent Controller (RAC) Connector in Iterator Mode cannot operate with a non-Windows installation of the Agent Controller. This problem is due to the instability of the Agent

Controller implementation. Any attempt to run the RAC Connector in Iterator Mode on any non-Windows operating system could cause the Agent Controller process to stop.

Slow network connection to the agent controller

If the network connection between the RAC Connector in Iterator mode and the Agent Controller is very slow, the slow network connection may have the following results:

- The Agent Controller may stop.
- The RAC connector may throw a timeout error.

No agent is registered by the RAC Connector in AddOnly mode

If the RAC Connector is run in **AddOnly** mode, but it does not register a logging agent in the local Agent Controller, it may be because the RAC cannot locate Agent Controller binaries. The AddOnly mode of the RAC Connector requires that the binaries of the Agent Controller (.dll, .so) be available for the dynamic library loader of the operating system. The preferred way to make the Agent Controller binaries available to the .dll of the operating system is to locate the binaries folder of the Agent Controller in :

- the `PATH` environment variable on Windows platforms.
- the `LD_LIBRARY_PATH` environment variable on Linux platforms.

You can point to the binaries globally or just for the process of the IBM Security Directory Integrator Server. For example:

- On Windows, modify the `PATH` environment variable from **My Computer** > **Properties** > **Advanced** > **Environment variables**
- On Linux, add lines like the following in the startup scripts (`ibmdisrv` and `ibmditk`) after the PATH definition and before the startup line:

  ```
  LD_LIBRARY_PATH=/AgentController/lib export LD_LIBRARY_PATH
  ```

Agent Controller is accessible using the LTA Eclipse tool but not by the RAC Connector in Iterator mode

The Agent Controller may be visible using the Log and Trace Analyzer Eclipse tool, but the RAC Connector in Iterator mode may report the following error:

```
Error: Unable to connect to the Agent Controller.
```

The reason for this error could be that the Agent Controller installation may not be a new technology Agent Controller. Releases of new technology Agent Controller support the new technology communication protocol. In Iterator mode, the RAC Connector uses the new technology communication protocol, but the Log and Trace analyzer uses the old communication protocol.

Assorted Connectors

This section documents the following issues:

- Axis Easy Web Service Server Connector.
- Inconsistency across Secure Socket Layer (SSL) clients.

Backlog parameter and server mode connectors: The Axis Easy Web Service Server Connector may generate exceptions if multiple clients are trying to access the server at the same time. The following exception code shows the content of the error:

```
2007-01-25 13:08:55,828 ERROR [AssemblyLine.AssemblyLines/Square_SimpleClient.753] - [EasyInvokeWebService]
  at com.ibm.di.fc.webservice.AxisEasyInvokeSoapWS.perform(Unknown Source)
  at com.ibm.di.server.FunctionComponent.callreply(Unknown Source)
  at com.ibm.di.server.AssemblyLine.msExecuteNextConnector(Unknown Source)
  at com.ibm.di.server.AssemblyLine.executeMainStep(Unknown Source)
  at com.ibm.di.server.AssemblyLine.executeMainLoop(Unknown Source)
  at com.ibm.di.server.AssemblyLine.executeMainLoop(Unknown Source)
  at com.ibm.di.server.AssemblyLine.executeAL(Unknown Source)
  at com.ibm.di.server.AssemblyLine.run(Unknown Source)
```

Cause: On initialization the AxisEasyWSServerConnector opens a server socket to accept connections from clients. In the listening state, the server socket adds each incoming client connection request to an internal queue called a *backlog*. If client requests arrive at a faster rate than the server program "accepts" them, the backlog starts filling up. Eventually the backlog fills up and newly arrived clients are refused a connection to the server.

Solution: Try increasing the value of the Connection Backlog parameter in the server mode connector. The maximum backlog size depends on the platform. For example, on Windows XP Professional the maximum limit for the backlog size is 200, so any backlog size above 200 will have no effect. Slow down the arrival of client connection requests. Use an IBM Security Directory Integrator script to introduce a time delay between clients as they start. The goal is to bring client request arrival speed below the servicing speed of the server.

Some platforms do not throw exceptions when accepting post-dated SSL server certificates

There is a potential inconsistency across Secure Socket Layer (SSL) clients running IBM Security Directory Integrator Version 7.2. IBM Security Directory Integrator components that use SSL can accept SSL server certificates whose "valid From" dates are not yet valid. Failure to issue an error could be a problem if users expect an exception to be thrown in these cases. This behavior is inconsistent across the platforms.

Cause: The JRE being used is accepting not yet "valid From" dates in certificates and is failing to warn the user of invalid certificates, therefore engaging in invalid behavior. If the client system has an earlier system date from the date of the certificate valid date, then the client should not connect to the server over SSL.

Example exception on Solaris when the issue is properly detected by the JRE:

```
javax.net.ssl.SSLHandshakeException: com.ibm.jsse2.util.h:
Certificate not valid yet
```

Note: The Solaris operating system demonstrates the desired behavior by throwing an exception when facing certificates with not yet valid "valid From" dates. By default, the IBM JRE will not throw the proper exception on any platform except Solaris. The Sun JRE will throw the proper exception on all platforms.

Solution: The Trust Manager configured in the JRE must be updated. For IBM JREs you can update the Trust Manager by doing the following:

1. Locate the line in the java.security file of the JRE that starts with the following:
   ```
   ssl.TrustManagerFactory.algorithm=
   ```
2. Modify the value to look like this if you want the JRE to validate the "valid From" dates in certificates and throw an exception when it encounters an error:
   ```
   ssl.TrustManagerFactory.algorithm=IbmX509
   ```
3. Modify the value to look like this if you want the JRE to ignore the "valid From" dates in certificates and not throw an exception:
   ```
   ssl.TrustManagerFactory.algorithm=PKIX
   ```
4. Restart the IBM Security Directory Integrator Server to enable the configuration change in the JRE.

Connectors whose libraries do not ship with IBM Security Directory Integrator

Some third-party libraries for IBM Security Directory Integrator connectors must be obtained from their proprietary sources, and do not ship with IBM Security Directory Integrator. Using the Configuration Editor, you can configure connectors. However, if a connector is missing its required library (.jar) file, the Connector in the Configuration Editor GUI looks as if it supports *all* Connector modes. For example, a Connector such as the Domino ChangeDetection Connector may support Iterator mode only, but if you configure the connector in the Configuration Editor with the required .jar file missing, it will show as supporting all other modes, such as Lookup, Update, Delete, etc. To avoid this problem, you must obtain and supply (to IBM Security Directory Integrator) the library for these connectors. The following connectors have libraries that do not ship with IBM Security Directory Integrator. Obtain the .jar files for these connectors before attempting to configure them in the Configuration Editor GUI:

IBM Security Directory Integrator Component Name	Component Internal Class Name
Domino Change Detection Connector	ibmdi.ChangeDetectionConnector
Domino Users' Connector	ibmdi.DominoUsersConnector
Lotus Notes Connector	ibmdi.Notes
SAP ALE IDoc Connector	ibmdi.SapALEIDocConnector
TAM Connector	ibmdi.TAM
Domino AdminP Connector	ibmdi.DominoAdminP
TADDM Connector	ibmdi.TADDMConnector
TADDM Change Detection Connector	ibmdi.TADDMCDConnector

For information on how to use Connectors, see the section below and the *IBM Security Directory Integrator Version 7.2 Reference Guide*.

For Domino or Lotus Notes connectors running on Linux operating systems, set PATH and LD_LIBRARY_PATH variables

Before using any of the Domino or Lotus Notes connectors, set environment variables for $PATH and for $LD_LIBRARY_PATH. Add the following two lines to the `ibmdisrv` and `ibmditk` scripts. Place the environment variable settings just before the last line of each script:

```
export PATH={notes.data.dir}:{notes.binary.dir}/notes/latest/linux/:$PATH export
LD_LIBRARY_PATH={notes.binary.dir}/notes/latest/linux/:$LD_LIBRARY_PATH
```

The `notes.data.dir` is the directory where the data for the Domino server or for the Lotus Notes client is installed. The

```
notes.binary.dir
```

is the directory where the Domino server or for the Lotus Notes client binary and executable files are installed. For example: The default directories for the Domino server on Linux platforms are:

```
{notes.data.dir} - /local/notesdata
{notes.binary.dir} - /opt/ibm/lotus
```

IBM Security Directory Integrator process privileges and Domino on Linux

The privileges of the IBM Security Directory Integrator server process are determined by the user that starts the server.

For security reasons, the Domino Server forbids execution of commands using root privileges. To run the Domino server, you must run with the user configured during the installation process, normally the Lotus Notes user. The IBM Security Directory Integrator server is required to run with the user configured during installation only when the Domino libraries enforcing this restriction are loaded. The IBM Security Directory Integrator server is able to run with root privileges only if no Domino or Lotus Notes connectors are used in an AssemblyLine.

It is possible, however, that you require both of the following privileges:

- To access a Domino server
- To execute certain tasks as root user

If you need to access a Domino server while executing certain tasks as a root user, you must:

1. The Lotus Notes user designs a single process that is responsible only for communicating with the Domino server. To achieve this single process, start the following server instances:
   a. Give one server instance root privileges `[TDIserverRoot]`
   b. Start another server instance by the Lotus Notes user `[TDIserverNotes]`
2. The `[TDIserverNotes]` requires a configuration with an AssemblyLine accessed by the `[TDIserverRoot]`. This AssemblyLine behaves as a proxy and handles the communication with the Domino server. The `[TDIserverRoot]` can use either the AssemblyLineConnector or the AssemblyLineFC to access the remote proxy AssemblyLine on the `[TDIserverNotes]`.

The `[TDIserverRoot]` could use either the AssemblyLineConnector or the AssemblyLineFC to access the remote proxy assembly line on the `[TDIserverNotes]`.

CommandLine Connector

AssemblyLine AssemblyLines/CommandLine failed with error: CreateProcess: dir error=2

If you are running Windows, and trying to execute an internal shell command (such as dir or any command listed by the command), you might have forgotten to prepend `cmd /c` . For example, the correct syntax for the `dir` command is `cmd /c dir`.

DOS-encoded output on Windows operating systems

When you use the Command Line Connector to run a program on a Windows operating system, the output from the program might be encoded using a DOS code page. This can cause unexpected results, because Windows programs usually use a Windows code page. Because a DOS code page is different from a Windows code page, it might be necessary to set the character encoding in the Command Line Connector's parser to the correct DOS code page for your region; for example: `cp850`.

JDBC Connector

Nullpointer exception while using Custom Prepared Statements

When the JDBC Connector is using a JDBC 2.0 driver (or less) for communicating with a database, there may be problems with Custom Prepared Statements. For instance, IBM solidDB® 6.5 provides only a JDBC 2.0 compliant driver. If you want to work with IBM solidDB and also enable the **Use custom SQL prepared statements** option of the Connector a `java.lang.NullPointerException` will be thrown when you try to start the AssemblyLine. The reason is that for handling custom prepared statements the JDBC Connector relies on functionality added in JDBC 3.0 and IBM solidDB driver is only JDBC 2.0 compliant. To solve this issue, use a JDBC 3.0 driver for your solution. If there is no such driver available for the needed database, as is with IBM solidDB 6.5, you will not be able to make use of the "Use custom SQL prepared statements" functionality.

COM.ibm.db2.jdbc.DB2Exception: CLI0616E Error opening socket. SQLSTATE=08S01

A server service named DB2® JDBC Applet Server must be running on the Windows system where the DB2 server is running. If The DB2 JDBC Applet Server service is not running you will get this message.

CLI0616E Error opening socket

The remote DB2 server is not configured for DB2 net driver communications. Refer to the FAQ that has more information on connecting to a DB2 server.

java.sql.SQLException: ORA-01830: date format picture ends before converting entire input string

If you are getting this when inserting or updating date-fields, you are probably passing the Oracle driver dates as a string that does not match what the driver expects. Problem Scenario: (For more detailed information about a situation where this can happen, skip to the “Suggestions” on page 30 section if not interested). You have an AssemblyLine with a JDBC Connector in AddOnly mode that writes some records to an Oracle table with a field of type DATE. Normally, you can insert something like:

```
 INSERT INTO table1 values (to_date('2005/03/01 10:05:13','YYYY/MM/DD HH:MI:SS'))
```

as part of an INSERT query. However with IBM Security Directory Integrator, you can only do something like this in the output map:

```
 ret.value = '2005/03/01 10:05:13';
```

But if Oracle fails with the following error:

```
 java.sql.SQLException: ORA-01830:
```

The **Date Format** picture ends before converting entire input string.

Suggestions: When dates are supplied as strings (which is what you are doing here) the IBM Security Directory Integrator JDBC Connector will attempt to parse the data using the pattern provided in its **Date Format** configuration parameter, as explained in the *IBM Security Directory Integrator Version 7.2 Reference Guide*. To debug your problem: What is your Data Pattern configuration? Find out how IBM Security Directory Integrator sees this field by checking in the schema tab of the Connector. A fair guess is that your JDBC driver will convert the Oracle Data type into a java.sql.TimeStamp or java.sql.Date type (and note that there are differences between java.util.Date and java.sql.Date, in terms of precision for example). In the case, for example, of a java.sql.Timestamp type, try specifying:

```
ret.value = java.sql.Timestamp(java.util.Date().getTime());
```

and see if this helps. Then you will be able to use:

```
ret.value = java.sql.Timestamp(system.parseDate(work.getString("yourDate"),
 "yyyyMMddHHmmssz").getTime());
```

If none of the above helps, run the Connector in detailed log mode and see whether the Connector is able to get the schema from the database. If not, the Connector does not use prepared statements, which makes it less efficient and more error-prone, so you'll have to make sure that the Connector's **schema** configuration parameter is set correctly.

Handling of CLOB/BLOB (Character/Binary large object)

If your attributes are of CLOB/BLOB type, the Connector does not handle them on output. On input, you can do something like this:

```
desc = conn.getObject("yourCLOBAttribute");
ret.value = desc.getSubString(1,desc.length());
```

but it is slow and clumsy. Also, it will only work if the JDBC driver actually returns a java.sql.Blob or java.sql.Clob interface object.

Disabling Prepared Statement can result in an exception for queries that exceed the maximum length value

If Prepared Statement is disabled, the JDBC connector attempts to construct a complete SQL query. If the database has a restriction on the length of the SQL query, and the query exceeds the maximum length value, an exception is thrown. This is a common problem with BLOB or binary data types.

Use ojdbc14.jar to transfer BLOB data from table to another in an Oracle database

Use ojdbc14.jar instead of using classes12.jar when using the JDBC Connector to transfer BLOB data from one table to another table in an Oracle database.

InitConnectors: com.ibm.db2.jcc.a.SqlException: The version of the IBM Universal JDBC driver in use is not licensed for connectivity to QDB2/<*OS*> databases.

To connect to this DB2 server, obtain a licensed copy of the IBM DB2 Universal Driver for JDBC and SQLJ.

Cause: IBM Security Directory Integrator Version 7.2 comes with updated Derby database (previously known as Cloudscape) and the driver needed for it. Version 7.2 also comes with a license file that is enables you to connect to Derby, but not to other DB2 databases.

Solution: As of DB2 UDB v8.1.2 the Universal JDBC driver requires a license JAR file to be in the CLASSPATH along with the db2jcc.jar file. Here are the names of the required license JAR files:

- For Cloudscape Network Server V5.1: `db2jcc_license_c.jar`
- For DB2 UDB V8 for Linux, UNIX, and Windows servers: `db2jcc_license_cu.jar`

An appropriate location for this license file to be placed in an IBM Security Directory Integrator system would be `<IBM Security Directory Integrator` *`Install Directory`*`>\_jvm\jre\lib\ext` directory.

For more information, see http://www-128.ibm.com/developerworks/db2/library/techarticle/0307zikopoulos/0307zikopoulos.html.

JNDI Connector

Problem

Excessive " com.ibm.dsml2.* " log messages may be received in the log of the AssemblyLine.

Symptom

Examples of the excessive log activity may include:

```
com.ibm.dsml2.jndi.DSML2DirContext [search] dc=HRLoad (uid=Vox) javax.naming.directory.SearchControls@2f9ad92
com.ibm.dsml2.jndi.SearchMessage [getFilter] filter: (uid=Vox)
com.ibm.dsml2.jndi.SearchMessage [getFilter] filterObject:
com.ibm.dsml2.parser.Filter@1bc52d92
com.ibm.dsml2.jndi.SearchMessage [checkResponse] reader is java.io.BufferedReader@17792d92
com.ibm.dsml2.jndi.SearchMessage [checkResponse] Starting unmarshaller thread
com.ibm.dsml2.jndi.SearchResultEnumeration Creating a search result enumeration
com.ibm.dsml2.jndi.SearchResultUnmarshaller [run] Starting unmarshal thread
com.ibm.dsml2.jndi.SearchResultUnmarshaller$ResultEnumeration [getNext] got a com.ibm.dsml2.parser.SearchResultEntry
```

Solution

To eliminate the excessive logging of the " com.ibm.dsml2.* " messages seen while using the JNDI Connector, add the following line to the **Provider Param** parameter of the JNDI Connector:

```
com.ibm.dsml2.jndi.logLevel:ERROR
```

Insufficient memory issue with Domino

When you are processing a very large amount of data in Domino server it is possible to receive errors similar to these:

- Your Domino server panics with the following error: - PANIC: Cannot attach to shared memory region, due to insufficient access (probably owned by another user or group)
- an "Insufficient memory" error is received from many tasks without any reference to a Domino pool.

Both of these errors indicate that your Domino server is running out of memory resources. The first error may occur on servers with very high process local memory usage. An example would be the HTTP server serving up large databases, port compression is enabled and there is a large population of users using the system.

In Domino the private and shared memory must reside in a limited virtual address space, which is usually 4 gigabytes. The error occurs when Domino runs out of virtual memory or out of shared memory. In order to prevent this from occurring you can use either of these two new `notes.ini` entries:

```
ConstrainedSHM=1
ConstrainedSHMSizeMB="size in megabytes"
```

The variable ConstrainedSHM=1 will restrict shared memory to a set of default sizes, as follows:

Windows and Macintosh platforms: 2 gigabytes
AIX platforms: 2.25 gigabytes
Solaris and Linux: 3 gigabytes
iSeries: 2 gigabytes

The ConstrainedSHMSizeMB="size in megabytes" will restrict memory to the "size in megabytes".

Domino User's Connector

This section explains exceptions for Domino User's Connector and provides a workaround.

java.lang.Exception: Connector Notes Thread not alive. Cannot perform.

```
at com.ibm.di.connector.dominoUsers.DominoUsersConnector.executeCommand(Unknown Source)
at com.ibm.di.connector.dominoUsers.DominoUsersConnector.initialize(Unknown Source)
at com.ibm.di.server.AssemblyLineComponent.initialize(Unknown Source)
at com.ibm.di.server.AssemblyLine.initConnectors(Unknown Source)
at com.ibm.di.server.AssemblyLine.msInitConn(Unknown Source)
at com.ibm.di.server.AssemblyLine.executeMainStep(Unknown Source)
at com.ibm.di.server.AssemblyLine.executeMainLoop(Unknown Source)
at com.ibm.di.server.AssemblyLine.executeMainLoop(Unknown Source)
at com.ibm.di.server.AssemblyLine.executeAL(Unknown Source)
at com.ibm.di.server.AssemblyLine.run(Unknown Source)
```

Cause: The exception can be caused by a wrong directory or misspelling in the LD_LIBRARY_PATH set within the "ibmditk" or "ibmdisrv" startup files.

For example, `LD_LIBRARY_PATH=/opt/lotus/notes/latest/linux`.

Solution: Add the following two lines to the shell script ("ibmditk" or "ibmdisrv") after the PATH definition and before the startup line:

```
LD_LIBRARY_PATH=<Domino Binary>
export LD_LIBRARY_PATH
```

where *<Domino Binary>* is the location of the Domino Binary folder.

Example file: ibmdisrv.sh

```
#! /bin/sh
# start up script for Directory Integrator v6.1 for Unix platforms
JRE_PATH=_jvm/bin
OS=`uname`
if [ $OS = "Linux" -o $OS = "AIX" ];then
JRE_PATH=_jvm/jre/bin
fi

PATH="/opt/IBM/ISecurity Directory Integrator 61/$JRE_PATH:$PATH:
     /opt/lotus/notes/latest/linux:/local/notesdata:"
export PATH

LD_LIBRARY_PATH=/opt/lotus/notes/latest/linux:
export LD_LIBRARY_PATH

#
# Only set Security Directory Integrator_SOLDIR if it hasn't been set already in caller's shell
#
if [ -z "$Security Directory Integrator_SOLDIR" ]; then
Security Directory Integrator_SOLDIR="."
fi

#
# -s overrides Security Directory Integrator_SOLDIR env
```

```
#
solnext=0
for s
do
case $s in
-s) solnext=1;;
-s*) Security Directory Integrator_SOLDIR="`echo $s | cut -c3-`";;
-*) solnext=0;;
*) if [ $solnext -eq 1 ]; then
Security Directory Integrator_SOLDIR=$s
solnext=0
fi;;
esac
done

if [ -n "$Security Directory Integrator_SOLDIR" ]; then
cd "$Security Directory Integrator_SOLDIR"
fi

# Check solution directory files
if [ ! -f IDILoader.jar -a ! -f log4j.properties ]; then
echo Copying log4j.properties to solution directory
cp -f "/opt/IBM/ISecurity Directory Integrator61/log4j.properties" log4j.properties
fi

"/opt/IBM/ISecurity Directory Integrator61/$JRE_PATH/java" -Dos.name=Linux
     -Djava.library.path=$PATH \
     "-Dlog4j.configuration=file:log4j.properties"
     -jar "/opt/IBM/ISecurity Directory Integrator61/IDILoader.jar" \
com.ibm.di.server.RS "$@"
```

For more information, see: IBM Security Directory Integrator: Post Release 6.0 Issue.

Windows Users and Groups Connector

java.lang.UnsatisfiedLinkError: can't find library NTMetaData (libNTMetaData.so)

This error occurs when you attempt to use the Windows Users and Groups Connector on a non-Windows platform. The Windows Users and Groups Connector is supported on Windows platforms only.

SAP Connection Suite

JCO.classInitialize(): Could not load middleware layer

After installation of the sapjco 2.1.7 SAP interface library, connections still fail. When the connector establishes a connection to the R/3 system, you get the following exception:

```
JCO.classInitialize(): Could not load middleware layer 'com.sap.mw.jco.rfc.MiddlewareRFC'JCO.nativeInit()
```

Cause: You are unable to start 32-bit programs from SAP Release 6.40 (or higher) because Microsoft runtime DLLs are missing (MSCVR71.dll and MSCVP71.dll).

Solution: For more information, see SAP Note 684106 for a procedure to fix this problem.

Function Components

Function Components are modeless components that facilitate wrapping of custom logic and external methods. Function Components are not data-source specific.

Currently there is no troubleshooting information about specific Function Components.

Parsers

Parsers are used in conjunction with a transport Connector to interpret or generate the content that travels over the Connector's byte stream.

LDIF Parser

Performance degradation

The IBM Security Directory Integrator Version 7.2 LDIF Parser shows some performance degradation in terms of execution time compared to the IBM Security Directory Integrator 6.0 LDIF Parser.

This is due to underlying JVM changes in IBM Security Directory Integrator Version 7.2, in which certain APIs experience a performance drop when working with very large data sets.

The degradation is dependent on various considerations such as hardware, RAM, processor speed, and disk input/output.

Chapter 8. Password Synchronization plug-ins

This chapter contains problem determination information regarding the IBM Security Directory Integrator Version 7.2 Password Synchronization plug-ins. For general information about the plug-ins, see *IBM Security Directory Integrator Version 7.2 Password Synchronization Plug-ins Guide*.

Problem with ICU4J on Windows when automatic daylight saving changes are disabled

The problem is manifested by the following exception in the log of the Java Proxy and/or the log of the Domino server:

```
java.lang.NullPointerException
 at com.ibm.icu.util.TimeZone.getDefault(TimeZone.java:700)
 at com.ibm.icu.util.Calendar.getInstance(Calendar.java:1613)
 at com.ibm.icu.text.DateFormat.get(DateFormat.java:942)
 at com.ibm.icu.text.DateFormat.getDateTimeInstance(DateFormat.java:736)
 at com.ibm.di.plugin.log.PWSyncLog.<init>(PWSyncLog.java:49)
```

To fix the problem open the `lib/ext` folder of the Domino server's JVM (for example, `C:\Program Files\IBM\Lotus\Domino\jvm\lib\ext`) and locate the ICU4J jars (there should be two of them – the original one of the Domino server and the one from the Domino Password Synchronizer). Remove the one named "icu4j.jar and restart the Domino server.

Some versions of the Domino server (8.0 and 8.5) ship with ICU4J version 3.4.5 (the "icu4j.jar" file in the "lib/ext" folder of the JVM). This version of ICU4J exibits problems on Windows when the "Automatically adjust clock for daylight saving changes" option is unchecked (**Control Panel -> Date and Time -> Time Zone**). More precisely, problems are observed when a non-zero DWORD value named "DisableAutoDaylightTimeSet" (before Windows Vista) or "DynamicDaylightTimeDisabled" (Windows Vista) exists under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation` in the Windows registry. The Domino Password Synchronizer ships with a newer version of the ICU4J library that does not have the same problem. To fix the issue, remove the original Domino ICU4J library and use the one from the Domino Password Synchronizer.

Chapter 9. Known limitations and general troubleshooting

This chapter contains miscellaneous problem determination information.

Known limitations

Troubleshoot problems with Delta Features and solidDB

Problem:

When using IBM solidDB as the default IBM Security Directory Integrator System Store the following error may be encountered:

```
CTGDIS810E handleException - cannot handle exception , get java.sql.SQLException:
[Solid JDBC 06.30.0029] SOLID Database Error 16503: Serializable isolation level
is not supported in M-tables.
```

This exception is thrown because the in-memory tables in IBM solidDB do not support the default isolation level set in the Delta settings. You can find more information about this at http://publib.boulder.ibm.com/infocenter/soliddb/v6r3/index.jsp?topic=/com.ibm.swg.im.soliddb.admin.doc/doc/choosing.transaction.isolation.levels.html.

Solution:

Possible workarounds are:

- Set "Row Locking" parameter in the Delta tab to "Repeatable Read", or
- Configure IBM solidDB to use disk-based tables.

Cannot start another queue manager for JMS

Problem:

If you start two IBM Security Directory Integrator Server instances using the same solution directory, with the default system queue, you may get this message from JMS:

```
javax.jms.JMSException: Cannot start a queue manager for JMS
   at com.ibm.mqe.jms.MQeConnectionFactory.startQueueManager(DashoA8173)
   at com.ibm.mqe.jms.MQeConnectionFactory.getQueueManager(DashoA8173)
   at com.ibm.mqe.jms.MQeConnectionFactory.startConnection(DashoA8173)
   at com.ibm.mqe.jms.MQeQueueConnectionFactory.createQueueConnection(DashoA8173)
   at com.ibm.mqe.jms.MQeQueueConnectionFactory.createQueueConnection(DashoA8173)
   at com.ibm.di.systemqueue.SystemQueue.<init>(SystemQueue.java:155)
   at com.ibm.di.systemqueue.SystemQueueEngine.initSystemQueue
   (SystemQueueEngine.java:158)
   at com.ibm.di.systemqueue.SystemQueueEngine.getInstance
   (SystemQueueEngine.java:119)
   at com.ibm.di.server.RS.initializeSystemQueue(RS.java:681)
...
```

IBM WebSphere MQ Everyplace® allows only once instance of a queue manager in one JVM, see http://publib.boulder.ibm.com/infocenter/iwedhelp/v6r0/index.jsp?topic=/com.ibm.mqe.doc/ovr51440.html.

The first IBM Security Directory Integrator Server/JVM will use the MQePWStore directory in the Solution Directory as its base directory.

Any subsequent IBM Security Directory Integrator Server that is started with the same Solution Directory will have a separate JVM, and could potentially have it's own IBM WebSphere MQ Everyplace. However, since it's using the same Solution Directory as the first JVM it doesn't have rights to that MQePWStore directory and hence the exception is thrown.

Solution:

Use different Solution Directories for your IBM Security Directory Integrator Servers, or use a different Queue Manager like IBM MQSeries®.

Regular Expression support in the IBM Java Script engine shipped with IBM Security Directory Integrator Version 7.2

Problem

IBM Security Directory Integrator Version 7.2 ships with the IBM Java Script Engine. The IBM Java Script Engine utilizes the regular express library shipped with Java 7.0.4 (`java.util.regex.Pattern`). This library is not fully compliant with the ECMA-262 specification regarding regular expressions.

Solution

IBM Security Directory Integrator does not claim support for the ECMA-262 specification with regards to regular expressions. See the following URL to get details on the behavior and proper usage of the particular regular expression library that the IBM Java Script Engine uses: http://docs.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html.

Launchpad exit confirmation window title bar displays incorrectly in Firefox browser

When you start **Launchpad**, one of the options in the left navigation area is **Exit**. When you click **Exit**, a confirmation dialog box appears, giving the options **OK** and **Cancel**. The title bar of the confirmation window should display IBM Security Directory Integrator Install Launchpad. Firefox browsers incorrectly display the following string in the **Exit** confirmation window: `Javascript Application`.

This is a current limitation of Mozilla Firefox browsers. The problem may be fixed in future versions of IBM Security Directory Integrator or Firefox browsers.

SSL connects with expired self signed certificates

The TrustManager shipped with IBM Java Runtime Environment (JRE) 7.0.4 verifies a certificate chain up to the trusted certificate; it does not verify the trusted certificate itself. If the self-signed certificate is the trusted certificate, CERTPATH will not examine it to see whether the certificate is expired. Because CERTPATH does not check for self-signed certificate expiration, an SSL connection can be established with an expired certificate.

The TrustManager shipped with IBM JRE 1.4.2 verifies the entire certificate chain up to and including the trusted certificate. As a result, if an expired certificate is encountered, an exception is thrown. If you are using IBM JRE 1.6.0, but want to revert to 1.4.2 behavior regarding expired certificates, make the following changes:

In the java.security file of the Client JVM, change the following entry:

```
ssl.KeyManagerFactory.algorithm=IbmX509
ssl.TrustManagerFactory.algorithm=PKIX
```

to

```
ssl.KeyManagerFactory.algorithm=IbmX509
ssl.TrustManagerFactory.algorithm=IbmX509
```

If the SSL Client-Auth value is set to True, make the same change in the Server JVM's java.security file.

Programmatically disabling components

To disable components you will need to use the Initial Work Entry (IWE) to pass a control flag. If your AssemblyLine has an Iterator, store the value in a script variable and zero out the Work Entry; otherwise the Iterator will not engage on the first cycle.

For example, to disable a branch, you can use a script like this:

```
var branchEnabled = work.getString( "enableBranch" );     task.setWork( null );
```

Then set your Branch to "Match All" and include a scripted condition like this:

```
 ret.value = branchEnabled.equals( "yes" );
```

If you intend to use IWE, you must use an extra attribute that you must clear out before continuing.

Disabling connectors is difficult and requires modifying the Config object before starting the AssemblyLine. If the connector is not disabled before you start the AssemblyLine, it will be initialized even if you disable it in the prolog before initialization. Modifying the in-memory Config object is possible, but not advised. An alternative is to set your connector to passive, but this will not help if you are trying to avoid an initialization completely.

Specifying multiple Configs to the ibmdisrv command

The `-c` switch does not work with multiple filenames.

Cause

The `-c` switch has been designed so that a single configuration filename can be passed to the `ibmdisrv` command. If you do not specify the `-d` switch, only one configuration file is allowed.

Solution

ibmdisrv cannot be used to specify the AssemblyLines, using the `-r` switch, when the `-c` (config file) option specifies multiple Configs. Because the `-r` option is not operative while loading multiple Configs, you have to use either the autostart option or use `-d` and start the AssemblyLine using the Administration and Monitoring Console Interface.

Example:

With the AssemblyLines in the autostart folder, use this command to start multiple configs and AssemblyLines using **ibmdisrv**. You must specify the autostart option for the corresponding AssemblyLines.

```
ibmdisrv -d -c C1.xml,C2.xml
```

You can also start AssemblyLines on a running server other than the Administration and Monitoring Console using the **tdisrvctl** command in the `bin` folder.

Problems with starting the IBM Security Directory Integrator Server

You can not start the IBM Security Directory Integratorhey Server if invalid characters are used in the installation directory path. Use only the following supported special characters in the path.

Special character	Description
-	Dash
)	Closing parenthesis
_	Underscore
.	Period

Special character	Description
`	Grave accent
{	Opening brace
}	Closing brace
[	Opening bracket
]	Closing bracket

Problems when migrating previous versions of IBM Security Directory Integrator to Version 7.2

Problem

Server fails to start after migrating IBM Security Directory Integrator from previous versions to Version 7.2 with the following error message:

```
CTGDIS210W An error has occurred on Server API initialization: com.ibm.di.api.DIException:
CTGDKD004E Could not create RMI custom socket factories.
Exception occurred: {0} : Keystore was tampered with, or password was incorrect.
com.ibm.di.api.DIException: CTGDKD004E could not create RMI custom socket factories.
Exception occurred: {0} : Keystore was tampered with, or password was incorrect.
```

Solution

Refer to the “Maintaining encryption artifacts – keys, certificates, keystores, encrypted files” section of *IBM Security Directory Integrator Version 7.2 Installation and Administrator Guide* for details.

General troubleshooting

The following sections describe general problems and solutions in IBM Security Directory Integrator:

Certain scripted utilities must be invoked in specific way

On Linux/UNIX systems, a number of utilities in the *TDI_install_dir*/bin directory must be invoked in a specific way due to scripting limitations. For example, a given utility script like tdiVerifyInstall.sh can be invoked as follows (assuming you are in the TDI_install_dir/bin directory):

```
./tdiVerifyInstall.sh
or
sh ./tdiVerifyInstall.sh
or
sh <absolute path>/tdiVerifyInstall.sh
or
tdiVerifyInstall.sh
or
sh tdiVerifyInstall.sh
```

The latter two invocations may yield an error like the following output shows:

```
which: no tdiVerifyInstall.sh in (/sbin:/usr/sbin:/usr/local/sbin:
/root/bin:/usr/local/bin:/usr/bin:/bin:/usr/bin/X11:
/usr/X11R6/bin:/usr/games:/usr/lib/mit/bin:/usr/lib/mit/sbin)
dirname: missing operand
Try `dirname --help' for more information.
```

This is because the script fails to determine the absolute path of itself if invoked in those ways. Use one of the three first invocation ways instead.

System Store database might get corrupted when shutting down an AssemblyLine that uses Derby in embedded mode

When the configuration instance of an AssemblyLine is terminated on demand, this may cause corruption of the Derby database (applies only to Derby in embedded mode).

If that happens, on subsequent runs the Server may report an error with the System Store like: "java.sql.SQLException: Directory C:\tdi\TDISysStore already exists.".

A configuration instance is terminated on demand when:

- `shutdownServer()` method is invoked on the config instance that contains the AssemblyLine (e.g. call "main.shutdownServer()" in a script inside the AssemblyLine)
- `stop()` method is invoked using the ConfigInstance Server API interface, while an AssemblyLine from that configuration instance is still running.

To avoid the problem, either do not use termination on demand or do not use Derby in embedded mode.

Cannot connect to IBM Security Directory Integrator server from a remote machine even though the IBM Security Directory Integrator server says the server API has started

This a problem that can occur on certain platforms. It all depends on how the platform resolves a hostname to an IP address when the hostname is represented by several IP addresses in the hosts file (or whatever mechanism is used to resolve hostnames). In order to troubleshoot the problem, check the following items:

1. Verify basic network connectivity

   First you should verify that there is a connection between the Config Editor (CE) workstation and the IBM Security Directory Integrator server machine. Use `ping` *`ip-address`* to see if there is a path to the server where the IBM Security Directory Integrator server runs. If the ping command fails, it could be that the firewall on the remote server has blocked this service.
2. Check firewalls

   Second, you should check the remote machine (or path to it) to see if it blocks access to ports used by the IBM Security Directory Integrator server.
3. Check RMI and multiple `/etc/hosts` entries

   The error message in the CE will indicate a connection failure to an IP address that does not match the IP address you specified in the server document.

   One reason for this may be that there are multiple entries in the `/etc/hosts` file on the IBM Security Directory Integrator server side and one of them is inaccessible from the CE workstation.

   On SLES 11 you will typically find an additional entry in the hosts file for the servers hostname (127.0.0.2 <hostname>). In the CE, if you see that it cannot connect to "127.0.0.*" this is an indication that this is the case. You can either remove this entry or tell IBM Security Directory Integrator specifically which IP address to use for the server API.

   If you choose the latter, then before starting "ibmdisrv" edit the script and modify the line that starts the server:

   ```
   "$TDI_JAVA_PROGRAM" -Djava.rmi.server.hostname=<ip-address>  $TDI_MIXEDMODE_FLAG
    -cp "$TDI_HOME_DIR/IDILoader.jar" "$LOG_4J" com.ibm.di.loader.IDILoader com.ibm.di.server.RS "$@"
   ```

   The <ip-address> should be replaced with the proper IP address for the server where the IBM Security Directory Integrator server runs. This is also the IP address you use in your server document connection string.

OutOfMemoryError thrown when an AL in manual mode makes huge number of attempts to initialize

Problem Description:

This problem is seen when your solution meets the following conditions:

- You have a configuration in which one AL is repeatedly started in manual mode.
- That AL have a connector that is not able to initialize normally due to some network related problem or a 3-rd party system failure.
- Your solution tries to make a great number of attempts to restart the AL in manual mode (the number depends on the amount of memory the JVM is allowed to occupy) and the 3-rd party system still fails on each attempt.

Test observations:

On a machine with 3 GB of system memory the AL had failed to initialize more than 30000 times before this could be seen.

Possible solution:

This only affects ALs failing to initialize when started in Manual Mode. If your solution allows it, start the AL in Normal Mode instead and wait for it to complete, otherwise please contact technical support.

java.lang.OutOfMemoryError exception when running an AssemblyLine with memory-intensive jobs

Problem:

The system runs out of memory when an AssemblyLine with memory-intensive jobs is running on the IBM Security Directory Integrator Server.

Solution:

Increase the heap size of Java Virtual Machine to resolve this problem. To increase the heap size, include `-Xms` and `–Xmx` options in the `ibmdisrv` script file. For example, to set the minimum heap memory size to 254 bytes and maximum heap memory size to 1024 bytes, change the following line in the script:

```
"$TDI_JAVA_PROGRAM" $TDI_MIXEDMODE_FLAG -cp
"$TDI_HOME_DIR/IDILoader.jar" "$LOG_4J"
com.ibm.di.loader.ServerLauncher "$@" &
```

change the script as shown:

```
"$TDI_JAVA_PROGRAM" $TDI_MIXEDMODE_FLAG -cp
"$TDI_HOME_DIR/IDILoader.jar" "$LOG_4J" -Xms254m -Xmx1024m
com.ibm.di.loader.ServerLauncher "$@" &
```

Remote Command Line Function Component can execute shell scripts remotely only if there are no carriage returns in the shell script

You can use the Remote Command Line Function Component to execute shell scripts remotely (limited to the capabilites of the shell), but do not insert carriage returns into your shell script. Perform these steps:

1. Enter target system details such as:
   - Hostname
   - Remote user

- Password

2. Enter the command /bin/sh.

   Note: Any shell script with a carriage return will not execute successfully. Avoid carriage returns in shell scripts.

3. Provide the local stdin source file as, for example, test.sh, where test.sh is the shell script, to be executed remotely, that is stored on the local system.

java.io.IOException: The pipe has been ended

You can find the following message: `The java class is not found: Files\IBM\Security Directory Integrator\V6.1\IDILoader.jar com.ibm.di.server.RS - r AssemblyLines.allied -S C:\Documents` in either the:

- IBM Security Directory Integrator Configuration Editor AssemblyLine output.
- ibmdisrv server log *Security Directory Integrator Installation*\logs\ibmdi.log.

Cause

This is a problem with the PATH variable that IBM Security Directory Integrator references from the OS. IBM Security Directory Integrator sets the PATH variable in both the ibmditk.bat and ibmdisrv.bat, and ends the assignment with the system path - %PATH%. If your system path ends with a "\", it will cause this error to occur.

Solution

The reason the PATH variable is misbehaving is because the last entry might have the PATH variable ending with a "\" , instead of ";".

Hence,

PATH=C:\SomeProgram\bin;C:\Security Directory Integrator (This is OK).
PATH=C:\SomeProgram\bin;C:\Security Directory Integrator; (This is OK).
PATH=C:\SomeProgram\bin;C:\Security Directory Integrator\; (This is OK).
PATH=C:\SomeProgram\bin;C:\Security Directory Integrator\ (This is **not** OK).

Error occurs when an encrypted password exceeds the size of the table column in which the password is stored

An error occurs when an encrypted password exceeds the size of the column where the password is stored:

```
ORA 12899 value too large for column "System".TESTPASSWD"."test1"(actual 178 , maximum 50)
```

To work around this problem, ensure that the tables used to store passwords are sufficiently large.

AssemblyLine Flow

Connector in Lookup mode with no match in a loop component causes error

Normally a connector in Lookup mode expects only one hit, and if more than one hit occurs, you are given the opportunity to remedy the situation using error Hooks **On Multiple Entries** or **On No Match**. Connectors in the Loop Component behave differently:

- **On Multiple Entry** is never called.
- **On No Match** is called only if no match is returned by the Lookup Connector.

If the Lookup Connector finds no entries, the following error occurs:

```
java.lang.Exception: [IF_MgrFound] Entry not found
```

Occasionally a crash also occurs if the exception is not caught.

To work around this error, enable the **No Entry Found** Hook without any code in it.

Advanced link criteria for a Lookup Connector in a Loop deleted when saving config

To prevent deletion of advanced link criteria, put your advanced Link Crit in a connector in your Library that you use in the Loop. Then you will inherit the Link Crit as well.

tdisrvctl not listing created tombstones when -c option specifies file name

The problem is observed for configurations that have a solution name defined. When you request tombstones for such configuration by specifying the configuration file name instead of the solution name, no tombstones are found.

When querying tombstones, you can use a configuration file name for the **-c** option only when the configuration file contains no Solution Name:

```
tdisrvctl -op tombstone -c myconfig.xml -r al
```

In all other cases you must specify a configuration instance id or you will get no results:

```
tdisrvctl -op tombstone -c myconfig -r al
```

Note that from version 7.0 the Config Editor puts a Solution Name in each configuration file by default.

Memory Leaks

Reinitialization of connectors

If you reinitialize connectors a lot, make sure to use their terminate() method before you call their initialize() method. The classic example is an AssemblyLine starting up but not able to connect to your data source. If the connector is not terminated before being initialized again, you might leak memory.

Platform specific problems

Domino User's Connector running on AIX 5.3 with Domino Server 7.0

The following issue is for the AIX operating system only.

While running the Local Server Session on AIX, the Domino User's Connector generates an error during initialization.

To avoid the error, use the Domino User's Connector on a different system and connect to the Domino server on AIX using a Local Client Session.

Chapter 10. Troubleshooting scenarios

This chapter contains some troubleshooting scenarios you might encounter and provides some solutions.

Log files not showing up or showing up after only the second run of the server

If log files are not showing up, the problem is probably that log4j.properties does not exists in the solution directory before the server is run. The log4j.properties is one of the places where (default) log-files location is configured, so you might want to check out the files content as well. For IBM Security Directory Integrator Version 7.2 this file is created by the server/ce batch-files that you start IBM Security Directory Integrator with. If you are running IBM Security Directory Integrator as a Windows service, make sure that you have followed the instructions on how to run IBM Security Directory Integrator as a Windows service.

Appendix A. Support information

This section describes the following options for obtaining support for IBM products:

- "IBM Support Assistant plug-in"
- "Searching knowledge bases" on page 50
- "Obtaining fixes" on page 51
- "Contacting IBM Software Support" on page 51

IBM Support Assistant plug-in

The IBM Support Assistant (ISA) is a free local software serviceability workbench that helps resolve questions and problems with IBM software products. It is a stand-alone application that can be installed on any workstation and then enhanced by installing plug-in modules for IBM products.

The three basic components of ISA are:

1. **Concurrent Search tool** – This searches across the bulk of IBM documentation as well as product infocenters and returns the results categorized by source for easy reviews.
2. **Product Information feature –** This has links to the product home page, support page, news groups, forums and other links relevant to the product.
3. **Service Feature** - This consists of a data collection tool and a problem submission tool. There are two types of data collection tools.

   The first type is the System Collector that is provided by ISA and gathers general information from your operating system, registry, and so forth.

   The second type is a product specific data collector that is driven by a control file defined by the respective product teams. Collector output file names have the format `collector_timestamp.jar`. These JARs can then be attached to a problem report.

   The problem submission tool helps in the creation and submission of problem reports. To log into the tool, called ESR (Electronic Service Request), you need the following information:

   - IBM ID
   - IBM password
   - IBM customer number
   - Country or region

IBM Support Assistant can be downloaded from http://www-306.ibm.com/software/support/isa/.

A useful demo on ISA and its features can be found at http://publib.boulder.ibm.com/infocenter/ieduasst/v1r1m0/index.jsp.

Detailed information for developers can be obtained from https://wst.austin.ibm.com/isahome/dev_corner.html.

The IBM Security Directory Integrator version of the Plug-in gathers the following info from the IBM Security Directory Integrator Installation (and Solution Directory, if defined):

1. Logs from the *TDI_install_dir*/logs folder – ibmdi.log and tdisrvctl.log
2. For IBM Security Directory Integrator versions prior to v7.0, all property, XML and rules files from the *TDI_install_dir*/etc folder:

   build.properties
   ce-log4j.properties

CSServersInfo.xml
derby.properties
executetask.properties
global.properties
jlog.properties
log4j.properties
reconnect.rules
tdisrvctl-log4j.properties

3. From IBM Security Directory Integrator v7.0 onwards various issues will be categorized. You will have the option to select a category and only the log files pertaining to that category will be collected. The following categories are available:
   - IBM Security Directory Integrator Server Related Issues.
   - AMC Related Issues.
   - IBM Security Directory Integrator Install Related Issues.
   - IBM Security Directory Integrator Config editor Related Issues.
   - IBM Security Directory Integrator Plug-in Related Issues.

   You have the option to select anyone of these issues and start collecting files by clicking the **Collect** button. After selecting the type of issue, you are prompted to specify appropriate directory paths to collect various log files. The default IBM Security Directory Integrator installation folders (on Windows/Linux/UNIX) are supplied by default for convenience.

   Also, a PMR number should be specified and the output .zip file with the collected info will be placed in the installation directory specified, with the following name:

   ```
   ISA_[Type]_PMR#[Number].zip
   ```

   where [Type] can be Server/AMC/Install/CE/Plugins and [Number] is the PMR number specified (none if left empty).

   Details about the files being collected are as follows:

   IBM Security Directory Integrator Server Related Issues

   You will be prompted to provide the IBM Security Directory Integrator installation directory as well as a solution directory (leave blank if you do not want to specify solution folder)) and a PMR number. Also, the following note prompts the user to turn his log level to DEBUG if his problem is easily re-creatable:

   Note: If your problem is easily re-creatable and you use the default Log4J logging it is best if you set your logging root category to DEBUG in `etc\log4j.properties` and enable detailed log for your problematic components. Then you should re-run your scenario and come back to this dialog to collect the logs with detailed information for your problem.

   The following files are collected:

   a. ibmditk.bat(.sh)
   b. ibmdisrv.bat(.sh)
   c. derby.log
   d. ibmdiservice.props
   e. `*TDI_install_dir*/etc/*.properties`
   f. `*TDI_install_dir*/etc/*.properties/*.xml`
   g. `*TDI_install_dir*/etc/*.properties/reconnect.rules`
   h. `*TDI_install_dir*/system_logs/*.log`
   i. `*TDI_install_dir*\win32_service\*.properties` (on Windows)
   j. List of all .jar files
   k. Component version information
   l. Host, memory, and list of started services.

AMC related issues

The following files are collected:

a. amc.properties
b. am_config.properties
c. am_logging.properties
d. tdimigam-log4j.properties
e. All files inside the *TDI_install_dir*\lwi\runtime\isc\eclipse\plugins\AMC_7.1.1.0\WEB-INF folder.
f. All the log files inside the *TDI_install_dir*\bin\amc\ActionManager\logs folder.
g. All properties files inside the *TDI_install_dir*\bin\amc folder
h. All properties files inside the *TDI_install_dir*\lwi\runtime\isc\eclipse\plugins\AMC_7.1.1.0\WEB-INF\classes folder

Note: The AMC feature is deprecated and will be removed in a future version of IBM Security Directory Integrator.

Install related issues

You will be prompted to provide the temp directory on the machine that the installer has used to store the collected files (for example, corresponding to the TEMP environment variable on Windows) as well as the IBM Security Directory Integrator installation directory, Common Solution Install directory and PMR Number.

The following files are collected:

a. *temp*/sdiv72install.log
b. *temp*/sdiv72uninstall.log
c. *temp*/tdiSoldir.log
d. *temp*/tdiSoldirERR.log
e. *temp*/tdiMQeCreate.log
f. *temp*/tdiMQeCreateERR.log
g. *common_solution_dir*/logs/*/si_trace.log
h. Information for installed components and fixpacks applied collected using applyUpdates.bat(.sh) script and saved in *TDI_install_dir*/TDIUpdateInstaller.txt

Config editor related issues

You will be prompted to provide the IBM Security Directory Integrator installation directory and PMR number.

The following files are collected:

a. *TDI_install_dir*/ibmditk.bat(sh)
b. *TDI_install_dir*/ce/eclipsece/configuration/config.ini
c. *workspace*/.metadata/*.log

IBM Security Directory Integrator Plugin Related Issues

You will need to specify the plugins installation directory (which normally is *TDI_install_dir*/pwd_plugins) and PMR number, and for each of the following plugins the files mentioned below them will be collected.

Domino Plug-in

a. *TDI_install_dir*\pwd_plugins\domino\*.props
b. *TDI_install_dir*\pwd_plugins\domino\*.log

PAM Plug-in

a. *TDI_install_dir*\pwd_plugins\pam\*.props

   b. *TDI_install_dir*\pwd_plugins\pam *.log

SunOne Plug-in

   a. *TDI_install_dir*\pwd_plugins\sun\*.props
   b. *TDI_install_dir*\pwd_plugins\sun *.log

IBM Security Directory Server Plug-in

   a. *TDI_install_dir*\pwd_plugins\tds\*.props
   b. *TDI_install_dir*\pwd_plugins\tds *.log

Windows Plug-in

   a. *TDI_install_dir*\pwd_plugins\windows\*.props
   b. *TDI_install_dir*\pwd_plugins\windows *.log
   c. *TDI_install_dir*\pwd_plugins\windows *.reg

4. A list of all jars present in the `TDI_install_dir/jars` folder
5. Versions of all IBM Security Directory Integrator components
6. If you have selected AMC related issues – amc.property files, all files in the WEB-INF folder and amc logs will be collected
7. If the Solution Directory is different from the *TDI_install_dir*, then along with solution.properties all logs and property files as mentioned above are collected from the solution directory

The IBM Security Directory Integrator version of the ISA plugin has been instrumented with the proper access information in order to support the process of sending the collected files through HTTP or FTP.

IBM Support Assistant for IBM Security Directory Integrator

These are the steps to use IBM Support Assistant to generate problem records for IBM Security Directory Integrator:

1. Download ISA version 4.0, from http://www-306.ibm.com/software/support/isa/.
2. Open ISA, select the **Updater** tab and then select the **New Products and Tools** tab.
3. Select IBM Security Directory Integrator Version 7.2 from the available plug-ins list and install.
4. Restart ISA to start using the tool for IBM Security Directory Integrator.
5. Or alternatively, if the plug-in and features folder are available then drop the plug-in (com.ibm.esupport.client.product.SSCQGF71_4.0.0.20080815) into the plugin and feature (com.ibm.esupport.client.product.SSCQGF71.feature_4.0.0.00) into features folder of ISA and restart ISA.

Searching knowledge bases

If you have a problem with your IBM software, you want it resolved quickly. Begin by searching the available knowledge bases to determine whether the resolution to your problem is already documented.

Search the product documentation on your local system or network

IBM provides extensive documentation that can be installed on your local computer or on an intranet server. You can use the search function of this product documentation to query conceptual information, instructions for completing tasks, reference information, and support documents.

Search the Internet

If you cannot find an answer to your question in the product documentation, search the Internet for the latest, most complete information that might help you resolve your problem. To search multiple Internet resources for your product, expand the product folder in the navigation frame to the left and select **Web search**. From this topic, you can search a variety of resources including:

- IBM technotes

- IBM downloads
- IBM Redbooks®
- IBM developerWorks®
- Forums and newsgroups
- Google

Obtaining fixes

A product fix might be available to resolve your problem. You can determine what fixes are available for your IBM software product by checking the product support Web site:

1. Go to the IBM Software Support Web site (http://www.ibm.com/software/support).
2. Under **Products A - Z**, select your product name. This opens a product-specific support site.
3. Under **Self help**, follow the link to **All Updates**, where you will find a list of fixes, fix packs, and other service updates for your product. For tips on refining your search, click **Search tips**.
4. Select the name of a fix to read the description and optionally download the fix.

To receive weekly e-mail notifications about fixes and other news about IBM products, follow these steps:

1. From the support page for any IBM product, click **My support** in the upper-right corner of the page.
2. If you have already registered, skip to the next step. If you have not registered, click register in the upper-right corner of the support page to establish your user ID and password.
3. Sign in to **My support**.
4. On the My support page, click **Edit profiles** in the left navigation pane, and scroll to **Select Mail Preferences**. Select a product family and check the appropriate boxes for the type of information you want.
5. Click **Submit**.
6. For e-mail notification for other products, repeat Steps 4 and 5.

For more information about types of fixes, see the *Software Support Handbook* (http://techsupport.services.ibm.com/guides/handbook.html).

Contacting IBM Software Support

IBM Software Support provides assistance with product defects.

Before contacting IBM Software Support, your company must have an active IBM software maintenance contract, and you must be authorized to submit problems to IBM. The type of software maintenance contract that you need depends on the type of product you have:

- For IBM distributed software products (including, but not limited to, Tivoli®, Lotus®, and Rational® products, as well as DB2 and WebSphere products that run on Windows or UNIX operating systems), enroll in Passport Advantage® in one of the following ways:
  - **Online**: Go to the Passport Advantage Web page (http://www.lotus.com/services/passport.nsf/WebDocs/ Passport_Advantage_Home) and click **How to Enroll**
  - **By phone**: For the phone number to call in your country, go to the IBM Software Support Web site (http://techsupport.services.ibm.com/guides/contacts.html) and select the name of your geographic region.
- For IBM eServer™ software products (including, but not limited to, DB2 and WebSphere products that run in zSeries, pSeries, and iSeries® environments), you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for eServer software products, go to the IBM Technical Support Advantage Web page (http://www.ibm.com/servers/eserver/techsupport.html).

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States or, from other countries, go to the contacts page of the IBM Software Support Handbook on the Web (http://techsupport.services.ibm.com/guides/contacts.html) and select the name of your geographic region for phone numbers of people who provide support for your location.

Follow the steps in this topic to contact IBM Software Support:

1. Determine the business impact of your problem.
2. Describe your problem and gather background information.
3. Submit your problem to IBM Software Support.

Determine the business impact of your problem

When you report a problem to IBM, you are asked to supply a severity level. Therefore, you need to understand and assess the business impact of the problem you are reporting. Use the following criteria:

Severity 1	**Critical** business impact: You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.
Severity 2	**Significant** business impact: The program is usable but is severely limited.
Severity 3	**Some** business impact: The program is usable with less significant features (not critical to operations) unavailable.
Severity 4	**Minimal** business impact: The problem causes little impact on operations, or a reasonable circumvention to the problem has been implemented.

Describe your problem and gather background information

When explaining a problem to IBM, be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently. To save time, know the answers to these questions:

- What software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can the problem be re-created? If so, what steps led to the failure?
- Have any changes been made to the system? (For example, hardware, operating system, networking software, and so on.)
- Are you currently using a workaround for this problem? If so, be prepared to explain it when you report the problem.

Submit your problem to IBM Software Support

You can submit your problem in one of two ways:

- **Online**: Go to the "Submit and track problems" page on the IBM Software Support site (http://www.ibm.com/software/support/probsub.html). Enter your information into the appropriate problem submission tool.
- **By phone**: For the phone number to call in your country, go to the contacts page of the IBM Software Support Handbook on the Web (techsupport.services.ibm.com/guides/contacts.html) and select the name of your geographic region.

If the problem you submit is for a software defect or for missing or inaccurate documentation, IBM Software Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Software Support provides a workaround for you to implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM product support Web pages daily, so that other users who experience the same problem can benefit from the same resolutions.

For more information about problem resolution, see Searching knowledge bases and Obtaining fixes.

Appendix B. 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 character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, 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 might 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
2Z4A/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 document 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 measurement 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.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds 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.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

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

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Index

Product Number: 5724-K74

Printed in USA

GC27-2709-02