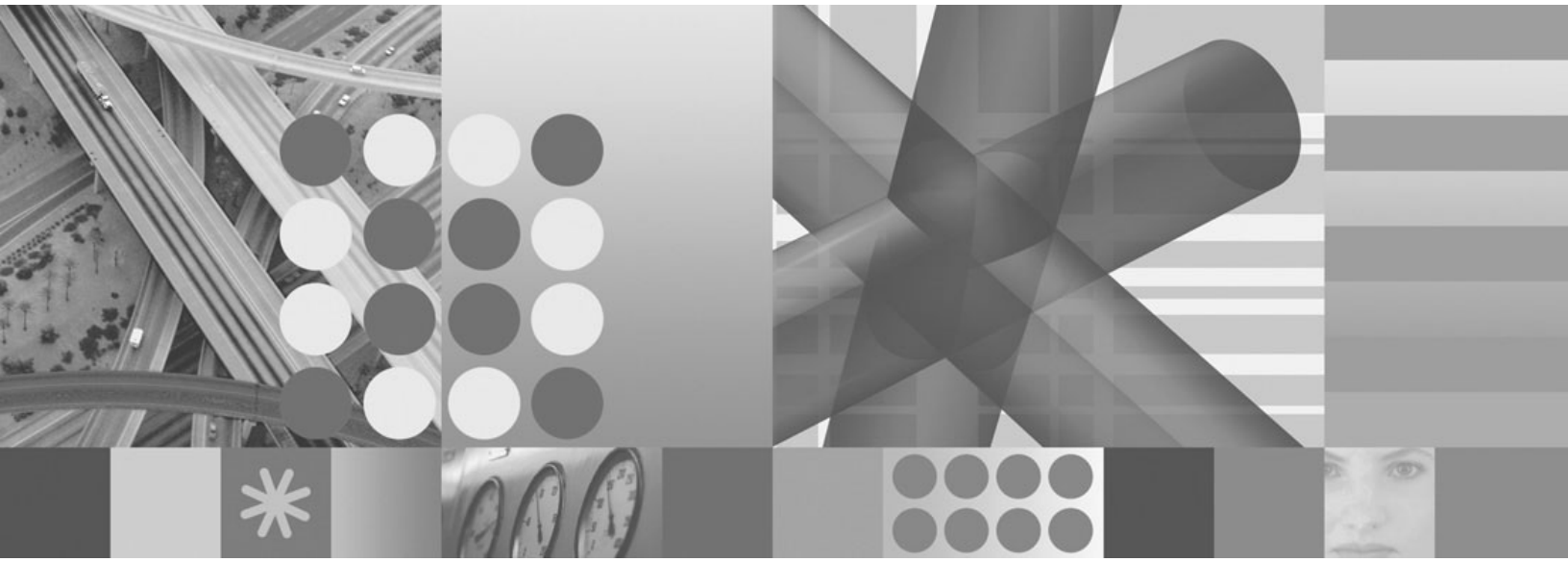
Tivoli® Composite Application Manager for SOA V6.1.0

Fix Pack 1 Readme

Tivoli® Composite Application Manager for SOA V6.1.0



Fix Pack 1 Readme

Note

Before using this information and the product it supports, read the information in “Notices,” on page 55.

This edition applies to version 6, release 1, modification 0 of IBM Tivoli Composite Application Manager for SOA (product number 5724-M07 for the distributed version, and 5698-A77 for the Enterprise version) and to all subsequent releases and modifications until otherwise indicated in new editions.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Chapter 1. Overview

IBM® Tivoli® Composite Application Manager for SOA, Version 6.1.0 (ITCAM for SOA v6.1.0) provides monitoring and management of services in a Service Oriented Architecture (SOA) environment. ITCAM for SOA v6.1.0 monitors a wide variety of metrics on a large number of application server runtime environments, and provides some management of mediations in WebSphere® Enterprise Service Bus (WESB).

Fix Pack 1 provides a Java™ patch for Daylight Saving Time, and includes additional new function, made available for v6.1.0 after the General Availability (GA) date for that release. This post-GA function is automatically installed when you install the fix pack, but you must perform additional steps to enable the function in your ITCAM for SOA v6.1.0 environment if you choose to use it.

The additional post-GA function provided in this fix pack continues IBM's commitment to expand management support for the SOA environment, building on the current version 6.1.0 function with support for additional application server runtime environments, limited support for one new operating system platform, new workspaces, views, Take Action commands, and workspace links that provide a more comprehensive visualization of monitored data, and additional management and configuration of ESB components.

This readme describes the installation of the fix pack, as well as the optional enabling, configuration, and operation of the post-GA functions included for ITCAM for SOA v6.1.0. This readme file supercedes the readme file that is included as part of the installation media, which is focused on the v6.1.0 release.

What is included in Fix Pack 1?

The following fix is added to IBM Tivoli Composite Application Manager for SOA by this fix pack:

- A Java patch for Daylight Saving Time

  The United States Energy Policy Act of 2005 changed the effective dates for the period known as Daylight Saving Time (DST) in the United States for 2007. This change altered the start and stop dates by four weeks.

  This Java patch is applied to all of the Java Virtual Machine (JVM) images provided with ITCAM for SOA v6.1.0.

This fix pack also adds the following new features and functions to the ITCAM for SOA v6.1.0 environment on a limited set of supported operating system platforms:

- Updates to the Java data collector to support the Apache Axis 1.2 SOAP engine running in a BEA WebLogic 8.1 SP5 application server runtime environment.
- Updates to the Java data collector to support the Apache Axis 1.2 SOAP engine running in a BEA WebLogic 9.2 application server runtime environment.
- Support for the Tivoli Enterprise™ Monitoring Agent (TEMA) running on an HP-UX 11i v2 Itanium®-based (64-bit) platform (support is limited to only the Axis 1.2 SOAP engine running in the BEA WebLogic 9.2 data collector application server runtime environment).
- A new data collector implementation to monitor services in an IBM WebSphere Message Broker 6.0.0.3 environment.
- The ability to collect and aggregate service metrics based on the requester that is invoking the service, for supported IBM WebSphere Application Server runtime environments.

- Updates to the Tivoli managed SCA mediation primitives to support promotion of properties in IBM WebSphere Enterprise Service Bus Version 6.0.2 and IBM WebSphere Process Server Version 6.0.2.
- The ability to register and run the IBM WebSphere DataPower® SOA Appliance (DataPower) data collector as a service on supported Microsoft® Windows® platforms.
- The ability to link workspaces from IBM WebSphere Message Broker services in ITCAM for SOA v6.1 to the corresponding message flow statistics in the OMEGAMON XE for Messaging product.

The rest of this document provides more information on installing, enabling, configuring, and using these new features and functions in the ITCAM for SOA v6.1.0 environment.

Supported operating systems

Fix Pack 1 can be installed on any operating system currently supported by IBM Tivoli Composite Application Manager for SOA V6.1.0. Other post-GA function provided in this fix pack is supported on a limited set of operating systems. See the chapters later in this publication for more information on supported operating systems for each function.

HP-UX operating system support

In addition to the upgrade support provided for operating system platforms currently supported by IBM Tivoli Composite Application Manager for SOA v6.1.0, this fix pack includes a full installation of the ITCAM for SOA v6.1.0 monitoring agent on the HP-UX 11i v2 Itanium-based (64-bit) platform for the Apache Axis data collector in the BEA WebLogic application server runtime environment. For more information, see Chapter 4, “The Axis data collector in the BEA WebLogic environment,” on page 23.

Related publications

Refer to the online IBM Tivoli Composite Application Manager for SOA V6.1.0 library for more information about the current version of the product:

`http://publib.boulder.ibm.com/tividd/td/IBMTivoliCompositeApplicationManagerforSOA6.1.html`

The IBM Tivoli Composite Application Manager for SOA v6.1 library contains the following publications:

- *IBM Tivoli Composite Application Manager for SOA Quick Start Guide*, GI11-7853
- *IBM Tivoli Composite Application Manager for SOA Release Notes*, GI11-4096
- *IBM Tivoli Composite Application Manager for SOA Installation and User's Guide*, GC32-9492
- *Configuring IBM Tivoli Composite Application Manager for SOA on z/OS®*, SC32-9493
- *Program Directory for IBM Tivoli Composite Application Manager for SOA, V6.1.0, Program Number 5698-A77, for Use with z/OS*, GI11-4100
- *IBM Tivoli Composite Application Manager for SOA Tools*, GC32-1539

You might also find the following publications useful:

- *IBM Tivoli OMEGAMON® XE for Messaging Installation Guide*
- *IBM Tivoli OMEGAMON XE for Messaging: WebSphere Message Broker Monitoring User's Guide*

- *IBM WebSphere Message Broker Configuration, Administration, and Security*

Obtaining Technote information

Click here for late-breaking technote information on issues related to this product, or refer to the IBM Software Support site at http://www.ibm.com/software/support/probsub.html and follow the instructions to search for additional information for this product.

Chapter 2. Installing Fix Pack 1

Fix Pack 1 is installed into your existing IBM Tivoli Composite Application Manager for SOA v6.1.0 environment as an upgrade, or, for the HP-UX 11i v2 Itanium-based (64-bit) platform, as a new full ITCAM for SOA v6.1.0 installation on HP-UX computers where Web services are to be monitored.

The installation of Fix Pack 1 requires the following prerequisites:

- IBM Tivoli Monitoring v6.1 with Fix Pack 4 or later is installed on one or more supported operating systems in your Web services environment, including Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal components installed on one or more computers.
- The installation program for this fix pack assumes that the IBM Eclipse Help Server is already installed in your IBM Tivoli Monitoring environment. If you have not already installed the IBM Eclipse Help Server into your environment, be sure to install it before installing this fix pack
- For supported operating systems other than the HP-UX 11i v2 Itanium-based (64-bit) platform, IBM Tivoli Composite Application Manager for SOA v6.1.0 is already installed in your Web services environment, including support files for the IBM Tivoli Monitoring components and the ITCAM for SOA v6.1.0 monitoring agent on computer systems where Web services are being monitored. For the supported HP-UX 11i v2 Itanium-based (64-bit) platform, the monitoring agent for ITCAM for SOA v6.1.0 is installed by this fix pack as a new, full installation.
- You must download the required compressed packages from the product support Web site, and unpack them into a local temporary location on computers in your environment where you want to install the fix pack.

To download and unpack the appropriate compressed file packages, complete the following steps:

1. Create a new directory location in which to unpack the compressed package.
2. Navigate to the IBM Product Support Web site for IBM Tivoli Composite Application Manager for SOA:

   ```
   www.ibm.com/software/sysmgmt/products/support
   /IBMTivoliCompositeApplicationManagerforSOA.html
   ```
3. Download the desired packages from the IBM Product Support Web site:
   - For supported Windows operating systems, locate and download the **6.1.0-TIV-ITCAMSOA-WINDOWS-FP0001.zip** compressed file package to a temporary directory, and then unpack it.
   - For supported Linux® (on Intel® IA32 and AMD64) operating systems, locate and download the **6.1.0-TIV-ITCAMSOA-Multi_ixLinux-FP0001.tar.gz** compressed file package to a temporary directory, and then unpack the files.
   - For supported Linux (on pSeries and zSeries) operating systems, locate and download the **6.1.0-TIV-ITCAMSOA-Multi_pzLinux-FP0001.tar.gz** compressed file package to a temporary directory, and then unpack the files.
   - For supported Solaris and AIX operating systems, locate and download the **6.1.0-TIV-ITCAMSOA-Multi_sol_aix-FP0001.tar.gz** compressed file package to a temporary directory, and then unpack the files.
   - For the supported HP-UX operating system, locate and download the **6.1.0-TIV-ITCAMSOA-HPUXIA64-LA0001.tar.gz** compressed file package to a temporary directory, and then unpack the files.

The full installation image for the fix pack on the HP-UX 11i v2 Itanium-based (64-bit) platform is a Limited Availability download. Look for the link to the *HP 11.23i Support + AXIS on BEA WebLogic Data Collector for ITCAM for SOA 6.1*. When you select the link for this package, you are prompted for your authorized user name and password to access this package.

4. For either zip or tar.gz packages, uncompress the package using your preferred tool.

Installing the fix pack

The following sections contain operating system specific procedures for upgrading the monitoring agent and agent support files to the Fix Pack 1 level. For supported HP-UX operating systems, the monitoring agent and agent support files are installed as a full installation installing the fix pack.

Upgrading application support on the monitoring server, portal server, and desktop client

The installation image that is provided for installing the fix pack on supported Windows and Linux operating systems is not a full installation image for ITCAM for SOA v6.1.0. Before installing this image, you must first install the support files from the full ITCAM for SOA v6.1.0 product on supported Windows and Linux computer systems in your environment where the IBM Tivoli Monitoring components (Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server) are located, and then upgrade that support to this fix pack level using this installation image.

The installation procedure for the fix pack is very similar to the procedure for installing ITCAM for SOA v6.1.0. To install the fix pack, complete the following steps:

- For Windows:
  1. Stop the Tivoli Enterprise Portal Server or Tivoli Enterprise Monitoring Server if they are running on the local computer.
  2. Close the Manage Tivoli Enterprise Monitoring Services console if it is open.
  3. If you also have application server runtime environments being monitored on the local computer, stop them as needed.
  4. From the temporary directory where you unpacked the fix pack, select the \Windows directory.
  5. Run the setup.exe command to start the installation.
  6. Follow the on-screen prompts and accept the provided default values whenever possible. Refer to the *IBM Tivoli Composite Application Manager for SOA Installation and User's Guide* for more information about the installation procedures.
- For Linux (you should be running this procedure with root authority):
  1. Depending on which IBM Tivoli Monitoring component (monitoring server, portal server, or desktop client) you are installing application support for, stop it by running the usual commands as described in the IBM Tivoli Monitoring documentation.
  2. Close the Manage Tivoli Enterprise Monitoring Services console if it is open.
  3. From the directory where you unpacked the fix pack files, run the following command to start the installation program:

     ```
     ./install.sh
     ```

  4. Follow the on-screen prompts and accept the default responses for all of the questions presented where a default is offered. Refer to the *IBM Tivoli*

Composite Application Manager for SOA Installation and User's Guide for more information about the installation procedures.

5. Depending on which IBM Tivoli Monitoring component (monitoring server, portal server, or desktop client) you are installing application support for, start it by running the usual commands as described in the IBM Tivoli Monitoring documentation.
6. If installing support on the monitoring server, run the following command to activate the application support::

   ```
   ./itmcmd support -t tems_name d4
   ```

   In this command, *tems_name* is the name of the monitoring server and *d4* is the product code for the IBM Tivoli Composite Application Manager for SOA monitoring agent.

   If installing support on the portal server, run the following command to configure the portal server:

   ```
   ./itmcmd config -A cq
   ```

   If installing support on the desktop client, run the following command to configure the desktop client:

   ```
   ./itmcmd config -A cj
   ```

   Complete the configuration as prompted.
7. Stop and restart the IBM Tivoli Monitoring component using the usual IBM Tivoli Monitoring commands.

Upgrading the monitoring agent on Windows, AIX, Solaris, and Linux operating systems

The installation procedure for the fix pack is very similar to the procedure for installing the monitoring agent for ITCAM for SOA v6.1.0. To install the fix pack, complete the following steps:

- For Windows operating systems:
  1. Optionally stop the Tivoli Enterprise Portal Server or Tivoli Enterprise Monitoring Server if they are running on the local computer.
  2. Close the Manage Tivoli Enterprise Monitoring Services console if it is open.
  3. Disable data collection and stop the appropriate application servers on the local computer as needed.
  4. From the temporary directory where you unpacked the fix pack, select the \Windows directory.
  5. Run the setup.exe command to start the installation.
  6. Follow the on-screen prompts and accept provided default values whenever possible. Refer to the *IBM Tivoli Composite Application Manager for SOA Installation and User's Guide* for more information about the installation procedures.
  7. Re-enable data collection and mediation primitive support and restart the appropriate application servers on the local computer as needed. See "Re-enabling data collectors and mediation primitive support" on page 14 for details.
- For AIX®, Solaris, and Linux operating systems: (you should be running this procedure with root authority):
  1. Optionally stop the monitoring server, portal server, or desktop client if they are running on the local computer.
  2. Close the Manage Tivoli Enterprise Monitoring Services console if it is open.

3. Disable data collection and stop the appropriate application servers on the local computer as needed.
4. From the directory where you unpacked the fix pack files, run the following command to start the installation program:

   ```
   ./install.sh
   ```
5. Follow the on-screen prompts and accept the default responses for all of the questions presented where a default is offered. Refer to the *IBM Tivoli Composite Application Manager for SOA Installation and User's Guide* for more information about the installation procedures.
6. If an IBM Tivoli Monitoring component (monitoring server, portal server, or desktop client) is also installed on this local computer, start it by running the usual commands as described in the IBM Tivoli Monitoring documentation.
7. Navigate to the *<ITM_Dir>*/bin directory, where *<ITM_Dir>* is the IBM Tivoli Monitoring home directory (such as /opt/IBM/ITM) and run the following command to configure the monitoring agent:

   ```
   ./itmcmd config -A d4
   ```

   Complete the configuration as prompted. When asked for the Tivoli Enterprise Monitoring Server hostname, specify the hostname of the computer system where your Tivoli Enterprise Monitoring Server is located.
8. Re-enable data collection and mediation primitive support and restart the appropriate application servers on the local computer as needed. See "Re-enabling data collectors and mediation primitive support" on page 14 for details. Restart the IBM Tivoli Monitoring components using the usual IBM Tivoli Monitoring commands.
9. Run the following command to start the ITCAM for SOA monitoring agent:

   ```
   <ITM_Dir>/bin/CandleAgent start d4
   ```
10. Run the KD4configDC script as needed to enable data collection for the application server runtime environment.

Upgrading the monitoring agent on z/OS

This section describes the general procedure for installing the fix pack on z/OS operating systems. This procedure is written based on these assumptions:

- The ITCAM for SOA V6.1.0 GA product is already installed in your environment.
- You have already updated the support files on all distributed Tivoli Enterprise Portal Server and Tivoli Enterprise Monitoring Server computers in your environment For more information, see "Upgrading application support on the monitoring server, portal server, and desktop client" on page 6.
- You are familiar with your z/OS environment and with modifying and submitting JCL jobs as needed for installation and configuration.

This procedure covers three basic tasks:

- "Receiving and applying PTF UA31777"
- "Rerunning ICAT configuration steps" on page 10
- "Reload the applicable runtime environment libraries" on page 11

Receiving and applying PTF UA31777

To receive and apply the PTF UA31777, complete these steps:

1. If the monitoring agent is running, stop and disable it using the usual procedures.

2. Backup your original Receive and Apply JCL jobs, because this procedure will modify them to install the fix pack. These are the names of the jobs located in your ITCAM for SOA V6.1.0 installation library *<installlib>*:
   - *<installlib>*.SMPJOBS(KD4J0REC)
   - *<installlib>*.SMPJOBS(KD4J0APP)
3. Edit the Receive JCL job *<installlib>*.SMPJOBS(KD4J0REC) to receive the PTF. Prior to editing, the original Receive JCL job should look similar to this example:

```
000059 //SMPPTFIN DD DSN=TDSHR.PKG.IBM.D46100W9.SMPMCS,
000060 // DISP=SHR
000061 // DD DSN=TDSHR.PKG.IBM.HKCI310.MAINT,
000062 // DISP=SHR
000063 // DD DSN=TDSHR.PKG.IBM.HKDS610.MAINT,
000064 // DISP=SHR
000065 // DD DSN=TDSHR.PKG.IBM.HKD4610.MAINT,
000066 // DISP=SHR
000067 // DD DSN=TDSHR.PKG.IBM.HKLV610.MAINT,
000068 // DISP=SHR
000069 //*
000070 //SMPCNTL DD *
000071 SET BDY(GLOBAL) .
000072 RECEIVE SYSMODS RFPREFIX(TDSHR.PKG)
000073 LIST
```

   Modify this JCL by completing these steps:

   a. Edit the SMPPTFIN step to contain only the one new DD referencing the PTF, similar to this example, where *<PTF.Location_Lib>* is the location for the PTF, and *<PTFname>* is the name of the PTF to receive:

```
000059 //SMPPTFIN DD DSN=<PTF.Location_Lib>(<PTFname>),
000060 // DISP=SHR
```

   b. Edit the RECEIVE statement to remove the RFPREFIX(TDSHR.PKG) portion, resulting in the modified statement:

```
000072 RECEIVE SYSMODS
```

   The resulting edited Receive JCL should now look similar to this example:

```
000059 //SMPPTFIN DD DSN=<PTF.Location_Lib>(<PTFname>),
000060 // DISP=SHR
000061 //*
000062 //SMPCNTL DD *
000063 SET BDY(GLOBAL) .
000064 RECEIVE SYSMODS
000065 LIST
```

4. Edit the Apply JCL job *<installlib>*.SMPJOBS(KD4J0APP) to apply the PTF. Prior to editing, the original Apply JCL job should look similar to this example:

```
000056 //SMPCNTL DD *
000057 SET BDY(TLIB1) . /* <== Note 2 */
000058 APPLY GROUPEXTEND
000059 SELECT( /* <== Note 4 */
000060 HKCI310
000061 HKDS610
000062 HKD4610
000063 HKLV610
000064 )
000065 FORFMID( /* <== Note 4 */
000066 HKCI310
000067 HKDS610
000068 HKD4610
000069 HKLV610
000070 )
000071 /* CHECK / / <== Note 5 */
000072 BYPASS(HOLDSYSTEM(DOC,ACTION,DEP))
000073 .
000074 /*
```

Modify this JCL by completing these steps:

a. Edit the SELECT statement, removing all of the HKxxxxx records and replacing them with *<PTFname>*, the name of the PTF to apply:

```
000059 SELECT( /* <== Note 4 */
000060 <PTFname>
000061 )
```

b. Edit the FORFMID statement, removing all of the HKxxxxx records and replacing them with *<PTFname>*, the name of the PTF to apply:

```
000062 FORFMID( /* <== Note 4 */
000063 <PTFname>
000064 )
```

The resulting edited Apply JCL should now look similar to this example:

```
000056 //SMPCNTL DD *
000057 SET BDY(TLIB1) . /* <== Note 2 */
000058 APPLY GROUPEXTEND
000059 SELECT( /* <== Note 4 */
000060 <PTFname>
000061 )
000062 FORFMID( /* <== Note 4 */
000063 <PTFname>
000064 )
000065 /* CHECK / / <== Note 5 */
000066 BYPASS(HOLDSYSTEM(DOC,ACTION,DEP))
000067 .
000068 /*
```

5. Submit the Receive job *<installib>*.SMPJOBS(KD4J0REC) to receive the PTF.
6. Submit the Apply job *<installib>*.SMPJOBS(KD4J0APP) to apply the PTF.

   PTF already installed: If the Apply job was already run for this PTF, you might receive a MAXCC=12 return code and this message:

   ```
   APPLY PROCESSING FAILED FOR SYSMOD <PTFname> BECAUSE IT HAS ALREADY
   BEEN INSTALLED.
   ```

   If this occurs, edit the Apply job to add a REDO statement after the BYPASS statement, similar to this example:

   ```
   000056 //SMPCNTL DD *
   000057 SET BDY(TLIB1) . /* <== Note 2 */
   000058 APPLY GROUPEXTEND
   000059 SELECT( /* <== Note 4 */
   000060 <PTFname>
   000061 )
   000062 FORFMID( /* <== Note 4 */
   000063 <PTFname>
   000064 )
   000065 /* CHECK / / <== Note 5 */
   000066 BYPASS(HOLDSYSTEM(DOC,ACTION,DEP))
   000067 REDO
   000068 .
   000069 /*
   ```

   After editing, submit the Apply job again.

Rerunning ICAT configuration steps

This fix pack provides new function that requires updates to existing runtime members and configuration jobs. To refresh the runtime environments (RTEs) where the product is configured, refer to *Configuring IBM Tivoli Composite Application Manager for SOA on z/OS* manual to recreate and rerun the configuration jobs generated from these applicable steps. Repeat these steps for each applicable RTE:

1. Refresh the KD4CAT catalog file and the KD4ATR attribute file members in the RKANDATV library, by completing either of these steps as appropriate for your environment:
   - If there is a local Tivoli Enterprise Monitoring Server configured in the RTE and the monitoring agent is registered to this local Tivoli Enterprise Monitoring Server, perform *A1. Step 3.3.1: Registering with the local Tivoli Enterprise Monitoring Server*. Recreate and rerun the *D4#4xxxx Register with local TEMS* job.
   - If the above conditions are not applicable to your environment, perform *A2. Step 3.3.4: Specifying agent address space parameters*. Recreate and rerun the *D4#3xxxx Specify Agent address space parameters* job.
2. Refresh the hierarchical file system (HFS) related RKANDATV files by performing *Step 3.3.7: Creating hierarchical file system directories and copying files on UNIX System Services.* Recreate and rerun the *D4#Uxxxx Create HFS directories and copy files on USS* job.

Reload the applicable runtime environment libraries

The RTE Load function is typically not required after applying maintenance using SMP/E for RTEs that share the SMP/E TARGET libraries. If you made copies of the SMP/E TARGET libraries (for example, a BASE RTE or a FULL RTE), then you still must run the RTE Load function to refresh the runtime libraries after applying maintenance using SMP/E. For more information, type *README RTE* on the command line from any configuration panel within the Configuration tool.

To reload the applicable RTEs, perform *Step 3.4: Loading runtime libraries*. Recreate and rerun the *D4#2xxxx Load all product libraries after SMP/E* job.

Installing the monitoring agent on HP-UX

The installation procedure for the fix pack on the HP-UX 11i v2 Itanium-based (64-bit) platform is very similar to the procedure for installing the monitoring agent for ITCAM for SOA v6.1.0 on Linux, except that this is a full installation rather than a fix pack upgrade to a previous v6.1.0 installation. Complete the following steps on each supported HP-UX operating system where you plan to monitor Web services:

1. You should run this procedure with root authority.
2. Close the Manage Tivoli Enterprise Monitoring Services console if it is open.
3. Stop the BEA WebLogic application server if it is running.
4. From the directory where you unpacked the fix pack files, run the following command to start the installation program:

   ```
   ./install.sh
   ```

5. When prompted for the IBM Tivoli Monitoring home directory, press Enter to accept the default (*/opt/IBM/ITM*) or type the full path to a different directory.

   Note: If you are installing over an existing installation of IBM Tivoli Monitoring, you must use the existing installation directory.

6. If the installation directory does not already exist, you are asked if you want to create it. Type *y* to create this directory and press Enter. The following prompt is displayed:

   ```
   Select one of the following:
   1) Install products to the local host.
   2) Install products to depot for remote deployment (requires TEMS)
   3) Exit install.

   Please enter a valid number:
   ```

Note: This prompt might vary depending on the installation image from which you are installing.

7. Type *1* to start the installation and press Enter.
8. Type the number that corresponds to the language (for example, English) in which you want to display the software license agreement, and press Enter.
9. Press Enter to display the agreement.
10. Type *1* to accept the agreement and press Enter.
11. Type a 32 character key for encrypting your Secure Socket Layer (SSL) connections with Tivoli Enterprise Monitoring Server to protect sensitive data being transmitted. This key should be the same key that is specified during the installation of the Tivoli Enterprise Monitoring Server to which this monitoring agent connects.
12. A numbered list of available operating systems is displayed. Type the number for the operating system on which you are installing. The default value is your current operating system. Press Enter.
13. Type *y* to confirm your operating system and press Enter.
14. A numbered list of available agents is displayed. Find the IBM Tivoli Composite Application Manager for SOA agent and type the corresponding number and press Enter.
15. A list of the components to install is displayed. Type *y* to confirm the installation.
16. The installation begins. After all of the components are installed, you are asked if you want to install additional products or product support packages. Accept the default response of *n* and press Enter.

See the IBM Tivoli Monitoring documentation for general procedures on installing monitoring agents.

Configuring the monitoring agent

Use the following steps to configure the monitoring agent on supported HP-UX operating systems:

1. Navigate to the *<ITM_Dir>*/bin directory, where *<ITM_Dir>* is the IBM Tivoli Monitoring home directory (such as /opt/IBM/ITM), and run the following command:

   ```
   ./itmcmd config -A d4
   ```

2. Press Enter when you are asked if the monitoring agent connects to a monitoring server.
3. Type the hostname for the monitoring server.
4. Type the type of protocol that the monitoring agent uses to communicate with the monitoring server. You have four choices: ip, sna, ip.spipe, or ip.pipe. Press Enter to accept the default protocol (IP.PIPE).
5. To set up a backup protocol, type the name of that protocol and press Enter. If you do not want to use backup protocol, press Enter without specifying a protocol name. If the method you have identified as Protocol 1 fails, Protocol 2 is used. See the IBM Tivoli Monitoring documentation for more information about available protocol selections.
6. Depending on the types of protocols you specified, provide the following information when prompted:

Table 1. Protocol settings for communicating between the monitoring agent and Tivoli Enterprise Monitoring Server

Protocol	Value	Description
IP.UDP	IP Port Number	The listening port for the Tivoli Enterprise Monitoring Server to which this monitoring agent is connected. The default value is *1918*.
IP.PIPE	IP.PIPE Port Number	The listening port for the Tivoli Enterprise Monitoring Server to which this monitoring agent is connected. The default value is *1918*.
IP.SPIPE	IP.SPIPE Port Number	The listening port for the Tivoli Enterprise Monitoring Server to which this monitoring agent is connected. The default value is *3660*.
SNA	Network Name	The SNA network identifier for your location.
	LU Name	The LU name for the Tivoli Enterprise Monitoring Server. This LU name corresponds to the local LU Alias in your SNA communications software.
	Log Mode	The name of the LU6.2 LOGMODE. The default value is *CANCTDCS*.

7. Press Enter to *not* specify the name of the KDC_PARTITION.
8. Press Enter when you are asked if you want to configure the connection to a secondary monitoring server. The default response is *No*.
9. Press Enter to accept the default for the Optional Primary Network Name (*none*).

Changing the file permissions for agents

If you used a non-root user to install the monitoring agent on the HP-UX operating system, the file permissions are initially set to a low level. Use the following procedure to change these file permissions:

1. Log on to the computer as root, or become the root user by running the **su** command.
2. Create a new group (such as *itmusers*) to own all of the files in the IBM Tivoli Monitoring installation directory. Run the following command:

   ```
   groupadd itmusers
   ```
3. Run the following command to ensure that the $CANDLEHOME environment variable correctly identifies the IBM Tivoli Monitoring installation directory:

   ```
   echo $CANDLEHOME
   ```
4. Change to the directory returned by the previous step:

   ```
   cd $CANDLEHOME
   ```

   Important: Be sure you are in the correct directory. Running the steps that follow using the wrong directory can change the permissions on every file in every file system on the computer.
5. Run the following command to ensure that you are in the correct directory:

   ```
   pwd
   ```
6. Run the following commands:

   ```
   chgrp -R itmusers .
   chmod -R o-rwx .
   ```
7. Run the following command to change the ownership of additional agent files:

   ```
   bin/SetPerm
   ```

8. If you want to run the agent as a particular user, add the user to the *itmusers* group. To do this, edit the /etc/group file and ensure that the user is in the list of users for the *itmusers* group.

   For example, if you want to run the agent as user *test1*, ensure that the following line is in the /etc/group file:

   ```
   itmusers:x:504:test1
   ```

9. Run the **su** command to switch to the user that you want to run the agent as or log in as that user.

After completing these steps, enable the data collector for the BEA WebLogic environment using the information in Chapter 4, “The Axis data collector in the BEA WebLogic environment,” on page 23.

Uninstalling the monitoring agent on HP-UX

To uninstall this monitoring agent from the HP-UX 11i v2 Itanium-based (64-bit) platform, disable data collection for any data collectors that are enabled, then navigate to the $CANDLEHOME/bin directory and run the following command:

```
./uninstall.sh
```

Follow the on-screen prompts to complete the uninstallation.

Re-enabling data collectors and mediation primitive support

Due to shared code between the data collector environments supported with Fix Pack 1 and existing data collectors for supported application server runtime environments, after installing this fix pack you must complete the following additional steps:

1. Run the KD4configDC script to disable and re-enable all of the data collectors that are deployed on the same computer, to ensure that the data collectors are running at the same product level for all environments. See the documentation library for IBM Tivoli Composite Application Manager for SOA for details on disabling and re-enabling applications for these other supported environments.
2. Disable and re-enable the mediation primitive runtime support on the target IBM WebSphere Enterprise Service Bus and IBM WebSphere Process Server computers by running these scripts:
   - KD4configMediationInstall
   - KD4configMediationDeploy

   Refer to the *IBM Tivoli Composite Application Manager for SOA Tools* publication for details on configuring runtime support for managed SCA mediation primitives.

Chapter 3. Enabling and activating Fix Pack 1 functions

All of the new post-GA function provided with this fix pack is installed when the fix pack is installed, however these new functions are either disabled or inactive by default. If you installed the fix pack only to obtain the Java patch for Daylight Saving Time provided for ITCAM for SOA v6.1, these disabled and inactive post-GA features do not affect your existing environment.

After installing or upgrading your ITCAM for SOA v6.1.0 environment to the Fix Pack 1 level, you need to complete the following activities to enable or activate the additional post-GA functions provided with this fix pack:

- To access the new workspaces and views that are provided in this fix pack, and the new support for workspace linking to OMEGAMON XE for Messaging, you must run an enabling command using the KfwSQLClient command line interface provided with IBM Tivoli Monitoring. This command is described in "Adding new workspaces, views, and linking."
- To enable data collection by requester identity, use the new Take Action commands provided with this fix pack to specify requester identities to be monitored, and to turn on data collection. For more information, see Chapter 6, "Monitoring by Web service requesters," on page 43.
- To access the new version of IBM Tivoli Composite Application Manager for SOA Tools that is provided with this fix pack, you must uninstall any existing previous version of the Tools, and then install this new version into a WebSphere Integration Developer v6.0.2 environment. After installing the new version of the Tools, you must upgrade the level of mediation primitive runtime support using the KD4configMediationInstall and KD4configMediationDeploy scripts. For more information, see "Upgrading support for managed SCA mediation primitives" on page 17.
- To run the DataPower data collector as a service on supported Windows operating systems, you must register the DataPower data collector as a service using the KD4configDC script. For more information, see "Running the DataPower data collector as a Windows service" on page 19.
- To access support for new ITCAM for SOA data collectors in the BEA WebLogic and WebSphere Message Broker environments, you must enable these data collectors using the KD4configDC script, with new syntax options that are described in the following chapters:
  - Chapter 4, "The Axis data collector in the BEA WebLogic environment," on page 23
  - Chapter 5, "The WebSphere Message Broker data collector," on page 29

Adding new workspaces, views, and linking

New workspaces and views are provided with this fix pack to display metric data that originates from specifically monitored sources, referred to in this fix pack as *requester identities*. In addition, new workspace links are provided to access these new workspaces from the Services Inventory view of the Performance Summary workspace.

Workspace linking is also provided to link from WebSphere Message Broker services data displayed in the Services Inventory view of the Performance Summary workspace to corresponding message flow statistics displayed in IBM Tivoli OMEGAMON XE for Messaging workspaces.

These workspaces, views, and workspace links are added to the Tivoli Enterprise Portal only when you run a command using the KfwSQLClient command line interface provided with IBM Tivoli Monitoring.

To add these new workspaces, views, and workspace links to the Tivoli Enterprise Portal, complete the following steps:

1. Verify that the Tivoli Enterprise Portal Server is running.
2. From the computer where the Tivoli Enterprise Portal Server is installed, open a command prompt.
3. Navigate to the *<ITM_Home>*\CNPS, where *<ITM_Home>* is the location where IBM Tivoli Monitoring is installed, for example (on Windows): C:\IBM\ITM.
4. Run the KfwSQLClient command:
   - For Windows operating systems, run the following command:

     ```
     KfwSQLClient –l –d KFW_DSN –f SQLLIB\kd4_sparkler61fp1.sql
     ```

   - For AIX, Solaris, or Linux operating systems, run the following commands to prepare the shell environment:

     ```
     cd /opt/IBM/ITM/config
     . ./cq.config
     cd /opt/IBM/ITM/<opsys>/cq/bin
     . ./pathsetup.sh
     ```

     In this command, *<opsys>* is the platform specific directory path to the appropriate /cq/bin directory (for example, *aix533* for AIX).

     Run the following command:

     ```
     ./KfwSQLClient -l -d KFW_DSN -f ../sqllib/kd4_sparkler61fp1.sql
     ```
5. Examine the *<ITM_Home>*\logs\KfwSQLClient*.log file for any errors.
6. Close the command prompt window.
7. Stop and then restart the Tivoli Enterprise Portal Server.
8. Sign on to the Tivoli Enterprise Portal.

Use only the KfwSQLClient command line interface: The kd4_sparkler61fp1.sql file is a support file for Tivoli Enterprise Portal Server, not Tivoli Enterprise Monitoring Server. For this reason, you cannot use the Tivoli Enterprise Monitoring Server Application Support user interface to add these new workspaces, views, and links. This also holds true during the upgrade process, when the kd4_sparkler61fp1.sql file might be included in the list of SQL files that you can select to add application support to the Tivoli Enterprise Monitoring Server. In this case do not select this file. You must use the KfwSQLClient command line interface.

For more information on workspace linking between WebSphere Message Broker services data in ITCAM for SOA and message flow statistics displayed in IBM Tivoli OMEGAMON XE for Messaging, see “Linking to IBM Tivoli OMEGAMON XE for Messaging” on page 40.

Enabling data collection by requester identity

After adding these new workspaces and views to the Tivoli Enterprise Portal, you must issue the new Take Action commands to create a list of requester identities for which metric data is to be collected, and turn on the collection function. These new workspaces, views, workspace links, and Take Actions are described in Chapter 6, “Monitoring by Web service requesters,” on page 43.

Upgrading support for managed SCA mediation primitives

IBM Tivoli Composite Application Manager for SOA Version 6.1 provided a new set of *managed SCA mediation primitives* that extend the set of base primitives provided in IBM WebSphere Integration Developer Version 6.0.1 and supported in the SCA runtime environments of IBM WebSphere Enterprise Service Bus Version 6.0.1 and IBM WebSphere Process Server Version 6.0.1. These new managed SCA mediation primitives have the same mediation function as the base primitives, but they also have the additional capability to be enabled or disabled at runtime.

After the release of IBM Tivoli Composite Application Manager for SOA Version 6.1.0, new versions of IBM WebSphere Integration Developer Version 6.0.2, IBM WebSphere Enterprise Service Bus Version 6.0.2, and IBM WebSphere Process Server Version 6.0.2 became available, offering new support that allows some of the properties of these base primitives to be *promoted*, so that the primitive properties and their values can be viewed and modified using the IBM WebSphere Administration Console.

Fix Pack 1 provides additional function to the managed SCA mediation primitives to also support the same property promotion capability as the base primitives. Note, however, that only those properties defined as promotable in the base primitives are enabled for promotion in the managed SCA mediation primitives. The additional property in the Tivoli managed SCA mediation primitives to enable or disable the primitive at runtime is not promotable, and therefore not available for viewing or modifying using the IBM WebSphere Administration Console. This property is still configured using the ConfigureMediation_610 and DeletePrimitiveProperty_610 Take Action commands and viewed in the Mediation Configuration workspace as documented in the ITCAM for SOA v6.1 library.

Installing new support for managed SCA mediation primitives

To install the new support for the Tivoli managed SCA mediation primitives, you must run a separate InstallShield MultiPlatform (ISMP) installation program in attended mode on the computer system where your IBM WebSphere Integration Developer version 6.0.2 is installed. Notice the following considerations when you run the installation program:

- The installation program does not support upgrading an existing installation of IBM Tivoli Composite Application Manager for SOA Tools. If you already have a previous installation of the Tools support from ITCAM for SOA version 6.1 installed on the target computer system, you must uninstall the previous version before installing this new support. For more information on uninstalling an existing installation, see the *IBM Tivoli Composite Application Manager for SOA Tools* publication.
- If you run the installation program on a computer system with IBM WebSphere Integration Developer version 6.0.1 installed, the installation program detects this version of IBM WebSphere Integration Developer and only installs the ITCAM for SOA v6.1.0 support for managed SCA mediation primitives. The new support for managed SCA mediation primitives is only available when it is installed in IBM WebSphere Integration Developer version 6.0.2 or later.
- You can still install the ITCAM for SOA v6.1.0 (GA level, prior to this fix pack) support for managed SCA mediation primitives into IBM WebSphere Integration Developer version 6.0.2 or later, but the property promotion capability *will not* be available.
- The new support for managed SCA mediation primitives is supported only in the following environments:

– Operating system platforms:
  - Windows 2003 Enterprise Server SP1
  - RedHat Enterprise Linux 4 Advanced Server
– Integrated Development Environment:
  - IBM WebSphere Integration Developer Version 6.0.2
– Runtime Environments:
  - IBM WebSphere Enterprise Service Bus Version 6.0.2
  - IBM WebSphere Process Server Version 6.0.2

  Version 6.0.1 of the IBM WebSphere Enterprise Service Bus and IBM WebSphere Process Server runtime environments support only SCA applications that are built using the ITCAM for SOA v6.1.0 level of managed SCA mediation primitives. Deploying an SCA application that uses the fix pack version of the managed SCA mediation primitive support in a version 6.0.1 runtime environment is not supported.

  Version 6.0.2 of either the IBM WebSphere Enterprise Service Bus or IBM WebSphere Process Server runtime environment will support SCA applications that are built using either the ITCAM for SOA v6.1 or the fix pack version of managed SCA mediation primitive support. SCA applications using the ITCAM for SOA v6.1 version of the support will not have any properties appear as promoted in the IBM WebSphere Administration Console.

Installing on Windows operating systems

To install the Fix Pack 1 version of managed SCA mediation primitives support into your IBM WebSphere Integration Developer environment on supported Microsoft Windows operating systems, complete the following steps:

1. Uninstall any previous version of ITCAM for SOA Tools from the target computer. For more information, refer to the *IBM Tivoli Composite Application Manager for SOA Tools* guide.
2. Access the IBM Tivoli Composite Application Manager for SOA Fix Pack 1 installation media, and navigate to the \KD4\Tools directory.
3. From the \KD4\Tools directory, run the following command to start the InstallShield wizard:

   ```
   setupwin32.exe
   ```
4. The installation procedure is essentially unchanged for this fix pack installation. For more information, refer to the *IBM Tivoli Composite Application Manager for SOA Tools* publication.

   The installation program verifies that a previous version of the Tools is not already installed on this computer. If found, an error message is displayed instructing you to uninstall the current Tools installation before installing again. This release does not support the ability to install over an existing installation.

   Continue through the installation program and follow the on-screen prompts. You are asked to select to install the IBM Web Services Navigator as well as the managed SCA mediation primitives, depending on the target environment. When you install the managed SCA mediation primitives you are asked for the base directory location of your existing IBM WebSphere Integration Developer environment. If your IBM WebSphere Integration Developer environment includes a IBM WebSphere Process Server or IBM WebSphere Enterprise Service Bus test environment that should be enabled with the runtime support for the managed SCA mediation primitives, you are asked for the location of the runtime directory (for example, <*WID_Dir*>\runtimes\bi_v6, where <*WID_Dir*> is the directory path where IBM WebSphere Integration Developer is installed).

Installing on Linux operating systems

The installation procedure for installing on supported Linux operating systems is similar to that for Windows operating system. From the product installation media, navigate to the \KD4\Tools directory and run the following command:

```
./setupLinux.bin
```

The installation screens prompt you for the information needed to install IBM Web Services Navigator and managed SCA mediation primitives. Refer to the *IBM Tivoli Composite Application Manager for SOA Tools* publication for details on the installation procedure.

Starting IBM WebSphere Integration Developer

After installing the Fix Pack 1 version of the managed SCA mediation primitives support, start IBM WebSphere Integration Developer using the **–clean** option.

If you have previously imported applications into the IBM WebSphere Integration Developer v6.0.2 environment, you might need to start IBM WebSphere Integration Developer a second time using the **–clean** option to be able to successfully open the imported mediation flow.

Configuring runtime support for managed SCA mediation primitives on Windows, Linux, and z/OS

To use the updated managed SCA mediation primitives, you must disable and re-enable the mediation primitive runtime support on the target IBM WebSphere Enterprise Service Bus and IBM WebSphere Process Server computers using the KD4configMediationInstall and KD4configMediationDeploy scripts. The runtime support for these updated managed SCA mediation primitives is available only after an SCA application built from the updated plug-ins is deployed to a IBM WebSphere Enterprise Service Bus v6.0.2 or IBM WebSphere Process Server v6.0.2 environment.

For details on configuring runtime support for managed SCA mediation primitives, refer to the *IBM Tivoli Composite Application Manager for SOA Tools* publication.

The runtime support for managed SCA mediation primitives is supported only in the following environments:

- Operating system platforms:
  - Windows 2003 Enterprise Server SP1
  - RedHat Enterprise Linux 4 Advanced Server
  - z/OS v1.8
- Runtime Environments:
  - IBM WebSphere Enterprise Service Bus Version 6.0.2
  - IBM WebSphere Process Server Version 6.0.2

Running the DataPower data collector as a Windows service

IBM Tivoli Composite Application Manager for SOA Version 6.1 provides a proxy data collector for monitoring Web services in the IBM WebSphere DataPower SOA Appliance environment. For the version 6.1 release, the DataPower data collector runs as a user-started command line application.

Fix Pack 1 adds an additional capability to register and start the DataPower data collector as a service on supported Windows operating systems. Running the DataPower data collector as a service improves availability, because the data collector can be automatically restarted in the event of a system restart.

After installing Fix Pack 1 for ITCAM for SOA v6.1, the DataPower data collector is not automatically registered as a service, so you can still start the data collector using the **startDPDC** script as described in the *IBM Tivoli Composite Application Manager for SOA Installation and User's Guide*.

Registering the DataPower data collector as a Windows service

To register the DataPower data collector as a Windows service, complete the following steps:

1. If the data collector is already running in console mode, stop the data collector.
2. Open a command prompt.
3. Navigate to the %CANDLE_HOME%\TMAITM6\KD4\bin directory.
4. Run the following script:

   ```
   KD4configDC.bat –registerService –env 8
   ```

Starting the DataPower data collector as a Windows service

After the DataPower data collector is registered as a service, it is set to start automatically when the system is rebooted. The data collector is not started immediately, however, in case the data collector is already running in console mode.

To start the DataPower data collector manually, use the Windows Service Manager, or run the following command:

```
net start kd4dpdc
```

You can still start the DataPower data collector using the existing startDPDC script, as supported in ITCAM for SOA v6.1. If the data collector is registered as a Windows service, however, the service starts instead of a console session.

After registering and starting the DataPower data collector as a service, you can operate the product as usual.

Stopping the DataPower data collector as a Windows service

To stop the DataPower data collector manually, use the Windows Service Manager, or run the following command:

```
net stop kd4dpdc
```

Removing the DataPower data collector from the list of Windows services

To remove the DataPower data collector from the list of Windows services, complete the following steps:

1. If the data collector is already running in console mode, stop it.
2. Open a command prompt.
3. Navigate to the %CANDLE_HOME%\TMAITM6\KD4\bin directory.
4. Run the following script:

   ```
   KD4configDC.bat –deregisterService –env 8
   ```

Deregister before uninstalling the product: Note that when you uninstall IBM Tivoli Composite Application Manager for SOA v6.1.0 with Fix Pack 1, the process does not include removing the DataPower data collector from the list of Windows services. Because this process uses the KD4configDC script, you should always deregister the DataPower data collector Windows service before uninstalling the product

For more information about the DataPower data collector, refer to the *IBM Tivoli Composite Application Manager for SOA Installation and User's Guide*.

Error handling

Errors that occur while registering, starting, stopping, or deregistering the service are written to the Windows event log, and also to the IBM Tivoli Monitoring RAS logs found in *<%CANDLE_HOME%>*\logs directory. This logfile name follows the IBM Tivoli Monitoring logfile naming convention for ITCAM for SOA, *<machinename>_d4_<logid>.log* (for example, omut3_d4_463742c2-01.log) Consult both the Windows event log and the IBM Tivoli Monitoring RAS logs in case of service errors.

Chapter 4. The Axis data collector in the BEA WebLogic environment

This chapter describes the support for a new data collector for the Apache Axis version 1.2 Web service SOAP engine running in the BEA WebLogic application server runtime environment.

Overview

Apache Axis is essentially a SOAP engine, defined on the official Apache Axis Web site (http://ws.apache.org/axis/java/install.html) as *a framework for constructing SOAP processors such as clients, servers, gateways, etc*. Axis runs as several servlets, while the BEA WebLogic application server provides the Web container for these Axis servlets. Conceptually, consider this environment as a BEA WebLogic server with Axis v1.2 Web service support.

When Axis is installed according to the basic Axis installation instructions (see the Apache Axis Web site for more information on basic and advanced installation options), Axis is deployed as a Web application to the Web container in either an exploded directory or a packaged war file, for example *axis.war*.

You deploy your Web services into this Axis Web application by adding new classes and registering the new service into the Axis Web application. The Axis data collector, when enabled for the Axis Web application, monitors these Web services. If you deploy additional Web services after the Axis data collector is enabled for data collection, the newly deployed Web services are monitored automatically.

Message logging and message rejection are supported in the same manner as the BEA WebLogic data collector for the ITCAM for SOA v6.1.0 GA product.

Supported operating systems

BEA WebLogic version 8.1 with Service Pack 4 continues to be supported on all platforms supported by the ITCAM for SOA v6.1.0 GA product.

Fix Pack 1 provides support for Apache AXIS v1.2 on the BEA WebLogic Server on the following operating system platforms:

- BEA WebLogic version 8.1 with Service Pack 5
  - Solaris 8
  - Solaris 10
  - Windows Server 2003 Enterprise SP1 (32 bit)
  - Red Hat Enterprise Linux 4.0 Advanced Server
- BEA WebLogic version 9.2
  - Windows Server 2003 Enterprise SP1 (32 bit)
  - Red Hat Enterprise Linux 4.0 Advanced Server
  - HP-UX 11i v2 Itanium-based (64-bit) platform

Enabling the AXIS data collector in a BEA WebLogic single-server environment

Before enabling the AXIS data collector, verify that the BEA Web Logic server is running.

To enable the AXIS data collector, complete the following steps:

1. Before running the KD4configDC script on supported HP-UX operating systems, switch to the Korn shell (/usr/bin/ksh) interactive command interpreter.

   Run a script to set up all of the environment variables and Java options before running the KD4configDC.bat or KD4configDC.sh scripts.

   - For Windows operating systems:

     `<DOMAIN_HOME>\setDomainEnv.cmd (or setEnv.cmd)`

   - For Linux, AIX, or Solaris operating systems:

     `<DOMAIN_HOME>/setDomainEnv.sh (or setEnv.sh)`

2. Navigate to the *<ITCAM4SOA_Home>*/KD4/bin directory. In this directory path, *<ITCAM4SOA_Home>* is the location where IBM Tivoli Composite Application Manager for SOA is installed (for example, /opt/IBM/ITM/hpi116/d4).
3. Run the following KD4configDC script:

   `KD4configDC.sh –enable –env 3 <URL> <userID> <password> –axis`

   Specify the following options for the script:

   URL The Web address of the BEA WebLogic Server (for example, t3://localhost:7001). *t3* and *t3s* are proprietary BEA protocols.

   userID
   A valid WebLogic user name with the authority to configure applications.

   password
   A valid password associated with the specified WebLogic user name.

   –axis Enables the AXIS data collector in the BEA WebLogic environment. If this option is not specified then the ITCAM for SOA v6.1.0 GA data collector for BEA WebLogic is enabled.

Example:

```
KD4configDC.sh -enable -env 3 "t3://localhost:7001" weblogic weblogic -axis
```

To enable the ITCAM for SOA v6.1.0 GA version of the data collector for BEA WebLogic (version 8.1 only), run the KD4configDC script, leaving off the **–axis** option:

```
KD4configDC.sh -enable -env 3 "t3://localhost:7001" weblogic weblogic
```

Disabling the AXIS data collector in a BEA WebLogic single-server environment

Before disabling the AXIS data collector, verify that the BEA WebLogic server is running.

To disable the AXIS data collector, complete the following steps:

1. Before running the KD4configDC script on supported HP-UX operating systems, switch to the Korn shell (/usr/bin/ksh) interactive command interpreter.
2. Run a script to set up all of the environment variables and Java options before running the KD4configDC script.

- For Windows operating systems:

  <*DOMAIN_HOME*>\setDomainEnv.cmd (or setEnv.cmd)
- For Linux, AIX, or Solaris operating systems:

  <*DOMAIN_HOME*>/setDomainEnv.sh (or setEnv.sh)

3. Navigate to the *<ITCAM4SOA_Home>*/KD4/bin directory, where *<ITCAM4SOA_Home>* is the location where IBM Tivoli Composite Application Manager for SOA is installed (for example, /opt/IBM/ITM/hpi116/d4).
4. Run the following KD4configDC script:

   KD4configDC.sh –disable –env 3 <*URL*> <*userID*> <*password*> –axis

   Specify the following options for the script:

   URL The Web address of the BEA WebLogic Server (for example, t3://localhost:7001). *t3* and *t3s* are proprietary BEA protocols.

   userID
   A valid WebLogic user name with the authority to configure applications.

   password
   A valid password associated with the specified WebLogic user name.

   –axis Disables the AXIS data collector in the BEA WebLogic environment. If this option is not specified then the ITCAM for SOA v6.1.0 GA data collector for BEA WebLogic is disabled.

Example:

```
KD4configDC.sh -disable -env 3 "t3://localhost:7001" weblogic weblogic -axis
```

To disable the ITCAM for SOA v6.1.0 GA version of the data collector for BEA WebLogic (version 8.1 only), run the KD4configDC script as usual, leaving off the **–axis** option:

```
KD4configDC.sh -disable -env 3 "t3://localhost:7001" weblogic weblogic
```

Enabling the AXIS data collector in a BEA WebLogic multi-server environment

A typical BEA WebLogic domain contains one administrative server and one or more managed servers. To enable the AXIS data collector in the domain, you need to enable the AXIS data collector only on the administrative server and then restart the managed servers for the configuration to take effect.

This procedure assumes that the IBM Tivoli Composite Application Manager for SOA monitoring agent is already installed on each BEA WebLogic server computer.

To enable the AXIS data collector on WebLogic servers in a domain, complete the following steps:

1. Before running the KD4configDC script on supported HP-UX operating systems, switch to the Korn shell (/usr/bin/ksh) interactive command interpreter.
2. Run a script to set up all of the environment variables and Java options before running the KD4configDC script.
   - For Windows operating systems:

     <*DOMAIN_HOME*>\setDomainEnv.cmd (or setEnv.cmd)
   - For Linux, AIX, or Solaris operating systems:

     <*DOMAIN_HOME*>/setDomainEnv.sh (or setEnv.sh)

3. Stop all of the managed servers and ensure that the administrative server is running.
4. On the administrative server, navigate to the *<ITCAM4SOA_Home>*/KD4/bin directory, where *<ITCAM4SOA_Home>* is the location where IBM Tivoli Composite Application Manager for SOA is installed (for example, /opt/IBM/ITM/hpi116/d4).
5. Run the following KD4configDC script:

   `KD4configDC.sh –enable –env 3 <URL> <userID> <password> –axis`

   Specify the following options for the script:

   URL The Web address of the BEA WebLogic Server (for example, t3://localhost:7001). *t3* and *t3s* are proprietary BEA protocols.

   userID
   A valid WebLogic user name with the authority to configure applications.

   password
   A valid password associated with the specified WebLogic user name.

   –axis Enables the AXIS data collector in the BEA WebLogic environment. If this option is not specified then the ITCAM for SOA v6.1.0 GA data collector for BEA WebLogic is enabled.

   Example:

   ```
   KD4configDC.sh -enable -env 3 "t3://localhost:7001" weblogic weblogic -axis
   ```
6. Start the managed servers.

Disabling the AXIS data collector in a BEA WebLogic multi-server environment

A typical BEA WebLogic domain contains one administrative server and one or more managed servers. To disable the AXIS data collector in the domain, you only need to disable the AXIS data collector on the administrative server and then restart the managed servers for the change to take effect.

This procedure assumes that the IBM Tivoli Composite Application Manager for SOA monitoring agent is already installed on each BEA WebLogic server computer.

To disable the AXIS data collector on WebLogic servers in a domain, complete the following steps:

1. Before running the KD4configDC script on supported HP-UX operating systems, switch to the Korn shell (/usr/bin/ksh) interactive command interpreter.
2. Run a script to set up all of the environment variables and Java options before running the KD4configDC script.
   - For Windows operating systems:

     `<DOMAIN_HOME>\setDomainEnv.cmd (or setEnv.cmd)`
   - For Linux, AIX, or Solaris operating systems:

     `<DOMAIN_HOME>/setDomainEnv.sh (or setEnv.sh)`
3. Stop all of the managed servers and ensure that the administrative server is running.
4. On the administrative server, navigate to the *<ITCAM4SOA_Home>*/KD4/bin directory, where *<ITCAM4SOA_Home>* is the location where IBM Tivoli Composite Application Manager for SOA is installed (for example, /opt/IBM/ITM/hpi116/d4).
5. Run the following KD4configDC script:

```
KD4configDC.sh –disable –env 3 <URL> <userID> <password> –axis
```

Specify the following options for the script:

URL The Web address of the BEA WebLogic Server (for example, t3://localhost:7001). *t3* and *t3s* are proprietary BEA protocols.

userID
A valid WebLogic user name with the authority to configure applications.

password
A valid password associated with the specified WebLogic user name.

–axis Disables the AXIS data collector in the BEA WebLogic environment. If this option is not specified then the ITCAM for SOA v6.1.0 GA data collector for BEA WebLogic is disabled.

Example:

```
KD4configDC.sh -disable -env 3 "t3://localhost:7001" weblogic weblogic -axis
```

6. Start the managed servers.

Error codes

The following error codes might be returned if you experience problems while running the KD4configDC script:

Table 2. KD4configDC error codes

Error code	Explanation	Action
119	Unsupported WebLogic version: the version of the WebLogic Server is not supported by the current ITCAM for SOA v6.1.0 release.	Install a WebLogic version that is supported by the current ITCAM for SOA v6.1.0 release or contact IBM Software Support to upgrade to the correct version.
120	Failure when opening or parsing the registry file, %BEA_HOME%\ registry.xml or $BEA_HOME/ registry.xml. You might also receive this return code if you did not switch to the Korn shell (ksh) before running KD4configDC on HP-UX operating systems.	Check the WebLogic server version and verify that the WebLogic server is properly installed. Check for the existence of the registry file. On HP-UX operating systems, switch to ksh before running the KD4configDC script.
156	Failure when you attempt to run the KD4configDC script without first setting up the BEA WebLogic Server environment variables and Java options.	Before running the KD4configDC script, set the BEA WebLogic server environment variables and Java options by running the *<DOMAIN_HOME>*\ setDomainEnv.cmd or setDomainEnv.sh scripts (or setEnv.cmd/.sh, as documented in the *IBM Tivoli Composite Application Manager for SOA Installation and User's Guide*)
201	The number of options specified with the KD4configDC script is valid and not null, but one or more options are not valid (for example, the URL might be incorrect).	Examine the options provided with the KD4configDC script and correct them as needed, then run the script again.

Table 2. KD4configDC error codes (continued)

Error code	Explanation	Action
203	Connection error: cannot connect to WebLogic server. Either the port or the URL is incorrect, or the server is not running.	Verify that the correct port and URL are specified, and that the server is running before issuing the script.
204	Unknown host error: The URL cannot be reached.	Check the URL and verify that it points to a known host.
205	Authentication error: The user name or password is not valid for login.	Verify the user name and password or provide a valid user name and password to login.
206	General error: Either the discovery, start, stop, backup, update or rollback application is not successful. (One return code covers all of these problems because these are application level errors, and because more than one application might be enabled at the same time.)	Refer to the trace log and operation log for detailed information about which error occurred for which application, and take corrective action as needed.

Limitations

The Axis data collector has the following limitations:

- The Axis data collector supports monitoring Web services in Axis SOAP engines that are installed with *basic* installation (Web application) and *advanced* installation (adding Axis to an existing enterprise application) procedures. The KD4configDC script cannot be used to enable monitoring of *customized* installations. See the Axis documentation for more details.
- The Axis data collector monitors both requester side and provider side Web service events, but only within supported application server runtime environments. Stand-alone client Axis applications are not supported.
- When monitoring both the Axis SOAP engine (provided in this fix pack) and the *native* SOAP engine (supported by the base ITCAM for SOA V6.1.0 product) of BEA WebLogic 8.1 application servers, all services are displayed in the Tivoli Enterprise Portal as though they are running in the same runtime environment. There is no way to tell from the Tivoli Enterprise Portal which services are deployed to the Axis SOAP engine and which are deployed to the native SOAP engine.

Additional considerations

The port number attribute for the application server is always displayed with a value of *0* in the ITCAM for SOA attribute groups when running on BEA WebLogic v9.2. If you have more than one server instance using the same name, and they are on the same computer, the data collected and processed for these instances is displayed as if they all came from a single server.

See the documentation library and online help information provided with IBM Tivoli Composite Application Manager for SOA for information on starting and stopping data collectors, configuring monitoring and filtering settings, understanding workspaces, views, Take Action commands, and other features that help you monitor and manage your Web services in the BEA WebLogic application server runtime environment.

Chapter 5. The WebSphere Message Broker data collector

Fix Pack 1 provides support for a new data collector to monitor services in a WebSphere Message Broker version 6.0.0.3 environment, with APARs IC52137 and IC52138 applied.

Overview

IBM WebSphere Message Broker version 6.0.0.3 provides a *user exit* structure in which applications can provide message processing extensions. This user exit structure is the interception mechanism for the WebSphere Message Broker data collector.

Mapping Message Broker concepts to the service model

The WebSphere Message Broker environment is different from a typical Web application server environment. WebSphere Message Broker uses *message flows* to deal with request and response messages for the services that are being monitored. These message flows are associated with user exits. A single message flow can be mapped into multiple services.

WebSphere Message Broker separates message flows in different operating system processes. These operating system processes are called *execution groups*. Each execution group can contain one or more message flows.

One or more execution groups are defined within a message broker.

Generally, Message Broker components can be mapped into the ITCAM for SOA services model as shown in Table 3:

Table 3. Mapping Message Broker concepts to the ITCAM for SOA Web services model

Concept in WebSphere Message Broker	ITCAM for SOA Web services model
Message Broker	Application server node (for example, *tivu02Node*)
Execution Group	Application server, such as server1, server2 in WebSphere.
Message Flow	Service port (for the purpose of enabling flows to be monitored)

The WebSphere Message Broker data collector determines the service port and operation names and namespaces using the following information available in the user exit:

- The message flow name of the request message is used as the service port name (for both the request and response messages, even if the response is handled by a different message flow).
- A portion of the endpoint URL is used as the service port namespace. For HTTP URLs, the namespace is the portion of the URL that follows the *<schema>://<hostname>:<port>* string. For Java Message Service (JMS) URLs, the namespace is the value of the *targetService=* portion of the URL.
- The first child element of the SOAP *<body>* element is used as the operation name.
- The namespace of this child element is used as the operation namespace.

Supported operating systems

The WebSphere Message Broker data collector is supported on the following operating systems:

- Windows Server 2003 Enterprise SP1
- Red Hat Enterprise Linux 4.0 Advanced Server
- z/OS Version 1.8

WebSphere Message Broker supports services that are started over HyperText Transfer Protocol (HTTP), JMS, and Message Queue (MQ) transport protocols, and supports a variety of message formats (SOAP, XML/non-SOAP and unstructured binary messages). For this fix pack, only the following subset of these transport protocol and message format combinations are supported:

- SOAP messages over HTTP
- SOAP messages over JMS

Monitoring data is displayed in the existing Tivoli Enterprise Portal workspaces and views similar to other data collectors. Message content logging is supported in the same manner as other data collectors, but message rejection is not supported because WebSphere Message Broker provides its own capabilities for rejecting messages.

While the ITCAM for SOA v6.1.0 data collector for WebSphere Message Broker is supported on Windows, Linux, and z/OS operating systems, the procedures for enabling and disabling the data collector is different between distributed and z/OS platforms.

Enabling and Disabling data collection on distributed platforms

The data collector for the WebSphere Message Broker environment on supported Windows and Linux operating systems is enabled and disabled using the KD4configDC script, specifying a new value for the **–env** environment option and additional options for the Message Broker environment.

The KD4configDC script runs WebSphere Message Broker commands to enable or disable the data collector for the specified execution group and message flow.

On supported Windows operating systems, log in as the Message Broker owner (the default is *Administrator*), and bring up the Message Broker Command Console (**Start –> All Programs –> IBM WebSphere Message Broker 6.0 –> Command Console**), and run the KD4configDC script.

On supported Linux operating systems, log in as the Message Broker owner (the user who installed Message Broker). Ensure that the Message Broker profile is in your shell profile, or source it manually by running the command:

```
. /opt/IBM/mqsi/6.0/bin/mqsiprofile
```

To enable the data collector, the KD4configDC script runs the WebSphere Message Broker commands to perform the following tasks:

- Add the runtime directory of the data collector user exit code (mqsisoauserexit.lel) to the WebSphere Message Broker user exit path.
- Update the list of active user exits for the specified execution group and message flow to include the data collector user exit.

To disable data collection, KD4configDC runs the WebSphere Message Broker commands to perform the following tasks:

- Update the list of active user exits for the specified execution group and message flow to remove the data collector user exit.
- Remove the data collector user exit runtime directory from the WebSphere Message Broker user exit path.

This is the syntax of the KD4configDC script in the distributed environment:

```
KD4configDC.bat/.sh [–enable | –disable] –env 10 broker_name
execution_group_name message_flow_name
```

In this version of the script, these are the options:

–enable
Enable data collection for the specified message flow within the specified message broker and execution group.

–disable
Disable data collection on the specified message flow.

–env The application server environment to configure, *10* (Message Broker)

Broker_name
Name of the message broker.

Execution_group_name
Name of the execution group within the specified message broker to be configured.

Message_flow_name
Name of the message flow within the specified execution group to be configured.

When you run the KD4configDC script, you are prompted to confirm that you want to stop the specified message broker to complete the configuration. If you want to stop the message broker, press Enter to continue. If you do not want to stop the message broker, enter CTRL-C to exit the script.

The script verifies that there is not already another instance of the script running on the same message broker by looking for the file KD4/config/wmb/config/ configMBDC_*<broker_name>*.runflow. This file is usually created each time the script is run, and then deleted automatically after the script completes. If another instance of KD4configDC is running on the same message broker, a message is displayed informing you that another instance is already running, and your instance of the script is stopped. You should wait for the other instance of the script to complete, and then run your script again.

If, however, you are sure that another instance of the KD4configDC script is not currently running, it is possible that this configMBDC_*<broker_name>*.runflow file might not have been deleted from a previous run of the KD4configDC script. You can delete this file manually and then run your script again.

Enable Example: To enable a message flow named *testFlow*, which is associated with the Execution Group named *testEGroup*, which in turn belongs to the message broker named *testBroker* on Windows, run the KD4configDC script as follows:

```
KD4ConfigDC.bat  -enable -env 10 testBroker testEGroup testFlow
```

Disable Example: To disable a message flow named *testFlow*, which is associated with the Execution Group named *testEGroup*, which in turn belongs to the message broker named *testBroker* on Windows, run the KD4configDC script as follows:

```
KD4ConfigDC.bat  -disable -env 10 testBroker testEGroup testFlow
```

Upgrading: In the future, if you upgrade your ITCAM for SOA environment after applying this fix pack, you must re-enable at least one message flow within the Message Broker. All of the message flows within that Message Broker are then upgraded. Repeat this for all enabled Message Brokers as needed.

Disabling data collection on message flows: If you have data collection enabled for a message flow that you no longer need to monitor, be sure to disable data collection for the message flow before stopping the Message Broker and uninstalling the monitoring agent. If you do not disable the message flow first, you will not be able to list the message flow using the mqsilist command.

If this problem occurs, use one of the following procedures to recover the message flow:

- Using the Toolkit, remove the message flow and then re-deploy it.
- Restore the original mqsisoauserexit.lel file to the correct location by completing the following steps:
  1. Reinstall the ITCAM for SOA 6.1.0 monitoring agent
  2. Create the directory *$Install_DIR*\KD4\config\wmb\lib*$BrokerName*
  3. Obtain the mqsisoauserexit.lel file from *$Install_DIR*\KD4\lib directory
  4. Copy this file to *$Install_DIR*\KD4\config\wmb\lib*$BrokerName*
  5. Restart the message broker
  6. Use the **mqsilist** command to verify that the message flow exists.

After recovering the message flow, disable data collection using the KD4configDC script.

Enabling and Disabling data collection on the z/OS operating system

To enable or disable data collection for WebSphere Message Broker on supported z/OS operating systems, you use a combination of the KD4configDC script and several additional steps to submit JCL jobs from the Time Sharing Option (TSO) environment.

WebSphere Message Broker on z/OS provides a set of template JCL files that you can use to run the WebSphere Message Broker commands that manage the user exit path and the list of active user exits for execution groups and message flows.

The template JCL files are located in the SBIPPROC dataset (for example, BIP.V6R0M0.SBIPPROC). These JCL files are only templates, and you must customize them for your specific z/OS environment before you submit them for processing. You should make a copy of these templates, customize them for your z/OS environment, and use these copies to keep track of the WebSphere Message Broker configuration settings.

The following sections describe how to use the KD4configDC script and the WebSphere Message Broker template JCL files to enable and disable the ITCAM for SOA data collector for WebSphere Message Broker on z/OS. For more detailed information on using the JCL templates provided by WebSphere Message Broker, see the appropriate WebSphere Message Broker publications.

Enabling data collection on the z/OS operating system

To enable the data collector on z/OS, complete the following steps:

1. For each message broker instance that has message flows to be monitored by the data collector, run the KD4configDC script from the UNIX® System Services (USS) environment on z/OS, similar to the following example:

   ```
   KD4configDC.sh –enable –env 10 <broker_name>
   ```

   In this version of the script, these are the options:

   –enable
   Enable data collection for the specified message flow within the specified message broker and execution group.

   –env The application server environment to configure, *10* (Message Broker)

   <broker_name>
   Name of the message broker.

   The KD4configDC script copies the data collector user exit (mqsisoauserexit.lel) to a runtime directory and issues a message indicating the location of this directory.

2. Add the user exit runtime directory to the WebSphere Message Broker user exit path by completing the following steps:

   a. Make a copy of the BIPCHBK JCL template file from the SBIPPROC dataset (for example, BIP.V6R0M0.SBIPPROC). If you already have your own copy of this file, use it to avoid overwriting the existing configuration.

      The BIPCHBK JCL file looks similar to the following example:

      ```
      //BIPCHBK JOB
      //*********************************************************************
      //*                                                                   *
      //* @START_COPYRIGHT@                                                 *
      //*                                                                   *
      //* Licensed Materials - Property of IBM;                             *
      //* 5655-G97 (c) Copyright IBM Corp. 2004;                            *
      //* All Rights Reserved;                                              *
      //* US Government Users Restricted Rights - use,                      *
      //* duplication or disclosure restricted by GSA                       *
      //* ADP Schedule Contract with IBM Corp.;                             *
      //* See Copyright Instructions                                        *
      //*                                                                   *
      //* @END_COPYRIGHT@                                                   *
      //*                                                                   *
      //*********************************************************************
      //*              IBM WebSphere Event/Message Brokers                  *
      //*                                                                   *
      //* Sample job to change a broker setting (mqsichangebroker).         *
      //*                                                                   *
      //*********************************************************************
      //* MORE INFORMATION - See:                                           *
      //*                                                                   *
      //*    WebSphere Event/Message Brokers Information Centre.            *
      //* Topic "an07090"                                                   *
      //*                                                                   *
      //*********************************************************************
      //* CUSTOMIZE THIS JCL HERE FOR YOUR INSTALLATION
      //* YOU MUST DO GLOBAL CHANGES ON THESE PARAMETERS USING YOUR EDITOR
      //*                                                                   *
      //*    Replace   ++HOME++
      //*                      Home directory where ENVFILE and STDERR
      //*                      and STDOUT files will be created.
      //*                      e.g. '/u/home'
      //*
      //*    Replace   ++INSTALL++
      ```

```
//*                     WBI Brokers installation directory.
//*                     e.g. '/usr/lpp/mqsi'
//*
//*    Replace   ++COMPONENTNAME++
//*                     Broker name.
//*                     e.g. 'MQ01BRK'
//*
//*    Replace   ++OPTIONS++
//*                     Options for mqsichangebroker command.
//*                     e.g. '-s MQ01'
//*
//*    Replace   ++DB2HLQ++
//*                     DB2 high-level-qualifier.
//*                     e.g. 'SYS2.DB2.V810'
//*
//*    Replace   ++WMQHLQ++
//*                     WebSphere MQ high-level-qualifier.
//*                     e.g. 'MQM.V530'
//*
//*********************************************************************
//*
//*********************************************************************
//* Copy ENVFILE to SYSOUT
//*********************************************************************
//*
//COPYENV  EXEC PGM=IKJEFT01,
//         PARM='OCOPY INDD(BIPFROM) OUTDD(ENVFILE)'
//SYSTSPRT DD DUMMY
//BIPFROM  DD PATHOPTS=(ORDONLY),
//            PATH='++HOME++/ENVFILE'
//ENVFILE  DD SYSOUT=*,DCB=(RECFM=V,LRECL=256)
//SYSTSIN  DD DUMMY
//*
//*********************************************************************
//* Run mqsichangebroker command
//*********************************************************************
//*
//BIPCHBK  EXEC PGM=IKJEFT01,REGION=0M
//*        DB2 Runtime Libraries
//STEPLIB  DD DISP=SHR,DSN=++DB2HLQ++.SDSNEXIT
//         DD DISP=SHR,DSN=++DB2HLQ++.SDSNLOAD
//         DD DISP=SHR,DSN=++DB2HLQ++.SDSNLOD2
//*        MQSeries Runtime Libraries
//         DD DISP=SHR,DSN=++WMQHLQ++.SCSQANLE
//         DD DISP=SHR,DSN=++WMQHLQ++.SCSQAUTH
//         DD DISP=SHR,DSN=++WMQHLQ++.SCSQLOAD
//STDENV   DD PATHOPTS=(ORDONLY),
//            PATH='++HOME++/ENVFILE'
//STDOUT   DD SYSOUT=*
//STDERR   DD SYSOUT=*
//SYSTSPRT DD SYSOUT=*
//SYSTSIN  DD *
BPXBATSL PGM -
  ++INSTALL++/bin/-
mqsichangebroker -
  ++COMPONENTNAME++ -
  ++OPTIONS++
/*
//
```

The comments in the JCL template describe how to specify the following environment specific information:

++HOME++
The home directory for WebSphere Message Broker, for example, */u/home*.

++INSTALL++
The installation directories for WebSphere Message Broker, for example, */usr/lpp/mqsi*.

++DB2HLQ++
The DB2® high level qualifier, for example, *SYS2.DB2.V810*.

++WMQHLQ++
The WebSphere MQ high level qualifier, for example, *MQM.V530*

b. The last part of the JCL template shows how to run the mqsichangebroker command to change various WebSphere Message Broker settings, including the user exit path. Refer to the WebSphere Message Broker publications for detailed information on the **mqsichangebroker** command and its syntax.

Know what directories are in the user exit path: When using the **mqsichangebroker** command to change the WebSphere Message Broker user exit path, you must know in advance the complete list of user exit directories that are already in the user exit path before adding the ITCAM for SOA data collector user exit directory to the user exit path. You should already be maintaining a current set of user exit path directories in a customized copy of this JCL template.

For example, suppose the user exit path currently consists of two directories: *userExitDir1* and *userExitDir2*. To add the data collector user exit directory *<dataCollectorUserExitDir>* to the user exit path, modify the following lines in the BIPCHBK JCL:

- Replace *++COMPONENTNAME++* with the name of the Message Broker instance whose user exit path is being modified.
- Replace *++OPTIONS++* with the user exit path option *–x*, along with the new, full user exit path, with each directory in the path separated with a colon character (:), similar to the following example:

```
–x userExitDir1:userExitDir2:<dataCollectorUserExitDir>
```

In this example, *<dataCollectorUserExitDir>* is the directory displayed when you ran the KD4configDC script using the **–enable** option.

c. Start the message broker control process.

d. Stop the message broker.

e. Submit the JCL for processing, and review the output from the submitted job to verify that the job completed successfully.

f. Restart the message broker.

3. Update the active user exit list for message flows by completing the following steps:

a. Make a copy of the BIPCHUE JCL template file from the SBIPPROC dataset (for example, BIP.V6R0M0.SBIPPROC). If you already have your own copy of this file, use it to avoid overwriting the existing configuration.

The BIPCHUE JCL file looks similar to the following example:

```
//BIPCHUE JOB
//*******************************************************************
//*                                                                 *
//* @START_COPYRIGHT@                                               *
//*                                                                 *
//* Licensed Materials - Property of IBM;                           *
//* 5655-G97 (c) Copyright IBM Corp. 2006;                          *
//* All Rights Reserved;                                            *
//* US Government Users Restricted Rights - use,                    *
//* duplication or disclosure restricted by GSA                     *
//* ADP Schedule Contract with IBM Corp.;                           *
//* See Copyright Instructions                                      *
```

```
//*                                                                   *
//* @END_COPYRIGHT@                                                   *
//*                                                                   *
//*********************************************************************
//*             IBM WebSphere Event/Message Brokers                   *
//*                                                                   *
//* Sample job to change properties (mqsichangeflowuserexits).        *
//*                                                                   *
//*********************************************************************
//* MORE INFORMATION - See:                                           *
//*                                                                   *
//*    WebSphere Event/Message Brokers Information Centre.            *
//*                                                                   *
//*                                                                   *
//*********************************************************************
//* CUSTOMIZE THIS JCL HERE FOR YOUR INSTALLATION
//* YOU MUST DO GLOBAL CHANGES ON THESE PARAMETERS USING YOUR EDITOR
//*                                                                   *
//*    Replace   ++HOME++
//*                      Home directory where ENVFILE and STDERR
//*                      and STDOUT files will be created.
//*                      e.g. '/u/home'
//*
//*    Replace   ++INSTALL++
//*                      WBI Brokers installation directory.
//*                      e.g. '/usr/lpp/mqsi'
//*
//*    Replace   ++BROKERNAME++
//*                      Broker name.
//*                      e.g. 'MQ01BRK'
//*
//*    Replace   ++EXECUTIONGROUPNAME++
//*                      Execution group name.
//*                      e.g. '-e default'
//*
//*    Replace   ++MESSAGEFLOWNAME++
//*                      Message flow name.
//*                      e.g. '-f Flow1'
//*
//*    Replace   ++ACTIVEUSEREXITLIST++
//*                      Active user exit list.
//*                      e.g. '-a exit1:exit2'
//*
//*    Replace   ++ACTIVEUSEREXITLIST++
//*                      Inactive user exit list.
//*                      e.g. '-i exit3:exit4'
//*
//*    Replace   ++DB2HLQ++
//*                      DB2 high-level-qualifier.
//*                      e.g. 'SYS2.DB2.V810'
//*
//*    Replace   ++WMQHLQ++
//*                      WebSphere MQ high-level-qualifier.
//*                      e.g. 'MQM.V530'
//*
//*********************************************************************
//*
//*********************************************************************
//* Copy ENVFILE to SYSOUT
//*********************************************************************
//*
//COPYENV  EXEC PGM=IKJEFT01,
//         PARM='OCOPY INDD(BIPFROM) OUTDD(ENVFILE)'
//SYSTSPRT DD DUMMY
//BIPFROM  DD PATHOPTS=(ORDONLY),
//            PATH='++HOME++/ENVFILE'
//ENVFILE  DD SYSOUT=*,DCB=(RECFM=V,LRECL=256)
```

```
//SYSTSIN  DD DUMMY
//*
//*******************************************************************
//* Run mqsichangeflowuserexits command
//*******************************************************************
//*
//BIPCHUE  EXEC PGM=IKJEFT01,REGION=0M
//*        DB2 Runtime Libraries
//STEPLIB  DD DISP=SHR,DSN=++DB2HLQ++.SDSNEXIT
//         DD DISP=SHR,DSN=++DB2HLQ++.SDSNLOAD
//         DD DISP=SHR,DSN=++DB2HLQ++.SDSNLOD2
//*        MQSeries Runtime Libraries
//         DD DISP=SHR,DSN=++WMQHLQ++.SCSQANLE
//         DD DISP=SHR,DSN=++WMQHLQ++.SCSQAUTH
//         DD DISP=SHR,DSN=++WMQHLQ++.SCSQLOAD
//STDENV   DD PATHOPTS=(ORDONLY),
//            PATH='++HOME++/ENVFILE'
//STDOUT   DD SYSOUT=*
//STDERR   DD SYSOUT=*
//SYSTSPRT DD SYSOUT=*
//SYSTSIN  DD *
BPXBATSL PGM -
  ++INSTALL++/bin/-
mqsichangeflowuserexits -
  ++BROKERNAME++ -
  -e ++EXECUTIONGROUPNAME++ -
  -f ++MESSAGEFLOWNAME++ -
  -a ++ACTIVEUSEREXITLIST++ -
  -i ++INACTIVEUSEREXITLIST++ -
/*
//
```

The comments in the JCL template describe how to specify the following environment specific information:

++HOME++
The home directory for WebSphere Message Broker, for example, */u/home*.

++INSTALL++
The installation directories for WebSphere Message Broker, for example, */usr/lpp/mqsi*.

++DB2HLQ++
The DB2 high level qualifier, for example, *SYS2.DB2.V810*.

++WMQHLQ++
The WebSphere MQ high level qualifier, for example, *MQM.V530*.

b. The last part of the JCL template shows how to run the **mqsichangeflowuserexits** command to change the list of active and inactive user exits. Refer to the WebSphere Message Broker publications for detailed information on the **mqsichangeflowuserexit** command and its syntax.

Know what user exits are already in the active and inactive lists: When using the **mqsichangeflowuserexit** command to change the list of user exits, you must know in advance the complete list of user exits that are already in the active and inactive user exit lists before adding the ITCAM for SOA data collector user exit to the active user exit list. You should already be maintaining current lists of active and inactive user exits in a customized copy of this JCL template.

For example, suppose the active user exit list currently consists of two active user exits: *activeUserExit1* and *activeUserExit2*, and the inactive user exit list includes one inactive user exit, *inactiveUserExit1*. To add the ITCAM

for SOA data collector user exit *MqsiSOAExit* to the active user exit list, modify the following lines in the BIPCHUE JCL:

- Replace *++BROKERNAME++* with the name of the Message Broker instance of the execution group containing the message flow.
- Replace *++EXECUTIONGROUPNAME++* with the name of the execution group.
- Replace *++MESSAGEFLOWNAME++* with the name of the message flow to be monitored.
- Leave the *++INACTIVEUSEREXITLIST++* unchanged. Optionally, you can omit it if there are no user exits in the inactive user exit list.
- Replace *++ACTIVEUSEREXITLIST++* with the list of active user exits, where each user exit name is separated by a colon character (:), similar to the following example:

  `activeUserExit1:activeUserExit2:MqsiSOAExit`

  Account for user exit execution times: Note that user exits are run in the order in which they appear in the exit list. You might need to adjust where you place the data collector user exit in the active list to avoid including the execution time of other user exits in the response time measurements of the ITCAM for SOA data collector.

c. Submit the JCL for processing, and review the output from the submitted job to verify that the job completed successfully.

   You do not need to restart the WebSphere Message Broker after running the BIPCHUE JCL job.

4. Repeat this process for each message flow to be monitored by the WebSphere Message Broker data collector.

Disabling data collection on the z/OS operating system

To disable the ITCAM for SOA data collector for WebSphere Message Broker on z/OS, use the same BIPCHUE and BIPCHBK JCL templates described in the preceding section.

To disable the data collector on the z/OS operating system, complete the following steps:

1. Modify your copy of the BIPCHUE JCL to remove the ITCAM for SOA data collector user exit, *MqsiSOAExit*, from the active user exit list (*++ACTIVEUSEREXITLIST++*) of each message flow that was being monitored by the data collector.

   Be sure to leave all other user exits in the active user exit list for each message flow, so that only the WebSphere Message Broker data collector user exit *MqsiSOAExit* is inactivated.

   Submit the JCL for processing, and review the output from the submitted job to verify that the job completed successfully.

   You do not need to restart the WebSphere Message Broker after running the BIPCHUE JCL job.

2. After removing the WebSphere Message Broker data collector user exit from the active user exit list of all message flows, modify your copy of the BIPCHBK JCL to remove the data collector user exit directory from the user exit path of the Message Broker instances being monitored:

   a. Edit *++OPTIONS++* in the JCL to remove *<dataCollectorUserExitDir>* from the list of user exit directories. Be sure to leave all other directories in the user exit path unchanged, so that only the SOA data collector user exit directory is removed from the user exit path.

b. Stop the message broker.
c. Submit the JCL for processing, and review the output from the submitted job to verify that the job completed successfully.
d. Restart the message broker.

3. Run the KD4configDC script under UNIX System Services (USS), similar to the following example:

   ```
   KD4configDC.sh –disable –env 10 <broker_name>
   ```

   In this script, *<broker_name>* is the name of the WebSphere Message Broker for which you are disabling data collection.
4. After all of the message flows belonging to the message broker are disabled, you can optionally delete the mqsisoauserexit.lel file from the KD4/config/wmb/lib/*<broker_name>* runtime directory.

Managing active user exit lists

These procedures describe how to enable the ITCAM for SOA data collector user exit at the individual message flow level. But WebSphere Message Broker actually provides a great deal of flexibility in how you can define user exits.

For example, if you add a user exit to the active user exit list for an execution group using the BIPCHUE JCL template, it is applied to all message flows in that execution group, unless the same user exit is included in the inactive user exit list for specific message flows.

If you include a user exit in the active user exit list at the Message Broker instance level using the BIPCHBK JCL template, it is applied to all messages flows in all execution groups of that Message Broker instance, unless the same user exit appears in the inactive user exit list of a specific execution group or message flow.

You might find that defining the ITCAM for SOA data collector user exit at the message broker instance or execution group level is easier than for each individual message flow. For more information, see the appropriate WebSphere Message Broker documentation.

Limitations

This section describes several limitations you might experience with the data collector in the WebSphere Message Broker environment.

SOAP fault message unavailable

There are certain conditions in the WebSphere Message Broker environment in which an error can occur in a message flow, causing the transaction to be rolled back. In this situation the actual SOAP fault message is unavailable to be written into the content log when content logging is turned on. An empty text string is written to the content log instead.

When this kind of error occurs in the WebSphere Message Broker environment, the message length is reported as zero because the actual SOAP fault message is unavailable. This zero value might result in an inaccurate calculation of the average message length.

Performance

When the data collector for the WebSphere Message Broker is enabled, you might experience CPU overhead greater than 5%. The performance of this data collector is to be addressed in a later release.

Linking to IBM Tivoli OMEGAMON XE for Messaging

Fix Pack 1 adds a new workspace link from IBM WebSphere Message Broker services displayed in the Services Inventory view of the Performance Summary workspace to corresponding message flow statistics displayed in the Message Flow Statistics workspace in the IBM Tivoli OMEGAMON XE for Messaging product.

The information displayed by ITCAM for SOA gives you a *service view* of monitored message flows, while IBM Tivoli OMEGAMON XE for Messaging offers a more detailed display of message flow statistics, and node statistics, among others.

Monitoring message flows with the CandleMonitor node: Message flows that you are monitoring with ITCAM for SOA are displayed in the Message Flow Statistics workspace only if the optional CandleMonitor node component of IBM Tivoli OMEGAMON XE for Messaging has been placed in the message flow. For more information about installing and using the CandleMonitor node in message flows, see the *WebSphere Message Broker Monitoring User's Guide* (SC32-1827) in the documentation library for IBM Tivoli OMEGAMON XE for Messaging.

When both monitoring agents are installed on a managed system and are monitoring the same message flows, you can use a workspace link from the Services Inventory view to the Message Flow Statistics workspace for the selected message flow. The workspace is automatically filtered to the correct message flow. If multiple message broker instances are defined, you are prompted to choose the appropriate broker from a selection list. Figure 1 and Figure 2 on page 41 show an example of displaying message broker data in both product workspaces.

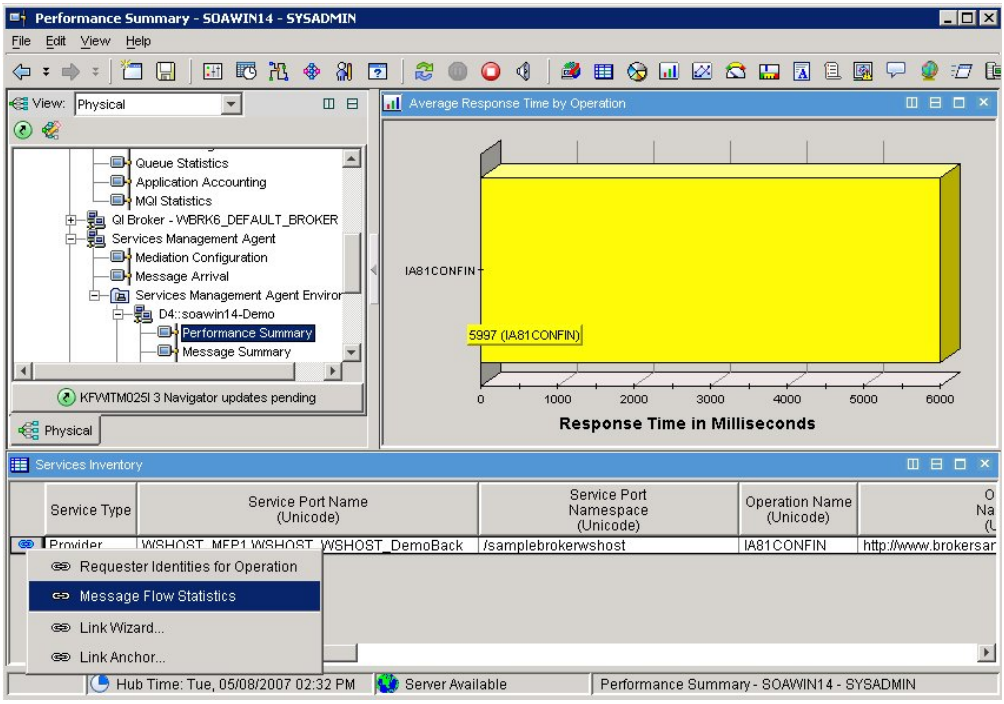


Figure 1. Linking from the Performance Summary workspace to the OMEGAMON XE for Messaging product

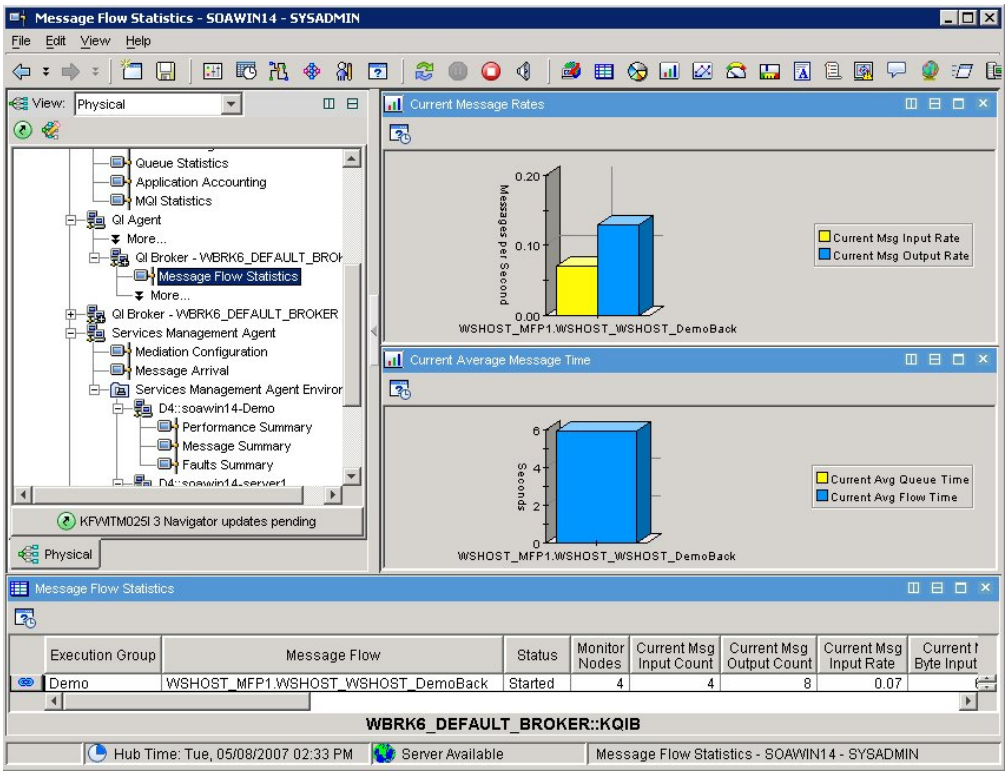


Figure 2. The Message Flow Statistics workspace in IBM Tivoli OMEGAMON XE for Messaging

This workspace link is available only after you enable the function in your ITCAM for SOA v6.1 environment. For more information on running the KfwSQLClient command to enable this new function in the Tivoli Enterprise Portal, see “Adding new workspaces, views, and linking” on page 15.

Once enabled, this new workspace link is defined only for rows in the Services Inventory table that represent WebSphere Message Broker services (message flows). This workspace link is not available for rows in the Services Inventory table that represent services in other application server runtime environments. Selecting this workspace link sends you to the Message Flow Statistics workspace of the IBM Tivoli OMEGAMON XE for Messaging product. Data displayed in this workspace corresponds to the message flow that handles the *request* message for the WebSphere Message Broker service. The message flow that handles service response messages is not supported by this workspace link function.

Using the portal server on Linux and the browser client on Windows

If you are running with IBM Tivoli OMEGAMON XE for Messaging v6.0 support files installed in a Tivoli Enterprise Portal Server on a Linux operating system, and you attempt to use the Tivoli Enterprise Portal browser client on a Windows operating system, there is a known problem that causes the browser client to suspend operation while attempting to log in to the portal server.

See the IBM Product Support Web Site for a technote with more information on this problem.

Limitations

The following limitations apply to using these workspace links with respect to the target message broker:

- The filter specified when the workspace link is taken does not include the name of the target message broker because the link can fail if you are using alias names for the message broker nodes.
- If on the same machine ITCAM for SOA v6.1.0 is monitoring message flows in one message broker, and IBM Tivoli OMEGAMON XE for Messaging is monitoring a different message broker, this workspace link takes you to the only available IBM Tivoli OMEGAMON XE for Messaging Message Flow Statistics workspace, even though it is displaying data for a different message broker. That message broker will not include any of the SOA message flows of interest.

Chapter 6. Monitoring by Web service requesters

Typical views displayed in the Tivoli Enterprise Portal for IBM Tivoli Composite Application Manager for SOA show metric data that is aggregated by each service and operation name pair, without regard for the specific source (the end user or business partner) from which the request for the service and operation originated. These origin points, also referred to as *Web services requesters*, can be tracked and monitored for the quality of the service being requested.

This additional level of end-to-end monitoring of Web services helps you to verify that service expectations are being provided to end users and business partners. This fix pack introduces the capability to configure monitoring for one or more *requester identities*, and to display metric data for each monitored combination of service, operation, and requester identity. This data is displayed in a new set of predefined Tivoli Enterprise Portal workspaces and views. These new views, similar to those in the Performance Summary and Message Summary workspaces, show metric data and relationships broken down by requester identity within a particular service and operation pair.

Though there are several ways to identify the origin of a Web services request, for this fix pack only the *security principal* (the user ID with which the requester authenticated, for example, *joe@us.ibm.com*) is supported, and only for supported IBM WebSphere Application Server environments. The WebSphere data collector obtains the identity of the user associated with the request from the WebSphere authentication subsystem.

Several new Take Action commands are also included in the fix pack that you can use to add requester identities to a list that you want to monitor, to enable or disable the monitoring function for all of the requester identities in the list, and to remove requester identities from the list when you no longer want to monitor them. These new Take Action commands are described in “Configuring Requester Identities” on page 49.

Enabling new workspaces, views, and Take Actions: After installing the post-GA function as part of the fix pack, these new workspaces, views, and Take Action commands are not available until you enable these functions by running an additional manual command. For more information, see “Adding new workspaces, views, and linking” on page 15.

Workspaces and views for monitoring requester identities

This section describes the workspaces and views that are provided with Fix Pack 1 to support configuring and monitoring of requester identities.

Requester Identity Monitoring Configuration workspace

Use the Requester Identity Monitoring Configuration workspace to create a list of all of the requester identities to be monitored. You can use Take Action commands to add requester identities to the list or remove them from the list, and you can turn on or turn off data collection for all of the requester identities in the list at any time.

To access this workspace from the Physical Navigator view, right-click the **Services Management Agent** workspace node and select **Workspace –> Requester Identity Monitoring Configuration**, as shown in Figure 3 on page 44.

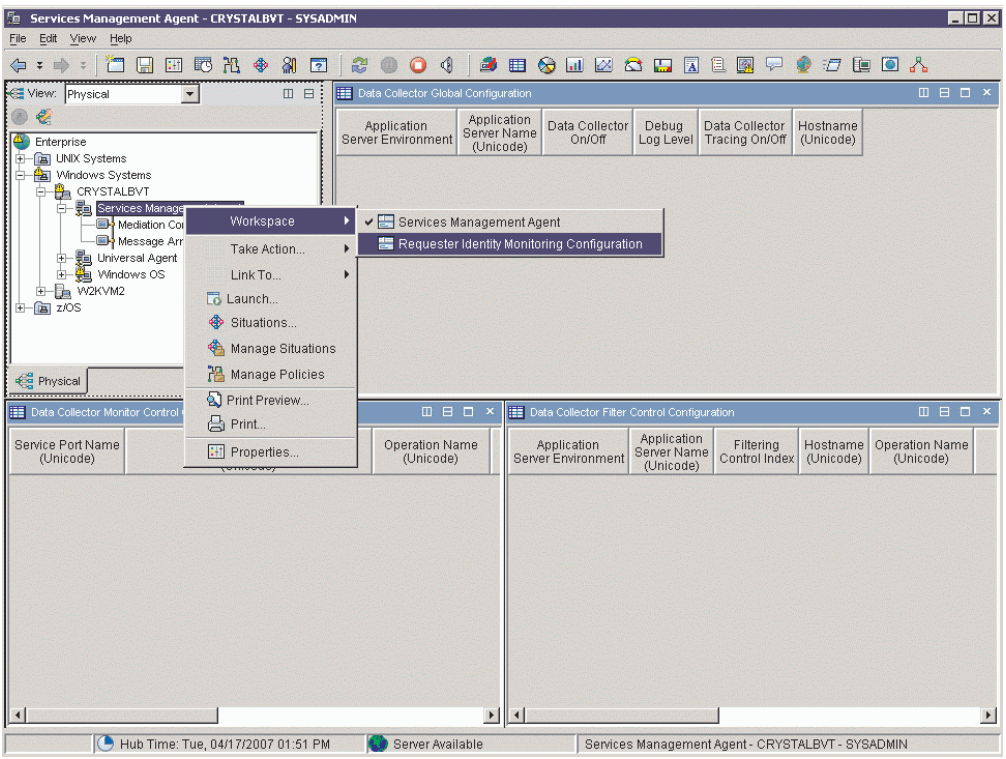


Figure 3. Accessing the Requester Identity Monitoring Configuration workspace from the Services Management Agent workspace node

An example of this predefined workspace is shown in Figure 4 on page 45. This workspace contains the following information:

- **Requester Identity Monitoring Status table view**

  This single column view displays a single property setting of *On* or *Off* to indicate whether data collection is enabled or disabled for all requester identities that are displayed in the Monitored Requester Identities table view. The default setting is *Off*.

  Use these Take Action commands to turn on or turn off your requester identity monitoring configuration property settings:

  – EnableReqIDMntr_610
  – DisableReqIDMntr_610

  For more information on these Take Action commands, see “Configuring Requester Identities” on page 49.

- **Monitored Requester Identities table view**

  This single column view displays the list of requester identities that are being monitored for data collection and aggregation when the property setting is turned on or enabled. If a row in the Requester Identity (Unicode) column contains the asterisk (*) wild card character, all requester identities are monitored for each unique combination of service port and operation name. Initially this table is empty, signifying that no requester identities are configured to be monitored.

  Using the asterisk (*) wild card: Be aware that with a large number of unique requester identities, usage of this wild card character can result in a large amount of data collected.

  Use these Take Action commands to add a requester identity to the list of monitored identities, or to remove a requester identity from the list:

  – AddRequesterIdentity_610

– DeleteRequesterIdentity_610

For more information on these Take Action commands, see “Configuring Requester Identities” on page 49.

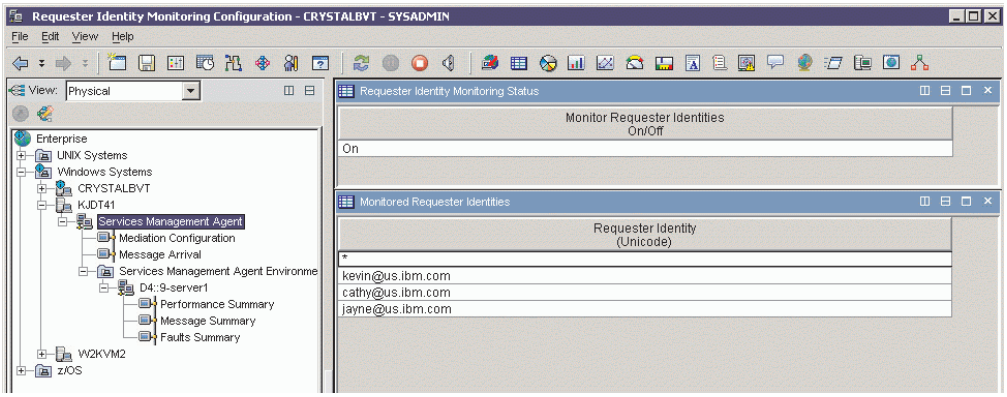


Figure 4. The Requester Identity Monitoring Configuration workspace

Requester Identities for Operation workspace

In IBM Tivoli Composite Application Manager for SOA V6.1.0, the Services Inventory table view in the Performance Summary workspace displays metric data that is aggregated for each unique combination of service port name and operation name. These aggregated metrics are generated from monitored service requests that originate from one or more different sources, or requesters. While viewing the data displayed in the Services Inventory table view, you cannot readily distinguish the metric data associated with a single requester for a particular service and operation pair.

Fix Pack 1 provides additional capability so that you can add one or more requester identities to the list in the Requester Identity Monitoring Configuration workspace, and turn on monitoring for all of the specified requester identities (see “Requester Identity Monitoring Configuration workspace” on page 43). When message traffic originating from those monitored requester identities is observed by the data collector, the aggregated metric data is displayed in the Services Inventory table view. You can then right-click a row in the Services Inventory table view that represents a specific service and operation pair for which requester identities are being monitored, and then select the **Link To –> Requester Identities for Operation** workspace link to dynamically link to the Requester Identities for Operation workspace.

Alternatively, you can click the row link indicator for the selected row in the Services Inventory table view and select **Requester Identities for Operation**, similar to the example shown in Figure 5 on page 46.

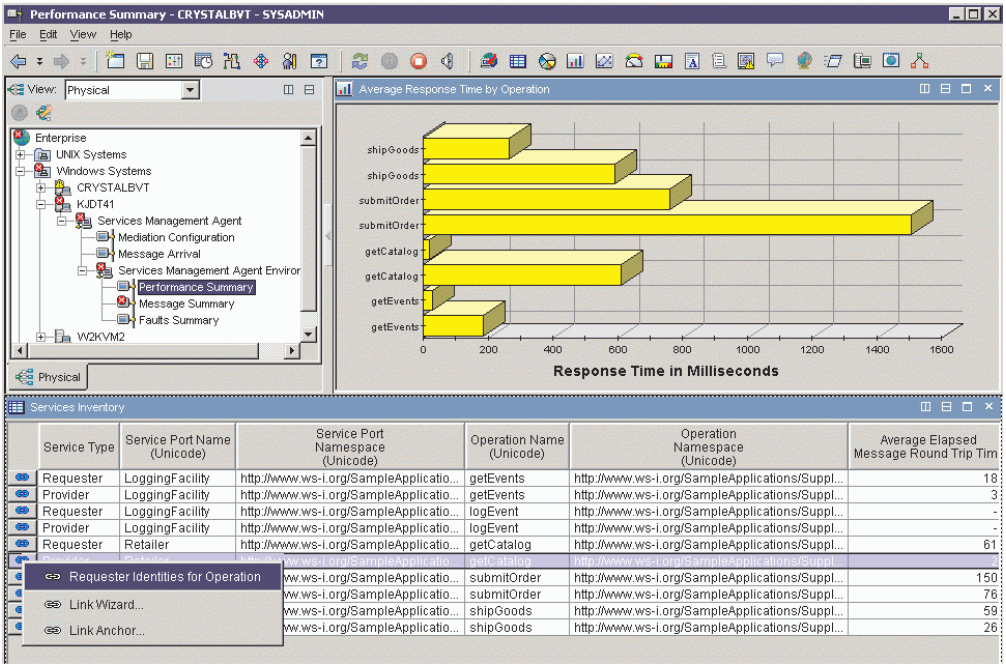


Figure 5. Accessing the Requester Identities for Operation workspace from the Services Inventory table view by link row indicator

The Requester Identities for Operation workspace, similar to the example in Figure 6, shows the aggregated metric data for each unique combination of service, operation, and requester identity. This workspace displays another table view, similar to the Services Inventory table view, that includes an additional column identifying the unique requester identities that are associated with the selected row from the Services Inventory table view. This table view displays the set of monitored requester identities that requested the specified service and operation pair.

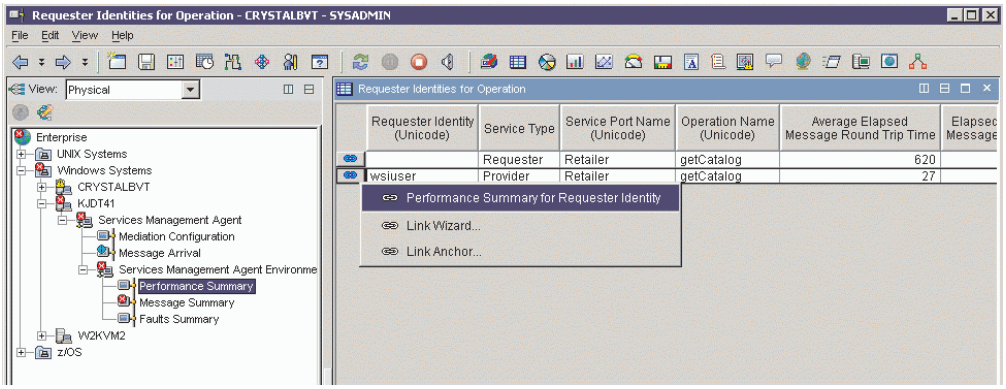


Figure 6. The Requester Identities for Operation workspace

Using this workspace, you can examine the metrics and relationships by requester identity for a specific service and operation pair.

From this workspace, you can also select a specific requester identity and then link to the Performance Summary for Requester Identity workspace, which shows table and bar chart views of message size, round trip response time, message counts, and fault counts for the selected requester identity. To access further information about the metric data for a particular requester identity, right-click a row in the

Requester Identities for Operation table view and select **Link To –> Performance Summary for Requester Identity** (or select the workspace link icon as shown in Figure 6 on page 46 and select the **Performance Summary for Requester Identity** link). For more information, see “Performance Summary for Requester Identity workspace.”

You can add or delete entries to the list of monitored requester identities by using the AddRequesterIdentity_610 or DeleteRequesterIdentity_610 Take Action commands, and enable and disable monitoring of all of the requester identities in the list using the EnableReqIDMntr_610 and DisableReqIDMntr_610 Take Action commands. For more information, see “Configuring Requester Identities” on page 49.

Performance Summary for Requester Identity workspace

The Performance Summary for Requester Identity workspace provides a table view and bar charts that display the Web services activity for a specific requester identity associated with a particular combination of service port and operation. This workspace is not displayed on the Navigator Physical view and is accessible only by using a workspace link from a row in the Requester Identities for Operation view table within the Requester Identities for Operation workspace (for more information, see “Requester Identities for Operation workspace” on page 45). An example of this workspace is shown in Figure 7. The requester identity for which data is being displayed is included in the view titles for each view in this workspace.

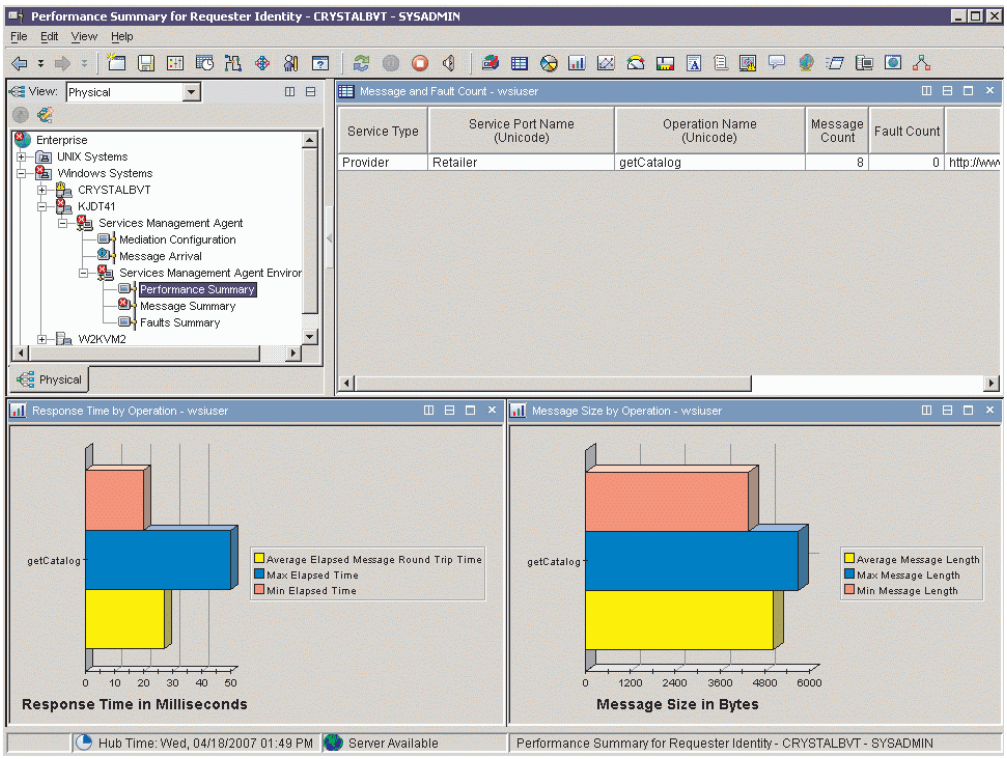


Figure 7. The Performance Summary for Requester Identity workspace

You can access this workspace by traversing several workspace links from the Services Inventory table of the Performance Summary workspace:

1. In the Services Inventory table view, right click a row, and select **Link To –> Requester Identities for Operation** or click the row link indicator and select **Requester Identities for Operation**.
2. In the Requester Identities for Operation table view, right-click a requester identity row and select **Link To –> Performance Summary for Requester Identity** or click the row link indicator.

This predefined workspace contains the following information:

- **Message and Fault Count table view**

  This view displays the number of messages and faults reported for the specified combination of service and operation twice: once for the provider, and once for the requester. This table view is an aggregate view of the most recent sampling interval.

  When the monitoring agent is first started, at least one 5 minute interval must be completed before any data is displayed in the view. After the first 5 minute interval is complete, this table view shows the number of messages and faults by service and operation combination for all Web services within the 5 minute time interval. If the Web service has no traffic during the time interval, then a zero is displayed.

- **Response Time by Operation bar chart**

  This view displays the average, minimum and maximum response time, in milliseconds, for the specified combination of service port and operation name, with the message being intercepted as it leaves the server or as the client responds. This bar chart shows each operation twice: once for the provider, and once for the requester. The data displayed is for the most recently completed 5 minute interval.

  When the monitoring agent is first started, at least one 5 minute interval must be completed before any data is displayed in the view. After the first 5 minute interval is complete, this bar chart shows the average response time for all services that had a valid average response time within the interval. If the Web service has no traffic during the interval, then the average response time is indicated with a value of *-1* and is not included in the bar chart.

- **Message Size by Operation bar chart**

  This view displays the average, minimum and maximum message size, in bytes, of messages received for the specified combination of service port and operation name. This bar chart shows each operation twice: once for the provider, and once for the requester.

  When the monitoring agent is first started, at least one 5 minute interval must be completed before any data is displayed in the view. After the first 5 minute interval is complete, this bar chart shows the average message size for all Web services within the 5 minute time interval. If the Web service has no traffic during the time interval, then the average message size is indicated with a value of *-1* and is not included in the bar chart.

Note: For this version, the labels on the bar charts contain only the operation portion of the combination of service port name, operation name, and message type.

Configuring Requester Identities

Fix Pack 1 provides several Take Action commands that you can use to define the list of requester identities to be monitored, and turn on or turn off monitoring on the entire list of requester identities. These Take Action commands are described in the following sections:

- "AddRequesterIdentity_610 (Add a requester identity to the list of identities to be monitored)"
- "DeleteRequesterIdentity_610 (Delete a requester identity from the list of identities to be monitored)" on page 50
- "EnableReqIDMntr_610 (Enable data collection by requester identity)" on page 51
- "DisableReqIDMntr_610 (Disable data collection by requester identity)" on page 52

These Take Action commands are included in the list of available commands, similar to the example shown in Figure 8.

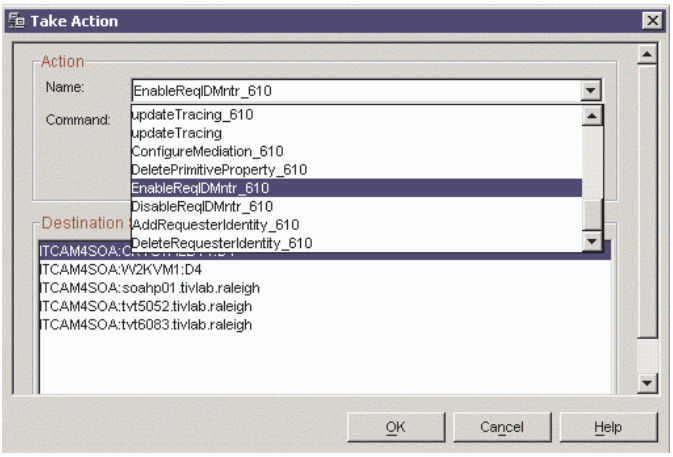


Figure 8. Available Take Action commands

AddRequesterIdentity_610 (Add a requester identity to the list of identities to be monitored)

Use the AddRequesterIdentity_610 action to add a specific Web services requester identity to a list of requester identities to be monitored.

The Web services requester identity is displayed in the Monitored Requester Identities view of the Requester Identity Monitoring Configuration workspace. For more information, see "Requester Identity Monitoring Configuration workspace" on page 43.

Command

To run the AddRequesterIdentity_610 action, complete the following steps:

1. From the Tivoli Enterprise Portal, navigate to the Services Management Agent workspace.
2. Right-click the Services Management Agent node and select **Workspace –> Requester Identity Monitoring Configuration**.
3. In the Monitored Requester Identities view, right-click anywhere in the table and select **Take Action –> Select** to display the Take Action window.

4. Under Action, click the **Name** field to display the list of available actions for this agent.
5. From the list of available actions, click AddRequesterIdentity_610.
6. The **Command** field is filled in with the command syntax. The Edit Argument Values window opens.
7. In the **ReqID_Mntr_Ctrl_610.Requester_Identity_U** argument field, enter the name of the requester identity to be monitored (for example, *joe@us.ibm.com*).

   Note: The capitalization and spacing of the Requester Identity argument must match the way that this string is returned by the monitored runtime environment. You might want to monitor all requester identities using the wildcard asterisk (*) character for a short time, or in a test environment to confirm the spacing and capitalization of your requester identities, then use this Take Action again to specify the precise format of the requester identity name.
8. After editing the argument, click **OK**. The Edit Argument Values window closes, and you are returned to the Take Action window, with the entered monitor criteria now included in the **Command** field.
9. The **Destination System(s)** field contains one or more target systems where you can send the command. Click the desired system name and then click **OK**.
10. The Action Status window displays with the resulting return code. Click **OK** to close the window. The Take Action window also closes.

Arguments

Table 4 describes the arguments that you can specify for this Take Action command:

Table 4. Arguments for the AddRequesterIdentity_610 Take Action command

Name	Value
ReqID_Mntr_Ctrl_610.Requester_Identity_U	The requester identity that you are adding or including to the list of identities. The asterisk (*) wild card character indicates that all requester identities can be monitored.

Return Codes

When you run the Take Action command, you might receive one of the following return codes:

- 0 = The action completed successfully and the requester identity was added to the list of identities to be monitored.
- 2 = The action completed unsuccessfully. The list of requester identities that are being monitored is not changed.

DeleteRequesterIdentity_610 (Delete a requester identity from the list of identities to be monitored)

Use the DeleteRequesterIdentity_610 action to delete a specific Web services requester identity from the list of identities to be monitored.

The Web services requester identity is displayed in the Monitored Requester Identities view of the Requester Identity Monitoring Configuration workspace. For more information, see “Requester Identity Monitoring Configuration workspace” on page 43.

Command

To run the DeleteRequesterIdentity_610 action, complete the following steps:

1. From the Tivoli Enterprise Portal, navigate to the Services Management Agent workspace.
2. Right-click the Services Management Agent node and select **Workspace –> Requester Identity Monitoring Configuration**.
3. In the Monitored Requester Identities view, select the identity row, right-click, and select **Take Action –> Select** to display the Take Action window.
4. Under Action, click the **Name** field to display the list of available actions for this agent.
5. From the list of available actions, click DeleteRequesterIdentity_610.
6. The **Command** field is filled in with the command syntax and the requester identity value from the command row that you selected.
7. The Edit Argument Values window is pre-filled with the name of the requester identity that you selected. Click **Arguments** to change the requester identity. Click **OK** to remove the requester identity from the list. The Edit Argument Values window is closed, and you are returned to the Take Action window, with the entered monitor criteria now included in the **Command** field.
8. The **Destination System(s)** field contains one or more target systems where you can send the command. Click the desired system name and then click **OK**.
9. The Action Status window displays with the resulting return code. Click **OK** to close the window. The Take Action window also closes.

Arguments

Table 5 describes the arguments that you can specify for this Take Action command:

Table 5. Arguments for the DeleteRequesterIdentity_610 Take Action command

Name	Value
ReqID_Mntr_Ctrl_610.Requester_Identity_U	The requester identity that you are deleting from the list of identities.

Return Codes

When you run the Take Action command, you might receive one of the following return codes:

- 0 = The action completed successfully and the requester identity was removed from the list of identities that are being monitored.
- 1 = The action completed unsuccessfully because the requester identity that you selected or specified was not found in the list of identities that are being monitored. The list of requester identities that are being monitored is not changed.
- 2 = The action completed unsuccessfully. The list of identities that are being monitored is not changed.

EnableReqIDMntr_610 (Enable data collection by requester identity)

Use the EnableReqIDMntr_610 action to enable (turn on) the aggregation of data collection by requester identity for all of the Web services requester identities that you want to monitor.

The requester identity monitoring status (*On* or *Off*) is displayed in the Requester Identity Monitoring Status view of the Requester Identity Monitoring Configuration workspace. For more information, see “Requester Identity Monitoring Configuration workspace” on page 43.

Command

To run the EnableReqIDMntr_610 action, complete the following steps:

1. From the Tivoli Enterprise Portal, navigate to the Services Management Agent workspace.
2. Right-click the Services Management Agent node and select **Workspace –> Requester Identity Monitoring Configuration**.
3. In the Requester Identity Monitoring Status view, right-click anywhere in the table and select **Take Action –> Select** to display the Take Action window.
4. Under Action, click the **Name** field to display the list of available actions for this agent.
5. From the list of available actions, click EnableReqIDMntr_610.
6. The **Destination System(s)** field contains one or more target systems where you can send the command. Click the desired system name and then click **OK**.
7. The Action Status window displays with the resulting return code. Click **OK** to close the window. The Take Action window also closes.

Arguments

There are no arguments that you can specify for this Take Action command.

Return Codes

When you run the Take Action command, you might receive one of the following return codes:

- 0 = The action completed successfully and requester identity monitoring was enabled.
- 2 = The target agent does not support this command.

DisableReqIDMntr_610 (Disable data collection by requester identity)

Use the DisableReqIDMntr_610 action to disable (turn off) the aggregation of data collection by requester identity for all of the requester identities that are being monitored.

The requester identity monitoring status (*On* or *Off*) is displayed in the Requester Identity Monitoring Status view of the Requester Identity Monitoring Configuration workspace. For more information, see “Requester Identity Monitoring Configuration workspace” on page 43.

Command

To run the DisableReqIDMntr_610 action, complete the following steps:

1. From the Tivoli Enterprise Portal, navigate to the Services Management Agent workspace.
2. Right-click the Services Management Agent node and select **Workspace –> Requester Identity Monitoring Configuration**.
3. In the Requester Identity Monitoring Status view, right-click anywhere in the table and select **Take Action –> Select** to display the Take Action window.
4. Under Action, click the **Name** field to display the list of available actions for this agent.
5. From the list of available actions, click DisableReqIDMntr_610.

6. The **Destination System(s)** field contains one or more target systems where you can send the command. Click the desired system name and then click **OK**.
7. The Action Status window displays with the resulting return code. Click **OK** to close the window. The Take Action window also closes.

Arguments

There are no arguments that you can specify for this Take Action command.

Return Codes

When you run the Take Action command, you might receive one of the following return codes:

- 0 = The action completed successfully and requester identity monitoring was disabled.
- 2 = The target agent does not support this command.

Appendix. Notices

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

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

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

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

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, 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 (I) 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.

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.

Trademarks

AIX, DataPower, DB2, IBM, the IBM logo, OMEGAMON, pSeries, Tivoli, Tivoli Enterprise, WebSphere, zSeries, and z/OS are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

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

Intel and Itanium are registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

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

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

Printed in USA