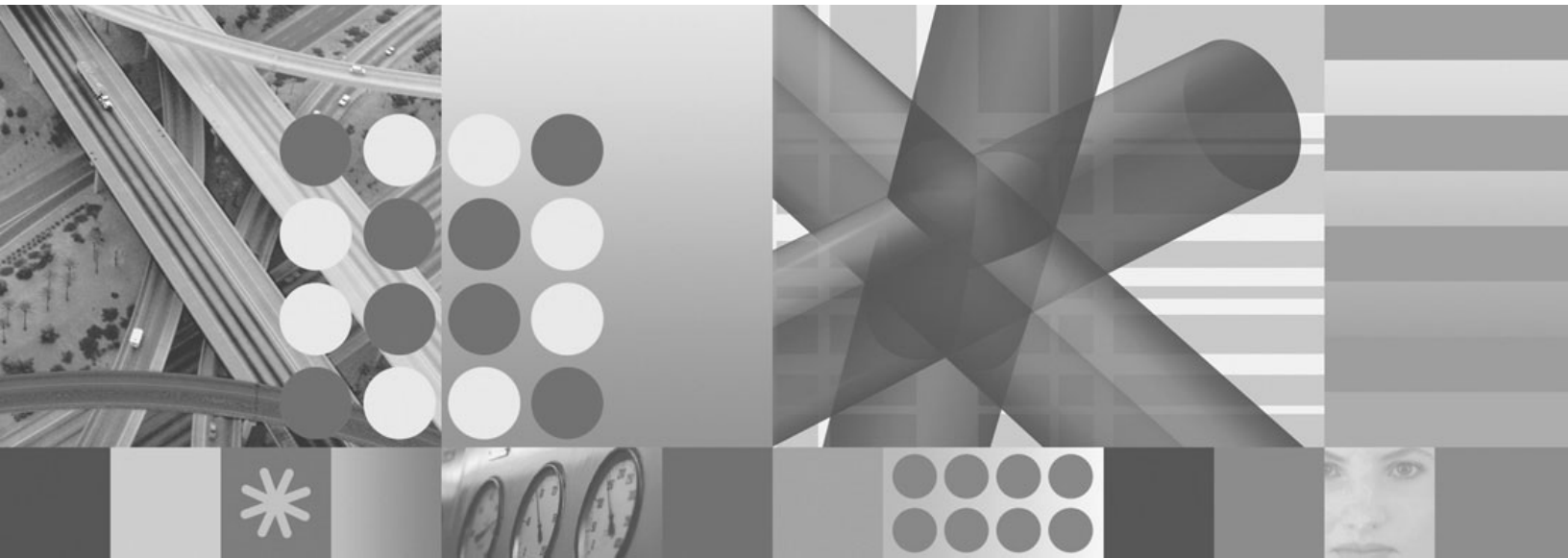




Installation and User's Guide



Installation and User's Guide

Note

Before using this information and the product it supports, read the information in Appendix C, "Notices," on page 83.

First Edition (June 2006)

This edition applies to Sparkler 2 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.

© Copyright International Business Machines Corporation 2006. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Tables	vii
Chapter 1. Overview	1
Linux operating system support	2
What is included in Sparkler 2?	2
Related publications	3
Support information.	4
Chapter 2. Installing Sparkler 2	5
Installing Sparkler 2	6
Installing support for Tivoli Enterprise Portal Server	6
Installing support for Tivoli Enterprise Monitoring Server	7
Installing support for Tivoli Enterprise Portal.	8
Installing data collector support	8
Chapter 3. The JBoss data collector	11
Enabling applications for the data collector.	11
Disabling applications for the data collector	13
Additional considerations	13
Chapter 4. The SCA data collector	15
Enabling applications for the data collector.	15
Using the data collector in multiple environments	17
Monitoring controls	17
Communication between SCA modules on different application servers	17
Logging and Filtering.	18
Disabling applications for the data collector	18
Limitations	18
Chapter 5. The DataPower data collector	21
The DataPower data collector as a proxy	21
Planning for deployment	22
Aggregation	23
Deployment steps.	23
Configuring the DataPower appliance for monitoring	24
Enabling the XML Management Interface	24
Checking additional optional settings	24
Configuring a user account on the DataPower appliance	24
Configuring for data collection in the DataPower environment.	25
The DataPower configuration file	25
Running the KD4configDC command.	26
Specifying KD4configDC parameters	26
Creating node names in Tivoli Enterprise Portal	28
Examples of configuring for data collection.	29
Considerations for configuration of DataPower monitoring	30
Multiple connections to the same DataPower appliance	30
Restricting the list of domains being monitored	31
Separating and aggregating data with the <code>-displaygroup</code> parameter	31
Separating data by host name or display group	31
Separating data between domains by domain list	32
Aggregating data across multiple domains	32
Aggregating data across multiple domains under multiple nodes.	32
Aggregating data across all domains on a single host with multiple users	33

Aggregating data for a cluster of appliances	33
Additional considerations	34
Disabling the data collector	34
Communication between data collector and appliance	34
Optimizing performance	35
Limitations	35
Starting and stopping the data collector	35
Troubleshooting	36
Communication failures	36
Synchronizing time between computer systems	36
Password problems	36
Logging and Tracing	36
Launching the DataPower Web browser interface	37
Considerations when launching the DataPower WebGUI client	38
Chapter 6. The SAP NetWeaver data collector	43
Enabling the application for the data collector	44
Running the KD4configDC utility	47
Disabling the application for the data collector	49
Running the KD4configDC utility	49
Additional considerations	51
Chapter 7. The WebSphere Community Edition data collector	53
Enabling applications for the data collector.	53
Running the KD4configDC utility	54
Enabling applications manually	57
Disabling applications for the data collector	60
Running the KD4configDC utility	61
Disabling applications manually	64
Additional considerations	64
Chapter 8. Problem Determination	65
Running the KD4configDC utility	65
KD4configDC terminates with CTRL-C	65
Running multiple KD4configDC instances at the same time	65
The SAP NetWeaver environment	65
SAP applications disabled after changing the application directory	65
Fault code and string displayed as <i>unknown</i> in the Services Inventory table	66
The WebSphere CE environment	66
Multiple WebSphere CE server instances using the same port	66
Service name displayed as <i>unknown</i> in Tivoli Enterprise Portal	66
Appendix A. Messages	67
Appendix B. Obtaining IBM software support for IBM Tivoli Composite Application Manager for SOA	79
Searching knowledge bases	79
Searching the information center	79
Searching the Internet	79
Obtaining fixes	79
Receiving weekly support updates.	80
Contacting IBM Software Support	80
Determining the business impact	81
Describing problems and gathering information	82
Submitting problems	82

Appendix C. Notices	83
Trademarks	85
Index	87

Tables

1. DataPower key and value pairs for KD4configDC 27

Chapter 1. Overview

IBM® Tivoli® Composite Application Manager for SOA provides the management function for managing the services and mediations in a service oriented architecture (SOA) running on Web application servers and the IBM WebSphere Enterprise Service Bus (WESB). For supported environments, IBM Tivoli Composite Application Manager for SOA monitors and performs simple control of message traffic between Web services in the SOA. IBM Tivoli Composite Application Manager for SOA relies on a distributed network of data collectors to feed data into Tivoli Management Services for analysis and management.

IBM Tivoli Composite Application Manager for SOA works in concert with other products to support the logical services management layer in a complete SOA management solution, and to manage the resources that support the services and the IBM WebSphere Enterprise Service Bus.

IBM Tivoli Composite Application Manager for SOA focuses on discovery of services in a wide range of application server runtime environments that are most common in early SOA adoption projects, such as Microsoft .NET, BEA WebLogic Server, IBM WebSphere Application Server, and others. IBM Tivoli Composite Application Manager for SOA supports production IT environments, and status and situation generation.

IBM Tivoli Composite Application Manager for SOA is installed and operates within the management infrastructure of the Tivoli Management Services environment. The following list describes the primary components of IBM Tivoli Composite Application Manager for SOA:

- A *monitoring agent* that interacts with the managed application servers and infrastructure middleware to collect data, and store the data in a log file. The monitoring agent consists of the following sub-components:
 - An Intelligent Remote Agent (IRA)
 - One or more Data Collectors (DCs) that are installed locally on every application server runtime environment where Web services are to be managed. The data collector is the lowest-level component of the monitoring agent. This component is responsible for actually observing what is happening in the environment that it is designed to monitor. The data collected by the data collector is provided to the Data Collector Adapter through a log file on the monitored machine, for transmittal through the Tivoli Management Services infrastructure. Data collectors typically have access to the following types of information about the message traffic it monitors:
 - Source and destination (machine name, application server name, service name and operation name)
 - Whether the message is a request or a response
 - Interaction type (synchronous or asynchronous)
 - The association of a request to its response during an asynchronous interaction
 - The response time for the message
 - Whether or not the message generated a fault
 - Whether the message is a one-way or a two-way message
 - Optionally, the actual header and body content of the message itself
 - A Data Collector Adapter (DCA), used to communicate between the Data Collector and Intelligent Remote Agent. The Data Collector Adapter accesses

the data stored in the log file by the data collector, and stores data collector configuration data in a configuration file that is accessed by the data collectors on each managed system.

- A set of management data using logical table constructs.
- A set of queries and commands

IBM Tivoli Composite Application Manager for SOA can also process correlation information from the message traffic to create pattern and sequence views in the IBM Web Services Navigator, a separate tool provided with IBM Tivoli Composite Application Manager for SOA.

IBM Tivoli Composite Application Manager for SOA provides basic control of message traffic, including the logging of messages and filtering messages based on criteria that you can configure (machine name, service name, operation name, and IP address of the requester).

Linux operating system support

In addition to the operating system platforms supported by IBM Tivoli Composite Application Manager for SOA v6.0, additional support for Linux[®] operating systems is available through the installation of the IBM Tivoli Composite Application Manager for SOA v6.0 Linux Platforms Media Delivery Pack. This additional function provides support for running IBM Tivoli Composite Application Manager for SOA in all supported application server runtime environments on Linux operating systems. If you plan to install Sparkler 2 on a supported Linux operating system, you must first install this Media Delivery Pack on top of the base IBM Tivoli Composite Application Manager for SOA product.

See the IBM Passport Advantage[®] Web site for more information on obtaining and installing this Media Delivery Pack for Linux operating system support:

http://www-306.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm

What is included in Sparkler 2?

Version 6.0 of IBM Tivoli Composite Application Manager for SOA provides support for monitoring and simple control of Web services running in IBM WebSphere Application Server, BEA WebLogic Server and Microsoft .NET. This support includes a set of data collectors within the OMEGAMON[®] infrastructure, taking advantage of functions available in the Tivoli Enterprise Portal. These data collectors also operate in the IBM Tivoli Monitoring v6.1 infrastructure.

A *Sparkler* is an IBM delivery mechanism used to include additional features in a current product release. This document describes the installation and operation of the additional features included in Sparkler 2 for IBM Tivoli Composite Application Manager for SOA v6.0. Sparkler features are provided with limited function.

Previously, an earlier Sparkler, called *Sparkler 1*, was made available, and included the following features added to the base product:

- Support for JAX-RPC Web services running in the JBoss 4.0.3 application server runtime environment.
- Instrumentation and monitoring support for the Services Component Architecture (SCA) infrastructure of IBM WebSphere Process Server and IBM WebSphere Enterprise Service Bus.

- Monitoring support for Web service flows through a DataPower appliance acting as a proxy between the Web service client and server.

Sparkler 2 includes all of the function provided in Sparkler 1, in addition to the following new features being added to IBM Tivoli Composite Application Manager for SOA v6.0:

- Support for Web services running in the SAP NetWeaver 6.40 application server runtime environment.
- Support for JAX-RPC Web services running in the WebSphere Community Edition (CE) application server runtime environment.
- The ability to launch the DataPower Web browser based user interface from a row in the Services Inventory table to configure the DataPower appliance.

With Sparkler 2, the data collectors for IBM Tivoli Composite Application Manager for SOA support these application server runtime environments with functions similar to those environments supported in the base v6.0 product. Data from these environments are displayed as additional environment types in Tivoli Enterprise Portal workspaces and views, with the following limitations:

- The SCA data collector does not provide the same level of functionality as other data collectors.
- SCA data is displayed in the same set of existing workspaces and views as the IBM WebSphere Application Server data collector.
- The DataPower data collector does not provide any filtering capabilities.
- There is no support in the IBM Web Services Navigator for the DataPower and SCA data collectors.

The rest of this document describes the procedure for installing Sparkler 2 and provides more information on configuring and enabling the applications for these data collectors to run in these new application server runtime environments.

Related publications

This section lists publications in the IBM Tivoli Composite Application Manager for SOA library. Refer to this documentation for more information about the base product for this Sparkler 2, and for additional information on how to access IBM Tivoli publications online and how to order IBM Tivoli publications.

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

- *IBM Tivoli Composite Application Manager for SOA Release Notes*, GI11-4096
Contains late-breaking information about IBM Tivoli Composite Application Manager for SOA product limitations and workarounds, and pointers to other documentation to help you begin installing and using the product.
- *IBM Tivoli Composite Application Manager for SOA Installation and User's Guide*, GC32-9492

Provides an overview of the Tivoli Management Services environment and the planning information and procedures you need to install and configure the IBM Tivoli Composite Application Manager for SOA monitoring agent. This guide also provides use information on monitoring and managing resources with IBM Tivoli Composite Application Manager for SOA. This guide also provides troubleshooting information about the various components of IBM Tivoli Composite Application Manager for SOA, as well as information about log files and informational, warning, and error messages.

- *Configuring IBM Tivoli Composite Application Manager for SOA on z/OS®*, SC32-9493

Provides information about configuring IBM Tivoli Composite Application Manager for SOA to operate in the z/OS operating system environment. Before using this publication, you must complete the installation procedures as documented in the *Program Directory for IBM Tivoli Composite Application Manager for SOA, V6.0, Program Number 5698-A77, for Use with z/OS*, G111-4100. This publication is written for system administrators and others who are responsible for installing and configuring IBM Tivoli Composite Application Manager for SOA in the z/OS environment.

- *Installing and Troubleshooting IBM Web Services Navigator*, GC32-9494

Provides information about installing and using an Eclipse based plug-in for extracting Web services information that has been collected by IBM Tivoli Composite Application Manager for SOA data collectors and stored in a database, and displaying the data in several views to assist a Web services architect in visualizing relationships between services.

In addition to the documentation library for Release 1, see “Linux operating system support” on page 2 for more information about additional support provided in the Linux Platforms Media Delivery Pack, available on the IBM Passport Advantage Web site.

Support information

Appendix B, “Obtaining IBM software support for IBM Tivoli Composite Application Manager for SOA,” on page 79 describes the following options for obtaining support for IBM products:

- “Searching knowledge bases” on page 79
- “Obtaining fixes” on page 79
- “Contacting IBM Software Support” on page 80

You can find specific support information for the IBM Tivoli Composite Application Manager for SOA product, its Sparklers and Technotes, on the product support Web site:

<http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliCompositeApplicationManagerforSOA.html>

Chapter 2. Installing Sparkler 2

The installation of Sparkler 2 involves downloading the required zipped packages from the product support Web site, and unpacking them into existing IBM Tivoli Composite Application Manager for SOA product directories, then configuring the Tivoli Enterprise Portal Server, Tivoli Enterprise Monitoring Server, and data collectors (for each supported platform) as needed.

Do you already have Sparkler 1 installed? If you already have Sparkler 1 installed over your base v6.0 product, you can install Sparkler 2 over Sparkler 1. If you do not already have Sparkler 1 installed, just install Sparkler 2 over the base v6.0 product, as it already includes all of the function provided with Sparkler 1.

This installation assumes that you have already successfully installed IBM Tivoli Composite Application Manager for SOA v6.0 in your Tivoli Management Services environment. See “Related publications” on page 3 for installation and configuration procedures.

Installing on Linux operating systems: If you are installing this Sparkler 2 on a supported Linux operating system, this installation also assumes that you have already installed the IBM Tivoli Composite Application Manager for SOA v6.0 Linux Platforms Media Delivery Pack for this support before installing this Sparkler. See “Linux operating system support” on page 2 for more information on this prerequisite.

Do you have a distributed installation? If so, install Sparkler 2 first on the computer system where Tivoli Enterprise Portal Server is installed, followed by the Tivoli Enterprise Monitoring Server system, and then the systems where data collectors are located.

Note that you do not need to reseed the Tivoli Enterprise Monitoring Server after installing Sparkler 2.

Are applications (or servers) for other data collectors already enabled? The computer system where you install Sparkler 2 might already have applications (or servers, depending on your environment) enabled for other IBM Tivoli Composite Application Manager for SOA data collectors. Any combination of supported IBM Tivoli Composite Application Manager for SOA environment types can coexist on a single system. You can enable applications (or servers) for as many environment types as you choose. Note that throughout this document we refer to enabling applications for the data collector, but for environments such as WebSphere, assume we are referring to enabling the server.

Re-enable existing applications after installing: Due to shared code between the data collector environments supported with this Sparkler 2 and other environments supported with IBM Tivoli Composite Application Manager for SOA (IBM WebSphere Application Server, JBoss, and BEA WebLogic Server only), after installing this Sparkler, you must run the KD4configDC utility to disable and re-enable applications for these types of existing environments that are deployed on the same system, to ensure that the data collector is 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.

See the *IBM Tivoli Composite Application Manager for SOA Release Notes* and the ReadMe for the Linux patch for information on supported operating system platforms and other hardware and software requirements.

Installing Sparkler 2

Complete the following steps to install this Sparkler into your existing IBM Tivoli Composite Application Manager for SOA product environment:

1. This procedure assumes that you have already installed the base IBM Tivoli Composite Application Manager for SOA product in your Tivoli Management Services environment, with or without Sparkler 1 installed. See the publications provided with IBM Tivoli Composite Application Manager for SOA for more information.
2. If you are installing on a Linux operating system supported by the IBM Tivoli Composite Application Manager for SOA v6.0 Linux Platforms Media Delivery Pack, you should have already applied this media delivery pack to the base IBM Tivoli Composite Application Manager for SOA product. See the documentation provided with the delivery pack for more information.
3. The installation of Sparkler 2 involves downloading and unpacking a set of compressed files into the existing Tivoli Management Services environment. Follow your local enterprise procedures to backup the Tivoli Management Services environment prior to installing Sparkler 2 in case you need to restore your environment to the current state.
4. **Is a BEA WebLogic Server running?:** If you already have BEA WebLogic Server running on the same target computer system where you are installing this Sparkler, stop the BEA WebLogic Server before installing Sparkler 2.
5. **Is a DataPower proxy being used?:** If you already have a DataPower proxy running on the same target computer system where you are installing this Sparkler, stop the proxy before installing Sparkler 2.
6. If you are installing support for Tivoli Enterprise Portal Server, Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal, or data collector support on each computer system where Web services are to be monitored, see the sections that follow.

Installing support for Tivoli Enterprise Portal Server

To install support for Tivoli Enterprise Portal Server, complete the following steps:

1. Stop the Tivoli Enterprise Portal Server.
2. Download and unpack the appropriate compressed file package as follows:
 - For supported Windows® operating systems:
 - a. Locate and download the **6.0.0-TIV-ITCAMSOAS2_TEPS-WIN-FT002.zip** compressed file package to a temporary directory on the Tivoli Enterprise Portal Server computer system.
 - b. Unpack the files into the `<TMS_DIR>` directory, where `<TMS_DIR>` is the directory where Tivoli Management Services is installed (for example, `C:\ibm\itm` or `C:\Candle` on Windows). The files will be unpacked into their correct location in the `\CNPS` subdirectory.
 - For supported Linux operating systems:
 - a. Locate and download the **6.0.0-TIV-ITCAMSOAS2_TEPS-UNIX-FT002.tar.gz** compressed file package to a temporary directory `<TEMP_DIR>` on the Tivoli Enterprise Portal Server computer system.
 - b. Unpack the compressed file package with the following command:

```
gzip -d 6.0.0-TIV-ITCAMSOAS2_TEPS-UNIX-FT002.tar.gz
```


- c. Navigate to the `$CANDLE_HOME/li6243` directory where Tivoli Enterprise Portal Server is installed.
 - d. Verify that there is a subdirectory named `/cq` in this directory.
 - e. Run the following command:


```
tar -xvf <TEMP_DIR>/6.0.0-TIV-ITCAMSOAS2_TEPS-UNIX-FT002.tar
```
3. Navigate to the CNPS directory and run the `InstallPresentation.bat` (or, for Linux operating systems, `InstallPresentation.sh`) script to install updates to the IBM Tivoli Composite Application Manager for SOA presentation definitions for the Tivoli Enterprise Portal Server:
 - Open the Manage Tivoli Enterprise Monitoring Services console and verify that the Tivoli Enterprise Portal Server is running.
 - For supported Windows operating systems, do the following:
 - a. From a command line, navigate to the `%CANDLE_HOME%\CNPS` directory and issue the following command:


```
InstallPresentation.bat
```
 - For supported Linux operating systems, navigate to the `/bin` folder in the IBM Tivoli Monitoring home directory (`/opt/IBM/ITM/bin`), and issue the following command:


```
./CandleExecute cq InstallPresentation.sh
```
 4. Restart the Tivoli Enterprise Portal Server.

Installing support for Tivoli Enterprise Monitoring Server

To install support for Tivoli Enterprise Monitoring Server, complete the following steps:

1. Stop the Tivoli Enterprise Monitoring Server.
2. Download and unpack the appropriate compressed file package as follows:
 - For supported Windows operating systems:
 - a. Locate and download the **6.0.0-TIV-ITCAMSOAS2_TEMS_CMS-WIN-FT002.zip** compressed file package to a temporary directory on the Tivoli Enterprise Monitoring Server computer system.
 - b. Unpack the files into the `<TMS_DIR>` directory, where `<TMS_DIR>` is the directory where Tivoli Management Services is installed (for example, `C:\ibm\itm` or `C:\Candle`). The files will be unpacked into their correct location in the `\CMS` subdirectory.
 - For supported AIX, Solaris, or Linux operating systems:
 - a. Locate and download the **6.0.0-TIV-ITCAMSOAS2_TEMS_CMS-UNIX-FT002.tar.gz** compressed file package to a temporary directory `<TEMP_DIR>` on the Tivoli Enterprise Monitoring Server computer system.
 - b. Unpack the compressed file package with the following command:


```
gzip -d 6.0.0-TIV-ITCAMSOAS2_TEMS_CMS-UNIX-FT002.tar.gz
```
 - c. Navigate to the `$CANDLE_HOME/tables/<TEMS_Server>` directory, where `<TEMS_Server>` is the name of the Tivoli Enterprise Monitoring Server.
 - d. Verify that there are subdirectories named `/ATTRIB` and `/RKDSCATL` under this subdirectory.
 - e. Run the following command:


```
tar -xvf <TEMP_DIR>/6.0.0-TIV-ITCAMSOAS2_TEMS_CMS-UNIX-FT002.tar
```
3. Restart the Tivoli Enterprise Monitoring Server.

Installing support for Tivoli Enterprise Portal

To install support for Tivoli Enterprise Portal, complete the following steps:

1. Stop the Tivoli Enterprise Portal desktop client.
2. Download and unpack the appropriate compressed file package as follows:
 - For supported Windows operating systems:
 - a. Locate and download the **6.0.0-TIV-ITCAMSOAS2_TEP-WIN-FT002.zip** compressed file package to a temporary directory on the Tivoli Enterprise Portal computer system.
 - b. Unpack the files into the *<TMS_DIR>* directory, where *<TMS_DIR>* is the directory where Tivoli Management Services is installed (for example, C:\ibm\itm or C:\Candle on Windows). The files will be unpacked into their correct location in the \CNP subdirectory.
 - For supported Linux operating systems:
 - a. Locate and download the **6.0.0-TIV-ITCAMSOAS2_TEP-UNIX-FT002.tar.gz** compressed file package to a temporary directory *<TEMP_DIR>* on the Tivoli Enterprise Portal computer system.
 - b. Unpack the compressed file package with the following command:

```
gzip -d 6.0.0-TIV-ITCAMSOAS2_TEP-UNIX-FT002.tar.gz
```
 - c. Navigate to the ITM home directory (for example, /opt/IBM/ITM) directory
 - d. Navigate to the operating system specific directory where the Tivoli Enterprise Portal is installed. For example, /li6243 for Tivoli Enterprise Portal running on Linux on an Intel processor.
 - e. Verify that there is a subdirectory named **/cj** in this directory.
 - f. Run the following command:

```
tar -xvf <TEMP_DIR>/6.0.0-TIV-ITCAMSOAS2_TEP-UNIX-FT002.tar
```
3. Restart the Tivoli Enterprise Portal.

Installing data collector support

To install data collector support on each computer system where services are to be monitored, or where the DataPower data collector proxy will be running (see Chapter 5, “The DataPower data collector,” on page 21 for more information), complete the following steps:

1. Use the Manage Tivoli Monitoring Services console to stop the IBM Tivoli Composite Application Manager for SOA service.
2. **Reminder:** If you have not already stopped an existing BEA WebLogic Server or DataPower proxy, do so now before unpacking the compressed file packages.
3. Download and unpack the appropriate compressed file package as follows:
 - For supported Windows operating systems, locate and download the **6.0.0-TIV-ITCAMSOAS2_DCA-WIN-FT002.zip** compressed file package to a temporary directory, and then unpack the files into the *<TMS_DIR>* directory. The files will be unpacked into their correct location in the \CMA subdirectory.
 - For supported AIX[®] operating systems, locate and download the **6.0.0-TIV-ITCAMSOAS2_DCA-AIX433-FT002.tar.gz** compressed file package to a temporary directory, and then unpack the files into the *<TMS_DIR>* directory. The files will be unpacked into their correct location in the /aix433 subdirectory.
 - For supported Solaris operating systems, locate and download the **6.0.0-TIV-ITCAMSOAS2_DCA-SOL283-FT002.tar.gz** compressed file

package to a temporary directory, and then unpack the files into the <TMS_DIR> directory. The files will be unpacked into their correct location in the /sol283 subdirectory.

- For supported Linux (on Intel®) operating systems, locate and download the **6.0.0-TIV-ITCAMSOAS2_DCA-LI6243-FT002.tar.gz** compressed file package to a temporary directory, and then unpack the files into the <TMS_DIR> directory. The files will be unpacked into their correct location in the /li6243 subdirectory.
 - For supported Linux (on z/OS) operating systems, locate and download the **6.0.0-TIV-ITCAMSOAS2_DCA-LS3243-FT002.tar.gz** compressed file package to a temporary directory, and then unpack the files into the <TMS_DIR> directory. The files will be unpacked into their correct location in the /ls3243 subdirectory.
4. If there are existing applications that are enabled for the IBM Tivoli Composite Application Manager for SOA data collector on these computer systems, re-enable them by completing the following basic steps:
 - a. Stop the applications servers that are currently enabled for the IBM Tivoli Composite Application Manager for SOA data collector.
 - b. Re-enable the application by running the KD4configDC utility (see the IBM Tivoli Composite Application Manager for SOA documentation for details).
 - c. Restart the application servers.
 5. Restart the IBM Tivoli Composite Application Manager for SOA service.

The chapters that follow describe the new data collector support provided with Sparkler 2.

Chapter 3. The JBoss data collector

This chapter describes the support for JAX-RPC Web services running in the JBoss Java™ 2 Enterprise Edition (J2EE) version 4.0.3 application server runtime environment.

Enabling applications for the data collector

To enable JBoss applications for the data collector, complete the following steps:

1. You should have already completed the installation procedure for installing Sparkler 2 in the existing IBM Tivoli Composite Application Manager for SOA environment on the computer where your JBoss application server is installed. See “Installing Sparkler 2” on page 6 for details.
 2. Optionally stop the JBoss application server before enabling the application for the data collector. You do not have to stop the application server before running the KD4configDC utility, but the data collector does not begin to collect data until after the JBoss application server is stopped and restarted. You might prefer to stop and restart the JBoss application server during off shift hours. Refer to your JBoss documentation for the specific procedure to stop the JBoss application server.
 3. Run the KD4configDC utility to enable the application for the data collector. When there are multiple server instances within the same JBoss application server runtime environment, you must run the KD4configDC utility for each instance. Run the KD4configDC utility as follows:
 - a. Depending on your operating system, navigate to one of the following locations:
 - For supported Windows operating systems, navigate to %CANDLE_HOME%\CMA\KD4\bin.
 - For supported AIX operating systems, navigate to \$CANDLEHOME/aix433/d4/KD4/bin.
 - For supported Solaris operating systems, navigate to \$CANDLEHOME/sol283/d4/KD4/bin.
 - For supported Linux (on Intel) operating systems, navigate to \$CANDLEHOME/li6243/d4/KD4/bin.
 - For supported Linux (on z/OS) operating systems, navigate to \$CANDLEHOME/ls3243/d4/KD4/bin.
 - b. Run the following command:
 - For supported Windows operating systems:
KD4configDC.bat -enable -env 4 <server configuration> <JBoss_Home>
 - For supported AIX, Solaris, and Linux operating systems:
KD4configDC.sh -enable -env 4 <server configuration> <JBoss_Home>
- In these commands, the following parameters are specified:
- <server configuration> is the type of JBoss application server to be configured. Valid values are:

default

This configuration type contains everything needed to run a standalone J2EE server.

all

This configuration type starts all available services, including the RMI/IIOP and clustering services, and the Web services deployer, which are not loaded in the *default* configuration.

A third possible configuration type, **minimal**, is not supported.

You can also create your own server configuration type by modifying the *default* or *all* types, or mixing and matching capabilities from either or both, and saving it as a new server configuration type name. You can then specify that new server configuration type in the KD4configDC utility.

- *<JBoss_Home>* is the directory path name where the JBoss application server is installed, for example, *C:\JBoss* on a Windows operating system (note that if this path name contains a blank space, the entire path is surrounded with quotation marks). If you have this directory path defined in the environment variable, *JBOSS_HOME*, then this parameter is optional.

Examples:

- `KD4configDC.bat -enable -env 4 default`

In this example, the **default** server configuration is used, and the *JBOSS_HOME* environment variable is used to specify the JBoss base installation directory. The command completes with a return code of 0.

- `KD4configDC.bat -enable -env 4 all C:\JBoss`

In this example, the **all** server configuration type is specified to enable monitoring for the JBoss configuration that has all services started. The JBoss base installation directory is explicitly specified, and because there are no blank spaces in the path, the argument can be specified without surrounding quotation marks.

- `KD4configDC.bat -enable -env 4 myConfig`

In this example, the user-customized server configuration type *myConfig* is specified, and the *JBOSS_HOME* environment variable is used by default to specify the JBoss base installation directory.

- `KD4configDC.bat -enable -env 4 default "C:\App Servers\JBoss"`

In this example, the JBoss base installation directory is specified explicitly, and because there is a blank space in the path, the argument is surrounded by quotation marks.

- `KD4configDC.sh -enable -env 4 all /opt/IBM/JBoss`

This example is for running KD4configDC on a supported AIX, Solaris, or Linux operating system.

You can issue the following command to view the online help for KD4configDC:

- For supported Windows operating systems:

```
KD4configDC.bat -h
```

- For supported AIX, Solaris, or Linux operating systems:

```
KD4configDC.sh -h
```

4. Restart the JBoss application server (refer to your JBoss documentation for the specific procedure). The data collector becomes active after the JBoss application server is restarted.

You only need to enable the JBoss application for the data collector once in the JBoss application server runtime environment. If you add new applications to the environment, the data collector begins monitoring the new applications automatically.

Disabling applications for the data collector

You can disable JBoss applications for the data collector using the KD4configDC utility as follows:

1. Optionally stop the JBoss application server.
2. Depending on your operating system, navigate to one of the following locations:
 - For supported Windows operating systems, navigate to %CANDLE_HOME%\CMA\KD4\bin.
 - For supported AIX operating systems, navigate to \$CANDLEHOME/aix433/d4/KD4/bin.
 - For supported Solaris operating systems, navigate to \$CANDLEHOME/sol283/d4/KD4/bin.
 - For supported Linux operating systems, navigate to \$CANDLEHOME/li6243/d4/KD4/bin.
3. Run the following command:
 - For supported Windows operating systems:

```
KD4configDC.bat -disable -env 4 <server configuration> <JBoss_Home>
```
 - For supported AIX, Solaris, and Linux operating systems:

```
KD4configDC.sh -disable -env 4 <server configuration> <JBoss_Home>
```
4. After the command completes, restart the JBoss application server.

The JBoss data collector continues to collect data until after the JBoss application server is restarted.

Additional considerations

As you enable and use the JBoss application for the data collector, keep in mind the following additional considerations:

- If the JBoss application server is stopped, you can successfully enable or disable the application for the data collector.
- If you attempt to enable or disable the application for the data collector multiple times in a row (for example, an enable followed by another enable), only the first invocation takes effect.

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 JBoss application server runtime environment.

Chapter 4. The SCA data collector

This chapter describes the support for configuring and monitoring the Service Component Architecture (SCA) infrastructure of IBM WebSphere Process Server and IBM WebSphere Enterprise Service Bus. Note that this Sparkler does not provide full data collector support for the SCA environment.

IBM WebSphere Process Server and IBM WebSphere Enterprise Service Bus introduce a new way to model services in an SOA, called the *Service Component Architecture* (SCA). SCA was designed to separate business logic from its implementation, so that you can focus on assembling an integrated application without knowing implementation details.

The Service Component Architecture is based on *SCA modules* and *SCA components*. An SCA module is made up of multiple SCA components. In IBM Tivoli Composite Application Manager for SOA, SCA components are treated as *services*.

With additional support for the IBM WebSphere Enterprise Service Bus and IBM WebSphere Process Server initially provided in Sparkler 1 and included in Sparkler 2, IBM Tivoli Composite Application Manager for SOA discovers information about when a message flows between SCA components.

The SCA data collector is installed and applications are configured once in the IBM WebSphere Process Server or IBM WebSphere Enterprise Service Bus environment. The data collector does not require each SCA application to be configured. When new SCA applications are added to the monitored environment, they are automatically monitored as well.

The SCA data collector supports both synchronous and asynchronous interactions flowing through the SCA application server runtime environment. Note that some asynchronous interactions between SCA components might result in requests or responses being reported multiple times or not at all. This is caused by thread switching in the SCA application server runtime environment and limitations of the SCA data collector in tracking flows across these thread switches. Monitoring of asynchronous interactions is provided in this Sparkler to give you a more complete picture of the services that exist in the environment, however you should not expect the metrics collected for asynchronous interactions to be precise.

Refer to your IBM WebSphere Integration Developer documentation for more information about these synchronous and asynchronous interactions.

Enabling applications for the data collector

To enable the SCA applications for the data collector, complete the following steps:

1. You should have already completed the installation procedure for installing Sparkler 2 in the existing IBM Tivoli Composite Application Manager for SOA environment on the computer where the IBM WebSphere Enterprise Service Bus and IBM WebSphere Process Server application server runtime environments are installed. See “Installing Sparkler 2” on page 6 for details.
2. Optionally stop the IBM WebSphere Enterprise Service Bus or IBM WebSphere Process Server application server before enabling applications for the data collector. You do not have to stop the application server before running the KD4configDC utility, but the data collector does not begin to collect data until after the application server is stopped and restarted. You might prefer to stop

and restart the application server during off shift hours. Refer to your WebSphere® documentation for the specific procedure to stop and restart the application server.

3. Run the KD4configDC utility as follows:
 - a. Depending on your operating system, navigate to one of the following locations:
 - For supported Windows operating systems, navigate to %CANDLE_HOME%\CMA\KD4\bin.
 - For supported AIX operating systems, navigate to \$CANDLEHOME/aix433/d4/KD4/bin.
 - For supported Solaris operating systems, navigate to \$CANDLEHOME/sol283/d4/KD4/bin.
 - For supported Linux (on Intel) operating systems, navigate to \$CANDLEHOME/li6243/d4/KD4/bin.
 - For supported Linux (on z/OS) operating systems, navigate to \$CANDLEHOME/ls3243/d4/KD4/bin.

- b. Run the following command:
 - For supported Windows operating systems:

```
KD4configDC.bat -enable -env 9 <WESB_HOME> | <WPS_HOME>
```
 - For supported AIX, Solaris, and Linux operating systems:

```
KD4configDC.sh -enable -env 9 <WESB_HOME> | <WPS_HOME>
```

In these commands, the following parameters are specified:

- <WESB_HOME> is the directory path name where IBM WebSphere Enterprise Service Bus is installed.
- <WPS_HOME> is the directory path name where IBM WebSphere Process Server is installed.

If the directory path name contains a blank space, the entire path must be surrounded with quotation marks. If you have this directory path defined in an environment variable, WBI_HOME, then this parameter is optional.

Examples:

- ```
KD4configDC.bat -enable -env 9 %WBI_HOME%
```

In this example, the %WBI\_HOME% environment variable is used to specify the IBM WebSphere Enterprise Service Bus base installation directory. The command completes with a return code of 0.
- ```
KD4configDC.bat -enable -env 9 C:\WPS
```

In this example, the IBM WebSphere Process Server base installation directory is explicitly specified, and because there are no blank spaces in the path, the argument can be specified without surrounding quotation marks.
- ```
KD4configDC.bat -enable -env 9 "C:\Program Files\WPS"
```

In this example, the IBM WebSphere Process Server base installation directory is specified explicitly, and because there is a blank space in the path, the argument is surrounded by quotation marks.
- ```
KD4configDC.sh -enable -env 9 /opt/IBM/WPS
```

This example is for running KD4configDC on a supported AIX, Solaris, or Linux operating system.

You can issue the following command to view the online help for KD4configDC:

- For supported Windows operating systems:

```
KD4configDC.bat -h
```
- For supported AIX, Solaris, or Linux operating systems:

```
KD4configDC.sh -h
```

4. Restart the IBM WebSphere Enterprise Service Bus or IBM WebSphere Process Server application server (refer to your documentation for the specific procedure). The data collector becomes active after the application server is restarted.

Using the data collector in multiple environments

The data collector support for the IBM WebSphere Application Server environment provided with IBM Tivoli Composite Application Manager for SOA v6.0 can also be used in the IBM WebSphere Enterprise Service Bus and IBM WebSphere Process Server environments to monitor Web service flows, similar to basic IBM WebSphere Application Server environments.

When used together, the data collector support for the SCA environment and the existing IBM WebSphere Application Server environment provide monitoring for both SCA flows and Web services flows, respectively, in the IBM WebSphere Enterprise Service Bus and IBM WebSphere Process Server application server runtime environments. IBM recommends that you install support and enable applications for both of these environment types in your WebSphere environment. Applications for each of these data collector environment types can be independently enabled and disabled.

Because data collector support for both SCA and IBM WebSphere Application Server environments runs in the same application server runtime environment, these environments share the same configuration settings, they share a common set of log files (metric, operational, and trace), and they appear as one application server node in the Tivoli Enterprise Portal.

Monitoring controls

Using the Tivoli Enterprise Portal controls to turn monitoring on or off for the WebSphere application server runtime environment results in data collector support for both the IBM WebSphere Application Server and SCA environments being turned on or off. The monitor controls defined for the WebSphere application server runtime environment apply to both the IBM WebSphere Application Server and SCA environments (though for SCA, when monitoring is enabled, the only valid message content level option is *none*). Any changes to the configuration parameters in the Tivoli Enterprise Portal views affect data collection for both environment types.

Communication between SCA modules on different application servers

The data collector in the SCA environment monitors flows between SCA components within a single SCA module. For flows between SCA modules on different application servers, IBM Tivoli Composite Application Manager for SOA can only monitor flows that use Web services bindings. These flows are monitored only for applications that are enabled for Web service flows in the IBM WebSphere Application Server environment. Other types of bindings between SCA modules are not monitored by IBM Tivoli Composite Application Manager for SOA.

IBM recommends that you enable applications for both the SCA and IBM WebSphere Application Server environment types in your IBM WebSphere Enterprise Service Bus or IBM WebSphere Process Server application server runtime environments.

Logging and Filtering

The SCA data collector supports the monitor controls to define which SCA services and operations to monitor, but ignores the message content logging setting (*none*, *headers*, *body*, *full*) and never records message content.

The filter controls (rejection of messages) are not supported by the SCA data collector. This function is supported by IBM WebSphere Enterprise Service Bus and IBM WebSphere Process Server mediations to manage the rejection of messages. To record message content, use the log mediation function of IBM WebSphere Enterprise Service Bus or IBM WebSphere Process Server.

Disabling applications for the data collector

You can disable applications for the SCA data collector using the KD4configDC utility. Optionally stop the WebSphere application server and run the KD4configDC utility as follows:

1. Depending on your operating system, navigate to one of the following locations:
 - For supported Windows operating systems, navigate to %CANDLE_HOME%\CMA\KD4\bin.
 - For supported AIX operating systems, navigate to \$CANDLEHOME/aix433/d4/KD4/bin.
 - For supported Solaris operating systems, navigate to \$CANDLEHOME/sol283/d4/KD4/bin.
 - For supported Linux operating systems, navigate to \$CANDLEHOME/li6243/d4/KD4/bin.
2. Run the following command:
 - For supported Windows operating systems:
`KD4configDC.bat -disable -env 9 <WBI_HOME> | <WPS_HOME>`
 - For supported AIX, Solaris, and Linux operating systems:
`KD4configDC.sh -disable -env 9 <WBI_HOME> | <WPS_HOME>`

After the command completes, restart the application server. The data collector continues to collect data until the application server is restarted.

Limitations

You should be aware of the following limitations for this Sparkler 2 version of data collector support for the SCA environment:

- The data collector in the SCA environment only supports monitoring, not filtering. You can define monitoring controls to limit which SCA services or operations are monitored, but any filter controls defined to reject messages are ignored.
- Monitor control for the message content parameter (*none*, *headers*, *body*, *full*) only supports the *none* value. All other values are ignored and treated as *none*.
- The message length for SCA interactions is always reported as zero.
- Information collected in the SCA environment might not render properly in the IBM Web Services Navigator topology, sequence diagram and patterns views.
- Some asynchronous interactions between SCA components might result in requests or responses being reported multiple times or not at all. This is caused by thread switching in the SCA application server runtime environment and limitations of the data collector in tracking flows across these thread switches. Monitoring of asynchronous interactions is provided in this Sparkler to give you a

more complete picture of the services that exist in the environment, however you should not expect the metrics collected for asynchronous interactions to be precise.

Chapter 5. The DataPower data collector

This chapter describes the support for monitoring of Web services flows through a DataPower appliance acting as a proxy between the Web services client and server.

IBM recently acquired DataPower, a manufacturer of XML and Web services acceleration and security *appliances*. Using a DataPower appliance, you can improve the security and performance of Web services by offloading functions from the application server that is hosting the target Web service to a DataPower appliance. Typical functions that are off-loaded include authentication and authorization, XML schema validation, and Web services encryption and decryption.

Sparkler 2 for IBM Tivoli Composite Application Manager for SOA v6.0 includes the DataPower data collector that was initially provided in Sparkler 1. The DataPower data collector monitors Web services flows through a DataPower appliance and provides similar services management and availability information that IBM Tivoli Composite Application Manager for SOA currently provides for application server runtime environments. This information is displayed in the Tivoli Enterprise Portal using the usual predefined or user-defined workspaces and views.

Upgrade your firmware: Before using the DataPower data collector, you must upgrade the firmware on DataPower appliances that you want to monitor, to include the necessary monitoring and data transformation capabilities. Be sure to upgrade your firmware to version **3.5.0.5** or later.

The DataPower data collector as a proxy

Data collectors provided with IBM Tivoli Composite Application Manager for SOA are usually installed directly into the application server runtime environment hosting the services being monitored. The DataPower appliance, however, does not support the installation of additional software, such as a data collector. Instead, the DataPower appliance provides a communication mechanism that allows external software applications to receive data from its internal transaction log.

The DataPower data collector is installed on a separate machine and uses this communication mechanism to retrieve monitoring data about Web services requests flowing through one or more DataPower appliances, and converts the data into a format that IBM Tivoli Composite Application Manager for SOA can process. In this way, the DataPower data collector acts as a *proxy* between the DataPower appliances and the IBM Tivoli Composite Application Manager for SOA intelligent remote agent (IRA). The DataPower data collector can be installed on a dedicated machine, or it can run on a machine that is also running data collectors for other application server runtime environments. Note that IBM supports only one instance of the DataPower data collector running on any given machine.

When the DataPower data collector starts, it subscribes to each monitored DataPower appliance and then polls (at an interval that you can configure) the appliance for monitoring data. The data retrieved from the DataPower appliance is written to metric log files in the format used by IBM Tivoli Composite Application Manager for SOA. When this data is later displayed in the Tivoli Enterprise Portal, nodes are displayed in the Tivoli Enterprise Portal Navigation view that represent the DataPower appliances being monitored. You can select workspaces under these nodes and view the service management data for the Web services requests flowing through the monitored DataPower appliances.

The DataPower data collector can subscribe to multiple DataPower appliances, and retrieve and manage data from multiple domains. This data can then be separated by DataPower domain or aggregated across multiple domains and appliances, depending on how you configure the data collector. The DataPower data collector uses a configuration file that contains information about which DataPower appliances are being monitored and information needed to establish communication with each monitored appliance.

Planning for deployment

DataPower Web services proxies are defined within *application domains*, and DataPower users can be restricted to access some or all domains. When configuring the DataPower data collector, you must understand how the domains and users are defined on the monitored DataPower appliances, to ensure that the data collector uses valid authentication credentials. This refers to user IDs and passwords that have access to the DataPower domains containing the Web services proxies to be monitored. In addition, you must decide how you want to aggregate or separate the data collected from those domains for display in the Tivoli Enterprise Portal.

You can use DataPower appliances in several typical configurations:

- **Single appliance, single domain:** The data collector monitors a single DataPower appliance, with all of the monitored resources defined in a single domain on the appliance.
- **Single appliance, multiple domains:** The data collector monitors a single DataPower appliance, but that appliance has monitored resources that are defined in more than one domain on the appliance.
- **Multiple appliances with different configurations:** The data collector monitors multiple DataPower appliances, and each appliance has a different configuration of resources to be monitored. Each appliance is configured for a particular job, with no intention of load-balancing or fail-over between appliances.
- **Multiple appliances with identical configurations:** The data collector monitors multiple DataPower appliances, and all of the appliances have an identical configuration of resources being monitored. All of the appliances are configured for the same job, taking advantage of load-balancing and fail-over capabilities between appliances.

Given these typical configurations, the DataPower data collector provides a great deal of flexibility in defining how the collected monitoring data should be separated or aggregated, across a single appliance or multiple appliances, for display in the Tivoli Enterprise Portal. The following examples illustrate how data can be separated or aggregated for managing the data from various domains and appliances:

- **Separation of data at the domain:** You can view the services management data for the resources in a single domain, separate from the data for resources in other domains.
- **Aggregation of data across domains:** You can view the services management data for the resources in several domains (for example, all of the domains on a given DataPower appliance) in an aggregated form, with no regard for the domain in which individual resources are defined.
- **Separation of data at the appliance:** You can view the services management data for resources on a single DataPower appliance, separate from the data for resources on other appliances.

- **Aggregation of data across appliances:** You can view the services management data for the resources on several DataPower appliances (for example, all of the appliances in a load-balancing *cluster*) in an aggregated form, with no regard for what activity occurs on each individual appliance.

By default, the DataPower data collector aggregates data for all of the monitored domains on a single DataPower appliance (even if the domains are accessed using different credentials), and keeps the data from each DataPower appliance separated. See “Configuring for data collection in the DataPower environment” on page 25 for more information.

A single instance of the DataPower data collector can monitor any number of DataPower appliances, limited only by the memory, CPU power and other resources available to it. Note that IBM only supports running a single instance of the data collector on any given system.

Aggregation

For most IBM Tivoli Composite Application Manager for SOA data collectors, aggregation of data is performed for each application server runtime environment. The nodes in the Tivoli Enterprise Portal Navigator view represent individual application server runtime environments that have their own individual data collectors. Because the DataPower data collector can monitor multiple DataPower appliances and multiple domains within each appliance, this single application server runtime environment, single data collector model no longer applies.

Using the DataPower data collector, you assign names to groups of data, referred to as *display groups*. Each group of data is displayed as its own node in the Tivoli Enterprise Portal. Using these named display groups, you can configure the DataPower data collector to gather information from any domains on any DataPower appliances for aggregation and display.

By carefully managing the way in which you name these display groups, the DataPower data collector can separate or aggregate the data in different ways, such as isolating data specific to an individual domain on a single DataPower appliance, or aggregating data across several DataPower appliances into a single display group. This simple display group naming mechanism gives you great flexibility in the separation and/or aggregation of the data displayed in the Tivoli Enterprise Portal.

Deployment steps

To deploy the DataPower data collector in your environment, complete the following general steps as described in this document:

1. Install Sparkler 2 into your existing IBM Tivoli Composite Application Manager for SOA environment (see Chapter 2, “Installing Sparkler 2,” on page 5 for details).
2. Configure your DataPower appliances for monitoring (see “Configuring the DataPower appliance for monitoring” on page 24 for details).
3. Enable the DataPower data collector (see “Configuring for data collection in the DataPower environment” on page 25 for details).
4. Run the **startDPDC** script to start the data collector (see “Starting and stopping the data collector” on page 35 for details).

Configuring the DataPower appliance for monitoring

Before a DataPower appliance can be monitored by the DataPower data collector, configure the DataPower appliance as follows:

- Enable the XML Management Interface on the appliance.
- Check additional optional settings for each domain to be monitored.
- Configure a user account on the DataPower appliance for use with the DataPower data collector.

Enabling the XML Management Interface

The XML Management Interface on the appliance must be enabled using the DataPower administration console. To enable this service, complete the following steps:

1. Start the DataPower administration console in a Web browser (<https://hostname:9090/login.xml>).
2. Login to the administration console as **admin** in the default domain.
3. In the list at the left side of the console, navigate to **Objects** → **Network** → **XML Management Interface**.
4. On the **Main** tab, find the **WS-Management Endpoint** option and select the **on** radio button.
5. Click **Apply** to activate the changes and enable the WS-Management Endpoint.

Checking additional optional settings

For each domain to be monitored, check the following settings:

- In the list at the left side of the console, navigate to **Services** → **Miscellaneous** → **Web Services Agent**.
- Set **Admin State** to *enabled*.
- **Optional:** If you want the DataPower appliance to save metrics records when the DataPower data collector is not running, set **BufferMode** to *buffer*. With this setting, the appliance reports the saved metric data when the data collector starts.
- **Optional:** Adjust the values for **MaxRecords** and **MaxMemoryKB**
- **Optional:** If you want the data collector to record message content in addition to summary metrics, change **CaptureMode** from *faults* to *all-messages*.

Configuring a user account on the DataPower appliance

The DataPower user ID used by the data collector must belong to a user group with the following permissions:

- *Read* permission on the **Login XML-Mgmt** Resource Type in the default domain.
- *Read* permission on the **XML-mgmt** Resource Type in each domain to be monitored using this user ID.
- *Read* permission on the **(any)** Resource Type in each domain to be monitored using this user ID.

See your *DataPower WebGUI Guide* or *DataPower CLI Reference Guide* for details on configuring user group permissions.

Configuring for data collection in the DataPower environment

You should have already completed the installation procedure for installing Sparkler 2 in the existing IBM Tivoli Composite Application Manager for SOA environment on the computer where a supported application server runtime environment is installed. See “Installing Sparkler 2” on page 6 for details.

The DataPower configuration file

For the DataPower data collector, the KD4configDC utility manipulates the contents of a special DataPower configuration file by adding sections to the file when new DataPower monitoring is enabled, and removing sections from the file when monitoring is disabled. Each invocation of the KD4configDC utility is adding, updating or removing one section of the DataPower configuration file. Each section of the DataPower configuration file might be associated with its own data group, or it might be part of a larger data group to which other sections of the configuration file also belong.

The DataPower data collector uses this configuration file to identify the DataPower appliances that are to be monitored and to specify all of the information needed to communicate with those appliances. Typical information that is stored for each connection includes hostname and port, user ID and password, domains to monitor, and polling interval.

The configuration file is located in the `<TMS_DIR>/cma/kd4/config` directory and is called **KD4.dpdcConfig.properties**. This file is maintained separately from the existing configuration file, **KD4.dc.properties**. Here is a sample DataPower configuration file:

```
# Sample DataPower data collector configuration file
DataPower.count=3
#
DataPower.host.1=dpbox1
DataPower.port.1=5550
DataPower.path.1=/
DataPower.poll.1=60
DataPower.user.1=admin
DataPower.encpswd.1=#$*&
DataPower.domainlist.1=default,testdom1
DataPower.displaygroup.1=dpbox1
#
DataPower.host.2=dpbox2
DataPower.port.2=5550
DataPower.path.2=/
DataPower.poll.2=30
DataPower.user.2=user1
DataPower.encpswd.2=&*%$#
DataPower.domainlist.2=userdom1,userdom2,userdom3
DataPower.displaygroup.2=user_doms
#
DataPower.host.3=dpbox2
DataPower.port.3=5550
DataPower.path.3=/
DataPower.poll.3=30
DataPower.user.3=admin
DataPower.encpswd.3=*%$#&
DataPower.displaygroup.3=all_doms
```

In this example, there are three sections in the configuration file. The properties in each of the three sections provide all of the information needed to establish and manage a single connection or session with each DataPower appliance.

Change the information in this configuration file using the KD4configDC utility. Using various combinations of parameters in the KD4configDC utility, you can achieve different monitoring configurations to separate or aggregate data among domains and appliances. See “Considerations for configuration of DataPower monitoring” on page 30 for more information.

Before configuring the DataPower data collector using KD4configDC, consult with your local systems management planners to understand which domains on which DataPower appliances are to be monitored and how the data from these domains and appliances should be separated or aggregated for display in the Tivoli Enterprise Portal.

Running the KD4configDC command

The syntax for running the KD4configDC utility for the DataPower environment is similar to the syntax for other supported IBM Tivoli Composite Application Manager for SOA data collector environments. To run the KD4configDC utility, first navigate to the following location, depending on your operating system:

- For supported Windows operating systems, navigate to %CANDLE_HOME%\CMA\KD4\bin.
- For supported AIX operating systems, navigate to \$CANDLEHOME/aix433/d4/KD4/bin.
- For supported Solaris operating systems, navigate to \$CANDLEHOME/sol283/d4/KD4/bin.
- For supported Linux (on Intel) operating systems, navigate to \$CANDLEHOME/li6243/d4/KD4/bin.
- For supported Linux (on z/OS) operating systems, navigate to \$CANDLEHOME/ls3243/d4/KD4/bin.

Run the KD4configDC utility as follows:

- For supported Windows operating systems:
KD4configDC [-enable | -disable] -env 8 <env specific parameters>
- For supported AIX, Solaris, and Linux operating systems:
KD4configDC.sh [-enable | -disable] -env 8 <env specific parameters>

You can issue the following command to view the online help for KD4configDC:

- For supported Windows operating systems:
KD4configDC.bat -h
- For supported AIX, Solaris, or Linux operating systems:
KD4configDC.sh -h

Specifying KD4configDC parameters

The *<env specific parameters>* defined for the DataPower invocation of the KD4configDC command are a series of key and value pairs that define the necessary properties for the affected section of the DataPower configuration file. These key and value pairs, which you can specify in any order on the command line, are shown in Table 1 on page 27.

Table 1. DataPower key and value pairs for KD4configDC

Parameter	Optional / Required	Default value	Description
-host <hostname or IP address>	Required		Defines the DataPower appliance hostname or IP address. This hostname is used to establish a socket connection and is used as part of the Web address pointing to the DataPower appliance. This can be any length string, with no blank characters. See "Creating node names in Tivoli Enterprise Portal" on page 28 regarding possible truncation of this value in the node name.
-user <user ID>	Required		Defines the DataPower appliance authentication user. This user must be a valid user for the DataPower appliance defined by the -host parameter. See your DataPower documentation for information about creating and managing user IDs for DataPower appliances. See "Configuring a user account on the DataPower appliance" on page 24 for more information.
-pswd <password>	Optional	User is prompted, if necessary	Defines the DataPower appliance authentication password, entered in clear text (not encoded). This password must be valid for the user defined in the -user parameter, and must be valid for the DataPower appliance defined by the -host parameter. This password is automatically converted to an encoded (masked) form and is stored in the DataPower configuration file. See your DataPower documentation for information about creating and managing passwords for DataPower appliances.
-port <port number>	Optional	5550	Defines the DataPower appliance port number. This port number is used to establish a socket connection and is used as part of the Web address pointing to the DataPower appliance. This value must be an integer from 0 to 65535. If this parameter is not specified, the default value is used.
-path <path string>	Optional	/	Defines the DataPower appliance path. This path is used as part of the Web address pointing to the DataPower appliance. This can be any valid path string, with no blank characters.
-poll <polling interval>	Optional	10 seconds	Defines the DataPower appliance polling interval (in seconds). The data collector waits this amount of time between each poll of the DataPower appliance. This must be an integer value, specified in seconds, between 5 and 300 (5 seconds to 5 minutes).

Table 1. DataPower key and value pairs for KD4configDC (continued)

Parameter	Optional / Required	Default value	Description
<code>-domainlist</code> <i>domainA,</i> <i>domainB,</i> <i>...domainZ</i>	Optional	No domainlist property is generated	Defines the DataPower appliance domain list. This is a comma-separated list of domains to be monitored on the associated DataPower appliance. Any domains in this list that are not authorized to the user defined by the <code>-user</code> parameter are not monitored. Each domain can be any string, with no blank characters. If you specify more than one domain name, separated by commas, the entire domain list must be enclosed in double quotes (for example, <code>-domainlist "domain1, domain2, domain3"</code>). See "Considerations for configuration of DataPower monitoring" on page 30 for more information on using this domain list.
<code>-displaygroup</code> <i><display group></i>	Optional	No displaygroup property is generated	Defines the DataPower appliance display name. The name can be any string, with no blank characters, up to 16 characters long. See "Creating node names in Tivoli Enterprise Portal" regarding possible truncation of this value in the node name. See "Considerations for configuration of DataPower monitoring" on page 30 for more information on the use of this property.

Creating node names in Tivoli Enterprise Portal

The DataPower data collector host name is combined with the value of the `-displaygroup` parameter, separated by a hyphen, to form the node name seen in the Tivoli Enterprise Portal Navigator view.

For example, suppose that the KD4configDC is run with the `-displaygroup` parameter specified with a value of *dispName*:

```
KD4configDC -enable -env 8 -host appHost -user user1 -displaygroup dispName
```

If the DataPower data collector host name is *dpcHost*, then the node name that is displayed in the Tivoli Enterprise Portal Navigator view is *D4:dpcHost-dispName*.

If the `-displaygroup` parameter is not specified in the KD4configDC command, then the value of the `-host` parameter is used instead. The value of the `-host` parameter is combined with the DataPower data collector host name to form the node name that is displayed in the Tivoli Enterprise Portal Navigator view.

For example, suppose the KD4configDC is run without specifying the `-displaygroup` parameter:

```
KD4configDC -enable -env 8 -host appHost -user user1
```

In this case the node name that is displayed in the Tivoli Enterprise Portal Navigator view is *D4:dpcHost-appHost*.

Truncation of the node name: If the length of the node name exceeds 20 characters (including the hyphen), the node name is truncated from the end, meaning that the `-displaygroup` or `-host` portion is truncated. You should be aware

of this limitation of the Tivoli Enterprise Portal and choose values for *-displaygroup* and *-host* of appropriate length, to avoid truncation and possible confusion between similar names.

Examples of configuring for data collection

This section provides several examples of the kinds of monitoring that you can configure by running the KD4configDC utility using various combinations of parameters.

The simplest form of the command

When you run the KD4configDC utility to enable monitoring of a DataPower appliance, the simplest format of the command is:

```
KD4configDC -enable -env 8 -host <host> -user <user>
```

For example, with a host name of *dpbox1* and a user name of *admin*, the command is specified as:

```
KD4configDC -enable -env 8 -host dpbox1 -user admin
```

The DataPower configuration file is searched for an existing section that matches the specified host and user, and that has no domain list and no display group properties defined.

- If a matching section is found, you are prompted for a password, and the matching section is updated only by encoding the password and storing it in the configuration file for that section.
- If a matching section is not found in the configuration file, you are prompted for a password. A new section of the configuration file is created, with the specified values for *-host*, *-user* and *-pswd* stored in the configuration file for that section.

Note that no values for *-domainlist* or *-displaygroup* parameters are defined, and other optional properties for the section are set to their default values.

Because no value for *-displaygroup* is specified, the host name *dpbox1* is used as part of the node name that is displayed in the Tivoli Enterprise Portal (for example, *D4:dpdchost-dpbox1*)

Specifying domain list or display group parameters

If the *-domainlist* or *-displaygroup* parameters are specified in the KD4configDC utility, they become part of the matching criteria that determines whether the section already exists or must be created as new. If a new section must be created, the values provided for the *-domainlist* and *-displaygroup* parameters are stored in the new section of the configuration file.

For example, if you have two domains, *domainA* and *domainB* that you are monitoring on a DataPower appliance defined by a host named *host1* and authorized to user *userABC*, run the KD4configDC utility as:

```
KD4configDC -enable -env 8 -host host1 -user userABC -domainlist "domainA,domainB"
```

Note that the list of domains is surrounded by quotation marks, and there are no blank characters in the domain list.

As another example, suppose you want to create a node name to be displayed in the Tivoli Enterprise Portal Navigator view that contains the display group name of *all_domains*. This node name would be in the form of *D4:dpdchost-all_domains*. Specifying these parameters to run the KD4configDC utility, with authorized user *userABC*, would be as follows:

```
KD4configDC -enable -env 8 -host host1 -user userABC -displaygroup all_domains
```

Changing existing values for the domain list or display group: To update an existing section of the configuration file by changing the value of either the `-domainlist` or `-displaygroup` parameter, you must first disable that section of the configuration file by running the `KD4configDC` command using the `-disable` parameter (see “Disabling the data collector” on page 34), specifying the current values for the `-domainlist` or `-displaygroup` parameters.

After the section is disabled, run the `KD4configDC` command again, using the `-enable` parameter and specifying the desired values for `-domainlist` and `-displaygroup`.

Specifying the password parameter

The values specified by the `-user` and `-pswd` parameters are used to perform an HTTP basic authentication over the HTTPS session. The user and password combination must be a valid user ID and password defined using the administration interface of the DataPower appliance. Refer to your DataPower documentation for more information about creating authorized user names and passwords.

If the `-pswd` password parameter is specified in the `KD4configDC` utility, its value is immediately encoded and saved in the configuration file, and you are not prompted for the password. Any password that had previously been specified for an existing section (that matches the search according to the other parameters) is replaced by the new password value.

For example, if an existing section for host name `H100` specified an authorized user of `u2233`, there would already be an encoded value of the valid password stored in the configuration file. To change the password value to `x1y2z3`, run the `KD4configDC` utility as follows:

```
KD4configDC -enable -env 8 -host H100 -user u2233 -pswd x1y2z3
```

Specifying optional parameters

If any of the remaining optional parameters (`-port`, `-path`, or `-poll`) are specified as part of running the `KD4configDC` utility, their values are stored in the configuration file in either the existing or newly created section. These values are not used as part of the matching criteria for locating existing sections of the configuration file.

The data collector uses the values in the `-host`, `-port`, and `-path` properties to construct the URL in the form of `https://host:port/path` that is used as the target of the messages sent to the DataPower appliance.

Considerations for configuration of DataPower monitoring

As previously described, you can use variations of the parameters specified in the `KD4configDC` utility to define properties that configure the monitoring of one or more DataPower appliances. The following sections illustrate several possible configurations.

Multiple connections to the same DataPower appliance

The DataPower configuration file supports multiple connections to the same DataPower appliance by defining multiple sections of the configuration file with the same host and port properties. There are several reasons why you might want to do this, but the most obvious reason is to allow the data collector to use more than one set of authentication credentials.

For example, a DataPower appliance might have three domains (*dom1*, *dom2* and *dom3*) and two users (*userA*, with access only to *dom1* and *dom2*, and *userB* with access only to *dom3*).

In this situation, neither *userA* nor *userB* can be used to access all of the domains on the appliance. To monitor all of the domains on the appliance, you must define two sections in the DataPower configuration file, one that specifies *userA* in one section and *userB* in the other section.

To define the two sections in the configuration file, run `KD4configDC` twice, once for each user, as follows:

```
KD4configDC -enable -env 8 -host dpHost1 -user userA -domainlist "dom1,dom2"  
KD4configDC -enable -env 8 -host dpHost1 -user userB -domainlist dom3
```

Restricting the list of domains being monitored

The `-domainlist` parameter can be used to restrict the list of domains being monitored for a given user. For example, if *userA* has access to *dom1* and *dom2*, but you are interested in monitoring only *dom1*, the `-domainlist` parameter can specify only *dom1* to instruct the data collector to not monitor domain *dom2*:

```
KD4configDC -enable -env 8 -host dpHost1 -user userA -domainlist dom1
```

For each section in the DataPower configuration file, the domains that are monitored depend on the domains to which the user in that section has authorization, and the list of domains specified in the `-domainlist` parameter for that section. If this property is not specified, then all domains that are authorized to the user for that section are monitored.

Separating and aggregating data with the `-displaygroup` parameter

The `-displaygroup` parameter gives you substantial control over how the information from DataPower appliances is separated or aggregated in the Tivoli Enterprise Portal views. Following are some examples of the ways that the `-displaygroup` parameter can be used to separate or aggregate data.

Separating data by host name or display group

Suppose that you have two DataPower appliances (with different users and domains defined on each) and you want to view the information from these two appliances separately under two different nodes in the Tivoli Enterprise Portal Navigation view.

Because there are two DataPower appliances, there must be at least two sections in the DataPower configuration file, one for each appliance hostname or IP address. Separation of the information from these two appliances can be done without using the `-displaygroup` parameter if the two sections of the configuration file have different values for the `-host` parameter. For example:

```
KD4configDC -enable -env 8 -host dpHost1 -user userA  
KD4configDC -enable -env 8 -host dpHost2 -user userB
```

Note that the node name that is displayed in the Tivoli Enterprise Portal is based on the value of the `-host` parameter if the `-displaygroup` parameter is not specified. As long as the two sections of the configuration file have different values for the `-host` parameter, IBM Tivoli Composite Application Manager for SOA separates the data between the two appliances and displays it under two different nodes (for example, *D4:dpdcHost-dpHost1* and *D4:dpdcHost-dpHost2*) in the Tivoli Enterprise Portal Navigator view.

Alternatively, you could use the `-displaygroup` parameter to specify a more meaningful string than by using the value of the `-host` parameter. As long as the values for `-displaygroup` for the two sections are different, the data is separated under different Tivoli Enterprise Portal Navigator nodes. For example:

```
KD4configDC -enable -env 8 -host dpHost1 -user userA -displaygroup host1Domains
KD4configDC -enable -env 8 -host dpHost2 -user userB -displaygroup host2Domains
```

Because the `-displaygroup` parameter is specified, the node name is created from those values and should be displayed in the Tivoli Enterprise Portal Navigator view as `D4:dpdcHost-host1Domains` and `D4:dpdcHost-host2Domains`. However, note also that in this case, the length of the node name exceeds 20 characters, so each node name is truncated, as `D4:dpdcHost-host1Dom` and `D4:dpdcHost-host2Dom`.

Separating data between domains by domain list

Suppose that you have a DataPower appliance with a single user, `userA`, and two domains, `dom1` and `dom2`.

You can configure the data collector to separate the information from these two domains under two different nodes in the Tivoli Enterprise Portal Navigation view by creating two sections in the DataPower configuration file. The first section specifies a `-domainlist` value of `dom1` and a `-displaygroup` value of, for example, `Dom1`, and the second section specifies a `-domainlist` value of `dom2` and a `-displaygroup` value of, for example, `Dom2`.

Example:

```
KD4configDC -enable -env 8 -host dpHost1 -user userA -domainlist dom1
  -displaygroup Dom1
KD4configDC -enable -env 8 -host dpHost1 -user userA -domainlist dom2
  -displaygroup Dom2
```

The different values for the `-displaygroup` value cause IBM Tivoli Composite Application Manager for SOA to create two display groups that map to two different Tivoli Enterprise Portal Navigation view nodes: `D4:dpdcHost-Dom1` and `D4:dpdcHost-Dom2`, and the `-domainlist` values restrict the data collected in each of those display groups to just the intended domain, even though `userA` happens to have access to both domains.

Aggregating data across multiple domains

Suppose that you have a DataPower appliance with a single user, `userA`, and two domains, `dom1` and `dom2`. If the `-displaygroup` value is not specified in the section of the configuration file, the node name is created from the `-host` parameter value, and the information for both `dom1` and `dom2` is aggregated under a single node (`D4:dpdcHost-dpHost`) in the Tivoli Enterprise Portal Navigation view.

Aggregating data across multiple domains under multiple nodes

To aggregate the data from domains `domA1` and `domB1` under one node name and the data from `domA2` and `domB2` under a different node name, configure four sections in the DataPower configuration file, as follows:

- user `userA`, domainlist `domA1`, displaygroup `Group1`
- user `userB`, domainlist `domB1`, displaygroup `Group1`
- user `userA`, domainlist `domA2`, displaygroup `Group2`
- user `userB`, domainlist `domB2`, displaygroup `Group2`

Example:

```

KD4configDC -enable -env 8 -host dpHost -user userA -domainlist "domA1"
  -displaygroup Group1
KD4configDC -enable -env 8 -host dpHost -user userB -domainlist "domB1"
  -displaygroup Group1
KD4configDC -enable -env 8 -host dpHost -user userA -domainlist "domA2"
  -displaygroup Group2
KD4configDC -enable -env 8 -host dpHost -user userA -domainlist "domB2"
  -displaygroup Group2

```

This causes IBM Tivoli Composite Application Manager for SOA to aggregate the information from *domA1* and *domB1* under the Tivoli Enterprise Portal Navigation node *D4:dpdcHost-Group1* and to aggregate the information from *domA2* and *domB2* under the Tivoli Enterprise Portal Navigation node *D4:dpdcHost-Group2*

Aggregating data across all domains on a single host with multiple users

Suppose that you have a DataPower appliance with two users (*userA* and *userB*) that each have access to different sets of domains (*userA* has access to domains named *domA1* and *domA2*, the other user, *userB*, has access to domains named *domB1* and *domB2*, respectively). To monitor all of these domains, the DataPower configuration file must have at least two sections, one with a *-user* parameter value of *userA* and one with a *-user* parameter value of *userB*, but each specifying the same value for the host name in the *-host* parameter.

Example:

```

KD4configDC -enable -env 8 -host dpHost -user userA
KD4configDC -enable -env 8 -host dpHost -user userB

```

If the *-displaygroup* parameter is not specified, the information from all four domains would be aggregated under the same Tivoli Enterprise Portal Navigation node, for example, *D4:dpdcHost-dpHost*.

Aggregating data for a cluster of appliances

You might have a collection of DataPower appliances that are identically configured because they are used in a load-balancing or fail-over situation. Because each appliance has its own hostname or IP address, there must be at least one section in the configuration file for each appliance to inform the data collector how to communicate with each appliance.

If the *-displaygroup* parameter is not used, then the information for each of these appliances is separated into different nodes in the Tivoli Enterprise Portal Navigator view (for example, *D4:dpdcHost-dpHost1*), because the *-host* parameter value is used by default.

To see how this *cluster* of appliances is performing as a whole, without regard to the performance of individual appliances, specify the same *-displaygroup* value (for example, *Clust1*) for every appliance. This causes the data collector to aggregate the data from all of these devices into a single display group, which is then displayed under a single Tivoli Enterprise Portal Navigation node (for example, *D4:dpdcHost-Clust1*)

Example:

```

KD4configDC -enable -env 8 -host dpHost1 -user userA -displaygroup Clust1
KD4configDC -enable -env 8 -host dpHost2 -user userA -displaygroup Clust1

```

Additional considerations

You can mix and match any of the various configurations described in this chapter, which gives you a great deal of flexibility in defining how to aggregate or separate data in the Tivoli Enterprise Portal views. This flexibility might result in some DataPower domains being specified in more than one section. This is not considered an error.

You might want one section defined to allow data for a domain to be displayed on its own under one Tivoli Enterprise Portal Navigator node, and another section (or sections) defined to show the data for that domain aggregated with other domains, on the same or on a different machine. This is possible, but be aware that this results in the data for duplicated domains being retrieved multiple times by the data collector (once for each section in which it is configured). In this situation performance might be affected.

By default, if no *-domainlist* parameter and no *-displaygroup* parameter are used at all in the DataPower configuration file, the DataPower data collector aggregates data for all of the monitored domains on a single DataPower appliance (even if the domains are accessed using different credentials), and keeps the data from each DataPower appliance separated.

Disabling the data collector

When you run the KD4configDC utility to disable monitoring of a DataPower appliance, the simplest syntax for running the KD4configDC utility is:

```
KD4configDC -disable -env 8 -host <host> -user <user>
```

The DataPower configuration file is searched for an existing section that matches the specified host and user and that has no *-domainlist* parameter and no *-displaygroup* parameters defined. If a matching section is found, the section is removed from the file. If no matching section is found, an error message is issued and the file remains unchanged.

If the *-domainlist* or *-displaygroup* parameters are specified in the KD4configDC utility, they become part of the matching criteria that determines whether the section exists and removed if found.

All other parameters (*-port*, *-path*, *-poll*, or *-password*) are not required and are ignored, if specified on the command line.

Communication between data collector and appliance

Approximately every ten minutes, the data collector queries the DataPower appliance to see if the domain list has changed. If the domain list has changed, the data collector updates its information as needed and begins monitoring new domains defined on the Data Power appliance.

Communication errors between the data collector and the DataPower appliance that prevent the collection of data are logged to the console (the command line session where the **startDPDC** script was executed) and to the operations log. Additional information concerning the communications between the data collector and DataPower appliance can be obtained by setting the operations logging level for the data collector from *error* to *info* using the **updateLogging** Take Action command from the Tivoli Enterprise Portal.

Optimizing performance

The data collector is configured by default to monitor all services and operations, but with no logging of message content. This configuration optimizes the performance of processing data by not having to handle message content when it is not needed. When you modify any monitor controls to specify a content logging setting other than *none*, all of the full message content for all services and operations is retrieved from the appliance, and the data collector applies the configured monitor control rules (*headers/body/full*) by service and by operation.

Limitations

You can control the monitoring to limit the collection of data to specific services and operations, but you cannot use filter controls to reject messages to specific services or operations. To filter (reject) messages, use the Policy Rules and Actions of the DataPower Web Services Proxy configuration.

The data collector does not generate meaningful correlators for messages flowing through the DataPower appliance, so this data will not render properly in the topology, sequence diagram and pattern views in the IBM Web Services Navigator.

The DataPower data collector creates metric, content, operation and trace log files, but because message filtering is not supported, it does not create any action log files.

Depending on your configuration, the data collector can create multiple metric and content log files to emulate the existence of several different display groups. Each display group is represented as a separate node in the Tivoli Enterprise Portal Navigator view. The log files for each display group hold the data for all of the DataPower appliances that are configured for that display group, which might span multiple DataPower domains and include data from multiple DataPower appliances.

Before attempting to delete an application domain from DataPower that is being monitored by the DataPower data collector, you must either run the KD4configDC utility to disable monitoring of that application domain, or stop the data collector. Otherwise, when you attempt to delete the domain using the DataPower administration console, you receive an error and the domain cannot be deleted.

Starting and stopping the data collector

To start the DataPower data collector, open a command prompt window and run the **startDPDC** script. No support is provided to run this data collector as a Windows, AIX, Solaris, or Linux service.

Once started, the data collector monitors the console for commands entered by the user. The only supported commands are **stop**, **quit**, and **exit**, all of which initiate an orderly shutdown of the DataPower data collector. When one of these commands is entered, the data collector waits for all communication sessions to end before the process terminates.

While the data collector is running, you can use the KD4configDC utility to update the DataPower data collector configuration file and change which DataPower appliances and domains are being monitored. You do not need to stop and restart the data collector to activate these changes. The running data collector detects the changed configuration file within 40 seconds and adjust its monitoring to reflect the updated configuration.

Troubleshooting

Communication failures

In the event of a communications failure, the data collector attempts to initialize itself again and reestablish communication with the target DataPower appliance after the next polling interval (the polling interval is specified by the `-poll` value. This process is repeated each polling interval until communication is successfully reestablished, or until the data collector is stopped. Setting the operations logging level to *info* gives you the best indication of status of the communications between the data collector and the appliance.

Synchronizing time between computer systems

For data to display properly in the Tivoli Enterprise Portal, the DataPower appliance, the data collector system and the Tivoli Enterprise Monitoring Server system must have their clocks synchronized within 5 minutes of each other, in terms of the UTC time they report.

Password problems

User IDs and passwords for DataPower appliances are created and maintained at the appliance. See the documentation that is provided with your DataPower appliance for information about creating and managing user IDs and passwords. When you have reset this information at the DataPower appliance, use the `KD4configDC` utility to update the DataPower configuration file with the latest user ID and password values for the appropriate section of the file.

Logging and Tracing

The data collector in the DataPower environment uses the same operation and trace log files as other environment types supported by the IBM Tivoli Composite Application Manager for SOA product, but rather than creating separate operation and trace files for each display group, it creates a single operation file and a single trace file for all display groups.

The view in the Tivoli Enterprise Portal continues to operate as though you can configure logging and tracing for each display group, but the settings for all DataPower display groups are considered when the settings for the single log or trace writer instance are initialized, as follows:

- If any display group has trace set to ON, the DataPower data collector records tracing information for all display groups to the trace log.
- The DataPower data collector uses the lowest severity log setting (*Info*, *Warning*, or *Error*) of all display groups. For example, if a display group has a log setting of *Info*, then all informational, warning, and error messages for all display groups are written to the operations log.

The DataPower data collector will not update the global configuration settings seen in the Tivoli Enterprise Portal to reflect the actual settings being used for the various display groups. As a result, the Tivoli Enterprise Portal might still show different log and trace settings for each display group, even though the data collector is using common settings for all display groups.

In addition to the operations log, the DataPower data collector will also issue messages to the console where the `startDPDC` script was run. All messages issued to the console are also recorded in the operations log.

Launching the DataPower Web browser interface

You can select a DataPower appliance that is displayed in a row of the Services Inventory table in the Performance Summary workspace of the Tivoli Enterprise Portal, and follow the procedure described in this section to launch a Web browser session that brings up the DataPower WebGUI user interface. You can then use this sophisticated interface to configure the DataPower appliance and the policies that the appliance applies to Web services traffic.

To launch the DataPower WebGUI user interface, complete the following steps:

1. From the Tivoli Enterprise Portal, navigate to the Performance Summary workspace and display the Services Inventory table view.
2. Select a row in the table from the DataPower system referenced in the Node Name column, and right-click on the row to display a context menu, similar to the example shown in Figure 1.

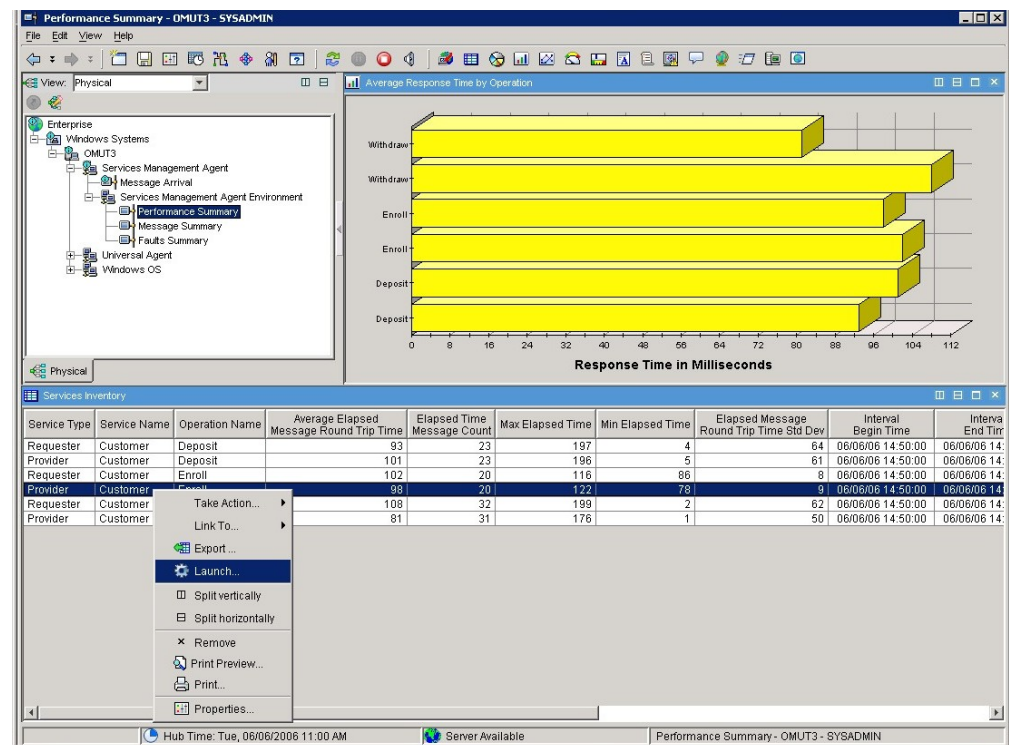


Figure 1. Selecting a DataPower row from the Services Inventory Attributes table

3. From the context menu, select **Launch** to display the Create or Edit Launch Definitions window, similar to the example shown in Figure 2 on page 38.

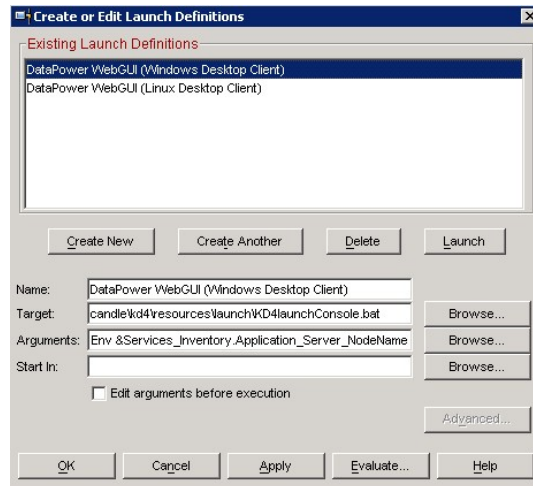


Figure 2. Selecting the Windows or Linux version

4. Select either the Windows or Linux version of the DataPower WebGUI Tivoli Enterprise Portal Desktop client, and then click **Launch**.
5. A new Web browser session is started using the Web address for the selected DataPower system selected from the table.

Considerations when launching the DataPower WebGUI client

The following sections provide additional limitations, restrictions, and considerations to keep in mind as you launch the DataPower WebGUI user interface.

Launch only from a row representing a DataPower environment

You cannot launch a DataPower WebGUI browser session from a row in the Services Inventory table that represents a non-DataPower application server runtime environment. DataPower appliances are identified by a value of *DataPower* in the Application Server Environment column of the Services Inventory table.

If you select a row that does not represent metrics data from a DataPower application server runtime environment, a browser session is launched with the KD4LN0001E error message displayed.

Cannot launch from a row with aggregated DataPower metrics

Because of the way that the data collector works and the way that the Application Server Node Name field is populated by the DataPower data collector, you cannot launch a Web browser session from a Services Inventory table row that represents metrics aggregated from more than one physical DataPower appliance.

In the case of aggregated metric data from more than one DataPower appliance, the Node Name field is blank to prevent possibly launching the browser to the wrong DataPower appliance. If you select a row in the table that represents metrics aggregated from more than one physical DataPower appliance, a browser session is launched with error message KD4LN0002E displayed.

Launch only from a Tivoli Enterprise Portal Desktop client

You can launch the DataPower WebGUI browser session only from the IBM Tivoli Monitoring v6.1 Tivoli Enterprise Portal Desktop client. You cannot launch from a Tivoli Enterprise Portal Browser client, nor from an OMEGAMON client.

Attempting to launch from a Tivoli Enterprise Portal Browser client results in message KFWITM069E, for example:

```
KFWITM069E The definition you selected could not be launched because of error:  
CreateProcess: <Launch_Console_path> <IP_Address> error=2.
```

In this message, <Launch_Console_path> is the path where the KD4launchConsole script is located, and <IP_Address> is the IP address of the DataPower appliance. See your IBM Tivoli Monitoring documentation for more information about this message.

Web browsers used for the launch

For supported Windows operating systems, the default Web browser that is configured for the local computer system is used for the launch. Refer to your Windows operating system documentation for information on configuring the default Web browser.

For supported Linux operating systems, you can define the default Web browser using the Manage Tivoli Services console:

1. From the <ITM_Home>/bin directory, run the ./CandleManage command to open the Manage Tivoli Services console.
2. Right-click **Tivoli Enterprise Portal Desktop Client** and select **Configure**.
3. In the configuration display, set the **Browser Path** to the location of the preferred Web browser.
4. If you specify an instance name, a script file is created with a name in the format of **cnp_<instance name>.sh**. For example, if you specify an instance name of *myinstance*, the resulting script name is *cnp_myinstance.sh*. If you do not specify an instance name, the default script file named *cnp.sh* is updated.
5. Click **Save** to save your script updates.

If there are multiple versions of this script, the launch of the DataPower user interface selects the first script (in alphabetical order) that it is able to run successfully, and this is the default Web browser that is used.

The DataPower WebGUI must be configured for Port 9090

The launch will operate correctly only if the DataPower WebGUI is configured for port *9090* (port 9090 is also the default port number). Refer to the *DataPower WebGUI Guide* and the *DataPower CLI Reference Guide* for information on configuring the port.

Launching into new or existing browser sessions

The launch of the DataPower WebGUI client either opens in a new browser session or returns to an existing browser session, based on the configuration of your Web browser settings.

To modify your browser settings for Internet Explorer, navigate to **Tools → Internet Options → Advanced → Browsing**:

- To always return to the same Web browser window on each launch, select the **Reuse windows for launching shortcuts** checkbox .
- To open a new browser window on each launch, clear the **Reuse windows for launching shortcuts** checkbox.

To modify your browser settings for Mozilla Firefox, navigate to **Tools → Options → Tabs**:

- To always return to the same Web browser window on each launch, select the radio button to **Open links from other applications in: the most recent tab/window**.
- To open a new browser window on each launch, select the radio button to **Open links from other applications in: a new window**.

For other Web browsers, refer to your documentation for more information to configure this behavior.

Logging in to DataPower

If you have not previously logged in to the DataPower WebGUI user interface in the current browser session, the Web browser session opens to the login page. You will need to log in with a valid user name and password to continue. If you have previously logged in, the session opens to the main page of the user interface.

Refer to your DataPower documentation for more information about user names and password, and consult your local system administrator for assistance if needed.

Launching on Linux Tivoli Enterprise Portal clients

When launching the DataPower Web browser user interface on supported Linux operating systems, the Web browser that is launched is determined by examining all of the Tivoli Enterprise Portal client startup scripts in the `<ITM_HOME>/li6243/cj/bin/` directory, looking specifically for the `kjr.browser.default` property. If that property is found with a value set to a Web browser for which the launch function has permission to execute, that Web browser is used as the default for launching the DataPower user interface. Note that there might be multiple scripts in the directory that have that value set. The default Web browser that is launched might not be the same default that was specified in your Tivoli Enterprise Portal startup script.

Online help available

The **Help** button on the **Create or Edit Launch Definitions** window displays the IBM Tivoli Monitoring v6.1 help information for this window. Refer to this online help for more information about the various features of the window.

For your reference, the text for the online help contains the following descriptions of the various fields:

Existing Launch Definitions

This area shows the launch definitions applicable to the current Navigator item or query.

Name The title of the definition.

Target The path to, and file name of, the application to launch. Click **Browse** to locate the file and select it or, if this is a Web site, type the URL. If any part of the target contains spaces, enclose the entire entry in double quotation marks (""). For example: `\Documents and Settings\Administrator\My Documents\notepad.exe`. To include an & ampersand or ^ caret in the name, precede it with a / forward slash. For example, `john&jane.lwp` would be entered as `john/&jane.lwp`.

Arguments

Enables you to pass a value to the application in one of three ways:

- As a specific value, such as `tuning.log` for the target `notepad.exe`. Click **Browse**, click **Filename**, then locate and select the file.
- As the detailed name of an attribute that will be replaced by the current value at launch time. Click **Browse**, click **Substitutable Items**, then

select an attribute. The attributes available are those associated with the Navigator item, table row or chart point. When you select an attribute, it is displayed in the **Arguments** field with its detailed name. In this example of substitutable item, *Product* was selected from the list and shows as *&ManagedSystem.Product*.

- As a prompt for a value to be entered at application launch time, such as *Day*. Precede the prompt with a ^ caret symbol.

If you would like to supply a default value, but also prompt for a value so the user can change it if necessary, append the prompt with an = equal sign and the value. For example, *^Name=Fred*, where *Name* is the prompt and *Fred* is the default value.

The prompt must contain no spaces.

To have a value hidden when the application is launched, such as a password, precede it with two caret marks (^ ^).

If your argument requires the ^ caret mark or & ampersand as a value, precede the special character with a / forward slash (/^ or /&).

Arguments are optional.

Start In

Enables you to select a starting disk and directory for the executable in the **Target** field. Use **Browse** to locate the folder where the program or other required files are located.

Edit arguments before execution

Select this check box to enable the user to change the values of arguments, whether a substitutable item or file, when the application is launched.

Advanced

This is available when the launch definition originates from a Navigator item; it is disabled for definitions originating from a chart point or table row. This button opens the **Advanced Options for Launch Definition** window, where you can specify whether the definition is available for this Navigator item only, for all Navigator items of the same type, or for all Navigator items in this and any other Navigator views.

Evaluate

This shows how the arguments will resolve when the application launches. The term *detailed name* refers to the name used in formulas, expert advice, take action commands, and headers and footers when referencing an attribute. In the Properties and Situation editors, click **Show Formula**, then check **Show detailed formula** to see.

Chapter 6. The SAP NetWeaver data collector

This chapter describes the support for monitoring of Web services flows in the SAP NetWeaver v6.40 SR9 (or later) environment. This data collector provides a similar level of support for the SAP NetWeaver environment as provided with other IBM Tivoli Composite Application Manager for SOA application server runtime environments, such as IBM WebSphere Application Server, BEA WebLogic Server, and JBoss.

Depending on the types of Web services applications you plan to monitor, you might need to enable or disable your SAP NetWeaver applications for the data collector using different procedures:

- For a server side application or for a standalone (running as a Java application) client application, you need to run only the KD4configDC utility to enable or disable the SAP NetWeaver application for the data collector.
- For a deployable (running on a J2EE container) client application, you must manually modify the client code as described in the sections that follow.

Manually enabling applications for open-source projects: The IBM Tivoli Composite Application Manager for SOA data collector includes third party software (also referred to as *excluded components*) as a part of monitoring Web services traffic in the SAP NetWeaver environment. See the license files in your appropriate language for more information on this third party software. These files are located in the **license\D4V600FT002** directory on the computer systems where the data collector support for Tivoli Management Services is installed.

If any of the applications in your server use any of these excluded components, you should manually enable your applications as described in the sections that follow. As with any change, back up your application prior to making this change, and test it thoroughly afterward.

If this is not a concern for your installed applications, you can use the KD4configDC utility to enable all of the applications in your server. The KD4configDC utility, however, cannot enable Web services client calls made from within another Web service. These calls must be enabled manually as described in the sections that follow in order to be monitored.

The KD4configDC utility can be run once to enable all SAP NetWeaver applications for the data collector, and the data collector will monitor all of the SAP NetWeaver related applications. If you add more SAP NetWeaver applications to the environment, you must run the KD4configDC utility again to enable these new applications. Applications that are already enabled are not affected.

Standalone client restriction: A supported SAP NetWeaver standalone client application must include an instance of the implementation for `com.sap.engine.services.webservices.jaxrpc.wsdl2java.ServiceBase`. To create an instance of `java.rmi.Remote, javax.xml.rpc.Stub`, the standalone client application must invoke `getPort()` or `getLogicalPort()` for the instance of `com.sap.engine.services.webservices.jaxrpc.wsdl2java.ServiceBase`. **Do not** use `new` to create the instance of `java.rmi.Remote, javax.xml.rpc.Stub`.

Enabling the application for the data collector

There are several different patterns through which Web services components can operate on your SAP NetWeaver application server, and each is configured slightly differently. Use the following sections to identify the correct mechanisms for your applications, and choose whether you should use the KD4configDC utility to enable or disable your applications, or whether you should do so manually:

- Web services (or Web service providers)
- Web services clients in standalone Java programs
- Web services clients built into their own JAR files
- Web services clients built into J2EE Web modules (WARs)

File changes in SAP NetWeaver applications directory: If you use the KD4configDC utility to enable or disable your server, certain changes are made to files in your SAP applications directory, and the undeploy operation of the SAP administration utilities might not remove all of those changed files. To ensure that upgraded versions of your applications deploy successfully, check the directory for each application after undeploying and delete any residual files that you might not have been expecting. You must enable upgraded applications again using the KD4configDC utility if they were not manually enabled during the upgrade.

To enable a SAP NetWeaver application for the IBM Tivoli Composite Application Manager for SOA data collector, complete the following steps:

1. You should have already completed the installation procedure for installing Sparkler 2 in the existing IBM Tivoli Composite Application Manager for SOA environment on the computer where your SAP NetWeaver application server is installed. See “Installing Sparkler 2” on page 6 for details.
2. Depending on the type of application, complete the following steps:
 - For a **server application**:
 - To enable a Web services application on your SAP NetWeaver server using the KD4configDC utility:
 - a. Stop the SAP NetWeaver application server following the procedures in your SAP NetWeaver documentation.
 - b. Run the KD4configDC utility to enable the application for the data collector.
 - c. Restart the SAP NetWeaver application server following the procedures in your SAP NetWeaver documentation.
 - To manually enable a Web services application on your server:
 - a. Add the kd4dcagent.jar and ibm-jaxrpc-client.jar files to your application, typically in the /WEB-INF/lib directory. If your application uses a Sun distribution of Java 1.4.2, you must also add xercesImpl.jar and xml-apis.jar. All of these jar files are provided in the KD4/lib directory.
 - b. Add the IBM Tivoli Composite Application Manager for SOA servlet filter to the web.xml file for the application, similar to the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<web-app>
  <display-name>SayHelloWS_Config1.war</display-name>
  <servlet>
    <servlet-name>SayHelloWS_Config1_SoapServlet</servlet-name>
    <display-name>SayHelloWS_Config1_SoapServlet</display-name>
    <servlet-class>SoapServlet</servlet-class>
```

```

        <load-on-startup>0</load-on-startup>
    </servlet>
    <servlet-mapping>
        <servlet-name>SayHelloWS_Config1_SoapServlet</servlet-name>
        <url-pattern>/*</url-pattern>
    </servlet-mapping>
    <session-config>
        <session-timeout>1</session-timeout>
    </session-config>
    <filter>
        <filter-name>KD4ServletFilter</filter-name>
        <filter-class>com.ibm.management.soa.agent.sap.WebServiceFilter
        </filter-class>
    </filter>
    <filter-mapping>
        <filter-name> KD4ServletFilter</filter-name>
        <url-pattern>/*</url-pattern>
    </filter-mapping>
</web-app>

```

- c. Install your upgraded application into your application server.
- For a **standalone client application**:
 - To enable Web services using the KD4configDC utility:
 - a. Run the KD4configDC utility with the **-clientappsdir** parameter to enable the application for the data collector.
 - b. Modify the classpath used to launch the standalone application to include the kd4dcagent.jar file, which is provided in the /KD4/lib directory.
 - c. Run the application.
 - To manually enable a Web service on your standalone client application:
 - a. Modify the classpath used to launch the standalone application to include the kd4dcagent.jar file, which is provided in the /KD4/lib directory:
 - b. Update lports_1.xml to define the feature needed for the IBM Tivoli Composite Application Manager for SOA protocol, similar to the following example (see the text in **bold type**):

```

<?xml version="1.0" encoding="UTF-8"?>
<LogicalPorts Name='CalculatorServer'
InterfaceName='test.proxy.CalculatorServer'>
<LogicalPort Name='Config1Port_Document'
    Endpoint='http://t10:50000/CalculatorServer
    /Config1?style=document'
    BindingName='Config1Binding'
    BindingUri='urn:CalculatorServerWsd/Config1/document'
    BindingImplementation='SOAP 1.1 HTTP Binding with Attachments'
    StubName='test.proxy.Config1BindingStub' Default='true'
    InterfaceName='test.proxy.CalculatorServerViDocument'
    Original='true' Valid='true'>
<globalFeatures>
<Feature Name='http://www.sap.com/webas/630/soap/features
    /authentication' Provider='SecurityProtocol' Original='true'>
    <Property Name='AuthenticationLevel' Value='None'>
    </Property>
    <Property Name='AuthenticationMechanism' Value='None'>
    </Property>
</Feature>
<Feature Name='http://www.sap.com/webas/630/soap/features
    /transportguarantee' Original='true'>
    <Property Name='Level' Value='No'></Property>
</Feature>
<Feature Name='http://www.sap.com/webas/630/soap/features/headers/'

```

```

    Provider='SoapHeadersProtocol' Original='false'>
  </Feature>
  <Feature Name='http://www.sap.com/webas/630/soap/features/session/'
    Provider='SessionProtocol' Original='false'>
    <Property Name='SessionMethod' Value='httpCookies'>
  </Property>
  </Feature>
  <Feature Name=' http://www.ibm.com/tivoli/itcam4soa/'
    Provider='KD4Protocol' Original='false'>
    <Property Name='portName' Value='Config1Port_Document'>
  </Property>
  </Feature>
</globalFeatures>
<localFeatures>
  <Operation Name='add'>
  </Operation>
  <Operation Name='divide'>
  </Operation>
  <Operation Name='multiply'>
  </Operation>
  <Operation Name='subtract'>
  </Operation>
</localFeatures>
</LogicalPort>
</LogicalPorts>

```

- c. Update protocols.txt to declare the IBM Tivoli Composite Application Manager for SOA protocol, similar to the following example (see the text in **bold type**):

```

#Default Protocol implementations
#Fri Nov 18 13:54:53 GMT+08:00 2005
SessionProtocol=com.sap.engine.services.webservices.jaxrpc
.wsd12java.features.builtin.SessionProtocol
MessageIdProtocol=com.sap.engine.services.webservices.jaxrpc
.wsd12java.features.builtin.MessageIdProtocol
SecurityProtocol=com.sap.security.core.client.ws.SecurityProtocol
SoapHeadersProtocol=com.sap.engine.services.webservices.jaxrpc
.wsd12java.features.builtin.SoapHeadersProtocol
KD4Protocol= com.ibm.management.soa.agent.sap.ITCAMClientProtocol

```

- d. Install your upgraded application into your application server.
- For a **Web services client packaged in its own JAR file** but being used by a WAR:
 - a. Modify the classpath for the application to include the kd4dcagent.jar file. This jar is provided in the /KD4/lib directory.
 - b. Do **either** of the following:
 - Run the KD4configDC utility with the **-clientappsdir** parameter to enable the application for the data collector.
 - add the IBM Tivoli Composite Application Manager for SOA protocol to the appropriate deployment descriptors as described in manual steps 3b on page 45 and 3c for the standalone client application.
 - c. Install your upgraded application into your application server.
 - For a **deployable client application** such as a JSP or another Web service:
 - a. You do not need to stop the SAP NetWeaver application server if it is already running.
 - b. Manually add the kd4dcagent.jar file to the **lib** directory for the application.
 - c. Manually modify application-j2ee-engine.xml, adding the following reference shown in bold text:


```

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE application-j2ee-engine SYSTEM "application-j2ee-engine.dtd">
<application-j2ee-engine>
  <reference
    reference-type="hard">
    <reference-target
      provider-name="sap.com"
      target-type="application">MathDepProxy</reference-target>
    </reference>
    <reference reference-type="hard">
      <reference-target provider-name="sap.com"
        target-type="library">sapxmltoolkit</reference-target>
    </reference>
    <provider-name>sap.com</provider-name>
    <fail-over-enable
      mode="disable"/>
</application-j2ee-engine>

```

- d. Manually modify the application code to add the ITCAMClientProtocol protocol to the protocol list for each of your client stubs.

Following is an example of how to modify a deployable client side application:

```

// initialization of the web service client
.....
// create a deployable proxy object.
SystemDetail service = new SystemDetailImpl();
SystemDetailViDocument port = service.getLogicalPort();
BaseGeneratedStub stub = (BaseGeneratedStub)port;
ProtocolList list = stub._getGlobalProtocols();
ITCAMClientProtocol protocol = new ITCAMClientProtocol();
list.add(protocol);

// call web service
.....

```

- e. Install your upgraded application into your application server.

Running the KD4configDC utility

Run the KD4configDC utility to enable the application for the data collector. Run the KD4configDC utility as follows:

- Depending on your operating system, navigate to one of the following locations:
 - For supported Windows operating systems, navigate to %CANDLE_HOME%\CMA\KD4\bin.
 - For supported AIX operating systems, navigate to \$CANDLEHOME/aix433/d4/KD4/bin.
 - For supported Solaris operating systems, navigate to \$CANDLEHOME/sol283/d4/KD4/bin.
 - For supported Linux (on Intel) operating systems, navigate to \$CANDLEHOME/li6243/d4/KD4/bin.
- Run the following command:
 - For supported Windows operating systems:


```
KD4configDC.bat -enable -env 6 {-sapappsdir <apps_dir> | -clientappsdir <apps_dir> | -sid <home> <sid>}
```
 - For supported AIX, Solaris, and Linux operating systems:


```
KD4configDC.sh -enable -env 6 {-sapappsdir <apps_dir> | -clientappsdir <apps_dir> | -sid <home> <sid>}
```

In these commands, the following parameters are specified:

-enable

Causes the command to enable the application for the data collector for the specified environment.

-env 6 Defines the environment to be enabled as SAP NetWeaver.

-sapappsdir <apps_dir>

Specifies that the directory path specified by <apps_dir> is the location of the Web services application to be monitored. Use this parameter for a server side application.

-clientappsdir <apps_dir>

Specifies that the directory path specified by <apps_dir> is the location of the Web services application to be monitored. Use this parameter for a standalone client application. There is no default path for the **-clientappsdir** parameter.

If your standalone client application is a .jar file, be sure to specify the full directory path for the location of the .jar file. See the examples that follow.

<apps_dir>

Specifies the directory path of the Web services application to be monitored.

-sid <home> <sid>

For this parameter, <home> is the SAP home directory, typically **/usr/sap** or **C:\usr\sap**, but it could reside on any drive. The <sid> argument is the SAP system ID. Both of these arguments are used to confirm that the directory corresponding to the specified SID exists under the specified home. All Web services applications that are found under the SID are enabled.

Examples:

- KD4configDC.bat -enable -env 6 -sid C:\usr\sap j2e

In this example, the SAP home directory **C:\usr\sap** is specified, along with the system ID *j2e*. All Web services applications found under this combination of home directory and SID are enabled for the data collector.

- KD4configDC.bat -enable -env 6 -sapappsdir /app1

In this example, the Web services application directory location */app1* is specified. This might be for enabling a server side or deployable client side application for the data collector.

- KD4configDC.bat -enable -env 6 -clientappsdir /app2

In this example, the Web services application directory location */app2* is specified. This command enables the standalone client side application for the data collector.

- KD4configDC.bat -enable -env 6 -sapappsdir
"C:\usr\sap\j2e\JC000\j2ee\cluster\server0\apps"

In this example, the Web services application directory is specified explicitly. This example also shows the directory path surrounded by quotation marks, which are needed if the path contains one or more blank characters.

- KD4configDC.sh -enable -env 6 -clientappsdir /opt/IBM/appsdir

This example is for running KD4configDC on a supported AIX, Solaris, or Linux operating system.

- KD4configDC.sh -enable -env 6 -clientappsdir
/usr/sap/Customer/EnterpriseSTDCClientProxy.jar

In this example, the standalone client application is a .jar file, so the full directory path location of the file is specified.

You can issue the following command to view the online help for KD4configDC:

- For supported Windows operating systems:
KD4configDC.bat -h
- For supported AIX, Solaris, or Linux operating systems:
KD4configDC.sh -h

Disabling the application for the data collector

To disable the SAP NetWeaver application for the data collector, depending on the type of application, complete the following steps:

- For a **server application**:
 1. Stop the SAP NetWeaver application server following the procedures in your SAP NetWeaver documentation.
 2. Run the KD4configDC utility to disable the application.
 3. Restart the SAP NetWeaver application server following the procedures in your SAP NetWeaver documentation.

If you manually enabled the server application for the data collector:

Remove the kd4dcagent.jar and ibm-jaxrpc-client.jar files from your application classpath, along with xercesImpl.jar and xml-apis.jar if your application uses a Sun distribution of Java 1.4.2. Remove the changes you made to the web.xml file during the manual enable process. Then reinstall your application into the application server.

- For a **standalone client application**:
 1. Run the KD4configDC utility to disable the data collector.
 2. Modify the classpath used to launch the standalone client application to remove the kd4dcagent.jar file.
 3. Run the application.

If you manually enabled the standalone client application for the data collector:

Remove the kd4dcagent.jar file from the classpath, and remove the changes you made to the lports_1.xml and protocols.txt files during the manual enable process. Then reinstall your application into the application server.

- For a **deployable client application**:
 1. You do not need to stop the SAP NetWeaver application server if it is already running.
 2. Manually remove the modifications you made to the application code when you enabled the application for the data collector.
 3. Remove the kd4dcagent.jar file from the deployable client application.
 4. Redeploy the application.

Running the KD4configDC utility

Run the KD4configDC utility to disable the application for the data collector as follows:

1. Depending on your operating system, navigate to one of the following locations:
 - For supported Windows operating systems, navigate to the directory location: %CANDLE_HOME%\CMA\KD4\bin.
 - For supported AIX operating systems, navigate to the directory location: \$CANDLEHOME/aix433/d4/KD4/bin.
 - For supported Solaris operating systems, navigate to the directory location: \$CANDLEHOME/sol283/d4/KD4/bin.

- For supported Linux (on Intel) operating systems, navigate to the directory location: \$CANDLEHOME/li6243/d4/KD4/bin.
2. Run the following command:

- For supported Windows operating systems:


```
KD4configDC.bat -disable -env 6 {-sapappsdir <apps_dir> |
  -clientappsdir <apps_dir> |
  -sid <home> <sid>}
```
- For supported AIX, Solaris, and Linux operating systems:


```
KD4configDC.sh -disable -env 6 {-sapappsdir <apps_dir> |
  -clientappsdir <apps_dir> |
  -sid <home> <sid>}
```

In these commands, the following parameters are specified:

-disable

Causes the command to disable the data collector for the specified environment.

-env 6 Defines the environment to be disabled as SAP NetWeaver.

-sapappsdir

Specifies that the directory path specified by *<apps_dir>* is the location of the Web services application being monitored. Use this parameter for either a server side application or a deployable client side application.

-clientappsdir

Specifies that the directory path specified by *<apps_dir>* is the location of the Web services application being monitored. Use this parameter for a standalone client side application. There is no default path for the **-clientappsdir** parameter.

If your standalone client application is a .jar file, be sure to specify the full directory path for the location of the .jar file. See the examples that follow.

<apps_dir>

Specifies the directory path of the Web services application being monitored.

-sid <home> <sid>

For this parameter, *<home>* is the SAP home directory, typically **/usr/sap** or **C:\usr\sap**, but it could reside on any drive. The *<sid>* argument is the SAP system ID. Both of these arguments are used to confirm that the directory corresponding to the specified SID exists under the specified home. All Web services applications that are found under the SID are disabled.

Examples:

- `./KD4configDC.sh -disable -env 6 -sid /usr/sap J2E`
 In this example, SAP_HOME and the SAP system name are provided to disable the application for the data collector. The directory **/usr/sap** is the directory where SAP NetWeaver is installed. *J2E* is the SAP system name.
- `KD4configDC.bat -disable -env 6 -sapappsdir /app1`
 In this example, the Web services application directory location */app1* is specified. This might be for disabling a server side or deployable client side application.
- `KD4configDC.bat -disable -env 6 -clientappsdir /app12`
 In this example, the Web services application directory location */app12* is specified. This command disables a standalone client side application.

- `KD4configDC.bat -disable -env 6 -sapappsdir "C:\usr\sap\j2e\JC000\j2ee\cluster\server0\apps"`

In this example, the Web services application directory is specified explicitly. This also shows the directory path surrounded in quotation marks, which must be used if the path contains blank spaces.

- `KD4configDC.sh -disable -env 6 -clientappsdir /usr/sap/j2e/JC000/j2ee/cluster/server0/apps`

This example is for running KD4configDC on a supported AIX, Solaris, or Linux operating system.

- `KD4configDC.sh -disable -env 6 -clientappsdir /usr/sap/Customr/EnterpriseSTDCliientProxy.jar`

In this example, the standalone client application is a .jar file, so the full directory path location of the file is specified.

Additional considerations

As you enable SAP NetWeaver applications for the data collector, keep in mind the following additional considerations:

- In the Tivoli Enterprise Portal, the display pattern for server instances is `D4:<hostname>-<SID>_<instance>_<server>`. This supports the requirement to display each server uniquely in the Tivoli Enterprise Portal.
For example, suppose there are two different SAP NetWeaver servers, *server1* and *server2*, on the same computer system:
 - The hostname of the system is *tiv121*.
 - The SID for both servers is *J2E*
 - The instance for both servers is *00*
 These two servers are each displayed uniquely in the Tivoli Enterprise Portal as `D4:tiv121-J2E_00_S0` and `D4:tiv121-J2E_00_S1`.
- IBM Tivoli Composite Application Manager for SOA uses the port name to identify services. If you have two or more ports deployed that have the same name, these will appear to be the same service in the Tivoli Enterprise Portal displays.
- The first time that the Web service is called, there might be a delay of several seconds due to the data collector loading the WSDL related information for the Web service. On subsequent calls of the Web service, however, data is retrieved as expected.
- When you run the KD4configDC utility to enable and disable applications for the data collector, the configuration file is backed up as follows:
 - For a **server application**, the web.xml file is backed up in the same directory where it is currently located. For example, if the original web.xml file is located in `<apps_dir>/<app01>/web.xml`, the file is backed up to `<apps_dir>/<app01>/web.xml.kd4backup.<timestamp>`, where `<timestamp>` is a timestamp for when the backup is performed.
 - For a **standalone client application that is not a JAR file**, the lport_1.xml file is backed up in the same directory where it is currently located. For example, if the original lport_1.xml file is located in `<standalone_dir>/lport_1.xml`, the file is backed up to `<standalone_dir>/lport_1.xml.kd4backup.<timestamp>`, where `<timestamp>` is a timestamp for when the backup is performed.
 - For a **standalone client application that is a JAR file**, the lport_1.xml file is backed up as `lport_1.xml.kd4backup.<timestamp>`, and packed into the JAR file.

If you experience errors after enabling or disabling your applications, you can restore the backed up configuration file manually.

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 SAP NetWeaver application server runtime environment.

Chapter 7. The WebSphere Community Edition data collector

This chapter describes the support for monitoring of Web services flows in the WebSphere Community Edition (CE) J2EE Application Server v1.0.1.1 environment.

Support for the data collector in this environment is provided for the following operating system platforms:

- RedHat 3
- RedHat 4
- SuSE 9
- Windows XP Pro
- Windows 2003

In general, the data collector for the WebSphere CE environment operates in the same way as the WebSphere, BEA WebLogic, and JBoss environments. The same types of log files are used, messages are filtered in a similar fashion, and performance is comparable. WebSphere CE server instances are identified in the Tivoli Enterprise Portal navigator view in the form of *d4::<hostname>-<port>*.

The KD4configDC utility can be run once to enable available WebSphere CE applications for monitoring. If additional applications are added to the environment after the KD4configDC utility has been run, you must run KD4configDC again to recognize the newly added applications. Applications that are already enabled are not affected.

Enabling applications for the data collector

To enable WebSphere CE applications for the data collector, complete the following steps:

1. You should have already completed the installation procedure for installing Sparkler 2 in the existing IBM Tivoli Composite Application Manager for SOA environment on the computer where your WebSphere CE application server is installed. See “Installing Sparkler 2” on page 6 for details.
2. Ensure that the application server is running before enabling the application for the data collector. Follow the procedures in your WebSphere CE documentation for starting the server.
3. Before enabling the application for the data collector, IBM recommends that you increase the WebSphere CE JVM maximum heap size (Xmx) to 256 MB, and the JVM maximum permanent generation size (MaxPermSize) to 128MB. You can set these values in the JAVA_OPTS keyword as follows:
 - For supported Windows operating systems, edit the <WASCE_HOME>\bin\setenv.bat script file:

```
set JAVA_OPTS=-Xms128m -Xmx256m -XX:PermSize=64m -XX:MaxPermSize=128m  
"-Djava.endorsed.dirs=%GERONIMO_BASE%/lib/endorsed" %JAVA_OPTS%
```
 - For supported Linux operating systems, edit the <WASCE_HOME>/bin/setenv.sh script file:

```
export JAVA_OPTS=-Xms128m -Xmx256m -XX:PermSize=64m -XX:MaxPermSize=128m  
-Djava.endorsed.dirs=$GERONIMO_BASE/lib/endorsed %JAVA_OPTS%
```
4. **Optional:** Run the KD4configDC utility using the `-list` parameter to create a list of applications to be enabled with subsequent runs of the KD4configDC utility.

5. **Optional:** Review and manually modify the file (specified by the **–file** *<filename>* argument specified when you ran the KD4configDC utility) containing the list of applications to be enabled, to exclude those applications that should not be enabled.
6. Run the KD4configDC utility again to enable the applications in the file list, this time not specifying the **–list** parameter. As a result of enabling the applications, each J2EE Web services application is redeployed automatically.
7. During this process each J2EE application is backed up as *<name>.<date>.<hour>.<min>.<sec>.bak.<type>* (where *<type>* is the file type, such as *jar*, *war*, or *ear*), and stored in the *<WASCE_HOME>/temp/KD4* directory, where *<WASCE_HOME>* is the location where WebSphere CE is installed.

These backup files are not automatically removed during the enable or disable process. You should consider removing them when they are no longer needed, to conserve available disk storage.

Running the KD4configDC utility

Run the KD4configDC utility to enable the application for the data collector. Run the KD4configDC utility as follows:

1. Depending on your operating system, navigate to one of the following locations:
 - For supported Windows operating systems, navigate to *%CANDLE_HOME%\CMA\KD4\bin*.
 - For supported Linux (on Intel) operating systems, navigate to *\$CANDLEHOME/li6243/d4/KD4/bin*.
2. Run the following command:
 - For supported Windows operating systems:

```
KD4configDC.bat –enable –env 7 {<WASCE_HOME>}
–user <user name> –passwd <password> [–list] –file <filename>
```
 - For supported Linux operating systems:

```
KD4configDC.sh –enable –env 7 {<WASCE_HOME>}
–user <user name> –passwd <password> [–list] –file <filename>
```

In these commands, the following parameters are specified:

–enable

Causes the command to enable the application for the specified environment.

–env 7

Defines the application server runtime environment for which the application is enabled as WebSphere CE.

<WASCE_HOME>

This is an optional parameter that specifies the directory path where WebSphere CE is installed. If you have already created a *WASCE_HOME* system environment variable, then this parameter is not required. Typical values for this variable are:

- For supported Windows operating systems:
C:\Program Files\IBM\WebSphere\AppServerCommunityEdition
- For supported Linux operating systems:
/opt/IBM/WebSphere/AppServerCommunityEdition

–user <user name>

Specifies a valid WebSphere CE user name that has Administrator authority. See your WebSphere CE documentation for more information

about creating Administrator user names and passwords. See your local system administrator for assistance, if needed.

-passwd *<password>*

Specifies a valid password that is associated with the specified WebSphere CE user name. See your WebSphere CE documentation for more information about creating Administrator user names and passwords. See your local system administrator for assistance, if needed.

-list

This is an optional parameter that, when specified, causes the utility to create a list of available applications that can be later enabled or disabled, and store this list in the specified file name indicated by the `-file <filename>` parameter. Note that the specified enable or disable operation is **not** performed at this time, only the file is created for future enable or disable operations (in this special case you must specify either `-enable` or `-disable` in the command, but it is ignored).

You should examine this file and modify it as needed to exclude certain applications from the list that you do not want to enable or disable with subsequent runs of the KD4configDC utility.

Is your application deployed with an external plan file? The application is redeployed as part of the enable or disable operation, so if your application must be deployed with an external plan file, you should exclude that application from the list.

Subsequent runs of the KD4configDC utility use the list of files in the specified `<filename>` until you overwrite the contents of the file with another command using the `-list` parameter.

-file *<filename>*

This parameter is used in two different ways, depending on whether or not the `-list` parameter is also specified in the KD4configDC command:

- If `-list` is specified, the file name indicated by `<filename>` is created relative to the current directory location. For example, if you navigated to `/KD4/bin` to run the KD4configDC utility, this file is created in that directory. You can also specify a fully qualified file and path. All WebSphere CE Web services applications that are eligible to be enabled or disabled in subsequent runs of the KD4configDC utility are discovered and listed in the designated file. Note that no enable or disable operation is performed on these applications at this time, only the list is created and stored in the file. After the list is created, you can modify this list manually to exclude applications that you do not want to be enabled or disabled with subsequent runs of the KD4configDC utility (for example, those deployed with an external plan file).
- If `-list` is not specified, then it is assumed that this file already exists (from a previous run of the KD4configDC utility) and contains the list of WebSphere CE applications that you want to enable or disable. The KD4configDC utility reads the file specified by `<filename>` and performs the enable or disable operation on each application that is not already enabled or disabled.

Note that applications in the list that are already enabled or disabled are not changed. A message is displayed indicating that they are ignored for this operation.

If the specified file name already exists, it is overwritten.

Do not use reserved file names: When you specify the file name to be created with the `-list -file <filename>` parameters, do not use the name of a reserved file that is already in the current directory. For example, if you are in the `\KD4\bin` directory, do not use existing file names, such as `KD4configDC.bat`, or `configWASCEDC.bat`. This will overwrite these files and cause errors in operation, and you will need to recover these files from the installation media.

You should either specify a fully qualified unique file and directory path, create a separate folder for this file within the current directory, or create a unique file name and use it consistently each time when you run the `KD4configDC` utility using the `-list` parameter. If you use different file names with different runs of the `KD4configDC` utility, they are all stored in the current directory and you must keep track of which file to specify in subsequent enable or disable operations.

Examples:

- `KD4configDC.bat -enable -env 7 C:\WASCE -user system -passwd manager -list -file filelist01`

In this example, the value of `WASCE_HOME` has been provided, along with a valid user name and password. Because the `-list` parameter is specified, the utility initiates a discovery of the eligible WebSphere CE applications that can be enabled or disabled with later runs of the `KD4configDC` utility, and writes that list to the file name `filelist01` in the current directory. Even though the `-enable` parameter is specified, it is ignored for this command and no applications are enabled.

After this command completes, you have the opportunity to manually modify this file and remove any applications that you do not want to be enabled or disabled with subsequent runs of the `KD4configDC` utility.

- `KD4configDC.bat -enable -env 7 C:\WASCE -user system -passwd manager -list -file files\filelist01`

In this example, the list of eligible files is stored in `filelist01`, which is created in the `\files` folder under the current directory. Specifying a separate folder might be a good practice to avoid potentially writing over existing reserved files in the current directory.

- `KD4configDC.bat -enable -env 7 C:\WASCE -user system -passwd manager -list -file "D:\WASCE files\filelist01"`

In this example, the list of eligible files is stored in `filelist01`, which is created in the `"\WASCE files"` folder on the D: drive. This example shows that you can specify a fully qualified file name and path for the file list. Also, if the fully qualified path contains a blank character, the path is surrounded with quotation marks.

- `KD4configDC.bat -enable -env 7 C:\WASCE -user system -passwd manager -file filelist01`

In this example, the `-list` parameter is not specified, and now `KD4configDC` reads the contents of the file `filelist01` in the current directory, and performs the enable operation on all applications in the list that are not already enabled for this data collector. If an application in the list is already enabled, it is ignored and its state is not changed. If an application is specified in the list that cannot be found, a message is displayed and the command continues to the next application in the file. If the specified file is not found in the current directory, an error message is displayed.

- `KD4configDC.bat -enable -env 7 -user cde321 -passwd xxx111xxx -file filelist01`

In this example, the `WASCE_HOME` environment variable has been set, and is used by default when the command is run.

- `KD4configDC.bat -enable -env 7 "C:\Program Files\IBM\WebSphere\AppServerCommunityEdition" -user abc123 -passwd xyz010 -file filelist01`

In this example, the value of `WASCE_HOME` is specified, and, because it includes a blank space, is surrounded with quotation marks.

- `KD4configDC.sh -enable -env 7 /opt/IBM/WebSphere/AppServerCommunityEdition -user user1 -passwd zz11zz -file filelist01`

This example is for running the `KD4configDC` utility on a supported UNIX operating system.

You can issue the following command to view the online help for `KD4configDC`:

- For supported Windows operating systems:

```
KD4configDC.bat -h
```

- For supported Linux operating systems:

```
KD4configDC.sh -h
```

Messages related to running the `KD4configDC` utility are documented in Appendix A, “Messages,” on page 67.

Enabling applications manually

You might have used a custom plan file to deploy your WebSphere CE application. If so, then you need to perform some additional manual steps to enable these WebSphere CE applications for the data collector:

1. If you have not already run the `KD4configDC` utility to enable other WebSphere CE applications that use the default plan file, you must run the `KD4configDC` utility (using the procedure described in the previous section) once to place the necessary JAR files into their correct locations. Specify an empty file as the value for the `-file` argument. This results in the message `KD4CF0038E` being displayed, indicating that there are no applications to be enabled. You can ignore this message.

If you have already run the `KD4configDC` utility for at least one WebSphere CE application that uses the default plan file, then this step is already completed and you do not need to run the utility again.

2. Edit the custom deployment plan file. Within each `<web-app>` or `<openejb-jar>` element, add the following `<dependency>` and `<hidden-classes>` elements:

```
<dependency xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
  <uri>KD4/kd4dcagent/6.0/jar</uri>
</dependency>
<dependency xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
  <uri>KD4/ibm-jaxrpc-client/6.0.2/jar</uri>
</dependency>
<hidden-classes xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
  <filter>com.ibm.wsd1</filter>
</hidden-classes>
<hidden-classes xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
  <filter>javax.wsd1.factory.WSDLFactory</filter>
</hidden-classes>
```

The following example shows how to add `<dependency>` and `<hidden-classes>` elements within a `<web-app>` element:

```
<web-app xmlns="http://geronimo.apache.org/xml/ns/web"
  xmlns:sys="http://geronimo.apache.org/xml/ns/deployment-1.0"
  xmlns:naming="http://geronimo.apache.org/xml/ns/naming-1.0"
  xmlns:security="http://geronimo.apache.org/xml/ns/security-1.0"
  configId="com/ibm/j2g/webservices.war">
  <dependency xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
    <uri>KD4/kd4dcagent/6.0/jar</uri>
```

```

</dependency>
<dependency xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
  <uri>KD4/ibm-jaxrpc-client/6.0.2/jar</uri>
</dependency>
<hidden-classes xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
  <filter>com.ibm.wsd1</filter>
</hidden-classes>
<hidden-classes xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
  <filter>javax.wsd1.factory.WSDLFactory</filter>
</hidden-classes>

<context-root>/webservises</context-root>
<context-priority-classloader>>false</context-priority-classloader>
</web-app>

```

The following example shows how to add <dependency> and <hidden-classes> elements within an <openejb-jar> element:

```

<openejb-jar xmlns="http://www.openejb.org/xml/ns/openejb-jar"
  configId="com/ibm/dw/bookshop" parentId="BookShopDB">
  <dependency xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
    <uri>KD4/kd4dcagent/6.0/jar</uri>
  </dependency>
  <dependency xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
    <uri>KD4/ibm-jaxrpc-client/6.0.2/jar</uri>
  </dependency>
  <hidden-classes xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
    <filter>com.ibm.wsd1</filter>
  </hidden-classes>
  <hidden-classes xmlns="http://geronimo.apache.org/xml/ns/deployment-1.0">
    <filter>javax.wsd1.factory.WSDLFactory</filter>
  </hidden-classes>

  <enterprise-beans>
    <entity>
      <ejb-name>CategoryBean</ejb-name>
      <jndi-name>CategoryBean</jndi-name>
      <table-name>categories</table-name>
      <cmp-field-mapping>
        <cmp-field-name>catId</cmp-field-name>
        <table-column>catId</table-column>
      </cmp-field-mapping>
      <cmp-field-mapping>
        <cmp-field-name>name</cmp-field-name>
        <table-column>name</table-column>
      </cmp-field-mapping>
      <resource-ref>
        <ref-name>jdbc/basic/BookShopDatabase</ref-name>
        <application>>null</application>
        <module>BooksShopDB</module>
        <name>BookShopDBPool</name>
      </resource-ref>
    </entity>
  </enterprise-beans>
</openejb-jar>

```

3. Add the IBM Tivoli Composite Application Manager for SOA server side handler to all of the handler chains in the webservises.xml files within the application (if the application does not contain webservises.xml, skip this step).

Modify the webservises.xml files by adding the following lines:

```

<handler>
  <handler-name>KD4ServerHandler</handler-name>
  <handler-class>
    com.ibm.management.soa.agent.wasce.ITMWASCEServerHandler
  </handler-class>
</handler>

```

The following example shows how to add the server side handler to webservices.xml:

```
<?xml version="1.0" encoding="UTF-8"?>
<webservices xmlns="http://java.sun.com/xml/ns/j2ee" version="1.1">
  <webservice-description>
    <webservice-description-name>SearchPhones</webservice-description-name>
    <wsdl-file>WEB-INF/wsdl/search-phones-service.wsdl</wsdl-file>
    <jaxrpc-mapping-file>
      WEB-INF/search-phones-server-mapping.xml
    </jaxrpc-mapping-file>
    <port-component>
      <port-component-name>SearchPhonesService</port-component-name>
      <wsdl-port>SearchPhonesService</wsdl-port>
      <service-endpoint-interface>
        com.ibm.j2g.webservices.server.SearchPhonesPortType
      <service-endpoint-interface>
      <service-impl-bean>
        <servlet-link>SearchPhonesServer</servlet-link>
      </service-impl-bean>
      <handler>
        <handler-name>KD4ServerHandler</handler-name>
        <handler-class>
          com.ibm.management.soa.agent.wasce.ITMWASCEServerHandler
        </handler-class>
      </handler>
    </port-component>
  </webservice-description>
</webservices>
```

If there are multiple <port-component> elements, you must add one <handler> element within each <port-component> element.

4. If the application contains a web.xml file and the web.xml file includes a <service-ref> element, you must add the IBM Tivoli Composite Application Manager for SOA client handler to the handler chain in web.xml. If there is no web.xml file or an existing web.xml file does not include a <service-ref> element, skip this step.

Modify the web.xml file by adding the following lines:

```
<handler>
  <handler-name>ClientHandler</handler-name>
  <handler-class>
    com.ibm.management.soa.agent.wasce.ITMWASCEClientHandler
  </handler-class>
</handler>
```

The following example shows how to add the client handler to the handler chain in web.xml:

```
<?xml version="1.0" encoding="UTF-8"?>
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee
    http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd" version="2.4">
  <servlet>
    <servlet-name>SearchPhonesServer</servlet-name>
    <servlet-class>
      com.ibm.j2g.webservices.server.SearchPhonesServer
    </servlet-class>
  </servlet>
  <servlet-mapping>
    <servlet-name>SearchPhonesServer</servlet-name>
    <url-pattern>/server</url-pattern>
  </servlet-mapping>
  <service-ref>
    <service-ref-name>service/SearchPhones</service-ref-name>
    <service-interface>
      com.ibm.j2g.webservices.client.SearchPhonesService
    </service-interface>
  </service-ref>
</web-app>
```

```

        </service-interface>
        <wsdl-file>WEB-INF/wsdl/search-phones-service.wsdl</wsdl-file>
        <jaxrpc-mapping-file>
            WEB-INF/search-phones-client-mapping.xml
        </jaxrpc-mapping-file>
        <handler>
            <handler-name>KD4ClientHandler</handler-name>
            <handler-class>
                com.ibm.management.soa.agent.wasce.ITMWASCEClientHandler
            </handler-class>
        </handler>
    </service-ref>
</web-app>

```

5. If the application contains the ejb-jar.xml file and the ejb-jar.xml file includes the <service-ref> element, you must add the IBM Tivoli Composite Application Manager for SOA client handler to the handler chain in ejb-jar.xml. If there is no ejb-jar.xml in the application, or if an existing ejb-jar.xml file does not include the <service-ref> element, skip this step.

The following example shows how to add the client handler to the handler chain in ejb-jar.xml:

```

<?xml version="1.0" encoding="UTF-8"?>
<ejb-jar xmlns="http://java.sun.com/xml/ns/j2ee" version="2.1"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee
    http://java.sun.com/xml/ns/j2ee/ejb-jar_2_1.xsd">
  <enterprise-beans>
    <session>
      <ejb-name>BookShopEJB</ejb-name>
      <local-home>com.ibm.dw.bookshop.ejb.BookShopLocalHome</local-home>
      <local>com.ibm.dw.bookshop.ejb.BookShopLocal</local>
      <ejb-class>com.ibm.dw.bookshop.ejb.BookShopBean</ejb-class>
      <session-type>Stateless</session-type>
      <transaction-type>Container</transaction-type>
      <service-ref>
        <service-ref-name>service/Service</service-ref-name>
        <service-interface>javax.xml.rpc.Service</service-interface>
        <wsdl-file>META-INF/wsdl/CurrencyExchangeService.wsdl</wsdl-file>
        <jaxrpc-mapping-file>
            META-INF/client-jaxrpc-mapping.xml
        </jaxrpc-mapping-file>
        <service-qname xmlns:ns=
            "http://www.xmethods.net/sd/CurrencyExchangeService.wsdl">
            ns:CurrencyExchangeService
        </service-qname>
        <handler>
            <handler-name>KD4ClientHandler</handler-name>
            <handler-class>
                com.ibm.management.soa.agent.wasce.ITMWASCEClientHandler
            </handler-class>
        </handler>
      </service-ref>
    </session>
  </enterprise-beans>
</ejb-jar>

```

6. Redeploy the application into the application server.

Disabling applications for the data collector

To disable WebSphere CE applications for the data collector, complete the following steps:

1. Ensure that the application server is running.

2. **Optional:** Run the KD4configDC utility using the `-list` parameter to create a list of applications to be disabled with subsequent runs of the KD4configDC utility.
3. **Optional:** Review and manually modify the file containing the list of applications to be disabled, to exclude those applications that should not be disabled.
4. Run the KD4configDC utility again to disable the applications in the file list, this time not specifying the `-list` parameter. As a result of disabling the applications, each J2EE Web services application is redeployed automatically.
5. If ALL Web services applications are disabled for this data collector, do the following:
 - a. Shut down the application server.
 - b. Navigate to the `<WASCE_HOME>/repository/KD4` directory and manually remove the entire directory and all contents.
 - c. Restart the WebSphere CE application server.

Running the KD4configDC utility

Run the KD4configDC utility to disable applications for the data collector as follows:

1. Depending on your operating system, navigate to one of the following locations:
 - For supported Windows operating systems, navigate to `%CANDLE_HOME%\CMA\KD4\bin`.
 - For supported Linux (on Intel) operating systems, navigate to `$CANDLEHOME/li6243/d4/KD4/bin`.
2. Run the following command:
 - For supported Windows operating systems:
`KD4configDC.bat -disable -env 7 {<WASCE_HOME>} -user <user name> -passwd <password> [-list] -file <filename>`
 - For supported Linux operating systems:
`KD4configDC.sh -disable -env 7 {<WASCE_HOME>} -user <user name> -passwd <password> [-list] -file <filename>`

In these commands, the following parameters are specified:

-disable

Causes the command to disable the applications for the specified environment.

-env 7 Defines the environment to be disabled as WebSphere CE.

<WASCE_HOME>

This is an optional parameter that specifies the directory path where WebSphere CE is installed. If you have already created a `WASCE_HOME` system environment variable, then this parameter is not required.

-user <user name>

Specifies a valid WebSphere CE user name that has Administrator authority. See your WebSphere CE documentation for more information about creating Administrator user names and passwords. See your local system administrator for assistance, if needed.

-passwd <password>

Specifies a valid password that is associated with the specified WebSphere CE user name. See your WebSphere CE documentation for more information about creating Administrator user names and passwords. See your local system administrator for assistance, if needed.

-list This is an optional parameter that, when specified, causes the utility to create a list of available applications that can be later enabled or disabled, and store this list in the specified file name indicated by the `-file <filename>` parameter. Note that the specified enable or disable operation is **not** performed at this time, only the file is created for future enable or disable operations (in this special case you can specify either `-enable` or `-disable` in the command, and it is ignored).

You should examine this file and modify it as needed to exclude certain applications from the list that you do not want to enable or disable with subsequent runs of the KD4configDC utility.

Is your application deployed with an external plan file? The application will be redeployed as a part of the enable or disable operation, so if your application must be deployed with an external plan file, you should exclude that application from the list.

Subsequent runs of the KD4configDC utility use the list of files in the specified `<filename>` until you overwrite the contents of the file with another command using the `-list` parameter.

-file <filename>

This parameter is used in two different ways, depending on whether or not the `-list` parameter is also specified when the KD4configDC utility is run:

- If `-list` is specified, the file name indicated by `<filename>` is created relative to the current directory location. For example, if you navigated to `/KD4/bin` to run the KD4configDC utility, this file is created in that directory. You can also specify a fully qualified file name and directory path. All WebSphere CE Web services applications that are eligible to be enabled or disabled in subsequent runs of the KD4configDC utility are discovered and listed in the designated file. Note that no enable or disable operation is performed on these applications at this time, only the list is created and stored in the file. After the list is created, you can modify this list manually to exclude applications that you do not want to be enabled or disabled with subsequent runs of the KD4configDC utility (for example, those deployed with an external plan file).
- If `-list` is not specified, then it is assumed that this file already exists (from a previous run of the KD4configDC utility) and contains the list of WebSphere CE applications that you want to enable or disable. The KD4configDC utility reads the file specified by `<filename>` and performs the enable or disable operation on each application that is not already enabled or disabled.

Note that applications in the list that are already enabled or disabled are not changed. A message is displayed indicating that they are ignored for this operation.

If the specified file name already exists, it is overwritten.

Do not use reserved file names: When you specify the file name to be created with the `-list -file <filename>` parameters, do not use the name of a reserved file that is already in the current directory. For example, if you are in the `\KD4\bin` directory, do not use existing file names, such as `KD4configDC.bat`, or `configWASCEDC.bat`. This overwrites these files and cause errors in operation, and you will need to recover these files from the installation media.

You should either create a separate folder for this file within the current directory, or create a unique file name and use it consistently each time when you run the KD4configDC utility using the `-list` parameter. If you use different file names with different runs of the KD4configDC utility, they are all stored relative to the current directory and you must keep track of which file to specify in subsequent enable or disable operations.

Examples:

- `KD4configDC.bat -disable -env 7 C:\WASCE -user system -passwd manager -list -file filelist01`

In this example, the value of `WASCE_HOME` has been provided, along with a valid user name and password. Because the `-list` parameter is specified, the utility initiates a discovery of the eligible WebSphere CE applications that can be enabled or disabled with later runs of KD4configDC, and writes that list to the file name *filelist01* in the current directory. Even though the `-disable` parameter was specified, it is ignored for this command and no applications are disabled.

After this command completes, you have the opportunity to manually modify this file and remove any applications that you do not want to be enabled or disabled with subsequent runs of the KD4configDC utility.

- `KD4configDC.bat -disable -env 7 C:\WASCE -user system -passwd manager -list -file files\filelist01`

In this example, the list of eligible files is stored in *filelist01*, which is created in the `\files` folder under the current directory. Specifying a separate folder might be a good practice to avoid potentially writing over existing reserved files in the current directory.

- `KD4configDC.bat -disable -env 7 C:\WASCE -user system -passwd manager -list -file "D:\WASCE files\filelist01"`

In this example, the list of eligible files is stored in *filelist01*, which is created in the "`\WASCE files`" folder on the D: drive. This example shows that you can specify a fully qualified file name and path for the file list. Also, if the fully qualified path contains a blank character, the path is surrounded with quotation marks.

- `KD4configDC.bat -disable -env 7 C:\WASCE -user system -passwd manager -file filelist01`

In this example, the `-list` parameter is not specified, and now KD4configDC reads the contents of the file *filelist01* in the current directory, and performs the disable operation on all applications in the list that are not already disabled for this data collector. If an application in the list is already disabled, it is ignored and its state is not changed. If an application is specified in the list that cannot be found, an message is displayed and the command continues to the next application in the file. If the specified file is not found in the current directory, an error message is displayed.

- `KD4configDC.bat -disable -env 7 -user cde321 -passwd xxx111xxx -file filelist01`

In this example, the `WASCE_HOME` environment variable has been set, and is used by default when the command is run.

- `KD4configDC.bat -enable -env 7 "C:\Program Files\IBM\WebSphere\AppServerCommunityEdition" -user abc123 -passwd xyz010 -file filelist01`

In this example, the value of `WASCE_HOME` is specified, and, because it includes a blank space, is surrounded with quotation marks.

- `KD4configDC.sh -enable -env 7 /opt/IBM/WebSphere/AppServerCommunityEdition -user user1 -passwd zz11zz -file filelist01`

This example is for running KD4configDC on a supported UNIX operating system.

Disabling applications manually

You might have used a custom plan file to deploy your WebSphere CE application. If so, you need to perform some additional manual steps to remove the <handler>, <dependency>, and <hidden-classes> declarations that you added manually when the data collector was enabled for these applications. See “Enabling applications manually” on page 57 for more information on these declarations that were manually added.

If this is the last WebSphere CE application using the data collector for IBM Tivoli Composite Application Manager for SOA, then after manually removing the declarations, run the KD4configDC utility to remove the associated JAR files from their locations.

After manually disabling the data collector, redeploy the WebSphere CE application.

Additional considerations

When you configure filter controls to block messages, the WebSphere CE data collector only supports the asterisk wild card (*) character in the **IP** field. If you specify a hostname or IP address in that field, the data collector filtering will not match any messages.

Chapter 8. Problem Determination

This chapter describes some typical problems you might encounter while installing or using the product, and procedures to recover from error situations.

Running the KD4configDC utility

This section includes information about problems that you might encounter while running the KD4configDC utility to enable and disable applications for the data collector.

KD4configDC terminates with CTRL-C

On supported Windows operating systems, if you type CTRL-C (press the CTRL and C keys at the same time on the keyboard) while the KD4configDC utility is running, you are asked if you want to terminate the batch job:

```
Terminate batch job (Y/N)?
```

If you respond by typing *N*, the utility is terminated anyway with return code of 130, and the following message is displayed:

```
The installation utility failed with RC = 130.
```

You should avoid typing CTRL-C when running the KD4configDC utility to allow it to complete normally. If the utility is terminated prematurely, you can run the command again to complete the enable or disable operation.

Running multiple KD4configDC instances at the same time

The KD4configDC utility is not designed to run with another instance of itself at the same time. Do not run more than one instance of this utility on the same computer system at the same time, for example, by attempting to enable two or more applications at the same time.

This also applies if you attempt to enable an application from one console while attempting to disable an application from another console. Both instances of KD4configDC will write to the install and trace log files at the same time, resulting in mixed content that is difficult to read.

The SAP NetWeaver environment

This section includes information about problems that you might encounter while using the data collector in the SAP NetWeaver application server runtime environment.

SAP applications disabled after changing the application directory

In the SAP NetWeaver environment, the Deploy Service feature of the Visual Administrator tool provides a way to change the default directory path within the file system where each deployed application is stored. For example, you might choose to change from the default directory path of *./apps* to *./apps66*.

After changing the application directory path, the SAP application server must be restarted. After restarting the server, the new directory path (for example, *./apps66*) is created, and all applications in the previous *./apps* directory path are now deployed to *./apps66*. The Web services applications that were already enabled in

the previous `./apps` directory are now **disabled** in the new directory. So you must enable these applications again in the new directory path using the `KD4configDC` utility.

Fault code and string displayed as *unknown* in the Services Inventory table

In the Services Inventory table of the Tivoli Enterprise Portal, you might see the information for SAP NetWeaver displayed with the fault code and faults string fields shown as *unknown*. Due to a known limitation with the data collector in the SAP NetWeaver environment, this information is not available.

The WebSphere CE environment

This section includes information about problems that you might encounter while using the data collector in the WebSphere CE application server runtime environment.

Multiple WebSphere CE server instances using the same port

If you run multiple instances of the WebSphere CE server at the same time but do not specify a unique port for each server, you might experience problems when attempting to enable or disable applications. The `KD4configDC` utility fails with return code 184, indicating a problem connecting to the JMX.

WebSphere CE version 1.0.1 does not support multiple servers using the same configuration port number.

To resolve this problem, stop all WebSphere CE server instances and then start only one server to enable or disable your applications.

Service name displayed as *unknown* in Tivoli Enterprise Portal

In the Tivoli Enterprise Portal, you might see the service name for WebSphere CE data displayed as *unknown*. If so, examine the WSDL file for the Web services application, located in a directory similar to `<WASCE_HOME>/config-store/<app_ID>/<app_type>/WEB-INF`.

You might see the WSDL file port information defined similar to the following example:

```
<port><soap:address location="REPLACE_WITH_ACTUAL_URL" /></port>
```

You must manually replace the string `REPLACE_WITH_ACTUAL_URL` with the real URL for the location, and then restart the application.

Appendix A. Messages

KD4CF0001E Connecting to the WebSphere CE JMX service was not successful. Verify that the user name: *user_name* and password are correct.

Explanation: To enable or disable data collector on WebSphere CE Application Server, you must provide a valid WebSphere CE administrator user name and password to connect to the JMX service.

Operator response: Ask your system administrator to provide a valid user name and password.

KD4CF0002E Cannot connect to the WebSphere CE JMX service.

Explanation: The attempt to connect to the WebSphere CE JMX service was not successful. Possible causes include:

- The WebSphere CE application server is not active.
- The JMX service is not configured correctly.

Administrator Response: Verify that the WebSphere CE application server is active and operational, and that the JMX service is configured correctly.

KD4CF0003E Cannot find any installed Web Services applications to enable for the data collector.

Explanation: No Web Services applications have been found to enable for data collection. It is possible that no Web services have been installed, or an unexpected error has occurred.

Operator response: Verify that Web services applications are installed. If the error continues after Web Services applications are installed, contact IBM Software Support.

KD4CF0004E Cannot read the configuration file: *config_file*

Explanation: The configuration file located at `$WASCE_HOME/var/config/config.xml` could not be read. Possible causes:

- The configuration file does not exist.
- The content of the configuration file is not correct.
- An unexpected error occurred while attempting to read the configuration file.

Operator response: Verify that the configuration file `config.xml` exists and is located under the WebSphere CE installation directory at `$WASCE_HOME/var/config/config.xml`. Verify that the content is correct. If the error continues after verifying these items, contact IBM Software Support.

KD4CF0005E Cannot read the application index properties file: *index_file*

Explanation: The application index properties file located at `$WASCE_HOME/config-store/index.properties` could not be read. Possible causes:

- The index properties file does not exist.
- The content of the index properties file is not correct.
- An unexpected error occurred while attempting to read the index properties file.

Operator response: Verify that the `index.properties` file exists and is located under the WebSphere CE installation directory at `$WASCE_HOME/config-store/index.properties`. Verify that the content is correct. If the error continues after verifying these items, contact IBM Software Support.

KD4CF0006E Cannot find the WebSphere CE installation home directory: *WASCE_HOME*.

Explanation: The installation home directory for WebSphere CE, usually identified by the environment variable `WASCE_HOME`, cannot be located. It is possible that this environment variable has not yet been set, or you are not allowed to access that location.

Operator response: Verify that the `WASCE_HOME` environment variable has been set to the location where WebSphere CE is installed, and verify that you are allowed to access that directory. See your local system administrator for assistance.

KD4CF0007E Cannot re-deploy the Web services application: *ModuleId*.

Explanation: An attempt to re-deploy the Web Services application using an automated script was not successful.

Operator response: Deploy the Web Services application manually, and examine the automated script to determine the cause of the error.

KD4CF0008E Cannot parse the deployment description file: *file* for the application: *app*.

Explanation: The deployment description file for the specified application cannot be parsed. The file might be damaged or an unexpected error might have occurred.

Operator response: Verify that the deployment description file is not damaged, or correct any unexpected errors. Deploy the application again and try

KD4CF0009E • KD4CF0021E

running the script again. If the error persists, contact IBM Software Support.

KD4CF0009E Cannot find any installed Web Services applications to disable for the Data Collector.

Explanation: No Web Services applications have been found to disable for data collection. It is possible that no Web services have been installed, or an unexpected error has occurred.

Operator response: Verify that Web services applications are installed. If the error persists after Web Services applications are installed, contact IBM Software Support.

KD4CF0010E An unexpected error has occurred.

Explanation: See message text.

Operator response: Contact IBM Software Support.

KD4CF0011W The backup of the application: *File* failed.

Explanation: The backup of the application was not successful. This might be caused by a lack of local storage space, or the user attempting to perform the enable or disable operation does not have proper write authority.

Operator response: Verify that there is sufficient space in local storage for the backup operation to complete successfully. Also verify that the user name running the enable or disable command has write access to the \$WASCE_HOME/temp/KD4 directory. Then try the backup again.

KD4CF0012I Application *File* is backed up to *File*

Explanation: A backup of the application has been stored in \$WASCE_HOME/temp/KD4.

Operator response: None.

KD4CF0013I All of the existing Web services applications are being backed up to: *File*

Explanation: The Web services applications are backed up and stored in the temporary location: \$WASCE_HOME/temp/KD4.

Operator response: None.

KD4CF0014E The parameters specified in the KD4configDC command to enable or disable the WebSphere CE data collector are not correct. The enable or disable operation did not complete successfully.

Explanation: The KD4configDC command was specified with one or more parameters or values that are not correct for enabling or disabling the WebSphere CE data collector.

Operator response: Refer to the documentation for the correct syntax of the KD4configDC command and try again.

KD4CF0015I The Web services application: *app* is disabled.

Explanation: No additional information is available for this message.

KD4CF0016I The Web services application: *app* is enabled.

Explanation: No additional information is available for this message.

KD4CF0018E An unexpected error has occurred.

Explanation: The installation program might not be configured correctly.

Operator response: Examine the trace log for more details, correct any errors, and try the operation again.

KD4CF0019E User privileges are not sufficient for accessing the following directory: *Directory*

Explanation: The current user does not have adequate privileges to access the specified directory. The user should have read and write authority.

Operator response: Check the user privileges for the directory and update them as needed. Contact your local system administrator for assistance.

KD4CF0020E The following file or directory was not found: *Directory*

Explanation: The specified file or directory could not be located.

Operator response: Verify that the specified file or directory exists and repeat the operation.

KD4CF0021E An error occurred while attempting to read from or write to the following directory: *Directory*

Explanation: The attempt to access the specified file during an enable or disable operation was not successful. Possible causes:

- There might be another process using the file.
- The disk storage space might be full.
- The user might not have write permission to the directory.

Operator response: Be sure to shut down the application server during an enable or disable operation. Verify that there is adequate disk space, and that the user has write permission to the directory, then try the operation again.

KD4CF0022I The enable operation for the SAP NetWeaver data collector completed successfully under the directory:
Directory

Explanation: No additional information is available for this message.

KD4CF0023I The disable operation for the SAP NetWeaver data collector completed successfully under the directory:
Directory

Explanation: No additional information is available for this message.

KD4CF0024I The following file is updated for the SAP NetWeaver data collector:
Directory

Explanation: No additional information is available for this message.

KD4CF0025E The parameters specified in enable or disable command for the SAP NetWeaver data collector are not correct. The enable or disable operation did not complete successfully. The incorrect input parameters are: *Param*

Explanation: An enable or disable operation for the SAP NetWeaver data collector using KD4configDC was attempted using one or more incorrect parameters.

Operator response: Refer to the documentation for the correct syntax of the KD4configDC command and try again.

KD4CF0026W The file *File* is missing, skip to delete it.

Explanation: An unexpected error occurred. The class file might be lost.

Operator response: This missing file can be ignored if it does not cause any other error.

KD4CF0027I The following file is updated for the SAP NetWeaver data collector:
Directory

Explanation: No additional information is available for this message.

KD4CF0028I The following file is removed for the SAP NetWeaver data collector:
Directory

Explanation: No additional information is available for this message.

KD4CF0029E No Web services client applications under the directory: *Directory* have been enabled for the SAP NetWeaver data collector.

Explanation: This error is caused by one of following conditions:

- There are no Web services client applications located in the specified directory.
- A Web services client application exists in the specified directory, but application has already been enabled for the data collector.

Operator response: Verify that there is a Web services client application located in the specified directory and that it has not already been enabled for the data collector.

KD4CF0030E No Web services client applications under the directory: *Directory* have been disabled for the SAP NetWeaver data collector.

Explanation: This error is caused by one of following conditions:

- There are no Web services client applications located in the specified directory.
- A Web services client application exists in the specified directory, but has not been enabled for the data collector.

Operator response: Verify that there is a Web services client application located in the specified directory and that the application has not already been enabled for that data collector.

KD4CF0031E No Web services servers under the directory: *Directory* have been enabled for the SAP NetWeaver data collector.

Explanation: This error is caused by one of following conditions:

- There are no Web services applications located in the specified directory.
- One or more Web services applications exist in the specified directory, but all of the applications have already been enabled for the data collector.

Operator response: Verify that there are Web services applications located in the specified directory and that one or more of the applications are not already enabled for the data collector.

KD4CF0032E No Web services servers under the directory: *Directory* have been disabled for the SAP NetWeaver data collector.

Explanation: This error is caused by one of following conditions:

- There are no Web services applications located in the specified directory.
- One or more Web services applications exist in the specified directory, but the all of the applications are already disabled for the data collector.

Operator response: Verify that there are Web services applications located in the specified directory and that one or more applicaitons are already enabled for the data collector.

KD4CF0033E An error occurred while updating the configuration file: *File*

Explanation: An error occurred while parsing or modifying the lports_1.xml file during the enabling or disabling of a standalone client Web services application for the data collector. Possible causes:

- The file might be in use by another application.
- The file might be damaged.
- The user does not have write permission to access the file.

Operator response: Verify that the configuration file lport.xml is not damaged or already in use, and that the user has authority to write to the file, then try the operation again. If the problem persists, contact IBM Software Support.

KD4CF0034E An error occurred while updating the configuration file: *File*

Explanation: An error occurred while parsing or modifying the protocols.txt file during the enabling or disabling of a stand-alone client Web services application for the data collector. Possible causes:

- The file might be in use by another application.
- The file might be damaged.
- The user does not have write permission to access the file.

Operator response: Verify that the configuration file protocol.txt is not damaged or already in use, and that the user has authority to write to the file, and try the operation again. If the problem persists, contact IBM Software Support.

KD4CF0035E An error occurred while updating the configuration file: *File*

Explanation: An error occurred while parsing or modifying the web.xml file during the enabling or disabling of a server Web services application for the data collector. Possible causes:

- The file might be in use by another application.
- The file might be damaged.
- The user does not have write permission to access the file.

Operator response: Verify that the configuration file web.txt is not damaged or already in use, and that the user has authority to write to the file, and try the operation again. If the problem persists, contact IBM Software Support.

KD4CF0036E The SAP HOME: *SAP Home* with SID: *SID* is not valid. Verify that it exists and is configured with the default settings.

Explanation: The values for SAP Home and SID are not valid. This command will be successful when the values for SAP Home and SID are correct and the system is configured with default settings.

Operator response: Correct the values for SAP Home and SID, and configure the system with the default settings. Then run the command again.

KD4CF0037E The file for the applications list: *Filename* is not valid. Verify the path and file name.

Explanation: You might have specified an incorrect file path for the file containing application lists, or an unexpected I/O exception might have occurred while accessing the file.

Operator response: Verify that the specified file name and directory path are correct.

Verify that the user name you are using has read and write permission to the file.

KD4CF0038E The file: *Filename* that was specified for the applications list does not contain any applications.

Explanation: The applications list file must contain at least one application defined in the file.

Operator response: Verify that at least one application is defined in the file, and try the operation again.

KD4CF0039W The application: *appname* defined in the file: *file* is already enabled for the data collector.

Explanation: The application is already enabled for the data collector, so the enable command has no effect on this application. The application remains enabled. Other applications in the file that are not already enabled for this data collector are enabled by this command.

Operator response: None.

KD4CF0040W The application: *appname* defined in file: *file* has not yet been enabled for the data collector.

Explanation: The application has not yet been enabled for the data collector, so the disable command has no effect on this application. The application remains disabled. Other enabled applications in the file are disabled by this command.

Operator response:

KD4CF0041W The application: *appname* defined in the file: *file* is not a valid Web services application. This operation has no effect.

Explanation: The specified application is not a valid Web services application.

Operator response: Verify that the application is a valid Web services application and try the operation again, or specify another valid Web services application.

KD4CF0042W No Web services applications have been discovered. No applications have been added to the list in: *filename* .

Explanation: It is possible that no Web services application is installed.

Operator response: Verify that there is at least one Web services application installed and try the operation again.

KD4CF0043W There are *num* discovered Web services applications, but they are already enabled for the data collector. No applications are added to the list in: *filename* .

Explanation: All of the Web services applications that have been discovered are already enabled for the data collector. No action is performed.

Operator response: Verify that there is at least one Web services application that is not already enabled for this data collector and try the operation again.

KD4CF0044W There are *num* discovered Web services applications, but they are already disabled for the data collector. No applications are added to the list in: *filename* .

Explanation: All of the Web services applications that have been discovered are already disabled for the data collector. No action is performed.

Operator response: Verify that there is at least one Web services application that is already enabled for this data collector and try the operation again.

KD4CF0045I The Web services application: *app* has been discovered, but is already enabled for the data collector. It is not added to the list in *filename* .

Explanation: The discovered Web services application is already enabled for the data collector. No action is performed.

Operator response: None.

KD4CF0046I The Web services application: *app* has been discovered, but is already disabled for the data collector. It is not added to the list in *filename* .

Explanation: The discovered Web services application is not enabled for the data collector yet. No action is performed.

Operator response: None.

KD4CF0047I *num* applications have been discovered. The list is in the file: *filename* .

Explanation: No additional information is available for this message.

KD4CF0048I REMINDER: When applications were first enabled for this data collector, the KD4configDC utility copied some JAR files into the following location: *path* . After disabling ALL Web services applications for this data collector, you must manually remove these JAR files by deleting the /KD4 directory. See the documentation for more information.

Explanation: After disabling all Web services applications for this data collector, the KD4configDC utility can not remove these copied JAR file programmatically. The user must remove them manually. Note, however, that if any Web services applications are still enabled for the data collector, these JAR files must NOT be removed until after all Web services applications have been disabled for this data collector.

Operator response: Verify that all Web services applications are disabled for this data collector. Refer to the documentation for procedures to manually remove these JAR files.

KD4CF0049I The specified application list file name: *filename* is not valid.

Explanation: This problem might have occurred because the file name contains characters that are not allowed in file system.

Operator response: Verify that the specified file name is valid for the file system.

KD4CF0050W Some files exist on the computer system that conflict with the data collector, possibly due to a version conflict. The list of files that conflict with the data collector are located in the file: *filename* .

Explanation: There are some files on the system that conflict with the data collector. These files might be for previous versions that are no longer compatible, and might cause problems with running the data collector.

Operator response: Examine the list of files that are in conflict and, if these files are not in use, delete them before attempting to enable the data collector.

KD4DP0001I The DataPower data collector is exiting.

Explanation: No additional information is available for this message.

KD4DP0002E The data collector is unable to locate or parse a configuration file named *fileName* due to the following error: *errorMessage*.

Explanation: This error indicates a problem processing the DataPower data collector configuration file.

Administrator Response: Verify that the configuration file specified in the error message exists and has the correct format. Run the data collector configuration program again, if necessary.

KD4DP0003I The data collector is monitoring domain: *domainName* on DataPower appliance: *hostName*.

Explanation: The DataPower data collector has discovered a domain on a DataPower appliance and starts a management subscription for the domain.

System action: The data collector attempts to start a subscription for the domain and begins retrieving Web services metric data from the domain.

Administrator Response: Modify the DataPower data collector configuration file to customize which DataPower domains are monitored.

KD4DP0004E The data collector could not retrieve a domain list for DataPower appliance: *hostName* using user ID: *userID*. Detailed error message: *errorMessage*

Explanation: The data collector was unable to list the domains on a DataPower appliance. Possible causes:

- The configured user ID is not defined on the DataPower appliance.
- The configured password is incorrect.

- A communications failure occurred while communicating with the DataPower appliance.

System action: The data collector periodically retries listing the domains.

Administrator Response: Verify that the DataPower data collector configuration file contains the correct host names, user IDs and passwords for the devices to be monitored.

KD4DP0005I The data collector has stopped monitoring domain: *domainName* on DataPower appliance: *domainName*.

Explanation: The DataPower data collector has cancelled the management subscription for the domain.

System action: The data collector cancels the subscription for the domain.

Administrator Response: Modify the DataPower data collector configuration file to customize which DataPower domains are monitored.

KD4DP0006W The data collector is running. Enter STOP to stop the data collector.

Explanation: The data collector is currently monitoring DataPower appliances. Enter STOP at the console to stop the data collector.

System action: The data collector continues to run until STOP is entered at the console.

Operator response: Enter STOP at the console to stop the DataPower data collector.

KD4DP0007W The *actionName* request to DataPower appliance: *hostName* using user ID: *userID* encountered an error and did not complete successfully. Detailed error or fault code: *faultCode*

Explanation: The data collector was unable to complete a request to a DataPower appliance and received an error indication in response to the request. Possible causes:

- The configured user ID is not defined on the DataPower appliance.
- The configured password is incorrect.
- The XML Management Interface is not configured on the DataPower appliance.
- A communications failure occurred while communicating with the DataPower appliance.

System action: The data collector periodically retries the request.

Administrator Response: Verify that the DataPower data collector configuration file contains the correct host names, user IDs and passwords for the appliances to be monitored. Verify that the XML Management

Interface is configured correctly on the DataPower appliance.

KD4DP0008E A communications failure occurred while the data collector was sending a request to DataPower appliance:
hostName using user ID: *userID*.
Detailed error message: *errorMessage*

Explanation: The data collector is unable to communicate with the DataPower appliance. Possible causes:

- The DataPower appliance is not in an operational state.
- An incorrect TCP/IP address, TCP/IP hostname or TCP/IP port is configured for this DataPower appliance.
- The DataPower XML Management Interface is not configured correctly.
- A communications configuration or other networking problem exists.

System action: The data collector periodically retries communications with the DataPower appliance.

Administrator Response: Verify that the DataPower data collector configuration file contains the correct host names, user IDs and passwords for the devices to be monitored. Verify that the XML Management Interface is configured correctly on the DataPower appliance.

KD4DP0009E The DataPower data collector is unable to initialize using the configuration file: *fileName*. The data collector is exiting. **Detailed error message:** *errorMessage*

Explanation: The data collector is unable to initialize successfully due to a configuration file error. Possible causes:

- The configuration file referenced in the error message does not exist.
- File permissions prevent the data collector from reading the configuration file.
- The format of the configuration file is not valid.

System action: The data collector displays an error message and exits.

Administrator Response: Verify that the DataPower data collector configuration file exists and is correctly formatted. Use the DataPower data collector configuration script to create a valid configuration file.

KD4DP0010E The value for property: *propName* in the data collector configuration file: *fileName* is not valid. The configuration for DataPower appliance with an index value of: *index* is ignored.

Explanation: The data collector encountered a value

for a required property that is not valid. The configuration for the DataPower appliance using this property is ignored.

System action: The data collector continues processing DataPower configuration definitions.

Administrator Response: Verify that the DataPower data collector configuration file exists and contains all required values. Use the DataPower data collector configuration script to create a valid configuration file.

KD4DP0011W The value for property: *propName* in the data collector configuration file: *fileName* is not valid. The data collector will use the default value for this property: *defaultValue*.

Explanation: The data collector encountered an incorrect value for a property that has a default value. The default value is used instead.

System action: The data collector continues processing DataPower configuration definitions.

Administrator Response: Verify that the DataPower data collector configuration file exists and contains all required values. Use the DataPower data collector configuration script to create a valid configuration file.

KD4DP0012E The DataPower data collector is unable to write the configuration file *fileName* with new property values. **Detailed error message:** *errorMessage*.

Explanation: The data collector is unable to successfully update the configuration file. Possible causes:

- The configuration file referenced in the error message does not exist.
- File permissions prevent the data collector from writing the configuration file.
- The configuration file is in use by another process.
- An operating system I/O error has occurred.

System action: The data collector displays an error message and continues without updating the configuration file. The values in the configuration file are unchanged but might be different from those that the data collector uses to communicate with the DataPower system.

Administrator Response: Verify that the DataPower data collector configuration file exists and is correctly formatted. Verify that permissions on the configuration file allow the data collector process to write to the file.

KD4DP0013E Syntax: Java *className* *propertiesFileName*.

Explanation: The start of the data collector is not

KD4DP0014I • KD4DP0019E

successful. The syntax entered for the startup script is not correct.

Operator response: Use the appropriate startup script to start the data collector.

KD4DP0014I Enter the password for user *userName* ; it will be readable as it is typed:

Explanation: The DataPower data collector configuration for this appliance requires that the password for the specified DataPower user be specified. The password is displayed in clear text as it is entered.

Operator response: Enter the password for the specified DataPower user to continue the configuration process.

KD4DP0015E No monitoring is enabled that matches the specified command parameters. The disable request is ignored.

Explanation: The DataPower data collector configuration command requested that monitoring for a DataPower appliance be disabled. No current sections of the DataPower data collector configuration file matched the attributes specified on the disable command. To match a section of the configuration file the host, user, displaygroup, and domainlist properties must match exactly.

System action: No DataPower appliances are removed from the configuration file.

Operator response: To disable the monitoring of a DataPower appliance, specify the host, user, displaygroup, and domainlist information which matches the appliance to be removed from the data collector configuration file.

KD4DP0016E Monitor enable failed due to the exception: *exceptionMsg*

Explanation: The DataPower configuration tool encountered a Java exception while attempting to enable monitoring of a DataPower appliance.

System action: No DataPower appliances are added to the configuration file.

Operator response:

- Examine the exception text and determine the cause of the problem. Correct if possible.
- Retry the task in progress when the error occurred.
- If the error continues to occur, contact IBM Software Support.

KD4DP0017E Monitor disable failed due to the exception: *exceptionMsg*

Explanation: The DataPower configuration tool encountered a Java exception while attempting to disable monitoring of a DataPower appliance.

System action: No DataPower appliances are removed from the configuration file.

Operator response:

- Examine the exception text to determine the cause of the problem and correct if possible.
- Retry the task in progress when the error occurred.
- If the error continues to occur, contact IBM Software Support.

KD4DP0018E The DataPower data collector configuration file: *fileName* could not be read. Detailed error message: *errorMessage*.

Explanation: The configuration tool was unable to successfully update the configuration file. Possible causes:

- File permissions prevent the data collector from writing the configuration file.
- An operating system I/O error has occurred.

System action: The configuration tool displays an error message and exits without modifying the configuration file.

Operator response: Verify that the DataPower data collector configuration file exists and is correctly formatted. Verify that permissions on the data collector configuration file allow the configuration tool process to write to the file. If the error continues to occur, contact IBM Software Support.

KD4DP0019E The DataPower data collector configuration file: *fileName* could not be written. Detailed error message: *errorMessage*.

Explanation: The configuration tool was unable to successfully read the configuration file. Possible causes:

- File permissions prevent the data collector from reading the configuration file.
- An operating system I/O error has occurred.
- Another process has the file locked.

System action: The configuration tool displays an error message and exits without modifying the configuration file.

Operator response: Verify that the data collector configuration file exists and is correctly formatted. Verify that permissions on the configuration file allow the configuration tool process to read the file. If the error continues to occur, contact IBM Software Support.

KD4DP0020E The DataPower data collector configuration file: *fileName* contains a DataPower.count property that is not valid.

Explanation: The DataPower configuration tool was unable to convert the DataPower.count property to a numeric value.

System action: The configuration tool displays an error message and exits without modifying the configuration file.

Operator response: Verify that the data collector configuration file contains a valid DataPower.count property. If the error continues to occur, contact IBM Software Support.

KD4DP0021E An incorrect number of command parameters was specified.

Explanation: The minimum number of parameters required to enable or disable a DataPower device were not specified on the command.

System action: The configuration tool displays an error message and exits without modifying the configuration file.

Operator response: See the documentation for the KD4configDC command for the correct command syntax.

KD4DP0022E The command parameter: *invalidKeyword* is not a valid keyword for this command.

Explanation: The DataPower configuration tool encountered an unrecognized keyword.

System action: The configuration tool displays an error message and exits without modifying the configuration file.

Operator response: See the documentation for the KD4configDC command for the correct command syntax.

KD4DP0023E The required parameter: *missingKeyword* was not specified.

Explanation: A required configuration parameter was not specified.

System action: The configuration tool displays an error message and exits without modifying the configuration file.

Operator response: See the documentation for the KD4configDC command for the correct command syntax.

KD4DP0024E The keyword: *duplicateKeyword* was specified more than once.

Explanation: A duplicate configuration parameter was specified.

System action: The configuration tool displays an error message and exits without modifying the configuration file.

Operator response: See the documentation for the KD4configDC command for the correct command syntax.

KD4DP0025E The value specified for keyword: *invalidValue* is not valid.

Explanation: The value specified for a configuration keyword is not valid.

System action: The configuration tool displays an error message and exits without modifying the configuration file.

Operator response: See the documentation for the KD4configDC command for the correct command syntax.

KD4DP0026E The encoding of the specified password failed due to the exception *exceptionMsg*.

Explanation: The DataPower configuration tool encountered a Java exception while attempting to encode a password for a user ID.

System action: The configuration tool displays an error message and exits without modifying the configuration file.

Operator response:

- Try to determine the problem from the exception text and correct if possible.
- Retry the task in progress when the error occurred.
- If the error continues to occur, contact IBM Software Support.

KD4DP0027E The password entered is not valid.

Explanation: The password entered is not valid. It was either zero bytes in length or contained embedded blanks.

System action: The configuration tool displays an error message and exits without modifying the configuration file.

Operator response: Retry the command with a valid DataPower user password.

KD4DP0028E The DataPower data collector encountered an initialization error and is exiting. Error details: *exceptionMsg*.

Explanation: The DataPower data collector was unable to initialize successfully and is exiting.

System action: The data collector issues an error message and exits.

Operator response:

- Try to determine the problem from the error text and correct if possible.
- Retry the task in progress when the error occurred.
- If the error continues to occur, contact IBM Software Support.

KD4DP0029E The DataPower data collector could not obtain an exclusive lock on the configuration lock file: *fileName*.

Explanation: The data collector or the data collector configuration tool was unable to successfully lock the configuration file in preparation to write to the file. Possible causes:

- File permissions prevent the data collector from locking the configuration lock file.
- An operating system I/O error has occurred.
- The file is in use by another operating system process.

System action: The configuration tool displays an error message and exits without modifying the configuration file. The data collector continues monitoring DataPower appliances without modifying the configuration file.

Operator response: Verify that no other processes have the lock file open for write access. If the error continues to occur, contact IBM Software Support.

KD4DP0030W The value for the required property: *propName* in the data collector configuration file: *fileName* is not valid or is missing. The data collector will attempt to reinitialize itself.

Explanation: The data collector encountered a missing or incorrect value for a property that does not have a default value. The data collector will attempt to reinitialize itself.

System action: The data collector waits for a short period of time and then reads the data collector configuration file again and attempt to reinitialize itself.

Administrator Response: Verify that the DataPower data collector configuration file exists and contains all required values. Use the DataPower data collector configuration script to create a valid configuration file.

KD4LN0001E The DataPower WebGUI could not be launched. The selected entry in the Services Inventory Attributes table does not represent a DataPower appliance.

Explanation: Only Services Inventory entries for DataPower appliances can be used to launch DataPower WebGUI sessions.

Operator response: Select a Services Inventory Attributes table entry for a DataPower appliance to perform this launch action. DataPower appliances are identified by a value of DataPower in the Application Server Environment column of the Services Inventory Attributes table.

KD4LN0002E The DataPower WebGUI could not be launched. The selected entry in the Services Inventory Attributes table has no value for the Application Server Node Name and contains data for more than one DataPower appliance.

Explanation: Entries in the Services Inventory table can represent data from more than one DataPower appliance. These entries have no value for the Application Server Node Name column and cannot be used to launch DataPower WebGUI sessions.

Operator response: Select a Services Inventory Attributes table entry that has an Application Server Node Name column with the host name or IP address of the desired DataPower appliance. Use this entry to perform the launch action.

KD4LN0003E The DataPower WebGUI could not be launched. The selected entry in the SNMP Attributes table does not represent a DataPower appliance.

Explanation: Only SNMP table entries for DataPower appliances can be used to launch DataPower WebGUI sessions.

Operator response: Select an SNMP table entry for a DataPower appliance.

KD4WT0001I *class_name* active, build level *build_level*.

Explanation: The component identified in the message became active during initialization. That component was compiled at the specified build level. The build level data should only be required when requested by IBM Software Support.

Operator response: None.

KD4WT0002E The following exception occurred:

Exception: *exception_code*
Stack trace: *stack_trace_data*

Explanation: See the exception code and trace data for details of the error.

Operator response:

- Examine the exception code and trace data to determine the problem and correct as needed.
- Try the operation again.
- If the error continues to occur, contact IBM Software Support.

KD4WT0003W The configuration file *filename* could not be loaded. The default configuration is used instead.

Explanation: See message.

System action: The system automatically uses its built-in default configuration.

KD4WT0004E The following error occurred while loading the default configuration: *errorMessage*. The *componentName* is inactive.

Explanation: This error indicates a problem with the internal libraries for the data collector.

System action: No Web services transactions are monitored.

Administrator Response: Contact IBM Software Support to correct the problem with the product libraries.

KD4WT0005E Unable to write to the data file *file_name*.

Explanation: The data collector is unable to write to the specified file. This might occur if, for example, the disk is full or the user does not have authorization to write to the file.

System action: The data collector is inactive until the problem is corrected. After the problem is corrected, the system automatically reactivates after a short delay.

Administrator Response: Examine the file system for problems with the specified file.

KD4WT0006E The data collector does not support the *server_name* server.

Explanation: This data collector relies upon a small set of vendor-specific features. The server you are using is not supported by this version of the data collector.

System action: The data collector becomes inactive.

Administrator Response: Use a supported server implementation. Refer to the product documentation for

a list of supported environments.

KD4WT0007E The component named: *componentName* is not able to initialize successfully. The following error occurred: *errorMessage*

Explanation: See message.

System action: The component is inactive.

Administrator Response: Correct the error indicated in the message and restart the application server.

KD4WT0008E The output file *fileName* cannot be renamed for rollover.

Explanation: When a certain file-size threshold is reached, the product rolls the specified file over to a backup copy and begins a new file. This error indicates that the basic file system operations involved in this task have failed.

System action: The product will continue accumulating data in the original file. After the problem is corrected, the product rolls the current file over to its backup and continues its normal work.

Administrator Response: Correct the problem with the files or file system as promptly as possible. Until this problem is corrected, the risk of filling the file system is greatly increased.

KD4WT0009E This WebSphere Application Server installation is missing a required APAR. Install PQ89492 or an equivalent APAR and restart the server.

Explanation: WebSphere APAR PQ89492 delivers function that is required for this product. You must install this APAR or an equivalent APAR for this product to operate properly.

System action: The data collector component ceases to collect information until the WebSphere runtime environment is upgraded with this APAR.

KD4WT0010E The data collector is unable to locate or parse a configuration property named: *property_name*.

Explanation: The data collector uses a configuration file named /KD4/config/KD4.dc.properties. Either this file does not contain the named property, or the value of that property does not conform to the required syntax. These properties are enumerated, starting from one, up to the number specified on the corresponding "count" property.

System action: The data collector ignores this property and continues to use the set of configuration properties that it is able to successfully locate and parse.

Administrator Response: Refresh the configuration display for the corresponding server and update the set of configuration parameters. If you have modified the configuration file manually, ensure the following:

- The Count property indicates the correct value.
- The correct number of Control properties are present.
- Each Control property contains the correct number and sequence of semicolon-delimited tokens.
- The server names on these properties match the server configuration and that they are free from typographic errors.

KD4WT0011E The Web service message has been rejected due to filter control configuration. WSDL Port = *port*, WSDL Operation = *operation*, remote system = *remote_system*, rejected at = *local_system*.

Explanation: The AddFiltrCntrl and DelFiltrCntrl Take Actions are used to control this feature. Refer to the product documentation for details about this feature.

System action: Web services messages that match the defined filter control criteria continue to be rejected until this filter control criteria is removed using the DelFiltrCntrl Take Action.

Administrator Response: Review the filter control criteria defined in the Data Collector Filter Control Configuration view of the Service Management Agent node for the system where the message was rejected. Use the DelFiltrCntrl and AddFiltrCntrl Take Actions to modify these filter criteria as needed. See the documentation or online help for more information about these commands.

KD4WT0012I The IPv6 address = *address* was found in the intercepted message. If the corresponding Web services message was incorrectly passed, check the filter criteria for an equivalent address and replace it with this one.

Explanation: IPv6 addresses may take any of several forms of text representations. The data collector requires these addresses to match as text. Therefore two representations that refer to the same address, but in different formats, will not match, allowing messages to pass the data collector's filter. This might or might not be the expected behavior.

Administrator Response: If you expected the Web services message to be rejected but it was allowed through, then add the address given in this message using the AddFiltrCntrl Take Action.

KD4WT0013E Cannot find the WSDL file: *wsdl*. Verify that the WSDL file is in the correct directory location.

Explanation: The data collector needs the Web Services Description Language (WSDL) file to provide monitor data, but the file cannot be found in the expected directory location.

Operator response: Verify that the WSDL file for the application is in the correct directory location and retry the operation.

Appendix B. Obtaining IBM software support for IBM Tivoli Composite Application Manager for SOA

If you have a problem with your IBM software, you want to resolve it quickly. This section describes the following options for obtaining support for IBM software products:

- “Searching knowledge bases”
- “Obtaining fixes”
- “Receiving weekly support updates” on page 80
- “Contacting IBM Software Support” on page 80

Searching knowledge bases

You can search the available knowledge bases to determine whether your problem was already encountered and is already documented.

Searching the information center

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

Searching the Internet

If you cannot find an answer to your question in the information center, search the Internet for the latest, most complete information that might help you resolve your problem.

To search multiple Internet resources for your product, use the **Web search** topic in your information center. In the navigation frame, click **Troubleshooting and support ► Searching knowledge bases** and select **Web search**. From this topic, you can search a variety of resources, including the following:

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

Obtaining fixes

A product fix might be available to resolve your problem. To determine what fixes are available for your IBM software product, follow these steps:

1. Go to the IBM Software Support Web site at <http://www.ibm.com/software/support>.
2. Click **Downloads and drivers** in the **Support topics** section.
3. Select the **Software** category.
4. Select a product in the **Sub-category** list.
5. In the **Find downloads and drivers by product** section, select one software category from the **Category** list.

6. Select one product from the **Sub-category** list.
7. Type more search terms in the **Search within results** if you want to refine your search.
8. Click **Search**.
9. From the list of downloads returned by your search, click the name of a fix to read the description of the fix and to optionally download the fix.

For more information about the types of fixes that are available, see the *IBM Software Support Handbook* at <http://techsupport.services.ibm.com/guides/handbook.html>.

Receiving weekly support updates

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

1. Go to the IBM Software Support Web site at <http://www.ibm.com/software/support>.
2. Click **My support** in the upper right corner of the page.
3. If you have already registered for **My support**, sign in and skip to the next step. If you have not registered, click **register now**. Complete the registration form using your e-mail address as your IBM ID and click **Submit**.
4. Click **Edit profile**.
5. In the **Products** list, select **Software**. A second list is displayed.
6. In the second list, select a product segment, for example, **Application servers**. A third list is displayed.
7. In the third list, select a product sub-segment, for example, **Distributed Application & Web Servers**. A list of applicable products is displayed.
8. Select the products for which you want to receive updates, for example, **IBM HTTP Server** and **WebSphere Application Server**.
9. Click **Add products**.
10. After selecting all products that are of interest to you, click **Subscribe to email** on the **Edit profile** tab.
11. Select **Please send these documents by weekly email**.
12. Update your e-mail address as needed.
13. In the **Documents** list, select **Software**.
14. Select the types of documents that you want to receive information about.
15. Click **Update**.

If you experience problems with the **My support** feature, you can obtain help in one of the following ways:

Online

Send an e-mail message to erchelp@ca.ibm.com, describing your problem.

By phone

Call 1-800-IBM-4You (1-800-426-4968).

Contacting IBM Software Support

IBM Software Support provides assistance with product defects.

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

- For IBM distributed software products (including, but not limited to, Tivoli, Lotus®, and Rational® products, as well as DB2® and WebSphere products that run on Windows, or UNIX® operating systems), enroll in Passport Advantage in one of the following ways:

Online

Go to the Passport Advantage Web site at http://www.lotus.com/services/passport.nsf/WebDocs/Passport_Advantage_Home and click **How to Enroll**.

By phone

For the phone number to call in your country, go to the IBM Software Support Web site at <http://techsupport.services.ibm.com/guides/contacts.html> and click the name of your geographic region.

- For customers with Subscription and Support (S & S) contracts, go to the Software Service Request Web site at <https://techsupport.services.ibm.com/ssr/login>.
- For customers with IBMLink™, CATIA, Linux, S/390®, iSeries™, pSeries®, zSeries®, and other support agreements, go to the IBM Support Line Web site at <http://www.ibm.com/services/us/index.wss/so/its/a1000030/dt006>.
- For IBM eServer™ software products (including, but not limited to, DB2 and WebSphere products that run in zSeries, pSeries, and iSeries environments), you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for eServer software products, go to the IBM Technical Support Advantage Web site at <http://www.ibm.com/servers/eserver/techsupport.html>.

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

To contact IBM Software support, follow these steps:

1. “Determining the business impact”
2. “Describing problems and gathering information” on page 82
3. “Submitting problems” on page 82

Determining the business impact

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

Severity 1

The problem has a *critical* business impact. You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.

Severity 2

The problem has a *significant* business impact. The program is usable, but it is severely limited.

Severity 3

The problem has *some* business impact. The program is usable, but less significant features (not critical to operations) are unavailable.

Severity 4

The problem has *minimal* business impact. The problem causes little impact on operations, or a reasonable circumvention to the problem was implemented.

Describing problems and gathering information

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

- What software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can you recreate the problem? If so, what steps were performed to recreate the problem?
- Did you make any changes to the system? For example, did you make changes to the hardware, operating system, networking software, and so on.
- Are you currently using a workaround for the problem? If so, be prepared to explain the workaround when you report the problem.

Submitting problems

You can submit your problem to IBM Software Support in one of two ways:

Online

Click **Submit and track problems** on the IBM Software Support site at <http://www.ibm.com/software/support/probsub.html>. Type your information into the appropriate problem submission form.

By phone

For the phone number to call in your country, go to the contacts page of the *IBM Software Support Handbook* at <http://techsupport.services.ibm.com/guides/contacts.html> and click the name of your geographic region.

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

Appendix C. 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 (l) 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, Candle[®], DB2, developerWorks, eServer, IBM, the IBM logo, IBMLink, iSeries, Lotus, OMEGAMON, Passport Advantage, pSeries, Rational, Redbooks, S/390, Tivoli, Tivoli Enterprise[™], the Tivoli logo, WebSphere, z/OS, and zSeries 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 is a registered trademark 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.

Index

A

- agent 1
- aggregation 23
 - across multiple domains 32
 - all domains, single host, multiple users 33
 - cluster of appliances 33
 - DataPower 21, 31
 - planning for 22
 - using display group 31
- appliance
 - aggregating multiple, DataPower 21
 - cluster, DataPower 33
 - communicating with data collector 34
 - DataPower 21
- application domain
 - DataPower 22
- application server runtime environment 1
- asynchronous flows
 - in SCA 15

B

- BEA WebLogic Server 2
- books
 - see publications 3

C

- cluster
 - DataPower appliances 33
- configuration file
 - DataPower 21, 25
- customer support
 - See Software Support

D

- data collector 1
 - applications enabled for multiple 5
 - communicating with appliance 34
 - configuring in DataPower environment 25
 - DataPower 21
 - DataPower, deploying 23
 - DataPower, starting 35
 - DataPower, stopping 35
 - disabling for DataPower 34
 - disabling JBoss applications for 13
 - disabling SAP NetWeaver application for 49
 - disabling SCA applications for 18
 - disabling WebSphere CE applications for 60
 - enabling JBoss applications for 11
 - enabling SAP NetWeaver application for 44
 - enabling SCA applications for 15
 - enabling WebSphere CE applications for 53
 - IBM WebSphere Application Server, in WESB and WPS 17
 - in multiple environments 17

- data collector (*continued*)
 - JBoss 11
 - SAP NetWeaver 43
 - SCA 15
 - support, installing 8
 - WebSphere Community Edition (CE) 53
- Data Collector Adapter 1
- DataPower 2, 21
 - appliance, cluster 33
 - appliance, configuring 24
 - appliance, polling 21
 - configuration file 25
 - configuring environment for the data collector 25
 - configuring optional settings 24
 - data collector, starting and stopping 35
 - disabling data collector 34
 - firmware upgrade 21
 - logging in 40
 - multiple connections 30
 - proxy 21
 - user account, configuring 24
 - user password 30
 - WebGUI user interface, launching 37
- DataPower WebGUI launch
 - considerations 38
 - from desktop client 38
 - on Linux 40
- developerWorks, searching for problem resolution in IBM 79
- display group
 - aggregation and separation 31
 - changing current value 30
 - DataPower 23
- displaygroup
 - in node name, DataPower 28
- domain
 - aggregating multiple, DataPower 21
 - application, DataPower 22
- domain list
 - changing current value 30
 - restricting user access 31

F

- filtering
 - SCA 18
- firmware
 - DataPower requirement 21
- fixes, obtaining 79

G

- getting help 4

H

host
in node name, Datapower 28

I

IBM developerWorks, searching for problem resolution
in 79
IBM Passport Advantage 2
IBM Redbooks, searching for problem resolution in 79
IBM software support 4
IBM technotes, searching for problem resolution in 79
IBM Web Services Navigator 2
IBM WebSphere Application Server 2
and SCA data collector 17
communicating between SCA modules 17
IBM WebSphere Enterprise Service Bus 1, 15
IBM WebSphere Integration Developer 15
IBM WebSphere Process Server 15
information centers, searching for problem
resolution 79
installation 5, 6
data collector support 8
distributed, order of 5
Tivoli Enterprise Monitoring Server 7
Tivoli Enterprise Portal 8
Tivoli Enterprise Portal Server 6
Intelligent Remote Agent 1
Internet
searching for problem resolution 79

J

JAX-RPC 2
JBoss 11
JBoss 2, 11
disabling applications for data collector 13
enabling applications for data collector 11

K

KD4configDC
DataPower, optional parameters 30
for DataPower 26
for JBoss 11
for SAP NetWeaver 47, 49
for SCA 15
for WebSphere CE 54, 61
parameters, DataPower 26
KD4LN0001E error message 38
KD4LN0002E error message 38
KFWITM069E error message 38
knowledge bases, searching for problem resolution 79

L

limitations
DataPower 35
Linux support 2, 5, 6

logging
DataPower 36
SCA 18

M

manuals
see publications 3
mediation 15
message
filtering 2
logging 2
messages 67
Microsoft .NET 2
monitor control
SCA 17
monitoring agent 1
multiple connections
DataPower 30

N

NetWeaver
see SAP NetWeaver 43
node name
in TEP, for DataPower 28

O

OMEGAMON 2

P

parameters
KD4configDC for DataPower, optional 30
password
DataPower, specifying 30
performance
DataPower 35
Performance Summary workspace 37
poll
DataPower appliance 21
problem determination
describing problems 82
determining business impact 81
submitting problems 82
proxy
DataPower 21
publications
feedback 3
online 3
ordering 3

R

Redbooks, searching for problem resolution in IBM 79

S

SAP 43

- SAP NetWeaver
 - disabling application for the data collector 49
 - enabling for data collector 44
- SCA 2, 15
 - communicating between SCA modules 17
 - components 15
 - disabling applications for data collector 18
 - enabling applications for data collector 15
 - filtering 18
 - IBM Web Services Navigator 18
 - limitations 18
 - logging 18
 - modules 15
 - monitor control 17
 - with IBM WebSphere Application Server data collectors 17
- separation
 - between domains by domain list 32
 - by display group 31
 - by host name 31
 - DataPower 31
 - using display group 31
- Service Component Architecture 15
- service oriented architecture 1
- services component architecture 2
- Services Inventory table 37
- SOA 1
- Software Support
 - contacting 80
 - describing problems 82
 - determining business impact 81
 - receiving weekly updates 80
 - submitting problems 82
- sparkler 2
- Sparkler 1 5
- start DPDC
 - starting DataPower data collector 23
- startDPDC 34, 35
- support information 4
- synchronous flows
 - in SCA 15

T

- technotes, searching for problem resolution in IBM 79
- Tivoli Enterprise Monitoring Server 7
- Tivoli Enterprise Portal 8
 - display group, DataPower 23
 - node names, DataPower 28
- Tivoli Enterprise Portal Server 6
- tracing
 - DataPower 36
- transaction log service
 - DataPower 21
- troubleshooting 36
 - appliance password 36
 - communication 36
 - synchronizing time 36

U

- updateLogging Take Action 34

W

- WebGUI user interface
 - DataPower 37
- WebSphere CE 53
 - disabling applications for data collector 60
 - disabling applications manually 64
 - enabling applications manually 57
 - enabling for the data collector 53
- WebSphere Community Edition 53
- WESB 1

X

- XML Management Interface
 - enabling, for DataPower 24



Printed in USA