IBM Tivoli Composite Application Manager for WebSphere Application Server 7.2 support for WebSphere Application Server 8.5

Installation and User Guide

GC23-9701-01

IBM Tivoli Composite Application Manager for WebSphere Application Server 7.2 support for WebSphere Application Server 8.5

Installation and User Guide

GC23-9701-01

Note

Before using this information and the product it supports, IBM Tivoli Composite Application Manager for WebSphere Application Server, read the information in "Notices" on page 175.

This edition applies to Version 7.2 of IBM Tivoli Composite Application Manager for WebSphere Application Server and to all subsequent releases and modifications until otherwise indicated in new editions.

About this guide

This guide provides instructions for installing, configuring, using, and troubleshooting IBM® Tivoli® Composite Application Manager for WebSphere® Application Server (ITCAM for WebSphere Application Server).

Intended audience

This publication is for administrators or users who want to install and use ITCAM for WebSphere Application Server. The publication assumes that readers are familiar with maintaining operating systems, administering IBM WebSphere Application Server, maintaining databases, and general information technology (IT) procedures. Specifically, readers of this publication must have some knowledge of the following topics:

- Operating systems on which you intend to install product components
- IBM WebSphere Application Server
- Internet protocols such as HTTP, HTTPS, TCP/IP, Secure Sockets Layer (SSL), and Transport Layer Security (TLS)
- Digital certificates for secure communication

ITCAM for WebSphere Application Server publications

The following is a list of the publications in the ITCAM for WebSphere Application Server library:

- *IBM Tivoli Composite Application Manager for WebSphere Application Server: Installation and User Guide*

  Provides instructions for installing, configuring, using, and troubleshooting ITCAM for WebSphere Application Server.

Related publications

The following documentation also provide useful information:

- IBM WebSphere Application Server 8.5 Information Center

  http://www-3.ibm.com/software/webservers/appserv/was/library
- IBM Tivoli Composite Application Manager for Application Diagnostics Information Center

  http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/index.jsp?toc=/com.ibm.ccmdb.doc/ccmdb_ic.xml
- IBM Support Assistant

  http://www-306.ibm.com/software/support/isa/index.html?rcss=rtlrre

Accessing terminology online

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

Accessing publications online

IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli Information Center website at http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp.

The ITCAM for WebSphere Application Server Installation and User Guide is available here: http://www.ibm.com/software/ismlibrary?NavCode=1TW10CD07

Note: If you print PDF documents on other than letter-sized paper, set the option in the **File → Print** window that allows Adobe Reader to print letter-sized pages on your local paper.

Ordering publications

About this task

There are several ways to order IBM publications:

- You can order many IBM publications online at the following website: http://www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi
- You can order by telephone by calling one of these numbers:
  - In the United States: 800-879-2755
  - In Canada: 800-426-4968
- In other countries, contact your software account representative to order IBM publications. To locate the telephone number of your local representative, perform the following steps:
  1. Go to the following website: http://www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi
  2. Select your country from the list and click **Go**.
  3. Click **About this site** in the main window to see an information page that includes the telephone number of your local representative.

Accessibility

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

For additional information, see Appendix F, “Accessibility,” on page 171.

Tivoli technical training

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

Support information

If you have a problem with your IBM software, IBM provides the following ways for you to obtain the support you need:

- Go to the IBM Software Support website: http://www.ibm.com/software/support/probsub.html

- IBM Support Assistant:

  IBM Support Assistant (ISA) is a free local software serviceability workbench that helps you resolve questions and problems with IBM software products. ISA provides quick access to support-related information and serviceability tools for problem determination.

Typeface conventions

This publication uses the following typeface conventions:

Bold

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as **Tip:** and **Operating system considerations**)
- Keywords and parameters in text

Italic

- Citations (titles of publications, diskettes, and CDs)
- Words defined in text (such as "a nonswitched line is called a *point-to-point line*.")
- Emphasis of words and letters: words as words (such as "Use the word *that* to introduce a restrictive clause." letters as letters (such as "The LUN address must start with the letter *L*.")
- New terms in text, except in a definition list, (such as "a *view* is a frame in a workspace that contains data.")
- Variables and values you must provide (such as "where *myname* represents...")

`Monospace`

- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

Tivoli command syntax

The following special characters define Tivoli command syntax:

[ ] Identifies elements that are optional. Required elements do not have brackets around them.

... Indicates that you can specify multiple values for the previous element. Separate multiple values by a space, unless otherwise directed by command information.

If the ellipsis for an element follows a closing bracket, use the syntax within the brackets to specify multiple values. For example, to specify two administrators for the option [**–a** *admin*]..., use **–a admin1 –a admin2**.

If the ellipsis for an element is within the brackets, use the syntax of the last element to specify multiple values. For example, to specify two hosts for the option [**–h** *host*...], use **–h host1 host2**.

| Indicates mutually exclusive information. You can use the element on either the left or right of the vertical bar.

{ } Delimits a set of mutually exclusive elements when a command requires one of them. Brackets ([ ]) are around elements that are optional.

In addition to the special characters, Tivoli command syntax uses the typeface conventions described in "Typeface conventions" on page v. The following examples illustrate the typeface conventions used in Tivoli command syntax:

- **wcrtpr** [**–a** *admin*]... [**–s** *region*] [**–m** *resource*]... *name*

  The *name* argument is the only required element for the **wcrtpr** command. The brackets around the options indicate they are optional. The ellipses after the **–a** *admin resource* option means that you can specify multiple administrators multiple times. The ellipses after the **–m** *resource* option means that you can specify multiple resources multiple times.
- **wchkdb** [**–o** *outfile*] [**–u**] [**–x**] {**–f** *infile* | **–i** | *object*...}

  The **–f**, **–i**, and *object* elements are mutually exclusive. Braces that surround elements indicate that you are including a required element. If you specify the *object* argument, you can specify more than one object.

Variables for directories

This guide refers to the following variables:

- *DC_home*: the directory where the ITCAM Data Collector for WebSphere is installed. The following are the default locations:

Table 1. Default locations for DC_home

UNIX or **Linux**	`/opt/ibm/itcam_install/7.2`
Windows	`c:\itcam_install\7.2`
IBM i	`DC_home`
IBMz/OS®	`/u/WAS80`

- *Appserver_home*: the directory where the application server core product files are installed. The following table shows the default locations:

Table 2. Default locations for appserver_home

UNIX or **Linux**	`/opt/IBM/WebSphere/AppServer`
Windows	`C:\Program Files\IBM\WebSphere\AppServer`
IBMz/OS	`/u/was8500`
IBM i	`/QIBM/ProdData/WebSphere/AppServer`

Note: If there are multiple application server installations in the same directory path, the path will end in a directory named after the particular application server installation. For example, *AppServer_home* will be *`IBM_home`*`/WebSphere/WAS8/`*`appserver_instance`*.

- *config_home*: IBM z/OS, This is the ITCAM for WebSphere Application Server configuration home directory. The default is `/u/itcam72`.

Contents

Tables

Chapter 1. Monitor performance with IBM Tivoli Composite Application Manager for WebSphere Application Server

ITCAM for WebSphere Application Server support for WebSphere Application Server 8.5 is available for download from Integrated Service Management Library.

The ITCAM for WebSphere Application Server component is composed of a data collector. This data collector is referred to as the *ITCAM Data Collector for WebSphere*.

Configure the data collector to monitor a WebSphere Application Server instance. The data collector then runs within the same JVM as the application server and captures information about the running applications. When you configure the data collector, a new Performance Monitoring Infrastructure (PMI) module is created in the application server. The data that ITCAM for WebSphere Application Server provides augments the data provided by the application server through the existing PMI statistics.

The *ITCAM Data Collector for WebSphere* can integrate with IBM SmartCloud™ Application Performance Management capabilities to enable you to:

- Track transactions for quick problem isolation.
- Monitor SOA environments to understand the performance of web services.
- Perform operational monitoring of products such as; WebSphere Application Server, IBM Business Process Manager, and WebSphere Portal.
- Use deep diagnostic functionality available in ITCAM for Application Diagnostics.

You can connect the data collector to any of the following products or components:

- ITCAM for SOA Monitoring Agent
- ITCAM Agent for WebSphere Applications Monitoring Agent
- ITCAM for Application Diagnostics Managing Server
- Tivoli Performance Viewer (ITCAM for WebSphere Application Server)
- ITCAM for Transactions

For a complete set of monitoring functionality for WebSphere Application Server, use ITCAM for Application Diagnostics. For more information about the features and benefits of ITCAM for Application Diagnostics, see the IBM Software website or the ITCAM for Application Diagnostics information center.

Chapter 2. Getting Started with ITCAM for WebSphere Application Server

To begin using ITCAM for WebSphere Application Server, perform the following tasks:

Table 3. Getting Started

Step	Description
Install ITCAM for WebSphere Application Server.	Installing on Windows Installing on UNIX/Linux Installing on IBM i Installing on z/OS
Configure ITCAM for WebSphere Application Server.	Following installation, you cannot use ITCAM for WebSphere Application Server until data collection is configured. ITCAM for WebSphere Application Server is composed of a data collector. Configure communication between the data collector and a WebSphere Application Server instance using the ITCAM Data Collector for WebSphere configuration utility. This enables data collection on the WebSphere Application Server instance. See: Configuring on Windows Configuring on UNIX/Linux Configuring on IBM i Configuring on z/OS
Restart WebSphere Application Server.	When you complete the configuration of ITCAM for WebSphere Application Server, restart the WebSphere Application Server instance. See WebSphere Application Server Information Center
Start ITCAM for WebSphere Application Server, enable counters and view data in the TPV.	Following installation and configuration, start ITCAM for WebSphere Application Server, enable counters, and view data. See Starting ITCAM for WebSphere Application Server
Customize counters.	You might need to customize counter settings, see.“Customizing ITCAM for WebSphere Application Server counters” on page 7
Disable ITCAM for WebSphere Application Server in the WebSphere Integrated Console.	You might need to disable ITCAM for WebSphere Application Server, for example, if you are upgrading WebSphere Application Server . See “Disabling ITCAM for WebSphere Application Server” on page 7

Start ITCAM for WebSphere Application Server, enable counters, and view data

The following procedure describes how to start ITCAM for WebSphere Application Server, enable counters, and view data. If you restart the WebSphere Application Server, you will need to start ITCAM for WebSphere Application Server and enable the counters again.

Procedure

1. To start ITCAM for WebSphere Application Server, complete the following steps:
   a. In the WebSphere Integrated Solutions console navigation tree, expand **Monitoring and Tuning** > **Performance Monitoring Infrastructure (PMI)**.

b. In the **Name** column, locate the application server that you want to start monitoring and click the name.
c. In the configuration tab, under Additional Properties, select **ITCAM for WebSphere Application Server**, or **ITCAM for WAS**.
d. If it is not already selected, select **Enable IBM Tivoli Composite Application Manager for WebSphere Application Server Data Collector** or **Enable ITCAM for WAS Data Collector**. Click **Apply**. In the top of the configuration tab, click **Save**.
e. Click the **Runtime** tab and select **Start Monitoring**.

2. To enable counters, complete the following steps:
   a. Click the **Configuration** tab, ensure that **Enable IBM Tivoli Composite Application Manager for WebSphere Application Server Data Collector** is selected. Click **Apply**.
   b. In the top of the **Configuration** tab, select **Save directly to the master configuration**, this will return you to the **Performance Monitoring Infrastructure** window.
   c. In the **Name** column, locate the application server that you want to start monitoring and click the name.
   d. Select the **Runtime** tab and click the **custom** link.
   e. To enable application server level counters, select the counters you want to enable.
   f. Some counters are only applicable at instance level. To enable instance level counters, expand **ITCAM Application Performance**, select the instance level node, and then select the counters you want to enable.

      Note:
      - You cannot enable instance level counters unless there is traffic for the instance.
      - When you enable instance level counters, they appear disabled at the **ITCAM Application Performance** level, but at request level, they are enabled. Also, when you view the performance graphs, the counters are enabled. For more information, see selecting_app_counters.dita.

   g. Click **Enable** to enable the counters you selected.
   h. In the navigation tree, select **Performance Viewer**>**Current**® **Activity**, select the application server you want to start monitoring and click **Start Monitoring**.
3. To view data, complete the following steps:
   a. In the **Server** column, locate the application server that you want to start monitoring and click the name.
   b. Under your server name, expand **Performance Modules**.
   c. Select **ITCAM Application Performance**.
   d. Click **View Modules**.

Results

You should now be able to view data.

Descriptions of counters displayed in the Tivoli Performance Viewer

The Tivoli Performance Viewer presents the data in charts. Use the charts to determine how performance metrics have changed over a time period and whether WebSphere Application Server is experiencing any performance issues.

Note: Some data does not display when correlative counters are disabled. The following table provides details of the metrics displayed in the Tivoli Performance Viewer:

Table 4. Descriptions of counters displayed in the Tivoli Performance Viewer

Counters	Descriptions of counters
90%CPUUsage	The 90% percent median of the processor usage of requests in milliseconds, where 90% of the cpu usage are less than this value. This counter is only available at application level. There is a maximum limit on the number of processor usage requests stored to calculate the 90% processor usage median. You can set this limit by defining the `eCAM.90Percent.buffer.limit` property in the `toolkit_custom.properties` file. The 90% median is calculated by taking the sample at the 90% of the total samples. The formula to calculate the 90% median sample is: `(number of samples - 1) * 0.9` For example, if the current sample size is 31, then the formula is: `(31 - 1) * 0.9 = 27` and the 27th sample is returned. If the result is not an integer, for example, when the current sample size is 32, then the formula is: `(32 - 1) * 0.9 = 27.9`. In this case, 10% of the 27th sample and 90% of the 28th sample is returned.
90%ResponseTime	90% percent median of requests in milliseconds, where 90% of the response times are less than this value. This counter is available only at the application level. There is a maximum limit on the number of request response times stored to calculate the 90% response time median. Set this limit by defining the `eCAM.90Percent.buffer.limit` property in the `toolkit_custom.properties` file. The default is 50. The 90% median is calculated by taking the sample at the 90% of the total samples. The formula to calculate the 90% median sample is: `(number of samples - 1) * 0.9` For example, if the current sample size is 31, then the formula is: `(31 - 1) * 0.9 = 27` and the 27th sample is returned. If the result is not an integer, for example, when the current sample size is 32, then the formula is: `(32 - 1) * 0.9 = 27.9`. In this case, 10% of the 27th sample and 90% of the 28th sample is returned.

Table 4. Descriptions of counters displayed in the Tivoli Performance Viewer (continued)

Counters	Descriptions of counters
AverageCPUUsage	The average processor usage of requests in milliseconds.
AverageResponseTime	The average response time of requests in milliseconds.
LastMinuteAverageCPUUsage	The average processor usage of requests completed in the last minute (when the counter value is retrieved) in milliseconds.
LastMinuteAverageResponseTime	The average response time of requests completed in the last minute (when the counter value is retrieved) in milliseconds.
MaximumCPUUsage	The most intensive processor usage since the counter is enabled or reset in milliseconds. This counter is available only at the application level.
MaximumResponseTime	The slowest response time since the counter is enabled or reset in milliseconds. This counter is available only at the application level.
MinimumCPUUsage	The least intensive processor usage since the counter was enabled or reset in milliseconds. This counter is available only at the application level.
MinimumResponseTime	The fastest response time since the counter is enabled or reset in milliseconds. This counter is available only at the application level.
RequestCount	The number of requests completed since the counter is enabled or reset.

Stopping ITCAM for WebSphere Application Server

Complete the following steps to stop ITCAM for WebSphere Application Server:

1. In the WebSphere Integrated Console navigation tree, select **Monitoring and Tuning** > **Performance Monitoring Infrastructure (PMI)**.
2. In the **Name** column, locate the application server that you want to stop monitoring and click the name.
3. In the configuration tab, under **Additional Properties**, select **ITCAM for WebSphere Application Server**, or **ITCAM for WAS**. Click **Apply**.
4. Click the **Runtime** tab and select **Stop Monitoring**

   The system stops monitoring the ITCAM for WebSphere Application Server module, and Tivoli Performance Viewer sends the signal to ITCAM for WebSphere Application Server through a JMX call. ITCAM for WebSphere Application Server unregisters all performance modules from the PMI registry and stops monitoring.

Disabling ITCAM for WebSphere Application Server counters

Complete the following steps to disable ITCAM for WebSphere Application Server counters:

1. In the WebSphere Integrated Console, from the **Monitoring and Tuning** menu, select **Performance Monitoring Infrastructure (PMI)**.
2. In the **Name** column, locate the application server that you want to stop monitoring and click the name.

3. Click the **Runtime** tab.
4. Click the **Custom** link.
5. Select **ITCAM Application Performance**.
6. Clear the application server level counters that you do not want to monitor,
7. If you enabled additional application level counters, expand **ITCAM Application Performance**, select the application level node, and then select the counters you want to disable.
8. Click **Disable**.

Disabling ITCAM for WebSphere Application Server

Complete the following steps to disable ITCAM for WebSphere Application Server:

1. In the WebSphere Integrated Solutions Console, click **Monitoring and Tuning**>**Performance Monitoring Infrastructure (PMI)**.
2. In the **Name** column, locate the application server that you want to stop monitoring and click the name.
3. Click the **Configuration** tab.
4. Under **Additional Properties**, click **ITCAM for WebSphere Application Server** or **ITCAM for WAS**.
5. Clear the **Enable ITCAM for WAS Data Collector** check box and click **Save Settings**. The system saves the change to the local repository, while Tivoli Performance Viewer sends the status to ITCAM for WebSphere Application Server through a MBean call. ITCAM for WebSphere Application Server updates the status in the local repository. For example, ITCAM for WebSphere Application Server sets the ITCAM_DC_ENABLED environment variable to false for the selected application server.

Customizing ITCAM for WebSphere Application Server counters

You might need to customize how counter values are calculated. To customize counters, use the *DC_home*/runtime/*server*/custom/toolkit_custom.properties file, for example, was85.ITEST01_dmgr1.itest01_ecam85.ecam85.wwt1. If the file does not exist, create it. Use the *parameter=value* format.

Restart the application server after you change parameter values.

Table 5. ITCAM for WebSphere Application Server configuration parameters

Configuration parameter	Description
eCAM.90Percent.buffer.limit	• This parameter controls the number of samples used to calculate the 90% metrics. • All statistics instances have one buffer for 90% request time and one for 90% processor usage if both are enabled. • All buffers have the same size, the default value is 50.

Table 5. ITCAM for WebSphere Application Server configuration parameters (continued)

Configuration parameter	Description
eCAM.PMI.Threadpool.size	• This parameter controls the thread pool size to update the PMI statistics. Updating the PMI statistics is decoupled from the application thread so it does not lengthen the application response time. • The default value is 2. If the thread pool size is too small, updating the PMI statistics slows down and more memory is used. Unless the application server is running out of memory, you do not have to fine-tune this parameter.
eCAM.memory.limit	This parameter controls the amount of memory in megabytes that the ITCAM for WebSphere Application Server uses. The default value is 20. When the memory limit is reached, new PMI statistics will not be created. New applications and requests are not shown in the PMI. The following error message is displayed: ⌂Exceeding memory limit defined in eCAM.memory.limit=*size limit*. New counter will not be created, please increase memory limit.⌂ is logged in the log file.
eCAM.disable.BCI	When this parameter is set to *true*, ITCAM for WebSphere Application Server disables the BCI engine when it first starts. This parameter is used to reduce the memory usage of the ITCAM for WebSphere Application Server. The default value is *true*.

Chapter 3. Installing and configuring ITCAM for WebSphere Application Server on Windows systems

ITCAM for WebSphere Application Server is an optional component that can be installed on an existing version of:

1. WebSphere Application Server Network Deployment, Version 8.5
2. WebSphere Application Server Express®, Version 8.5
3. WebSphere Application Server, Version 8.5

ITCAM for WebSphere Application Server is composed of the ITCAM Data Collector for WebSphere. When you install and configure this component, you can view performance data information in the Tivoli Performance Viewer in WebSphere Application Server 8.5. To collect this data, you must install ITCAM Data Collector for WebSphere on every application server host, and configure it for every instance.

Preinstallation Tasks

A number of tasks must be performed before installing ITCAM for WebSphere Application Server on Windows.

Checking Permissions

Run the configuration utilities using a Windows operating system user ID that owns the WebSphere Application Server profile that is being configured. If the WebSphere Application Server installer and profile owner do not map to the same Windows operating system user ID, follow the steps in the WebSphere Application Server information center on configuring the profile user. For more information, see information center.

Where WebSphere Global security is enabled, the configuration utility prompts you for a WebSphere Administrator user ID that has login privileges to the wsadmin tool. Please use the primary administrative user for WebSphere Application Server.

Checking the heap size

Ensure that the JVM heap size is sufficient. The default value is enough, but if the heap size was configured in WebSphere Application Server, make sure that it is not less than 384 MB. Complete the following steps for each server that you want to configure for ITCAM for WebSphere Application Server:

1. Log on to the IBM WebSphere Application Server administrative console.
2. Click **Servers > Server Types> WebSphere Application Servers** and select the *server_name*.
3. In the **Configuration** tab, go to **Server Infrastructure > Java and Process Management > Process Definition > Additional Properties: Java Virtual Machine**.
4. If the value in the **Maximum Heap Size** field is less than 384, set it to 384.

Installing the Data Collector

Install the ITCAM Data Collector for WebSphere on every host running the instances of WebSphere Application Server that you need to monitor. You can use one installation to collect data from any number of application server instances on the same host.

Before you begin

Download the data collector compressed file.

Procedure

1. Copy the data collector compressed file into a temporary directory.
2. Unpack the file.
3. Unpack the file into a new directory, for example, `C:\itcam_install\7.2.` This path is referred to as *DC_home* in this guide.

What to do next

After installing the data collector, you must take one of the following actions to monitor server instances with ITCAM for WebSphere Application Server:

- If any instances are already monitored with ITCAM for WebSphere Application Server, ITCAM for WebSphere, ITCAM for Application Diagnostics, or ITCAM for SOA, migrate monitoring of the instances to the new data collector. See "Migrating data collectors to the ITCAM Data Collector for WebSphere" on page 28 or "Migrating the ITCAM Data Collector for WebSphere in silent mode" on page 31.
- Otherwise, configure the data collector to monitor the instances. See "Configuring the ITCAM Data Collector for WebSphere" on page 11 or."Configuring the ITCAM Data Collector for WebSphere in silent mode" on page 17

Configuring ITCAM for WebSphere Application Server

If you have any of the following product versions installed and configured for the same WebSphere profile, you must migrate them to use the ITCAM Data Collector for WebSphere before configuring ITCAM for WebSphere Application Server:

- ITCAM for SOA version 7.1.1
- ITCAM for WebSphere version 6.1.4 or later
- WebSphere Data Collector version 6.1.4 included in ITCAM for Web Resources version 6.2
- ITCAM Agent for WebSphere Applications version 7.1 included in ITCAM for Applications Diagnostics version 7.1

Using the new ITCAM Data Collector for WebSphere Configuration Utility, you can connect the common ITCAM Data Collector for WebSphere to the following components:

- Tivoli Performance Viewer - (this is ITCAM for WebSphere Application Server)
- ITCAM for SOA Monitoring agent 7.1.1 or later
- ITCAM Agent for WebSphere Applications monitoring agent 7.1.0.3 or later
- ITCAM for Application Diagnostics Managing Server 7.1.0.3 or later
- ITCAM for Transactions Transaction 7.3

Configuring in a profile where there are no other ITCAM products configured in the same WebSphere Profile

If you are configuring the ITCAM for WebSphere Application in an environment where there are no other ITCAM products configured for application servers within the same profile, you can integrate the data collector with the Tivoli Performance Viewer and accept the default values.

Configuring the ITCAM Data Collector for WebSphere

You must configure the data collector for each application server instance that you want to monitor.

The ITCAM Data Collector for WebSphere Configuration Utility is a menu driven command-line utility for configuring the ITCAM Data Collector for WebSphere.

To configure the data collector to monitor one or more server instances, complete the following procedure:

1. From the command line, navigate to the *DC_home*\bin directory.
2. Set the location of the Java home directory before you run the utility.

   ```
   set JAVA_HOME=C:\Program~1\IBM\WebSphere\AppServer80\java
   ```
3. Run the following command to start the ITCAM Data Collector for WebSphere Configuration Utility.

   ```
   DC_home\bin\config.bat
   ```
4. The utility starts and displays the IP addresses of all network cards that are found on the local computer system and prompts you to specify the interface to use for the data collector:

   ```
   List of TCP/IP interfaces discovered:
     1. 9.111.98.108
   Enter a number [default is: 1]:
   ```
5. Enter the number that corresponds to the IP address to use.

   The utility searches for WebSphere Application Server home directories on the computer system and prompts you to select a home directory:

   ```
   List of WebSphere Application Server home directories discovered:
     1. C:\Program Files\IBM\WebSphere\AppServer
   Enter a number or enter the full path to a home directory
   [default is: 1]:
   ```
6. Enter the number that corresponds to a WebSphere Application Server home directory.

   The utility searches for all profiles under the specified home directory and prompts you to select a profile:

   ```
   List of WebSphere profiles discovered:
     1. AppSrv01
   Enter a number [default is: 1]:
   ```
7. Enter the number that corresponds to the WebSphere Application Server profile that you want to configure.

   The utility indicates whether WebSphere Global Security is enabled for the WebSphere Application profile that you specified:

   ```
   WebSphere Global Security is enabled.
   ```

   If global security is not enabled, skip to step 9 on page 12
8. The utility prompts you to specify whether to retrieve security settings from a client properties file:

```
Do you want to retrieve security settings from a client properties file
(soap.client.props or sas.client.props)?
[1 - YES, 2 - NO] [default is: 2]:
```

The data collector communicates with the WebSphere Administrative Services using the Remote Method Invocation (RMI) or the SOAP protocol. If global security is enabled for a profile, you must specify the user ID and password of a user who is authorized to log in to the IBM WebSphere Application Server administrative console for the profile. Alternatively, you can encrypt the user name and password and store them in client properties files before configuring the data collector. You must use the `sas.client.props` file for an RMI connection, or the `soap.client.props` file for an SOAP connection.

Enter `1` to allow the utility to retrieve the user name and password from the appropriate client properties file and skip to step 9. Otherwise, enter `2` to enter the user name and password.

```
CFG1018I Enter WebSphere admin user name:
CFG1019I Enter WebSphere admin password:
```

9. The utility searches for all application server instances under the specified profile. The utility displays all servers that are not configured yet for data collection and all servers that are configured to use the current version of the ITCAM Data Collector for WebSphere.

   The utility prompts you to select one or more application server instances from the list:

   ```
   Choose one or more servers to configure for data collection:
   Application servers not yet configured:
    1. co098170Node01Cell.co098170Node01.server1(AppSrv01)
   Enter a number or numbers separated by commas, or enter * to select all:
   ```

   Remember:

   - For a Network Deployment or Extended Deployment environment, the Node Agent and Deployment Manager must be running. For a stand-alone environment, application server instances must be running during the configuration of the data collector.
   - Ensure that the application server instances that you select are the actual nodes that host the applications or services that you want to monitor.

10. Enter the number that corresponds to the application server instance to configure for data collection or enter an asterisk `*` to configure all application server instances for data collection. To specify a subset of servers, enter the numbers, separated by commas, that represent the servers. For example: `1,2,3`.

11. In the **Integration with ITCAM for SOA Agent** section, the utility provides an option for integrating the data collector with the ITCAM for SOA agent.

    ```
    Do you want to integrate with an ITCAM for SOA Agent? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

    You must install and configure the ITCAM for SOA Agent and its application support files, and optionally configure topology support to complete the installation and configuration of the ITCAM for SOA Agent. For more information about installing and configuring the ITCAM for SOA Agent, see *IBM Tivoli Composite Application Manager for SOA Installation Guide*.

    Enter `1` to integrate the data collector with the ITCAM for SOA Agent. Otherwise, enter `2`.

12. In the **Integration with ITCAM Agent for WebSphere Applications** section, the utility provides an option for integrating the data collector with the ITCAM Agent for WebSphere Applications.

You can integrate the data collector with ITCAM Agent for WebSphere Applications, or with the ITCAM for Application Diagnostics Managing Server, or with both.

```
Do you want to integrate with an ITCAM Agent for WebSphere Applications?
 [1 - YES, 2 - NO]
[default is: 2]:
```

You must install and configure the ITCAM Agent for WebSphere Applications and its application support files to complete the installation and configuration of the ITCAM Agent for WebSphere Applications. For more information about installing and configuring the ITCAM Agent for WebSphere Applications, see *IBM Tivoli Composite Application Manager Agent for WebSphere Applications Installation and Configuration Guide*.

13. Enter 1 to integrate the data collector with the ITCAM Agent for WebSphere Applications. Otherwise, enter 2 and skip to step 16.

    You are prompted to enter the host name of the ITCAM Agent for WebSphere Applications.

    ```
    Enter the host name or IP address of the ITCAM Agent for WebSphere Applications TEMA:
    [default is: 127.0.0.1]:
    ```

14. Enter the fully qualified host name or IP address of the ITCAM Agent for WebSphere Applications monitoring agent. The monitoring agent is located on the local host, so you do not have to change the default.

    You are prompted for the port number of the ITCAM Agent for WebSphere Applications monitoring agent.

    ```
    Enter the port number of the ITCAM Agent for WebSphere Application TEMA:
    [default is: 63335]:
    ```

    You can change the port that is used for communication between the data collector and the ITCAM Agent for WebSphere Applications monitoring agent. This communication is on the local host; the default port is 63335. You can change the port at a later time, but it is most convenient to set it when initially configuring the data collector.

15. Enter the port number of the monitoring agent.

16. In the **Integration with ITCAM for Application Diagnostics Managing Server** section, the utility provides an option for integrating the data collector with the ITCAM for Application Diagnostics Managing Server, installed on a separate Windows, Linux, or UNIX server, for deep-dive diagnostics. For information about installing the Managing Server, see *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

    You are prompted to specify whether you want to integrate the data collector with a Managing Server.

    ```
    Do you want to integrate with an MS? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

    Remember:

    - To integrate with ITCAM for Application Diagnostics Managing Server for deep-dive analysis, you must have ITCAM for Application Diagnostics version 7.1 installed.
    - If you decide not to configure the Managing Server at this time, you can still configure the data collector to communicate with the Managing Server later.

17. Enter 1 to integrate with the Managing Server. Otherwise, enter 2 and skip to step 20 on page 14.

    You are prompted to specify the host name of the Managing Server:

```
Enter the host name  or IP address of the  MS
[default is: 127.0.0.1]:
```

18. Enter the fully qualified host name of the Managing Server.

    You are prompted to specify the port number of the Managing Server:

    ```
    Enter the code base port number of the MS
    [default is: 9122]:
    ```

    The port number is codebase port on which the Managing Server is listening.

    Tip: The port number is defined as the value of the key "PORT_KERNEL_CODEBASE01" in the .ITCAM61_MS_CONTEXT.properties file located under the Managing Server Home directory. See *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

    The configuration tool attempts to connect to the Managing Server and retrieve the value for the *MS_home* directory. If successful, the tool displays a message similar to the following message:

    ```
    MS home directory is: /opt/IBM/itcam/WebSphere/MS
    ```

19. If the connection to the Managing Server is *not* successful, you are prompted to enter the value for the *MS_home* directory:

    ```
    Enter ITCAM Managing Server install directory [default is C:\IBM\itcam\WebSphere\MS]:
    ```

    If prompted, enter the value of the *MS_home* directory.

20. The utility prompts you to specify whether you want to configure advanced settings for the Managing Server.

    ```
    Do you want to configure advanced settings for the MS? [1 - Yes, 2 - No]
    [default is: 2]:
    ```

    Enter 1 to configure advanced settings. Otherwise, enter 2 and skip to step 24.

21. You are prompted to enter the range of RMI port numbers that the data collector uses to accept incoming connections from the Managing Server:

    ```
    Enter the RMI port numbers [default is: 8200-8299]:
    ```

    Tip: Make sure that the ports are not being blocked by the firewall or other applications.

    Enter the RMI port numbers.

22. You are prompted to enter the range of Controller RMI port numbers:

    ```
    Enter the range of Controller RMI port numbers
    [default is: 8300-8399]:
    ```

    Enter the RMI Controller port numbers.

23. You are prompted to enter the RFS port number of the Managing Server:

    ```
    Enter the RFS port number of the MS:  [default is: 9120]:
    ```

    Enter the RFS port number.

24. In the **Integration with ITCAM for Transactions** section, the utility provides an option for integrating the data collector with ITCAM for Transactions.

    Remember: To integrate the data collector with ITCAM for Transactions, you must install ITCAM for Transactions within an IBM Tivoli Monitoring environment.
    You are prompted to specify whether you want to integrate with ITCAM for Transactions:

    ```
    Do you want to integrate with ITCAM for TT? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

After you configure the data collector to support ITCAM for Transactions, you must perform some additional configuration. For details of further configuration options and how to view the aggregated transaction information, see *IBM Tivoli Composite Application Agent for WebSphere Applications Configuring and Using TTAPI*.

25. Enter 1 to integrate the data collector with ITCAM for Transactions. Otherwise, enter 2 and skip to step 30.
26. You are prompted to specify the host name or IP address of the Transaction Collector, which is the component of ITCAM from Transactions that gathers metrics from multiple agents:

    ```
    Enter the host name or IP address for the Transaction Collector:
    [default is: 127.0.0.1]:
    ```
27. Enter the fully qualified host name or IP address of the Transaction Collector.
28. You are prompted to specify the port number that the data collector uses to connect to the Transaction Collector:

    ```
    Enter the port number for the Transaction Collector:
    [default is: 5455]:
    ```
29. Enter the port number for the interface to the Transaction Collector.
30. In the **Integration with Tivoli Performance Viewer** section, the utility provides an option for integrating the data collector with Tivoli Performance Viewer (TPV).

    ```
    Do you want to integrate with Tivoli Performance Viewer? [1 - YES, 2 - NO]
    [default is: 2]
    ```

    ITCAM for WebSphere Application Server version 7.2 can be used to monitor the performance of the WebSphere Application Server. Performance monitoring infrastructure (PMI) metrics are gathered using the ITCAM Data Collector for WebSphere and are displayed in the Tivoli Performance Viewer (TPV). The TPV is accessible from the WebSphere Application Server administrative console. ITCAM for WebSphere Application Server is installed separately from the WebSphere Application Server. For more information about installing ITCAM for WebSphere Application Server, see *IBM Tivoli Composite Application Manager for WebSphere Application Server version 7.2 Support for WebSphere Application Server version 8.5 Installation and User Guide*.

    ITCAM for WebSphere Application Server 7.2 support for WebSphere Application Server 8.5 includes the ITCAM Data Collector for WebSphere. Enter 1 to integrate the ITCAM Data Collector for WebSphere with the Tivoli Performance Viewer. Otherwise, enter 2.
31. In the **Integration with ITCAM diagnostics tool** section, the utility provides an option for integrating the data collector with the ITCAM Diagnostics Tool.

    ```
    Do you want to integrate with ITCAM diagnostics tool? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

    ITCAM Diagnostics Tool is built on Eclipse. The tool is used for diagnostic investigation of applications that are running on the WebSphere Application Server. Using this tool, you can analyze data in real time or you can save diagnostic information to a file for later analysis. For more information about installing the ITCAM Diagnostics Tool, see *ITCAM Diagnostic Tool Installation Guide*.

    Enter 1 to integrate the ITCAM Data Collector for WebSphere with the ITCAM Diagnostics Tool. Otherwise, enter 2.
32. In the **Advanced Settings** section, the utility provides options for performing advanced configuration of the data collector. The utility prompts you to specify whether to change the garbage collection log path:

    ```
    Do you want to specify a Garbage Collection log path? [1 - YES, 2 - NO] [default is: 2]:
    ```

Enter 1 to select a garbage collection log path. Otherwise, enter 2 and skip to step 16.

33. You are prompted to specify the garbage collection log path:

```
Enter the GC log path:
```

Enter a file name with its full path. The data collector automatically modifies the log file name, adding the server instance information to it. For example, if you specify `gc.log` as the file name, the actual name is set to *profile_name*`.`*cell_name*`.`*node_name*`.`*server_name*`.gc.log` for every configured application server instance.

Important: In the garbage collection log path, you can use WebSphere variables such as`${SERVER_LOG_ROOT}`. However, do not use templates, such as `%pid`.

34. You are prompted to specify whether you want to increase the heap size:

```
Do you want to add 128M to the heap size? [1 - YES, 2 - NO]
[default is: 2]:
```

Enter 2 to retain the existing heap size. Otherwise, enter 1.

35. In the **Data collector configuration summary** section, the utility provides a summary of the data collector configuration that will be applied to the specified application server instances:

```
 1) List of servers selected

   - WAS server: co098170Node01Cell.co098170Node01.server1(AppSrv01)
       WAS cell: co098170Node01Cell
        WAS node: co098170Node01

       WebSphere Profile home    :
          C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01

       wsadmin location          :
         C:\Program Files\IBM\WebSphere\AppServer\bin\wsadmin.bat

                    WAS version : 8.0.0.0
                     Deployment : Standalone
                        JVM mode : 32
                Configuration home : C\IBM\ITM\dchome

 2) Integrate with ITCAM for SOA Agent : Yes

 3) Integrate with ITCAM Agent for WebSphere Applications : Yes

       TEMA hostname or IP address : 127.0.0.1
                TEMA port number : 63335
                      Monitor GC : No

 4) Integrate with ITCAM for AD Managing Server : No

       MS hostname or IP address : 127.0.0.1
         MS codebase port number : 9122
               MS home directory : /opt/IBM/itcam/WebSphere/MS

 5) Integrate with ITCAM for Transactions : Yes

       Transaction Collector hostname : 127.0.0.1
       Transaction Collector port number : 5455

 6) Integrate with Tivoli Performance Viewer : No

 7) Integrate with ITCAM diagnostics tool : No
```

```
 8) Advanced settings :

       Set Garbage Collection log path : No
       Added 128M to the heap size : No

You may accept or update your configuration choices for the following actions:
 1) List of servers selected
 2) Integrate with ITCAM for SOA Agent
 3) Integrate with ITCAM Agent for WebSphere Applications
 4) Integrate with ITCAM for AD Managing Server
 5) Integrate with ITCAM for Transactions
 6) Integrate with Tivoli Performance Viewer
 7) Integrate with ITCAM diagnostics tool
 8) Advanced settings

To modify a section, enter the number. To modify all sections, enter '*'. To accept you
configuration without modifying, enter 'a'.
To quit the selection, enter 'q':
```

The summary section provides options to reconfigure parts of the data collector configuration before applying the changes and an option to exit the configuration tool without applying your changes. Enter the number that represents the section you want to edit. Enter an asterisk `*` to reconfigure all sections. Enter `a` to accept your changes. Enter `q` to exit the ITCAM Data Collector for WebSphere Configuration Utility without configuring the data collector.

36. When you enter `a` to accept your changes, you are prompted to specify whether you want to create a backup of your current WebSphere Application Server configuration:

    ```
    Do you want to backup current WebSphere configuration? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

37. Enter `1` to create a backup of the current configuration. Otherwise, enter `2`.

The changes are applied and a status message is presented to indicate that the configuration of the data collector for the profile is complete:

```
Successfully executed config for Cell: co098170Node01Cell
Node: co098170Node01 Profile: AppSrv01.
```

Important: After configuring the data collector to monitor application server instances, you must restart the instances. The data collector configuration takes effect when the application server instances are restarted.

Configuring the ITCAM Data Collector for WebSphere in silent mode

The common ITCAM Data Collector for WebSphere can be configured interactively with the ITCAM Data Collector for WebSphere Configuration Utility. Alternatively, to configure many application server instances, the ITCAM for WebSphere Applications Data Collector can be configured in silent mode.

Important: In an ITCAM for Application Diagnostics deployment, do not configure the data collector to monitor an instance of WebSphere Application Server that hosts the Managing Server Virtualization Engine (MSVE). However, you can use the data collector to monitor any other WebSphere Application Server instances that are on the same node.

When you configure the data collector in silent mode, you first specify configuration options in a properties file. A sample properties file,

sample_silent_config.txt, is packaged with the ITCAM Data Collector for WebSphere Configuration Utility. The file is available in the following location:

DC_home\bin

The *DC_home* variable is the location where the data collector is installed. A sample of a properties file is displayed in "Sample properties file" on page 20.

Complete the following steps to perform a silent configuration:

1. Specify configuration options in the properties file.
2. Go to the *DC_home*\bin directory.
3. Run the following command:
   config.bat -silent [*dir_path*]*silent file*
4. After configuring the data collector to monitor application server instances, you must restart the instances. The data collector configuration takes effect when the application server instances are restarted.

Properties file

When you create your properties file, keep in mind the following considerations:

- A line in the file that starts with a number sign (#) is treated as a comment, and is not processed. If the number sign is used elsewhere in the line, it is not considered to be the start of a comment.
- Each property is described on a separate line, in the following format: <*property*> = <*value*>.

  property
  Name of property. The list of valid properties that you can configure is shown in Table 6.

  value Value of the property. Default values for some properties are already provided. You can delete default values to leave property values blank, or empty. An empty value is treated as if the property is not specified, as opposed to using the default value. If you want to use default values, you can comment out the property in the file.
- Passwords are in plain text.
- Properties and their values are case-sensitive.
- Table 6 describes the properties that are available when configuring the data collector in silent mode:

Table 6. Available properties for running the ITCAM Data Collector for WebSphere Configuration Utility in silent mode

Property	Comment
default.hostip	If the computer system uses multiple IP addresses, specify the IP address for the data collector to use.
Integration of the data collector with the ITCAM for Application Diagnostics Managing Server	
ms.connect	Specifies whether the data collector is configured to connect to the Managing Server in an ITCAM for Application Diagnostics environment. Valid values are *True* and *False*.
ms.kernel.host	Specifies the fully qualified host name of the Managing Server.
ms.kernel.codebase.port	Specifies the codebase port on which the Managing Server is listening.
ms.am.home	Specifies the *MS_home* directory on the Managing Server.

Table 6. Available properties for running the ITCAM Data Collector for WebSphere Configuration Utility in silent mode (continued)

Property	Comment
ms.am.socket.bindip	Specifies the IP address or host name to be used by the data collector to communicate with the Managing Server. If more than one network interface or IP address is configured on data collector computer system, choose one of them.
ms.firewall.enabled	Specifies whether a firewall is enabled on the data collector host or you have special requirements to change the RMI ports for the data collector. Valid values are *True* and *False*.
ms.probe.controller.rmi.port	If the data collector is behind a firewall or you have special requirements to change the RMI port of data collector, set this port number range. Configure this port number as permitted by the firewall for the data collector host. For example: ms.probe.controller.rmi.port=8300-8399 or ms.probe.controller.rmi.port=8300.
ms.probe.rmi.port	If the data collector is behind a firewall, or you have special requirements to change the RMI Port of data collector, set this port number range. Configure this port number as permitted by the firewall for the data collector host. For example: ms.probe.rmi.port=8200-8299 or ms.probe.rmi.port=8200.
Integration of the data collector with the ITCAM for Transactions	
ttapi.enable	Specifies whether the data collector communicates with ITCAM for Transactions using the Transaction Tracking API (TTAPI). Valid values are *True* and *False*.
ttapi.host	Specifies the host name of the ITCAM for Transactions Transaction Collector to connect to.
ttapi.port	Specifies the port of the Transaction Collector to connect to.
Integration of the data collector with the ITCAM for SOA	
soa.enable	Specifies whether to integrate the data collector with ITCAM for SOA. The ITCAM for SOA agent must be installed to complete the configuration. **Important:** The data collector always connects with the ITCAM for SOA monitoring agent when enabled. No additional configuration of the ITCAM for SOA monitoring agent is required.
Integration of the data collector with the Tivoli Performance Monitoring	
tpv.enable	Specifies whether to integrate the data collector with the Tivoli Performance Monitoring when the data collector is included as part of ITCAM for WebSphere Application Server version 8.5. Tivoli Performance Monitoring is accessed with the WebSphere Application Server administrative console. Valid values are *True* and *False*.
Integration of the data collector with the ITCAM Diagnostics Tool	
de.enable	Specifies whether to integrate the data collector with the ITCAM Diagnostics Tool. The ITCAM Diagnostics Tool is a tool for diagnostic investigation of applications that are running on WebSphere Application Server. Valid values are *True* and *False*.
Integration of the data collector with the ITCAM Agent for WebSphere Applications monitoring agent	
temaconnect	Specifies whether the data collector connects to the ITCAM Agent for WebSphere Applications monitoring agent (TEMA). Valid values are *True* and *False*. Set this property to *False* if you plan to connect the ITCAM Agent for WebSphere Applications with the Managing Server only or you do not have the ITCAM Agent for WebSphere Applications installed and do not plan to install it.
tema.host	Specifies the fully qualified host name or IP address of the ITCAM Agent for WebSphere Applications monitoring agent.
tema.port	Specifies the port number of the ITCAM Agent for WebSphere Applications monitoring agent.
WebSphere Application Server backup	

Table 6. Available properties for running the ITCAM Data Collector for WebSphere Configuration Utility in silent mode (continued)

Property	Comment
was.backup.configuration	Specifies whether to back up the current configuration of the WebSphere Application Server configuration before applying the new configuration. Valid values are *True* and *False*.
was.backup.configuration.dir	Specifies the location of the backup directory.
Advanced configuration settings	
was.gc.custom.path	Specifies whether to set a custom path for the Garbage Collection log.
was.gc.file	Specifies the path to the custom Garbage Collection log. Set this value to a file name with its full path. The data collector automatically modifies the log file name, adding the server instance information to it. For example, if you specify `gc.log` as the file name, the actual name is set to *`profile_name.cell_name.node_name.server_name`*`.gc.log` for every configured application server instance. **Important:** In the Garbage Collection log path, you can use WebSphere variables, such as ${SERVER_LOG_ROOT}. However, do not use templates, such as %pid.
was.configure.heap	Specifies whether to add 128 MB to the heap size. Each time you run the silent configuration, 128 MB is added to the heap size if this property is set to *True*. Possible values are *True* and *False*.
WebSphere Application Server connection settings	
was.wsadmin.connection.host	Specifies the name of the host to which the wsadmin tool is connecting.
was.wsadmin.connection.type	Specifies the connection protocol for the wsadmin tool to use.
was.wsadmin.connection.port	Specifies the port that the wsadmin tool must use to connect to the WebSphere Application Server.
WebSphere Application Server global security settings	
was.wsadmin.username	Specifies the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server.
was.wsadmin.password	Specifies the password that corresponds to the user specified in the `was.wsadmin.username` property.
was.client.props	Specifies whether to retrieve security settings from a client properties file. Possible values are *True* and *False*.
WebSphere Application Server settings	
was.appserver.profile.name	Specifies the name of the application server profile that you want to configure.
was.appserver.home	Specifies the WebSphere Application Server home directory.
was.appserver.cell.name	Specifies the WebSphere Application Server cell name.
was.appserver.node.name	Specifies the WebSphere Application Server node name.
WebSphere Application Server runtime instance settings	
was.appserver.server.name	Specifies the application server instance within the application server profile to configure. **Tip:** The silent response file can have multiple instances of this property.

Sample properties file

```
#################################################################################################
#
#Comments:
#Locate the ITCAM Data Collector for WebSphere Configuration Utility (config.sh|bat) in <dc_home>/bin.
#Run config.sh|bat -silent [dir_path]/<properties_file> to configure the data collector silently.
#This file is a sample properties file.
#
```

```
#This file has 2 sections; [DEFAULT SECTION] and [SERVER].
#You can have one instance of [DEFAULT].
#You can have multiple instances of [SERVER].
#
#You can integrate the data collector with the following components:
#  ITCAM for Application Diagnostics Managing Server
#  ITCAM for Transactions
#  ITCAM for SOA agent
#  Tivoli Performance Viewer (for ITCAM for WebSphere Application Server)
#  ITCAM Diagnostics Tool
#  ITCAM Agent for WebSphere Applications monitoring agent
#
#Considerations:
#
#IP address to use:
#Uncomment and specify an IP address to use, if the system has multiple IP addresses.

#Modify Garbage Collection log path:
#The full path to the GC log file must exist.
#The server name, cell name, and node name are appended to the GC log file name.
#
#Increase the JVM heap size by 128MB:
#If set to true, each time the script is run, 128MB is added to the JVM heap size.
#
#Connect to WebSphere Administrative Services:
#The utility determines the connection type and port automatically.
#If the utility cannot determine the values, uncomment, and override the default values.
#
#Servers:
#You can configure multiple servers in the same profile.
#Uncomment the second [SERVER] and add the server name.
#Repeat for each additional server.
#
##############################################################################################

[DEFAULT SECTION]

#  IP addresses to use:
#default.hostip=9.9.9.9

#  ITCAM for Application Diagnostics Managing Server:
ms.connect=False
ms.kernel.host=msservername.yourcompany.com
ms.kernel.codebase.port=9122
ms.am.home=/opt/IBM/itcam/WebSphere/MS
ms.am.socket.bindip=servername.yourcompany.com
#ms.firewall.enabled=
ms.probe.controller.rmi.port=8300-8399
ms.probe.rmi.port=8200-8299

#  ITCAM for Transactions:
ttapi.enable=False
ttapi.host=ttservername.yourcompany.com
ttapi.port=5455

#  ITCAM for SOA agent:
soa.enable=False

#  Tivoli Performance Viewer:
tpv.enable=True

#  ITCAM Diagnostics Tool:
de.enable=False

#  ITCAM Agent for WebSphere Applications monitoring agent:
temaconnect=True
tema.host=127.0.0.1
tema.port=63335

#  Create a backup of WebSphere Application Server:
```

```
was.backup.configuration=False
was.backup.configuration.dir=/opt/IBM/ITM/dchome

#  Modify Garbage Collection log path:
#was.gc.custom.path=False
#was.gc.file=/opt/test.log

#  Increase the JVM heap size by 128MB:
was.configure.heap=False

#Connect to WebSphere Administrative Services:
was.wsadmin.connection.host=servername.yourcompany.com
#was.wsadmin.connection.type=SOAP
#was.wsadmin.connection.port=8881

#  WebSphere Global Security:
was.wsadmin.username=
was.wsadmin.password=
was.client.props=False

#  WebSphere Application Server details:
was.appserver.profile.name=AppSrv02
was.appserver.home=C:\Program Files\IBM\WebSphere\AppServer
was.appserver.cell.name=yourITCAMCell
was.appserver.node.name=yourITCAMNode

[SERVER]
was.appserver.server.name=server1

#[SERVER]
#was.appserver.server.name=server2
```

Reconfiguring the ITCAM Data Collector for WebSphere

If you configured the data collector to monitor one or more application server instances, you can reconfigure the data collector using the ITCAM Data Collector for WebSphere Reconfiguration Utility.

You can change the data collector connection to the following products or components:

- ITCAM Agent for WebSphere monitoring agent
- ITCAM for Application Diagnostics Managing Server
- ITCAM for SOA monitoring agent
- ITCAM for Transactions
- Tivoli Performance Viewer
- ITCAM Diagnostic Tool

You can also reconfigure garbage collection settings and add to the heap size.

To reconfigure data collection for one or more monitored application server instances, complete the following procedure:

1. From the command line, navigate to the *DC_home*\bin directory.
2. Set the location of the Java home directory before you run the utility.
   ```
   set JAVA_HOME=C:\Program~1\IBM\WebSphere\AppServer80\java
   ```
3. Run the following command to start the ITCAM Data Collector for WebSphere Reconfiguration Utility.
   ```
   DC_home\bin\reconfig.bat
   ```

   Tip: Running this utility has the same effect as running the `config.bat` script with the `-reconfig` argument

4. The utility starts and displays the IP addresses of all network cards found on the local computer system and prompts you to specify the interface to use for the data collector:

```
List of TCP/IP interfaces discovered:
  1. 9.111.98.108
Enter a number [default is: 1]:
```

5. Enter the number that corresponds to the IP address to use.

   The utility searches for all application server instances for which the data collector is configured on this host, and prompts you to select one or more application server instances from the list:

```
Choose one or more servers to configure for data collection:
Application servers not yet configured:
 1. co098170Node01Cell.co098170Node01.server1(AppSrv01)
Enter a number or numbers separated by commas, or enter * to select all:  1
```

   Tip: For a Network Deployment or Extended Deployment environment, the Node Agent and Deployment Manager must be running. For a stand-alone environment, application server instances must be running during the configuration of the data collector.

6. Enter the number that corresponds to the application server instance to configure for data collection or enter an asterisk * to configure all application server instances for data collection. To specify a subset of servers, enter the numbers, separated by commas, that represent the servers. For example: 1,2,3.

7. In the **Integration with ITCAM for SOA Agent** section, the utility provides an option for integrating the data collector with the ITCAM for SOA agent.

```
Do you want to integrate with an ITCAM for SOA Agent? [1 - YES, 2 - NO]
[default is: 2]: 1
```

   You must install and configure the ITCAM for SOA Agent and its application support files, and optionally configure topology support to complete the installation and configuration of the ITCAM for SOA Agent. For more information about installing and configuring the ITCAM for SOA Agent, see *IBM Tivoli Composite Application Manager for SOA Installation Guide*.

   Enter 1 to integrate the data collector with the ITCAM for SOA Agent. Otherwise, enter 2.

8. In the **Integration with ITCAM Agent for WebSphere Applications** section, the utility provides an option for integrating the data collector with the ITCAM Agent for WebSphere Applications.

   You can integrate the data collector with ITCAM Agent for WebSphere Applications, or with the ITCAM for Application Diagnostics Managing Server, or with both.

```
Do you want to integrate with an ITCAM Agent for WebSphere Applications?
 [1 - YES, 2 - NO]
[default is: 2]: 1
```

   You must install and configure the ITCAM Agent for WebSphere Applications and its application support files to complete the installation and configuration of the ITCAM Agent for WebSphere Applications. For more information about installing and configuring the ITCAM Agent for WebSphere Applications, see *IBM Tivoli Composite Application Manager Agent for WebSphere Applications Installation and Configuration Guide*.

9. Enter 1 to integrate the data collector with the ITCAM Agent for WebSphere Applications. Otherwise, enter 2 and skip to step 12 on page 24.

   You are prompted to enter the host name of the ITCAM Agent for WebSphere Applications.

```
Enter the host name or IP address of the ITCAM Agent for WebSphere Applications TEMA:
[default is: 127.0.0.1]: 127.0.0.1
```

10. Enter the fully qualified host name or IP address of the ITCAM Agent for WebSphere Applications monitoring agent. The monitoring agent is on the local host, so the default is correct.

    You are prompted for the port number of the ITCAM Agent for WebSphere Applications monitoring agent.

    ```
    Enter the port number of the ITCAM Agent for WebSphere Application TEMA:
    [default is: 63335]: 63335
    ```

    You can change the port that is used for communication between the data collector and the ITCAM Agent for WebSphere Applications monitoring agent. This communication is on the local host; the default port is 63335.

11. Enter the port number of the monitoring agent.
12. In the **Integration with ITCAM for Application Diagnostics Managing Server** section, the utility provides an option for integrating the data collector with the ITCAM Application Diagnostics Managing Server, installed on a separate UNIX or Windows server, for deep-dive diagnostics. For information about installing the Managing Server, see *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

    You are prompted to specify whether you want to integrate the data collector with a Managing Server.

    ```
    Do you want to integrate with an MS? [1 - YES, 2 - NO]
    [default is: 2]: 1
    ```

    Remember:

    - To integrate with ITCAM for Application Diagnostics Managing Server for deep-dive analysis, you must have ITCAM for Application Diagnostics version 7.1 installed.
    - If you decide not to configure the Managing Server at this time, you can still configure the data collector to communicate with the Managing Server later.

13. Enter 1 to integrate with the Managing Server. Otherwise, enter 2 and skip to step 16 on page 25.

    You are prompted to specify the host name of the Managing Server:

    ```
    Enter the host name  or IP address of the  MS
    [default is: 127.0.0.1]: 127.0.0.1
    ```

14. Enter the fully qualified host name of the Managing Server.

    You are prompted to specify the port number of the Managing Server:

    ```
    Enter the code base port number of the MS
    [default is: 9122]: 9122
    ```

    The port number is codebase port on which the Managing Server is listening.

    Tip: The port number is defined as the value of the key "PORT_KERNEL_CODEBASE01" in the .ITCAM61_MS_CONTEXT.properties file located under the Managing Server Home directory. See *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

    The configuration tool attempts to connect to the Managing Server and retrieve the value for the *MS_home* directory. If successful, the tools displays a message similar to the following message:

    ```
    MS home directory is: /opt/IBM/itcam/WebSphere/MS
    ```

15. If the connection to the Managing Server is *not* successful, you are prompted to enter the value for the *MS_home* directory:

    ```
    Enter ITCAM Managing Server Install Directory [default is C:\IBM\itcam\WebSphere\MS]:
    ```

    If prompted, enter the value of the *MS_home* directory.

16. The utility prompts you to specify whether you want to configure advanced settings for the Managing Server.

    ```
    Do you want to configure advanced settings for the MS? [1 - Yes, 2 - No]
    [default is: 2]: 1
    ```

    Enter 1 to configure advanced settings. Otherwise, enter 2 and skip to step 19.

17. You are prompted to enter the range of RMI port numbers that the data collector uses to accept incoming connections from the Managing Server:

    ```
    Enter the RMI port numbers
    [default is: 8200-8299] 8200-8299
    ```

    Tip: Make sure that the ports are not being blocked by the firewall or other applications.

    Enter the RMI port numbers.

18. You are prompted to enter the range of Controller RMI port numbers:

    ```
    Enter the range of Controller RMI port numbers
    [default is: 8300-8399]: 8300-8399
    ```

    Enter the RMI Controller port numbers.

19. In the **Integration with ITCAM for Transactions** section, the utility provides an option for integrating the data collector with ITCAM for Transactions.

    Remember: To integrate the data collector with ITCAM for Transactions, you must install ITCAM for Transactions within an IBM Tivoli Monitoring environment.
    You are prompted to specify whether you want to integrate with ITCAM for Transactions:

    ```
    Do you want to integrate with ITCAM for TT? [1 - YES, 2 - NO]
    [default is: 2]: 1
    ```

20. After you have configured the data collector to support ITCAM for Transactions, you then must perform some additional configuration. For details of further configuration options and how to view the aggregated transaction information, see *IBM Tivoli Composite Application Agent for WebSphere Applications Configuring and Using TTAPI*.

21. Enter 1 to integrate the data collector with ITCAM for Transactions. Otherwise, enter 2 and skip to step 26 on page 26.

22. You are prompted to specify the host name or IP address of the Transaction Collector, which is the component of ITCAM from Transactions that gathers metrics from multiple agents:

    ```
    Enter the host name or IP address for the Transaction Collector:
    [default is: 127.0.0.1]: 127.0.0.1
    ```

23. Enter the fully qualified host name or IP address of the Transaction Collector.

24. You are prompted to specify the port number of the interface to the Transaction Collector:

    ```
    Enter the port number for the Transaction Collector:
    [default is: 5455]: 5455
    ```

25. Enter the port number for the interface to the Transaction Collector.

26. In the **Integration with Tivoli Performance Viewer** section, the utility provides an option for integrating the data collector with Tivoli Performance Viewer (TPV).

    ```
    Do you want to integrate with Tivoli Performance Viewer? [1 - YES, 2 - NO]
    [default is: 2]
    ```

    ITCAM for WebSphere Application Server version 7.2 can be used to monitor the performance of the WebSphere Application Server. Performance monitoring infrastructure (PMI) metrics are gathered using the ITCAM Data Collector for WebSphere and are displayed in the Tivoli Performance Viewer (TPV). The TPV is accessible from the WebSphere Application Server administrative console. ITCAM for WebSphere Application Server is installed separately from the WebSphere Application Server. For more information about installing ITCAM for WebSphere Application Server, see *IBM Tivoli Composite Application Manager for WebSphere Application Server version 7.2 Support for WebSphere Application Server version 8.5 Installation and User Guide*.

    ITCAM for WebSphere Application Server 7.2 support for WebSphere Application Server version 8.5 includes the ITCAM Data Collector for WebSphere. Enter 1 to integrate the ITCAM Data Collector for WebSphere with the Tivoli Performance Viewer. Otherwise, enter 2 and skip to step 27.

27. In the **Integration with ITCAM diagnostics tool** section, the utility provides an option for integrating the data collector with the ITCAM diagnostics tool.

    ```
    Do you want to integrate with ITCAM diagnostics tool? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

    ITCAM Diagnostics Tool is a tool that is built on Eclipse. The tool is used for diagnostic investigation of applications that are running on WebSphere Application Server. Using this tool, you can analyze data in real time or you can save diagnostic information to a file for later analysis. For more information about installing the ITCAM Diagnostics Tool, see *ITCAM Diagnostic Tool Installation Guide*.

    Enter 1 to integrate the ITCAM Data Collector for WebSphere with the ITCAM diagnostics tool. Otherwise, enter 2 and skip to step 28.

28. In the **Advanced Settings** section, the utility provides options for performing advanced configuration of the data collector. The utility prompts you to specify whether to change the garbage collection log path:

    ```
    Do you want to specify a Garbage Collection log path? [1 - YES, 2 - NO]
    [default is: 2]: 2
    ```

    Enter 1 to select a garbage collection log path. Otherwise, enter 2 and skip to step 26.

29. You are prompted to specify the garbage collection log path:

    ```
    Enter the GC log path:
    ```

    Enter a file name with its full path. The data collector automatically modifies the log file name, adding the server instance information to it. For example, if you specify `gc.log` as the file name, the actual name is set to *`profile_name.cell_name.node_nameserver_name`*`.gc.log` for every configured application server instance.

    Important: In the garbage collection log path, you can use WebSphere variables such as`${SERVER_LOG_ROOT}`. However, do not use templates, such as `%pid`.

30. You are prompted to specify whether you want to increase the heap size:

```
Do you want to add 128M to the heap size? [1 - YES, 2 - NO]
[default is: 2]: 2
```

Enter 2 to retain the existing heap size. Otherwise, enter 1.

31. In the **Data collector configuration summary** section, the utility provides a summary of the data collector configuration that will be applied to the specified application server instances:

```
 1) List of servers selected

   - WAS server: co098170Node01Cell.co098170Node01.server1(AppSrv01)
       WAS cell: co098170Node01Cell
        WAS node: co098170Node01

       WebSphere Profile home    :
          C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01

       wsadmin location          :
         C:\Program Files\IBM\WebSphere\AppServer\bin\wsadmin.bat

                    WAS version : 8.0.0.0
                     Deployment : Standalone
                       JVM mode : 32
                Configuration home : C\IBM\ITM\dchome


 2) Integrate with ITCAM for SOA Agent : Yes

 3) Integrate with ITCAM Agent for WebSphere Applications : Yes

       TEMA hostname or IP address : 127.0.0.1
                TEMA port number : 63335
                      Monitor GC : No

 4) Integrate with ITCAM for AD Managing Server : No

       MS hostname or IP address : 127.0.0.1
         MS codebase port number : 9122
               MS home directory : /opt/IBM/itcam/WebSphere/MS

 5) Integrate with ITCAM for Transactions : Yes

       Transaction Collector hostname : 127.0.0.1
       Transaction Collector port number : 5455

 6) Integrate with Tivoli Performance Viewer : No

 7) Integrate with ITCAM diagnostics tool : No

 8) Advanced settings :

       Set Garbage Collection log path : No
       Added 128M to the heap size : No

You may accept or update your configuration choices for the following actions:
 1) List of servers selected
 2) Integrate with ITCAM for SOA Agent
 3) Integrate with ITCAM Agent for WebSphere Applications
 4) Integrate with ITCAM for AD Managing Server
 5) Integrate with ITCAM for Transactions
 6) Integrate with Tivoli Performance Viewer
 7) Integrate with ITCAM diagnostics tool
 8) Advanced settings
```

```
To modify a section, enter the number. To modify all sections, enter '*'. To accept you
configuration without modifying, enter 'a'.
To quit the selection, enter 'q':
```

The summary section provides options to change parts of the data collector configuration before applying the changes and an option to exit the configuration tool without applying your changes. Enter the number that represents the section that you want to edit. Enter an asterisk (*) to reconfigure all sections. Enter `a` to accept your changes. Enter `q` to exit the ITCAM Data Collector for WebSphere Reconfiguration Utility.

32. When you enter `a` to accept your changes, you are prompted to specify whether you want to create a backup of your current WebSphere Application Server configuration:

    ```
    Do you want to backup current WebSphere configuration? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

33. Enter 1 to create a backup of the current configuration. Otherwise, enter 2.
34. The changes are applied and a status message is presented to indicate that the configuration of the data collector for the profile is complete:

    ```
    Successfully executed config for Cell: co098170Node01Cell
    Node: co098170Node01 Profile: AppSrv01.
    ```

Important: After reconfiguring the data collector to monitor an application server instance, you must restart the application server instances. The data collector configuration takes effect when the application server instances are restarted.

Migrating data collectors to the ITCAM Data Collector for WebSphere

The ITCAM Data Collector for WebSphere Migration Utility is a menu driven command-line utility for migrating older version of the data collector to the ITCAM Data Collector for WebSphere.

You can upgrade the data collector to use the ITCAM Data Collector for WebSphere if your application server instances are being monitoring by any of the following products or components:

- ITCAM for WebSphere version 6.1 (fix pack 4 or later
- WebSphere Data Collector version 6.1 (fix pack 4 or later) included in ITCAM for Web Resources version 6.2
- ITCAM Agent for WebSphere Applications version 7.1 included in ITCAM for Applications Diagnostics version 7.1
- ITCAM for WebSphere Application Server version 7.2
- ITCAM for SOA version 7.1.1

For the procedure for migrating the ITCAM for SOA version 7.1.1 data collector to version 7.2, see “Migrating ITCAM for SOA version 7.1.1 data collector to the ITCAM Data Collector for WebSphere” on page 34.

To upgrade monitoring of server instances to the ITCAM Data Collector for WebSphere, complete the following procedure:

1. Set the location of the Java home directory before you run the utility.

   On Windows systems:

   ```
   set JAVA_HOME=C:\Program~1\IBM\WebSphere\AppServer80\java
   ```

2. Run the following command to start the ITCAM Data Collector for WebSphere Migration Utility.

On Windows systems:

```
DC_home\bin\migrate.bat
```

3. The utility displays the IP addresses of all network cards that are found on the local computer system and prompts you to specify the interface to use for the data collector:

```
List of TCP/IP interfaces discovered:
  1. 9.111.98.108
Enter a number [default is: 1]:
```

4. Enter the number that corresponds to the IP address to use.

   The utility prompts you to specify from the type of agent that you want to upgrade to ITCAM Data Collector for WebSphere.

```
List of ITCAM agents whose data collector can be upgraded to the
ITCAM Data Collector for WebSphere 7.2:

1. ITCAM for WebSphere 6.1 (fix pack 4 or later)
2. ITCAM WebSphere Agent 6.2 (fix pack 4 or later) [ITCAM for Web Resources 6.2]
3. ITCAM Agent for WebSphere Applications 7.1 [ITCAM for Application Diagnostics 7.1]
4. ITCAM for WebSphere Application Server 7.2
5. ITCAM for SOA 7.1.1
Enter the number [default is: 1]:
```

   Enter the number that represents the agent.

   For the procedure for migrating the ITCAM for SOA version 7.1.1 data collector to version 7.2, see "Migrating ITCAM for SOA version 7.1.1 data collector to the ITCAM Data Collector for WebSphere" on page 34.

5. The utility prompts you to specify the home directory of the previous version of the data collector.

```
Enter the home directory of the data collector to be upgraded:
```

6. Enter the home directory of the previous version of the data collector. For example, `C:\IBM\ITM\TMAITM6\wasdc\7.1.0.2`.

   If you are migrating ITCAM for WebSphere Application Server version 7.2, skip to step 9.

7. If the data collector was integrated with the ITCAM Agent for WebSphere monitoring agent, you are prompted to reenter the host name and port of the monitoring agent. If more than one version of the monitoring agent is available, you can connect the data collector to the correct version.

```
Enter the host name or IP address of the ITCAM Agent for WebSphere Applications TEMA:
[default is: 127.0.0.1]:
```

8. Enter the fully qualified host name or IP address of the ITCAM Agent for WebSphere Applications monitoring agent. It is on the local host, so the default is correct.

   You are prompted for the port number of the ITCAM Agent for WebSphere Applications monitoring agent.

```
Enter the port number of the ITCAM Agent for WebSphere Application TEMA:
[default is: 63335]:
```

   Enter the port number of the monitoring agent.

9. The utility searches for the list of application server instances that are configured by the specified data collector installation.

   The utility prompts you to select one or more application server instances from the list. The instances might be under different profiles.

```
Choose a Server or Servers to be migrate
 1. x336r1s37-vn01Cell01.x336r1s36-vn01Node03.server3
 2. x336r1s37-vn01Cell01.x336r1s36-vn01Node03.server5
```

```
 3. x336r1s37-vn01Cell01.x336r1s36-vn01Node03.server1
Enter a number or numbers separated by a comma, enter '*' to select all
servers listed, or enter 'q' to quit the selection.
```

Tip: If several instances under one profile are monitored, you must select them all for migrating at the same time.

Remember:

- For a stand-alone environment, application server instances must be running during the configuration.
- For a Network Deployment or Extended Deployment environment, the node agent and deployment manager must be running.

10. Enter the number that corresponds to the application server instance whose data collector is to be migrated or enter an asterisk (*) to migrate the data collector of all application server instances. To specify a subset of servers, enter the numbers, separated by commas, that represents the servers. For example: `1,2,3`.
11. The utility determines whether WebSphere Global Security was enabled for each of the profiles that are impacted by the migration task.
12. If WebSphere Global Security is enabled on one or more profiles, the utility prompts you to specify whether to retrieve security settings from a client properties file:

    ```
    Do you want to retrieve security settings from a client properties file
    (soap.client.props or sas.client.props)?
    [1 - YES, 2 - NO] [default is: 2]:
    ```

    The data collector communicates with the WebSphere Administrative Services using the Remote Method Invocation (RMI) or the SOAP protocol. If global security is enabled for a profile, you must specify the user ID and password of a user who is authorized to log in to the IBM WebSphere Application Server administrative console for the profile. Alternatively, you can encrypt the user name and password and store them in client properties files before configuring the data collector. You must use the `sas.client.props` file for an RMI connection, or the `soap.client.props` file for an SOA connection.

    Enter *1* to allow the utility to retrieve the user name and password from the appropriate client properties file and skip to step 13. Otherwise, enter *2* to enter the user name and password.

    ```
    CFG1018I Enter WebSphere admin user name:
    CFG1019I Enter WebSphere admin password:
    ```

    Important: It might take some time to log in to the WebSphere Application Server administrative console.
    The utility prompts you for the user name and password for each profile where WebSphere Global Security is enabled.
13. The utility migrates data collection for each selected application server instance and displays a status message that indicates whether the migration of each server completed successfully.

When the utility completes the migration of all application server instances configured by the previous version of the data collector, it displays the following message:

```
Migration of the Data Collector has successfully completed with return code 0.
```

Important: After migrating the data collector, you must restart the application server instances. The data collector configuration takes effect when the application server instances are restarted.

Remember: For server instances that were migrated, do not use the configuration utility for the old data collector version.

You can also configure or reconfigure integration with ITCAM for SOA, ITCAM Agent for WebSphere Applications monitoring agent, ITCAM for Application Diagnostics Managing Server, Tivoli Performance Viewer, and ITCAM diagnostics tool for the application server instances. For more information, see "Reconfiguring the ITCAM Data Collector for WebSphere" on page 22.

Migrating the ITCAM Data Collector for WebSphere in silent mode

A previous version of the ITCAM Data Collector for WebSphere can be migrated interactively with the ITCAM Data Collector for WebSphere Migration Utility. Alternatively, to migrate many application server instances to use the latest version of the data collector, you can migrate the data collectors in silent mode.

When you migrate the data collector in silent mode, you first specify configuration options in a properties file. A sample properties file, `sample_silent_migrate.txt`, is packaged with the ITCAM Data Collector for WebSphere Migration Utility. The file is available in the following location:

On Windows systems: *DC_home*\bin

A sample of a properties file is available here: "Sample properties file" on page 33

Complete the following steps to perform a silent migration:

1. Specify configuration options in the properties file.
2. Go to the *DC_home*\bin
3. Run the following command:

   ```
   migrate.bat -silent [dir_path]\silent file
   ```

During a silent migration, you can also configure or reconfigure integration with: ITCAM for SOA, ITCAM Agent for WebSphere Applications monitoring agent, ITCAM for Application Diagnostics Managing Server, ITCAM for WebSphere Application Server, and ITCAM Diagnostics Tool. Use the silent configuration parameters for these components, as described in "Configuring the ITCAM Data Collector for WebSphere in silent mode" on page 17.

To migrate ITCAM for SOA version 7.1.1 using the ITCAM Data Collector for WebSphere Migration Utility in silent mode, see "Migrating ITCAM for SOA version 7.1.1 to the ITCAM Data Collector for WebSphere in silent mode" on page 37.

Properties file

When you create your silent response properties file, keep in mind these considerations:

- A line in the file that starts with a number sign (#) is treated as a comment, and is not processed. If the number sign is used elsewhere in the line, it is not considered to be the start of a comment.

- Each property is described on a separate line, in the following format: *property* = *value*.

  property
  This is the name of property. The list of valid properties that you can configure is shown in Table 6 on page 18.

  value This is the value of the property. Default values for some properties are already provided. You can delete default values to leave property values blank, or empty. An empty value is treated as if the property is not specified, as opposed to using the default value. If you want to use default values, you can comment out the property in the file.
- Passwords are in plain text.
- Properties and their values are case-sensitive.
- Table 7 describes the available properties for running the migration utility in silent mode:

Table 7. Available properties for running the ITCAM Data Collector for WebSphere Migration Utility in silent mode

Property	Comment
default.hostip	If the computer system uses multiple IP addresses, specify the IP address for the data collector to use.
migrate.type	Type of agent whose data collector you want to migrate to the ITCAM Data Collector for WebSphere version 7.2. The value must be set to *AD*.
Location of data collector to be migrated	
itcam.migrate.home	Specifies the data collector home directory of the old version of the data collector. The directory is not deleted as part of the migration.
ITCAM Agent for WebSphere Applications monitoring agent settings	
temaconnect	Specifies whether the data collector connects to the ITCAM Agent for WebSphere Applications monitoring agent. Set this property to *False* if you do not want to connect the ITCAM Agent for WebSphere Applications with the monitoring agent, if you plan to connect the ITCAM Agent for WebSphere Applications with the Managing Server only, or if you do not have the ITCAM Agent for WebSphere Applications installed. Valid values are *True* and *False*. **Remember:** The Managing Server is not a component of ITCAM for Applications.
tema.host	Specifies the fully qualified host name or IP address of the ITCAM for Agent for WebSphere Applications monitoring agent.
tema.port	Specifies the port number of the ITCAM for Agent for WebSphere Applications monitoring agent.
WebSphere Application Server connection settings	
was.wsadmin.connection.host	Specifies the name of the host to which the wsadmin tool is connecting.
WebSphere Application Server global security settings	
was.wsadmin.username	Specifies the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server.
was.wsadmin.password	Specifies the password that corresponds to the user specified in the `was.wsadmin.username` property.
WebSphere Application Server settings	

Table 7. Available properties for running the ITCAM Data Collector for WebSphere Migration Utility in silent mode (continued)

Property	Comment
was.appserver.profile.name	Specifies the name of the application server profile you want to configure.
was.appserver.home	Specifies the WebSphere Application Server home directory.
was.appserver.cell.name	Specifies the WebSphere Application Server cell name.
was.appserver.node.name	Specifies the WebSphere Application Server node name.
WebSphere Application Server runtime instance settings	
was.appserver.server.name	Specifies the application server instance within the application server profile to migrate to the new version of the data collector. **Tip:** The silent response file can have multiple instances of this property.

Sample properties file

When you run the migrate script in silent mode, the configuration parameters are read from a simple text properties file, `silent_file`, that you create in advance. A typical properties file might look similar to the following example:

```
#################################################################################
#
#Comments:
#Locate the ITCAM Data Collector for WebSphere Migration Utility (migrate.sh|bat) in <dc_home>/bin.
#Run migrate.sh|bat -silent [dir_path]/<properties_file> to migrate an older version of the data collector silently.
#This file is a sample properties file.
#
#This file has 2 sections; [DEFAULT SECTION] and [SERVER].
#You can have one instance of [DEFAULT].
#You can have multiple instances of [SERVER].
#
#Use this sample file to migrate the data collector of any of the following products:
#  ITCAM for WebSphere 6.1 (fix pack 4 or later)
#  WebSphere Data Collector 6.1 (fix pack 4 or later)
#  ITCAM Agent for WebSphere Applications 7.1
#  ITCAM for WebSphere Application Server 7.2
#
#Considerations:
#IP address to use:
#Uncomment and specify an IP address to use, if the system has multiple IP addresses.
#
#Migration type:
#Important: Do not modify this value.
#
#Servers:
#You can migrate the data collector for multiple servers in the same profile.
#Uncomment the second [SERVER] and add the server name.
#Repeat for each additional server.
#
#
#################################################################################

[DEFAULT SECTION]

#  IP address to use:
#default.hostip=9.9.9.9

#Migration type:
migrate.type=AD

#  Old data collector home directory:
itcam.migrate.home=c:\ibm\itm\tmaitm6\wasdc\71
```

```
#  ITCAM Agent for WebSphere Applications monitoring agent:
temaconnect=True
tema.host=127.0.0.1
tema.port=63335

#  Connect to WebSphere Administrative Services:
was.wsadmin.connection.host=127.0.0.1
was.wsadmin.username=username
was.wsadmin.password=password

#  WebSphere Application Server details:
was.appserver.profile.name=AppSrv01
was.appserver.home=/opt/IBM/WebSphere/AppServer
was.appserver.cell.name=yourCellName
was.appserver.node.name=yourNodeName

[SERVER]
was.appserver.server.name=server1

#[SERVER]
#was.appserver.server.name=server2
```

Migrating ITCAM for SOA version 7.1.1 data collector to the ITCAM Data Collector for WebSphere

If your application server instances are being monitored by ITCAM for SOA version 7.1.1, you can upgrade the data collector to use the ITCAM Data Collector for WebSphere.

The ITCAM Data Collector for WebSphere Migration Utility is a menu driven command-line utility for migrating previous versions of the ITCAM Data Collector for WebSphere.

For the procedure for migrating the following data collector components to the ITCAM Data Collector for WebSphere, see "Migrating data collectors to the ITCAM Data Collector for WebSphere" on page 28:

- ITCAM for WebSphere version 6.1 (fix pack 4 or later)
- WebSphere Data Collector version 6.1 (fix pack 4 or later) included in ITCAM for Web Resources version 6.2
- ITCAM for WebSphere Application Server version 7.1 included in ITCAM for Applications Diagnostics version 7.1
- ITCAM for WebSphere Application Server version 7.2. Data Collector

To upgrade the monitoring of server instances from the ITCAM for SOA version 7.1.1 data collector to the ITCAM Data Collector for WebSphere, complete the following procedure:

1. Set the location of the Java home directory before you run the utility.

   ```
   set JAVA_HOME=C:\Program~1\IBM\WebSphere\AppServer80\java
   ```

2. Run the following command to start the ITCAM Data Collector for WebSphere Migration Utility.

   DC_home\bin\migrate.bat

3. The utility displays the IP addresses of all network cards that are found on the local computer system and prompts you to specify the interface to use for the data collector:

   ```
   List of TCP/IP interfaces discovered:
     1. 9.111.98.108
   Enter a number [default is: 1]:
   ```

4. Enter the number that corresponds to the IP address to use.

   The utility prompts you to specify the type of agent that you want to upgrade to ITCAM Data Collector for WebSphere version 7.2.

   ```
   List of ITCAM agents whose data collector can be upgraded to the
   ITCAM Data Collector for WebSphere 7.2:

   1. ITCAM for WebSphere 6.1 (fix pack 4 or later)
   2. ITCAM WebSphere Agent 6.2 (fix pack 4 or later) [ITCAM for Web Resources 6.2]
   3. ITCAM Agent for WebSphere Applications 7.1 [ITCAM for Application Diagnostics 7.1]
   4. ITCAM for WebSphere Application Server 7.2
   5. ITCAM for SOA 7.1.1
   Enter the number [default is: 1]:
   ```

   Enter 5 to migrate ITCAM for SOA version 7.1.1.

5. The utility prompts you to specify the WebSphere Application Server home directory where the previous version of the ITCAM for SOA version 7.1.1 data collector is configured.

   ```
   Specify SOA Websphere Home Directory:
   ```

6. The utility searches for WebSphere Application Server home directories on the computer system and prompts you to select a home directory.

   ```
   List of WebSphere Application Server home directories discovered:
     1. C:\Program Files\IBM\WebSphere\AppServer
   Enter a number or enter the full path to a home directory
   [default is: 1]:
   ```

7. Enter the number that corresponds to a WebSphere Application Server home directory.

   The utility searches for all profiles under the specified home directory and prompts you to select a profile:

   ```
   List of WebSphere profiles discovered:
     1. AppSrv01
   Enter a number [default is: 1]:
   ```

8. Enter the number that corresponds to the WebSphere Application Server profile you want to configure.

   The utility indicates whether WebSphere Global Security is enabled for the WebSphere Application profile that you specified:

   ```
   WebSphere Global Security is enabled.
   ```

   If global security is not enabled, skip to step 10 on page 36.

9. The utility prompts you to specify whether to retrieve security settings from a client properties file:

   ```
   Do you want to retrieve security settings from a client properties file
   (soap.client.props or sas.client.props)?
   [1 - YES, 2 - NO] [default is: 2]:
   ```

   The data collector communicates with the WebSphere Administrative Services using the Remote Method Invocation (RMI) or the SOAP protocol. If global security is enabled for a profile, you must specify the user ID and password of a user who is authorized to log in to the IBM WebSphere Application Server administrative console for the profile. Alternatively, you can encrypt the user name and password and store them in client properties files before configuring the data collector. You must use the `sas.client.props` file for an RMI connection, or the `soap.client.props` file for a SOAP connection.

   Enter 1 to allow the utility to retrieve the user name and password from the appropriate client properties file and skip to step 10 on page 36. Otherwise, enter 2 to enter the user name and password.

```
CFG1018I Enter WebSphere admin user name:
CFG1019I Enter WebSphere admin password:
```

10. The utility searches for all application server instances under the specified profile. The utility displays all servers that are not configured yet for data collection and all servers that have been configured to use the current version of the ITCAM Data Collector for WebSphere.

    The utility prompts you to select one or more application server instances from the list:

```
Choose one or more servers to configure for data collection:
Application servers not yet configured:
 1. co098170Node01Cell.co098170Node01.server1(AppSrv01)
Enter a number or numbers separated by commas, or enter * to select all:
```

    Important:

    - For a Network Deployment or Extended Deployment environment, the Node Agent and Deployment Manager must be running. For a stand-alone environment, application server instances must be running during the configuration of the data collector.
    - Ensure that the application server instances that you select are the actual nodes that host the BPM applications or services that you want to monitor.

11. Enter the number that corresponds to the application server instance to configure for data collection or enter an asterisk `*` to configure all application server instances for data collection. To specify a subset of servers, enter the numbers, separated by commas, that represents the servers. For example: `1,2,3`.

    The utility displays a summary list. By default, it configures the migrated instances to integrate with ITCAM for SOA only. You can specify other configurations.

```
+------------------------------------------------------------------------+
|                                                                        |
|  Data collector configuration summary                                  |
|                                                                        |
+------------------------------------------------------------------------+

Each of the servers will be configured for data collection

 1) List of servers selected

   - WAS server: IBM-6DA7F9C6EE6Node02Cell.IBM-6DA7F9C6EE6Node02.server1(AppSrv02)
       WAS cell: IBM-6DA7F9C6EE6Node02Cell
        WAS node: IBM-6DA7F9C6EE6Node02

       WebSphere Profile home    :
         C:\Program Files\IBM\WebSphere\AppServer80\profiles\AppSrv02

       wsadmin location          :
         C:\Program Files\IBM\WebSphere\AppServer80\bin\wsadmin.bat

                    WAS version : 8.0.0.0
                     Deployment : Standalone
                       JVM mode : 32
              Configuration home : C:\NewInstall\itcam_gdc_201204122100\bin\..

 2) Integrate with ITCAM for SOA Agent : Yes

 3) Integrate with ITCAM Agent for WebSphere Applications : No

 4) Integrate with ITCAM for AD Managing Server : No

 5) Integrate with ITCAM for Transactions : No
```

```
 6) Integrate with Tivoli Performance Viewer : No

 7) DE Integrate with ITCAM diagnostics tool : No

 8) Advanced settings :

       Set Garbage Collection log path : No
       Added 128M to the heap size : No


Configuration sections:

 1) List of servers selected
 2) Integrate with ITCAM for SOA Agent
 3) Integrate with ITCAM Agent for WebSphere Applications
 4) Integrate with ITCAM for AD Managing Server
 5) Integrate with ITCAM for Transactions
 6) Integrate with Tivoli Performance Viewer
 7) DE Integrate with ITCAM diagnostics tool
 8) Advanced settings

To modify a section, enter the number. To modify all sections, enter '*'. To accept your
configuration without modifying, enter 'a'. To quit the selection, enter 'q'.:
```

12. To enable integration with products and components other than ITCAM for SOA, select the corresponding number. For details on the configuration, see "Configuring the ITCAM Data Collector for WebSphere" on page 11. Otherwise, to accept the configuration, enter `a`.

    You are prompted to specify whether you want to create a backup of your current WebSphere Application Server configuration:

    ```
    Do you want to backup current WebSphere configuration? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

13. Enter 1 to create a backup of the current configuration. Otherwise, enter 2.

The changes are applied and a status message is presented to indicate that the configuration of the data collector for the profile is complete:

```
Successfully executed config for Cell: co098170Node01Cell
Node: co098170Node01 Profile: AppSrv01.
```

Important: After migrating from the ITCAM for SOA version 7.1.1 data collector, you must restart the application server instances. The data collector configuration takes effect when the application server instances are restarted.

You can also configure or reconfigure integration with ITCAM for SOA, ITCAM Agent for WebSphere Applications monitoring agent, ITCAM for Application Diagnostics Managing Server, Tivoli Performance Viewer, and ITCAM Diagnostics Tool for the application server instances at the same time. For more information about reconfiguring application server instances, see "Reconfiguring the ITCAM Data Collector for WebSphere" on page 22.

Migrating ITCAM for SOA version 7.1.1 to the ITCAM Data Collector for WebSphere in silent mode

The ITCAM for SOA version 7.1.1 data collector can be migrated to the ITCAM Data Collector for WebSphere interactively with the ITCAM Data Collector for WebSphere Migration Utility. Alternatively, to migrate many application server instances to use the latest version of the data collector, you can migrate the data collector in silent mode.

When you migrate the ITCAM for SOA version 7.1.1 data collector in silent mode, you first specify configuration options in a properties file. A sample properties file, `sample_silent_migrate_soa.txt`, is packaged with the ITCAM Data Collector for WebSphere Migration Utility. The file is available in the following location:

On Windows systems: *DC_home*\bin

A sample of a properties file is presented in "Sample properties file" on page 40.

Complete the following steps to perform a silent migration:

1. Specify configuration options in the properties file.
2. Go to the *DC_home*\bin .
3. Run the following command:

   ```
   migrate.bat -silent [dir_path]\silent file
   ```

During a silent migration, you can also configure or reconfigure integration with ITCAM for SOA, ITCAM Agent for WebSphere Applications monitoring agent, ITCAM for Application Diagnostics Managing Server, Tivoli Performance Monitoring, and the ITCAM Diagnostics Tool for the application server instances at the same time. To do this, use the silent configuration parameters for these components, as described in "Configuring the ITCAM Data Collector for WebSphere in silent mode" on page 17.

Properties file

When you create your silent response properties file, keep in mind these considerations:

- A line in the file that starts with a number sign (#) is treated as a comment, and is not processed. If the number sign is used elsewhere in the line, it is not considered to be the start of a comment. This means that you can use the number sign in passwords or for other uses.
- Each property is described on a separate line, in the following format: *property* = *value*.

  property
  : This is the name of property. The list of valid properties that you can configure is shown in: Table 6 on page 18.

  value
  : This is the value of the property. Default values for some properties are already provided. You can delete default values to leave property values blank, or empty. An empty value is treated as if the property is not specified, as opposed to using the default value. To use default values, you can comment out the property in the file.

- Passwords are in plain text.
- Properties and their values are case-sensitive.

Table 8. Available properties for running the ITCAM Data Collector for WebSphere Migration Utility in silent mode

Property	Comment
default.hostip	If the computer system uses multiple IP addresses, specify the IP address for the data collector to use.
migrate.type	Type of agent whose agent you want to migrate to the ITCAM Data Collector for WebSphere version 7.2. The value must be set to *SOA*.

Table 8. Available properties for running the ITCAM Data Collector for WebSphere Migration Utility in silent mode (continued)

Property	Comment
was.appserver.home	Location of the WebSphere Application Server home directory where the ITCAM for SOA version 7.1.1 data collector is configured. For example: `/opt/IBM/WebSphere85/AppServer`.
ms.connect	Specifies whether the data collector is configured to connect to the Managing Server in an ITCAM for Application Diagnostics environment. For a migration from ITCAM for SOA version 7.1.1, ignore this parameter.
ttapi.enable	Specifies whether the data collector communicates with ITCAM for Transactions using the Transaction Tracking API (TTAPI). Valid values are *True* and *False*.
soa.enable	Specifies whether to integrate the data collector with ITCAM for SOA. The ITCAM for SOA agent must be installed to complete the configuration.
tpv.enable	Specifies whether to integrate the data collector with the Tivoli Performance Monitoring when the data collector is included as part of ITCAM for WebSphere Application Server 8.5. Tivoli Performance Monitoring is accessed with the WebSphere Application Server administrative console. For a migration from ITCAM for SOA 7.1.1, ignore this parameter.
de.enable	Specifies whether to integrate the data collector with the ITCAM Diagnostics Tool. The ITCAM Diagnostics Tool is built on Eclipse. It is a tool for diagnostic investigation of applications that are running on WebSphere Application Server. For a migration from ITCAM for SOA version 7.1.1, ignore this parameter.
temaconnect	Specifies whether the data collector connects to the ITCAM Agent for WebSphere Applications monitoring agent (TEMA). For a migration from ITCAM for SOA version 7.1.1, ignore this parameter.
was.backup.configuration	Specifies whether to back up the current configuration of the WebSphere Application Server configuration before applying the new configuration. Valid values are *True* and *False*.
was.gc.custom.path	Specifies the path to the custom Garbage Collection log. For a migration from ITCAM for SOA version 7.1.1, ignore this parameter.
was.configure.heap	Specifies whether to add 128 MB to the heap size. Each time you run the silent configuration, 128 MB is added to the heap size if this property is set to *True*. For a migration from ITCAM for SOA version 7.1.1, ignore this parameter.
WebSphere Application Server connection settings	
was.wsadmin.connection.host	Specifies the name of the host to which the wsadmin tool is connecting.
was.wsadmin.connection.type	Specifies the connection protocol for the wsadmin tool to use.

Table 8. Available properties for running the ITCAM Data Collector for WebSphere Migration Utility in silent mode (continued)

Property	Comment
was.wsadmin.connection.port	Specifies the port that the wsadmin tool must use to connect to the WebSphere Application Server.
WebSphere Application Server global security settings	
was.wsadmin.username	Specifies the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server.
was.wsadmin.password	Specifies the password that corresponds to the user specified in the `was.wsadmin.username` property.
WebSphere Application Server settings	
was.appserver.profile.name	Specifies the name of the application server profile you want to configure.
was.appserver.cell.name	Specifies the WebSphere Application Server cell name.
was.appserver.node.name	Specifies the WebSphere Application Server node name.
WebSphere Application Server runtime instance settings	
was.appserver.server.name	Specifies the application server instance within the application server profile to configure. **Important:** The silent response file can have multiple instances of this property.

Sample properties file

When you run the *migrate* script in silent mode, the configuration parameters are read from a simple text properties file, *silent_file*, that you create in advance. A typical properties file might look similar to the following example:

```
#############################################################################################
#
#Comments:
#Locate the ITCAM Data Collector for WebSphere Migration Utility (migrate.sh|bat) in <dc_home>/bin.
#Run migrate.sh|bat -silent [dir_path]/<properties_file> to migrate an older version of the data collector silently.
#This file is a sample properties file.
#
#This file has 2 sections; [DEFAULT SECTION] and [SERVER].
#You can have one instance of [DEFAULT].
#You can have multiple instances of [SERVER].
#
#Use this sample file to migrate the ITCAM for SOA 7.1.1 data collector.
#To migrate all other older versions of the data collector, use sample_silent_migrate.txt.
#
#Considerations:
#IP address to use:
#Uncomment and specify an IP address to use, if the system has multiple IP addresses.
#
#Migration type:
# Important: Do not modify this value.
#
#Connect to WebSphere Administrative Services:
#The utility determines the connection type and port automatically.
#If the utility cannot determine the values, uncomment and override the default values.
#
#Servers:
#You can migrate the data collector for multiple servers in the same profile.
#Uncomment the second [SERVER] and add the server name.
#Repeat for each additional server.
#############################################################################################
```

```
[DEFAULT SECTION]
#IP address to use:
#default.hostip=9.9.9.9

#  Migration type:
migrate.type=SOA

#  Old WebSphere Application Server home directory:
was.appserver.home=/opt/IBM/WebSphere85/AppServer

#  ITCAM for Application Diagnostics Managing Server:
ms.connect=False

#  ITCAM for Transactions:
ttapi.enable=False

#  ITCAM for SOA agent:
soa.enable=True

#  Tivoli Performance Viewer:
tpv.enable=False

#  ITCAM Diagnostics Tool:
de.enable=False

#  ITCAM Agent for WebSphere Applications monitoring agent:
temaconnect=False

#  Create a backup of WebSphere Application Server:
was.backup.configuration=False

#  Modify Garbage Collection log path:
was.gc.custom.path=False

#  Increase the JVM heap size by 128MB:
was.configure.heap=False

#Connect to WebSphere Administrative Services:
was.wsadmin.connection.host=servername.yourcompany.com
was.wsadmin.username=
was.wsadmin.password=
#was.wsadmin.connection.type=SOAP
#was.wsadmin.connection.port=8881

#  WebSphere Application Server details:
was.appserver.profile.name=AppSrv01
was.appserver.cell.name=yourITCAMCell
was.appserver.node.name=yourITCAMNode

[SERVER]
was.appserver.server.name=server1

#[SERVER]
#was.appserver.server.name=server2
```

Unconfiguring the ITCAM Data Collector for WebSphere

If you no longer want the data collector to monitor one or more application server instances, you can unconfigure the data collector for them.

The ITCAM Data Collector for WebSphere Unconfiguration Utility is a menu driven command-line utility for unconfiguring the ITCAM Data Collector for WebSphere.

To unconfigure the data collector, complete the following procedure:

1. From a command-line, navigate to the *DC_home*\bin directory.

2. Set the location of the Java home directory before you run the script. For example:

   ```
   set JAVA_HOME=C:\Program~1\IBM\WebSphere\AppServer80\java
   ```

3. Run the following command to start the ITCAM Data Collector for WebSphere Unconfiguration Utility.

   DC_home\bin\unconfig.bat

   The utility searches for all server instances that are monitored by the ITCAM Data Collector for WebSphere.

   Remember:

   - Application server instances must be running during the unconfiguration procedure.
   - For Network Deployment environment, the node agent and deployment manager must also be running.

   The utility prompts you to select one or more application server instances from the list of configured servers:

   ```
   Choose one or more servers to unconfigure for data collection:
   Application servers configured:
    1. co098170Node01Cell.co098170Node01.server1(AppSrv01)
   Enter a number or numbers separated by commas, or enter * to select all:
   ```

4. Enter the number that corresponds to the application server instance to unconfigure for data collection or enter an asterisk (*) to unconfigure data collection for all application server instances. To specify a subset of servers, enter the numbers, separated by commas, that represent the servers. For example: 1,2,3.
5. The utility unconfigures the data collector for the specified application server instances. A status message is displayed to indicate that the data collector was successfully unconfigured:

   ```
   Unconfiguration of the Data Collector has successfully completed with return code 0.
   ```

Data collection is unconfigured for the specified application server instances.

Unconfiguring the ITCAM Data Collector for WebSphere in silent mode

The ITCAM Data Collector for WebSphere can be unconfigured interactively using the ITCAM Data Collector for WebSphere Unconfiguration Utility. Alternatively, to unconfigure data collection for many application server instances, you can unconfigure the data collectors in silent mode.

When you unconfigure the data collector in silent mode, you first specify configuration options in a properties file. A sample properties file, sample_silent_unconfig.txt, is packaged with the ITCAM Data Collector for WebSphere Unconfiguration Utility. The file is available in the following location:

On Windows systems: *DC_home*\bin

The variable *DC_home* is the location where the data collector is installed. A sample of a properties file is presented in Table 9 on page 43.

Complete the following steps to perform a silent unconfiguration:

1. Specify configuration options in the properties file.
2. Go to the *DC_home*\bin .

3. Run the following command:

   ```
   unconfig.bat -silent [dir_path]\silent file
   ```

4. After unconfiguring the data collector to monitor application server instances, you must restart the instances. The data collector configuration takes effect when the application server instances are restarted.

Properties file

When you create your silent response properties file, keep in mind these considerations:

- A line in the file that starts with a number sign (#) is treated as a comment, and is not processed. If the number sign is used elsewhere in the line, it is not considered to be the start of a comment.
- Each property is described on a separate line, in the following format: *<property> = value>*.

  property
  : This is the name of property. The list of valid properties that you can configure is shown in Table 9.

  value
  : This is the value of the property. Default values for some properties are already provided. You can delete default values to leave property values blank, or empty. An empty value is treated as if the property is not specified, as opposed to using the default value. To use default values, you can comment out the property in the file.

- Passwords are in plain text.
- Properties and their values are case-sensitive.

Table 9. Available properties for running the ITCAM Data Collector for WebSphere Unconfiguration Utility in silent mode

Property	Comment
WebSphere Application Server connecting settings	
was.wsadmin.connection.host	Specifies the name of the host to which the wsadmin tool is connecting.
WebSphere Application Server global security settings	
was.wsadmin.username	Specifies the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server.
was.wsadmin.password	Specifies the password that corresponds to the user specified in the `was.wsadmin.username` property.
WebSphere Application Server settings	
was.appserver.profile.name	Specifies the name of the application server profile you want to unconfigure.
was.appserver.home	Specifies the WebSphere Application Server home directory.
was.appserver.cell.name	Specifies the WebSphere Application Server cell name.
was.appserver.node.name	Specifies the WebSphere Application Server node name.
Backup of the WebSphere Application Server configuration	
was.backup.configuration	Specifies whether to back up the current configuration of the WebSphere Application Server data collector configuration before unconfiguring the data collector. Valid values are *True* and *False*.
was.backup.configuration.dir	Specifies the location of the backup directory.

Table 9. Available properties for running the ITCAM Data Collector for WebSphere Unconfiguration Utility in silent mode (continued)

Property	Comment
WebSphere Application Server runtime instance settings	
was.appserver.server.name	Specifies an application server instance within the application server profile for which you want to unconfigure the data collector. **Tip:** The silent response file can have multiple instances of this property.

Sample properties file

```
#################################################################################################
#
#Comments:
#Locate the ITCAM Data Collector for WebSphere Unconfiguration Utility (unconfig.sh|bat) in <dc_home>/bin.
#Run unconfig.sh|bat -silent [dir_path]/<properties_file> to unconfigure the data collector silently.
#This file is a sample properties file.
#
#This file has 2 sections; [DEFAULT SECTION] and [SERVER].
#You can have one instance of [DEFAULT].
#You can configure multiple [SERVER] sections, one for each server to be configured within the profile.
#Uncomment the second [SERVER] and add the server name.
#Repeat for each additional server.
#
#################################################################################################

[DEFAULT SECTION]

#Connect to WebSphere Administrative Services:
was.wsadmin.connection.host=servername.yourcompany.com
was.wsadmin.username=
was.wsadmin.password=

#  WebSphere Application Server details:
was.appserver.profile.name=AppSrv02
was.appserver.home=C:\Program Files\IBM\WebSphere\AppServer
was.appserver.cell.name=yourITCAMCell
was.appserver.node.name=yourITCAMNode

#  Create a backup of WebSphere Application Server:
was.backup.configuration=False
was.backup.configuration.dir=/opt/IBM/ITM/dchome/data

[SERVER]
was.appserver.server.name=server1

#[SERVER]
#was.appserver.server.name=server2
```

Chapter 4. Installing and configuring ITCAM for WebSphere Application Server on Linux and UNIX systems

ITCAM for WebSphere Application Server is an optional component that can be installed on an existing version of:

1. WebSphere Application Server Network Deployment, Version 8.5
2. WebSphere Application Server Express, Version 8.5
3. WebSphere Application Server, Version 8.5
4. ITCAM for Transactions

ITCAM for WebSphere Application Server is composed of the ITCAM Data Collector for WebSphere. When you install and configure this component, you can view performance data information in the Tivoli Performance Viewer in WebSphere Application Server 8.5. To collect this data, you must install ITCAM Data Collector for WebSphere on every application server host, and configure it for every instance.

ITCAM Data Collector for WebSphere can also integrate with other products and components:

- ITCAM Agent for WebSphere Applications
- ITCAM for Application Diagnostics Managing Server
- ITCAM for SOA

If the application server instance was monitored by a previous version of one of these products, as well as ITCAM for WebSphere or ITCAM for Web Resources, you must migrate its monitoring to the new ITCAM Data Collector for WebSphere. The existing product will continue to function with this data collector.

Installing ITCAM for WebSphere Application Server on Linux and UNIX systems

ITCAM for WebSphere Application Server is an optional component that can be installed on an existing version of:

1. WebSphere Application Server Network Deployment, Version 8.5
2. WebSphere Application Server Express, Version 8.5
3. WebSphere Application Server, Version 8.5

Prerequisites and preinstallation tasks for ITCAM for WebSphere Application Server on Linux and UNIX systems

A number of prerequisites need to be observed before installing ITCAM for WebSphere Application Server.

System and software prerequisites

The following hardware and software requirements need to be observed before installing ITCAM for WebSphere Application Server.

Hardware prerequisites for the ITCAM for WebSphere Application Server

The installation image requires 162 MB. Installation requires 390 MB.

Memory

ITCAM for WebSphere Application Server requires 1 GB of physical memory but 1.5 GB is recommended if the computer is running multiple installations of WebSphere Application Server or other applications that require a lot of memory.

Supported operating system and application server combinations

ITCAM for WebSphere Application Server must be installed on the same computer as the application server you will monitor. Thus, the set of supported operating systems is dependent on the supported operating systems for the application server you will monitor. For information about the UNIX and Linux platforms that WebSphere Application Server is supported on, see http://www-304.ibm.com/support/docview.wss?rs=180&uid=swg27006921

Supported JDKs

The supported JDKs for the ITCAM for WebSphere Application Server are the same as the supported JDKs for the particular application server you will monitor.

Installing the Data Collector

Install the ITCAM Data Collector for WebSphere on every host running the instances of WebSphere Application Server that you need to monitor. You can use one installation to collect data from any number of application server instances on the same host.

Before you begin

Download the data collector TAR file.

Procedure

1. Copy the Data Collector TAR file into a temporary directory.
2. Unpack the file into a new directory, for example, `/opt/IBM/itcam_install/7.2`. This path is referred to as *DC_home* in this guide.

What to do next

After installing the data collector, you must take one of the following actions to monitor server instances with the ITCAM for WebSphere Application Server:

- If any instances are already monitored with ITCAM for WebSphere Application Server, ITCAM for WebSphere, ITCAM for Application Diagnostics, or ITCAM for SOA, migrate monitoring of the instances to the new data collector. See "Migrating data collectors to the ITCAM Data Collector for WebSphere" on page 67 or "Migrating the ITCAM Data Collector for WebSphere in silent mode" on page 69.
- Otherwise, configure the data collector to monitor the instances. See "Configuring the ITCAM Data Collector for WebSphere" on page 49 or "Configuring the ITCAM Data Collector for WebSphere in silent mode" on page 56.

Configuring ITCAM for WebSphere Application Server on Linux and UNIX systems

Configure ITCAM for WebSphere Application Server using the ITCAM Data Collector for WebSphere Configuration Utility.

Pre-configuration notes

Before you run the configuration utility, there are some preconfiguration tasks you must perform and some preconfiguraiton information that you need to be aware of.

Permissions

Run the configuration utilities using a UNIX/Linux operating system user ID that owns the WebSphere Application Server profile that is being configured. If the WebSphere Application Server installer and profile owner do not map to the same UNIX/Linux operating system user ID, follow the steps in the WebSphere Application Server information center on configuring the profile user. For more information, see information center.

Where WebSphere Global security is enabled, the configuration utility prompts you for a WebSphere Administrator user ID that has login privileges to the wsadmin tool. Please use the primary administrative user for WebSphere Application Server.

Network Deployment environment

For a Network Deployment environment, supply the host name of the Deployment Manager to configure ITCAM for WebSphere Application Server for a node. It is not necessary to install or configure ITCAM for WebSphere Application Server on the Deployment Manager itself.

Checking the heap size

About this task

Ensure that the JVM heap size is sufficient. The default value is enough, but if the heap size was configured in WebSphere Application Server, make sure that it is not less than 384 MB. Complete the following steps for each server that you want to configure for ITCAM for WebSphere Application Server:

Procedure

1. Log on to the WebSphere Application Server administrative console.
2. Go to the area for specifying the heap size in the administrative console by completing the following steps:
   a. Click **Servers >Server Types>WebSphere Application Servers** and select the *server_name*.
   b. In the **Configuration** tab, go to **Server Infrastructure > Java and Process Management > Process Definition > Additional Properties: Java Virtual Machine**.
3. If the value in the **Maximum Heap Size** field is less than 384, set it to 384.

Network Deployment environment heap size: In a Network Deployment environment, increase the maximum heap size to a value greater than 256. If you don't increase the heap size, the installation might fail and the following error message is displayed:

CYNCR8522E: The system was unable to retrieve a list of known servers from server *server_name* using SOAP port *port_number*.

Optional: Enabling user ID and password input from sas.client.props for RMI connector types

About this task

When you use an RMI connection to WebSphere Application Server and global security is enabled, use the data collector configuration utility to retrieve the user ID and password from the sas.client.props file.

Procedure

1. Set the following properties in the *AppServer_home*/profiles/*profile_name*/properties/sas.client.props file:

   ```
   com.ibm.CORBA.loginSource=properties
   com.ibm.CORBA.securityEnabled=true
   com.ibm.CORBA.loginUserid=user_ID
   com.ibm.CORBA.loginPassword=password
   ```

2. Change to the *AppServer_home*/profiles/*profile_name*/bin directory and run the following command to encrypt the password:

   ```
   PropFilePasswordEncoder.sh path_to_props_file/sas.client.props com.ibm.CORBA
   .loginPassword
   ```

Optional: Enabling user ID and password input from soap.client.props for SOAP connector types

When you use a SOAP connection to WebSphere Application Server and global security is enabled, use the data collector configuration utility to retrieve the user ID and password from the soap.client.props file.

About this task

Procedure

1. Set the following properties in the *AppServer_home*/profiles/*profile_name*/properties/soap.client.props file:

   ```
   com.ibm.SOAP.securityEnabled=true
   com.ibm.SOAP.loginUserid=user_ID
   com.ibm.SOAP.loginPassword=password
   ```

2. Change to the: *AppServer_home*/profiles/*profile_name*/bin directory and run the following command to encrypt the password:

   ```
   PropFilePasswordEncoder.sh path_to_props_file/soap.client.props com.ibm.SOAP
   .loginPassword
   ```

Adjusting ports for firewalls or for use with other applications

During configuration in a Network Deployment environment, specify the SOAP or RMI port number that is used by ITCAM for WebSphere Application Server to communicate with the application server, Managing Server or ITCAM for Transactions. Ensure that the firewall does not prevent communication between ITCAM for WebSphere Application Server and the specified ports.

Configuring ITCAM for WebSphere Application Server

If you have any of the following product versions installed and configured for the same WebSphere profile, you must migrate them to use the ITCAM Data Collector for WebSphere before configuring ITCAM for WebSphere Application Server:

- ITCAM for SOA version 7.1.1

- ITCAM for WebSphere version 6.1.4 or later
- WebSphere Data Collector version 6.1.4 included in ITCAM for Web Resources version 6.2
- ITCAM Agent for WebSphere Applications version 7.1 included in ITCAM for Applications Diagnostics version 7.1

Using the new ITCAM Data Collector for WebSphere Configuration Utility, you can connect the common ITCAM Data Collector for WebSphere to the following components:

- Tivoli Performance Viewer - (this is ITCAM for WebSphere Application Server)
- ITCAM for SOA Monitoring agent 7.1.1 or later
- ITCAM Agent for WebSphere Applications monitoring agent 7.1.0.3 or later
- ITCAM for Application Diagnostics Managing Server 7.1.0.3 or later
- ITCAM for Transactions Transaction 7.3

Configuring in a profile where there are no other ITCAM products configured in the same WebSphere Profile

If you are configuring the ITCAM for WebSphere Application in an environment where there are no other ITCAM products configured for application servers within the same profile, you can integrate the data collector with the Tivoli Performance Viewer and accept the default values.

Configuring the ITCAM Data Collector for WebSphere

You must configure the data collector for each application server instance that you want to monitor.

The ITCAM Data Collector for WebSphere Configuration Utility is a menu driven command-line utility for configuring the ITCAM Data Collector for WebSphere.

Important: In an ITCAM for Application Diagnostics deployment, do not configure the data collector to monitor an instance of WebSphere Application Server that hosts the Managing Server Virtualization Engine (MSVE). However, you can use the data collector to monitor any other WebSphere Application Server instances that are on the same node.

To configure the data collector to monitor one or more server instances, complete the following procedure:

1. Navigate to the *DC_home*/bin directory.
2. Set the location of the Java home directory before you run the utility:
   ```
   export JAVA_HOME=/opt/IBM/AppServer80/java
   ```
3. Run the following command to start the ITCAM Data Collector for WebSphere Configuration Utility.
   ```
   DC_home/bin/config.sh
   ```
4. The utility starts and displays the IP addresses of all network cards that are found on the local computer system and prompts you to specify the interface to use for the data collector:
   ```
   List of TCP/IP interfaces discovered:
     1. 9.111.98.108
   Enter a number [default is: 1]:
   ```
5. Enter the number that corresponds to the IP address to use.

   The utility searches for WebSphere Application Server home directories on the computer system and prompts you to select a home directory:

```
List of WebSphere Application Server home directories discovered:
  1. /opt/IBM/WebSphere/AppServer
Enter a number or enter the full path to a home directory
[default is: 1]:
```

6. Enter the number that corresponds to a WebSphere Application Server home directory.

   The utility searches for all profiles under the specified home directory and prompts you to select a profile:

   ```
   List of WebSphere profiles discovered:
     1. AppSrv01
   Enter a number [default is: 1]:
   ```

7. Enter the number that corresponds to the WebSphere Application Server profile that you want to configure.

   The utility indicates whether WebSphere Global Security is enabled for the WebSphere Application profile that you specified:

   ```
   WebSphere Global Security is enabled.
   ```

   If global security is not enabled, skip to step 9.

8. The utility prompts you to specify whether to retrieve security settings from a client properties file:

   ```
   Do you want to retrieve security settings from a client properties file
   (soap.client.props or sas.client.props)?
   [1 - YES, 2 - NO] [default is: 2]:
   ```

   The data collector communicates with the WebSphere Administrative Services using the Remote Method Invocation (RMI) or the SOAP protocol. If global security is enabled for a profile, you must specify the user ID and password of a user who is authorized to log in to the IBM WebSphere Application Server administrative console for the profile. Alternatively, you can encrypt the user name and password and store them in client properties files before configuring the data collector. You must use the `sas.client.props` file for an RMI connection, or the `soap.client.props` file for an SOAP connection.

   Enter 1 to allow the utility to retrieve the user name and password from the appropriate client properties file and skip to step 9. Otherwise, enter 2 to enter the user name and password.

   ```
   CFG1018I Enter WebSphere admin user name:
   CFG1019I Enter WebSphere admin password:
   ```

9. The utility searches for all application server instances under the specified profile. The utility displays all servers that are not configured yet for data collection and all servers that are configured to use the current version of the ITCAM Data Collector for WebSphere.

   The utility prompts you to select one or more application server instances from the list:

   ```
   Choose one or more servers to configure for data collection:
   Application servers not yet configured:
    1. co098170Node01Cell.co098170Node01.server1(AppSrv01)
   Enter a number or numbers separated by commas, or enter * to select all:
   ```

   Remember:

   - For a Network Deployment or Extended Deployment environment, the Node Agent and Deployment Manager must be running. For a stand-alone environment, application server instances must be running during the configuration of the data collector.
   - Ensure that the application server instances that you select are the actual nodes that host the applications or services that you want to monitor.

10. Enter the number that corresponds to the application server instance to configure for data collection or enter an asterisk * to configure all application server instances for data collection. To specify a subset of servers, enter the numbers, separated by commas, that represent the servers. For example: 1,2,3.
11. In the **Integration with ITCAM for SOA Agent** section, the utility provides an option for integrating the data collector with the ITCAM for SOA agent.

    ```
    Do you want to integrate with an ITCAM for SOA Agent? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

    You must install and configure the ITCAM for SOA Agent and its application support files, and optionally configure topology support to complete the installation and configuration of the ITCAM for SOA Agent. For more information about installing and configuring the ITCAM for SOA Agent, see *IBM Tivoli Composite Application Manager for SOA Installation Guide*.

    Enter 1 to integrate the data collector with the ITCAM for SOA Agent. Otherwise, enter 2.
12. In the **Integration with ITCAM Agent for WebSphere Applications** section, the utility provides an option for integrating the data collector with the ITCAM Agent for WebSphere Applications.

    You can integrate the data collector with ITCAM Agent for WebSphere Applications, or with the ITCAM for Application Diagnostics Managing Server, or with both.

    ```
    Do you want to integrate with an ITCAM Agent for WebSphere Applications?
     [1 - YES, 2 - NO]
    [default is: 2]:
    ```

    You must install and configure the ITCAM Agent for WebSphere Applications and its application support files to complete the installation and configuration of the ITCAM Agent for WebSphere Applications. For more information about installing and configuring the ITCAM Agent for WebSphere Applications, see *IBM Tivoli Composite Application Manager Agent for WebSphere Applications Installation and Configuration Guide*.
13. Enter 1 to integrate the data collector with the ITCAM Agent for WebSphere Applications. Otherwise, enter 2 and skip to step 16.

    You are prompted to enter the host name of the ITCAM Agent for WebSphere Applications.

    ```
    Enter the host name or IP address of the ITCAM Agent for WebSphere Applications TEMA:
    [default is: 127.0.0.1]:
    ```
14. Enter the fully qualified host name or IP address of the ITCAM Agent for WebSphere Applications monitoring agent. The monitoring agent is located on the local host, so you do not have to change the default.

    You are prompted for the port number of the ITCAM Agent for WebSphere Applications monitoring agent.

    ```
    Enter the port number of the ITCAM Agent for WebSphere Application TEMA:
    [default is: 63335]:
    ```

    You can change the port that is used for communication between the data collector and the ITCAM Agent for WebSphere Applications monitoring agent. This communication is on the local host; the default port is 63335. You can change the port at a later time, but it is most convenient to set it when initially configuring the data collector.
15. Enter the port number of the monitoring agent.
16. In the **Integration with ITCAM for Application Diagnostics Managing Server** section, the utility provides an option for integrating the data collector with the ITCAM for Application Diagnostics Managing Server, installed on a

separate Windows, Linux, or UNIX server, for deep-dive diagnostics. For information about installing the Managing Server, see *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

You are prompted to specify whether you want to integrate the data collector with a Managing Server.

```
Do you want to integrate with an MS? [1 - YES, 2 - NO]
[default is: 2]:
```

Remember:

- To integrate with ITCAM for Application Diagnostics Managing Server for deep-dive analysis, you must have ITCAM for Application Diagnostics version 7.1 installed.
- If you decide not to configure the Managing Server at this time, you can still configure the data collector to communicate with the Managing Server later.

17. Enter 1 to integrate with the Managing Server. Otherwise, enter 2 and skip to step 20.

    You are prompted to specify the host name of the Managing Server:

    ```
    Enter the host name  or IP address of the  MS
    [default is: 127.0.0.1]:
    ```

18. Enter the fully qualified host name of the Managing Server.

    You are prompted to specify the port number of the Managing Server:

    ```
    Enter the code base port number of the MS
    [default is: 9122]:
    ```

    The port number is codebase port on which the Managing Server is listening.

    Tip: The port number is defined as the value of the key "PORT_KERNEL_CODEBASE01" in the .ITCAM61_MS_CONTEXT.properties file located under the Managing Server Home directory. See *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

    The configuration tool attempts to connect to the Managing Server and retrieve the value for the *MS_home* directory. If successful, the tool displays a message similar to the following message:

    ```
    MS home directory is: /opt/IBM/itcam/WebSphere/MS
    ```

19. If the connection to the Managing Server is *not* successful, you are prompted to enter the value for the *MS_home* directory:

    ```
    Enter ITCAM Managing Server install directory [default is /opt/IBM/itcam/WebSphere/MS:
    ```

    If prompted, enter the value of the *MS_home* directory.

20. The utility prompts you to specify whether you want to configure advanced settings for the Managing Server.

    ```
    Do you want to configure advanced settings for the MS? [1 - Yes, 2 - No]
    [default is: 2]:
    ```

    Enter 1 to configure advanced settings. Otherwise, enter 2 and skip to step 24 on page 53.

21. You are prompted to enter the range of RMI port numbers that the data collector uses to accept incoming connections from the Managing Server:

    ```
    Enter the RMI port numbers [default is: 8200-8299]:
    ```

Tip: Make sure that the ports are not being blocked by the firewall or other applications.

Enter the RMI port numbers.

22. You are prompted to enter the range of Controller RMI port numbers:

    ```
    Enter the range of Controller RMI port numbers
    [default is: 8300-8399]:
    ```

    Enter the RMI Controller port numbers.

23. You are prompted to enter the RFS port number of the Managing Server:

    ```
    Enter the RFS port number of the MS:  [default is: 9120]:
    ```

    Enter the RFS port number.

24. In the **Integration with ITCAM for Transactions** section, the utility provides an option for integrating the data collector with ITCAM for Transactions.

    Note: To integrate the data collector with ITCAM for Transactions, you must install ITCAM for Transactions within an IBM Tivoli Monitoring environment. You are prompted to specify whether you want to integrate with ITCAM for Transactions:

    ```
    Do you want to integrate with ITCAM for TT? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

    After you have configured the data collector to support ITCAM for Transactions, you then must perform some additional configuration. For details of further configuration options and how to view the aggregated transaction information, see *IBM Tivoli Composite Application Agent for WebSphere Applications Configuring and Using TTAPI*.

25. Enter 1 to integrate the data collector with ITCAM for Transactions. Otherwise, enter 2 and skip to step 30.

26. You are prompted to specify the host name or IP address of the Transaction Collector, which is the component of ITCAM from Transactions that gathers metrics from multiple agents:

    ```
    Enter the host name or IP address for the Transaction Collector:
    [default is: 127.0.0.1]:
    ```

27. Enter the fully qualified host name or IP address of the Transaction Collector.

28. You are prompted to specify the port number that the data collector uses to connect to the Transaction Collector:

    ```
    Enter the port number for the Transaction Collector:
    [default is: 5455]:
    ```

29. Enter the port number for the interface to the Transaction Collector.

30. In the **Integration with Tivoli Performance Viewer** section, the utility provides an option for integrating the data collector with Tivoli Performance Viewer (TPV).

    ```
    Do you want to integrate with Tivoli Performance Viewer? [1 - YES, 2 - NO]
    [default is: 2]
    ```

    ITCAM for WebSphere Application Server version 7.2 can be used to monitor the performance of the WebSphere Application Server. Performance monitoring infrastructure (PMI) metrics are gathered using the ITCAM Data Collector for WebSphere and are displayed in the Tivoli Performance Viewer (TPV). The TPV is accessible from the WebSphere Application Server administrative console. ITCAM for WebSphere Application Server is installed separately from the WebSphere Application Server. For more information about installing ITCAM for WebSphere Application Server, see *IBM Tivoli Composite Application Manager for WebSphere Application Server version 7.2 Support for WebSphere Application Server version 8.5 Installation and User Guide*.

ITCAM for WebSphere Application Server 7.2 support for WebSphere Application Server 8.5 includes the ITCAM Data Collector for WebSphere. Enter 1 to integrate the ITCAM Data Collector for WebSphere with the Tivoli Performance Viewer. Otherwise, enter 2.

31. In the **Integration with ITCAM diagnostics tool** section, the utility provides an option for integrating the data collector with the ITCAM Diagnostics Tool.

    ```
    Do you want to integrate with ITCAM diagnostics tool? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

    ITCAM Diagnostics Tool is built on Eclipse. The tool is used for diagnostic investigation of applications that are running on the WebSphere Application Server. Using this tool, you can analyze data in real time or you can save diagnostic information to a file for later analysis. Fore more information about installing the ITCAM Diagnostics Tool, see *ITCAM Diagnostic Tool Installation Guide*.

    Enter 1 to integrate the ITCAM Data Collector for WebSphere with the ITCAM Diagnostics Tool. Otherwise, enter 2.

32. In the **Advanced Settings** section, the utility provides options for performing advanced configuration of the data collector. The utility prompts you to specify whether to change the garbage collection log path:

    ```
    Do you want to specify a Garbage Collection log path? [1 - YES, 2 - NO] [default is: 2]:
    ```

    Enter 1 to select a garbage collection log path. Otherwise, enter 2 and skip to step summary.

33. You are prompted to specify the garbage collection log path:

    ```
    Enter the GC log path:
    ```

    Enter a file name with its full path. The data collector automatically modifies the log file name, adding the server instance information to it. For example, if you specify `gc.log` as the file name, the actual name is set to *`profile_name`*`.`*`cell_name`*`.`*`node_name`*`.`*`server_name`*`.gc.log` for every configured application server instance.

    Important: In the garbage collection log path, you can use WebSphere variables such as`${SERVER_LOG_ROOT}`. However, do not use templates, such as `%pid`.

34. You are prompted to specify whether you want to increase the heap size:

    ```
    Do you want to add 128M to the heap size? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

    Enter 2 to retain the existing heap size. Otherwise, enter 1.

35. In the **Data collector configuration summary** section, the utility provides a summary of the data collector configuration that will be applied to the specified application server instances:

    ```
     1) List of servers selected

       - WAS server: co098170Node01Cell.co098170Node01.server1(AppSrv01)
           WAS cell: co098170Node01Cell
            WAS node: co098170Node01

           WebSphere Profile home    :
              /opt/IBM/WebSphere/AppServer/profiles/AppSrv01


           wsadmin location          :
            /opt/IBM/WebSphere/AppServer/bin/wsadmin.bat
    ```

```
                        WAS version : 8.0.0.0
                         Deployment : Standalone
                           JVM mode : 32
                  Configuration home : /opt/IBM/ITM/dchome

 2) Integrate with ITCAM for SOA Agent : Yes

 3) Integrate with ITCAM Agent for WebSphere Applications : Yes

       TEMA hostname or IP address : 127.0.0.1
                TEMA port number : 63335
                      Monitor GC : No

 4) Integrate with ITCAM for AD Managing Server : No

       MS hostname or IP address : 127.0.0.1
         MS codebase port number : 9122
               MS home directory : /opt/IBM/itcam/WebSphere/MS

 5) Integrate with ITCAM for Transactions : Yes

       Transaction Collector hostname : 127.0.0.1
       Transaction Collector port number : 5455

 6) Integrate with Tivoli Performance Viewer : No

 7) Integrate with ITCAM diagnostics tool : No

 8) Advanced settings :

       Set Garbage Collection log path : No
       Added 128M to the heap size : No

You may accept or update your configuration choices for the following actions:
 1) List of servers selected
 2) Integrate with ITCAM for SOA Agent
 3) Integrate with ITCAM Agent for WebSphere Applications
 4) Integrate with ITCAM for AD Managing Server
 5) Integrate with ITCAM for Transactions
 6) Integrate with Tivoli Performance Viewer
 7) Integrate with ITCAM diagnostics tool
 8) Advanced settings

To modify a section, enter the number. To modify all sections, enter '*'. To accept you
configuration without modifying, enter 'a'.
To quit the selection, enter 'q':
```

The summary section provides options to reconfigure parts of the data collector configuration before applying the changes and an option to exit the configuration tool without applying your changes. Enter the number that represents the section you want to edit. Enter an asterisk (*) to reconfigure all sections. Enter `a` to accept your changes. Enter `q` to exit the ITCAM Data Collector for WebSphere Configuration Utility without configuring the data collector.

36. When you enter `a` to accept your changes, you are prompted to specify whether you want to create a backup of your current WebSphere Application Server configuration:

    ```
    Do you want to backup current WebSphere configuration? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

37. Enter 1 to create a backup of the current configuration. Otherwise, enter 2.

The changes are applied and a status message is presented to indicate that the configuration of the data collector for the profile is complete:

```
Successfully executed config for Cell: co098170Node01Cell
Node: co098170Node01 Profile: AppSrv01.
```

Important: After configuring the data collector to monitor application server instances, you must restart the instances. The data collector configuration takes effect when the application server instances are restarted.

Configuring the ITCAM Data Collector for WebSphere in silent mode

The common ITCAM Data Collector for WebSphere can be configured interactively with the ITCAM Data Collector for WebSphere Configuration Utility. Alternatively, to configure many application server instances, the ITCAM for WebSphere Applications Data Collector can be configured in silent mode.

Important: In an ITCAM for Application Diagnostics deployment, do not configure the data collector to monitor an instance of WebSphere Application Server that hosts the Managing Server Virtualization Engine (MSVE). However, you can use the data collector to monitor any other WebSphere Application Server instances that are on the same node.

When you configure the data collector in silent mode, you first specify configuration options in a properties file. A sample properties file, `sample_silent_config.txt`, is packaged with the ITCAM Data Collector for WebSphere Configuration Utility. The file is available in the following locations:

DC_home`/bin`

The variable *DC_home* is the location where the data collector is installed. A sample of a properties file is available in "Sample properties file" on page 59

Complete the following steps to perform a silent configuration:

1. Specify configuration options in the properties file.
2. Go to the *DC_home*`/bin` directory.
3. Run the following command:

   ```
   config.sh -silent [dir_path]/silent file
   ```

4. After configuring the data collector to monitor application server instances, you must restart the instances. The data collector configuration takes effect when the application server instances are restarted.

Properties file

When you create your properties file, keep in mind the following considerations:

- A line in the file that starts with a number sign (#) is treated as a comment, and is not processed. If the number sign is used elsewhere in the line, it is not considered to be the start of a comment.
- Each property is described on a separate line, in the following format: <*property*> = <*value*>.

  property
  : Name of property. The list of valid properties that you can configure is shown in Table 10 on page 57.

  value
  : Value of the property. Default values for some properties are already provided. You can delete default values to leave property values blank, or empty. An empty value is treated as if the property is not specified, as

opposed to using the default value. If you want to use default values, you can comment out the property in the file.

- Passwords are in plain text.
- Properties and their values are case-sensitive.
- The following table describes the properties that are available when configuring the data collector in silent mode:Table 10 describes the properties that are available when configuring the data collector in silent mode:

Table 10. Available properties for running the ITCAM Data Collector for WebSphere Configuration Utility in silent mode

Property	Comment
default.hostip	If the computer system uses multiple IP addresses, specify the IP address for the data collector to use.
Integration of the data collector with the ITCAM for Application Diagnostics Managing Server	
ms.connect	Specifies whether the data collector is configured to connect to the Managing Server in an ITCAM for Application Diagnostics environment. Valid values are *True* and *False*.
ms.kernel.host	Specifies the fully qualified host name of the Managing Server.
ms.kernel.codebase.port	Specifies the codebase port on which the Managing Server is listening.
ms.am.home	Specifies the *MS_home* directory on the Managing Server.
ms.am.socket.bindip	Specifies the IP address or host name to be used by the data collector to communicate with the Managing Server. If more than one network interface or IP address is configured on data collector computer system, choose one of them.
ms.firewall.enabled	Specifies whether a firewall is enabled on the data collector host or you have special requirements to change the RMI ports for the data collector. Valid values are *True* and *False*.
ms.probe.controller.rmi.port	If the data collector is behind a firewall or you have special requirements to change the RMI port of data collector, set this port number range. Configure this port number as permitted by the firewall for the data collector host. For example: ms.probe.controller.rmi.port=8300-8399 or ms.probe.controller.rmi.port=8300.
ms.probe.rmi.port	If the data collector is behind a firewall, or you have special requirements to change the RMI Port of data collector, set this port number range. Configure this port number as permitted by the firewall for the data collector host. For example: ms.probe.rmi.port=8200-8299 or ms.probe.rmi.port=8200.
Integration of the data collector with the ITCAM for Transactions	
ttapi.enable	Specifies whether the data collector communicates with ITCAM for Transactions using the Transaction Tracking API (TTAPI). Valid values are *True* and *False*.
ttapi.host	Specifies the host name of the ITCAM for Transactions Transaction Collector to connect to.
ttapi.port	Specifies the port of the Transaction Collector to connect to.
Integration of the data collector with the ITCAM for SOA	
soa.enable	Specifies whether to integrate the data collector with ITCAM for SOA. The ITCAM for SOA agent must be installed to complete the configuration. **Important:** The data collector always connects with the ITCAM for SOA monitoring agent when enabled. No additional configuration of the ITCAM for SOA monitoring agent is required.
Integration of the data collector with the Tivoli Performance Monitoring	

Table 10. Available properties for running the ITCAM Data Collector for WebSphere Configuration Utility in silent mode (continued)

Property	Comment
tpv.enable	Specifies whether to integrate the data collector with the Tivoli Performance Monitoring when the data collector is included as part of ITCAM for WebSphere Application Server version 8.5. Tivoli Performance Monitoring is accessed with the WebSphere Application Server administrative console. Valid values are *True* and *False*.
Integration of the data collector with the ITCAM Diagnostics Tool	
de.enable	Specifies whether to integrate the data collector with the ITCAM Diagnostics Tool. The ITCAM Diagnostics Tool is a tool for diagnostic investigation of applications that are running on WebSphere Application Server. Valid values are *True* and *False*.
Integration of the data collector with the ITCAM Agent for WebSphere Applications monitoring agent	
temaconnect	Specifies whether the data collector connects to the ITCAM Agent for WebSphere Applications monitoring agent (TEMA). Valid values are *True* and *False*. Set this property to *False* if you plan to connect the ITCAM Agent for WebSphere Applications with the Managing Server only or you do not have the ITCAM Agent for WebSphere Applications installed and do not plan to install it.
tema.host	Specifies the fully qualified host name or IP address of the ITCAM Agent for WebSphere Applications monitoring agent.
tema.port	Specifies the port number of the ITCAM Agent for WebSphere Applications monitoring agent.
WebSphere Application Server backup	
was.backup.configuration	Specifies whether to back up the current configuration of the WebSphere Application Server configuration before applying the new configuration. Valid values are *True* and *False*.
was.backup.configuration.dir	Specifies the location of the backup directory.
Advanced configuration settings	
was.gc.custom.path	Specifies whether to set a custom path for the Garbage Collection log.
was.gc.file	Specifies the path to the custom Garbage Collection log. Set this value to a file name with its full path. The data collector automatically modifies the log file name, adding the server instance information to it. For example, if you specify `gc.log` as the file name, the actual name is set to *`profile_name`*`.`*`cell_name`*`.`*`node_name`*`.`*`server_name`*`.gc.log` for every configured application server instance. **Important:** In the Garbage Collection log path, you can use WebSphere variables, such as ${SERVER_LOG_ROOT}. However, do not use templates, such as %pid.
was.configure.heap	Specifies whether to add 128 MB to the heap size. Each time you run the silent configuration, 128 MB is added to the heap size if this property is set to *True*. Possible values are *True* and *False*.
WebSphere Application Server connection settings	
was.wsadmin.connection.host	Specifies the name of the host to which the wsadmin tool is connecting.
was.wsadmin.connection.type	Specifies the connection protocol for the wsadmin tool to use.
was.wsadmin.connection.port	Specifies the port that the wsadmin tool must use to connect to the WebSphere Application Server.
WebSphere Application Server global security settings	

Table 10. Available properties for running the ITCAM Data Collector for WebSphere Configuration Utility in silent mode (continued)

Property	Comment
was.wsadmin.username	Specifies the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server.
was.wsadmin.password	Specifies the password that corresponds to the user specified in the `was.wsadmin.username` property.
was.client.props	Specifies whether to retrieve security settings from a client properties file. Possible values are *True* and *False*.
WebSphere Application Server settings	
was.appserver.profile.name	Specifies the name of the application server profile that you want to configure.
was.appserver.home	Specifies the WebSphere Application Server home directory.
was.appserver.cell.name	Specifies the WebSphere Application Server cell name.
was.appserver.node.name	Specifies the WebSphere Application Server node name.
WebSphere Application Server runtime instance settings	
was.appserver.server.name	Specifies the application server instance within the application server profile to configure. **Tip:** The silent response file can have multiple instances of this property.

Sample properties file

```
################################################################################################
#
#Comments:
#Locate the ITCAM Data Collector for WebSphere Configuration Utility (config.sh|bat) in <dc_home>/bin.
#Run config.sh|bat -silent [dir_path]/<properties_file> to configure the data collector silently.
#This file is a sample properties file.
#
#This file has 2 sections; [DEFAULT SECTION] and [SERVER].
#You can have one instance of [DEFAULT].
#You can have multiple instances of [SERVER].
#
#You can integrate the data collector with the following components:
#  ITCAM for Application Diagnostics Managing Server
#  ITCAM for Transactions
#  ITCAM for SOA agent
#  Tivoli Performance Viewer (for ITCAM for WebSphere Application Server)
#  ITCAM Diagnostics Tool
#  ITCAM Agent for WebSphere Applications monitoring agent
#
#Considerations:
#
#IP address to use:
#Uncomment and specify an IP address to use, if the system has multiple IP addresses.

#Modify Garbage Collection log path:
#The full path to the GC log file must exist.
#The server name, cell name, and node name are appended to the GC log file name.
#
#Increase the JVM heap size by 128MB:
#If set to true, each time the script is run, 128MB is added to the JVM heap size.
#
#Connect to WebSphere Administrative Services:
#The utility determines the connection type and port automatically.
#If the utility cannot determine the values, uncomment, and override the default values.
#
#Servers:
#You can configure multiple servers in the same profile.
#Uncomment the second [SERVER] and add the server name.
```

```
#Repeat for each additional server.
#
################################################################################################

[DEFAULT SECTION]

#  IP addresses to use:
#default.hostip=9.9.9.9

#  ITCAM for Application Diagnostics Managing Server:
ms.connect=False
ms.kernel.host=msservername.yourcompany.com
ms.kernel.codebase.port=9122
ms.am.home=/opt/IBM/itcam/WebSphere/MS
ms.am.socket.bindip=servername.yourcompany.com
#ms.firewall.enabled=
ms.probe.controller.rmi.port=8300-8399
ms.probe.rmi.port=8200-8299

#  ITCAM for Transactions:
ttapi.enable=False
ttapi.host=ttservername.yourcompany.com
ttapi.port=5455

#  ITCAM for SOA agent:
soa.enable=False

#  Tivoli Performance Viewer:
tpv.enable=True

#  ITCAM Diagnostics Tool:
de.enable=False

#  ITCAM Agent for WebSphere Applications monitoring agent:
temaconnect=True
tema.host=127.0.0.1
tema.port=63335

#  Create a backup of WebSphere Application Server:
was.backup.configuration=False
was.backup.configuration.dir=/opt/IBM/ITM/dchome

#  Modify Garbage Collection log path:
#was.gc.custom.path=False
#was.gc.file=/opt/test.log

#  Increase the JVM heap size by 128MB:
was.configure.heap=False

#Connect to WebSphere Administrative Services:
was.wsadmin.connection.host=servername.yourcompany.com
#was.wsadmin.connection.type=SOAP
#was.wsadmin.connection.port=8881

#  WebSphere Global Security:
was.wsadmin.username=
was.wsadmin.password=
was.client.props=False

#  WebSphere Application Server details:
was.appserver.profile.name=AppSrv02
was.appserver.home=C:\Program Files\IBM\WebSphere\AppServer
was.appserver.cell.name=yourITCAMCell
was.appserver.node.name=yourITCAMNode

[SERVER]
was.appserver.server.name=server1

#[SERVER]
#was.appserver.server.name=server2
```

Reconfiguring the ITCAM Data Collector for WebSphere

If you configured the data collector to monitor one or more application server instances, you can reconfigure the data collector using the ITCAM Data Collector for WebSphere Reconfiguration Utility.

You can change the data collector connection to the following products or components:

- ITCAM Agent for WebSphere monitoring agent
- ITCAM for Application Diagnostics Managing Server
- ITCAM for SOA monitoring agent
- ITCAM for Transactions
- Tivoli Performance Viewer
- ITCAM Diagnostic Tool

You can also reconfigure garbage collection settings and add to the heap size.

To reconfigure data collection for one or more monitored application server instances, complete the following procedure:

1. From the command-line, navigate to *DC_home*/bin directory.
2. Set the location of the Java home directory before you run the utility:

   ```
   export JAVA_HOME=/opt/IBM/AppServer80/java
   ```
3. Run the following command to start the ITCAM Data Collector for WebSphere Reconfiguration Utility:

   ```
   DC_home/bin/reconfig.sh
   ```

   Tip: Running this utility has the same effect as running the `config.sh` script with the `-reconfig` argument.
4. The utility starts and displays the IP addresses of all network cards found on the local computer system and prompts you to specify the interface to use for the data collector:

   ```
   List of TCP/IP interfaces discovered:
     1. 9.111.98.108
   Enter a number [default is: 1]:
   ```
5. Enter the number that corresponds to the IP address to use.

   The utility searches for all application server instances for which the data collector is configured on this host, and prompts you to select one or more application server instances from the list:

   ```
   Choose one or more servers to configure for data collection:
   Application servers not yet configured:
    1. co098170Node01Cell.co098170Node01.server1(AppSrv01)
   Enter a number or numbers separated by commas, or enter * to select all:  1
   ```

   Tip: For a Network Deployment or Extended Deployment environment, the Node Agent and Deployment Manager must be running. For a stand-alone environment, application server instances must be running during the configuration of the data collector.
6. Enter the number that corresponds to the application server instance to configure for data collection or enter an asterisk `*` to configure all application server instances for data collection. To specify a subset of servers, enter the numbers, separated by commas, that represent the servers. For example: `1,2,3`.
7. In the **Integration with ITCAM for SOA Agent** section, the utility provides an option for integrating the data collector with the ITCAM for SOA agent.

```
Do you want to integrate with an ITCAM for SOA Agent? [1 - YES, 2 - NO]
[default is: 2]: 1
```

You must install and configure the ITCAM for SOA Agent and its application support files, and optionally configure topology support to complete the installation and configuration of the ITCAM for SOA Agent. For more information about installing and configuring the ITCAM for SOA Agent, see *IBM Tivoli Composite Application Manager for SOA Installation Guide*.

Enter 1 to integrate the data collector with the ITCAM for SOA Agent. Otherwise, enter 2.

8. In the **Integration with ITCAM Agent for WebSphere Applications** section, the utility provides an option for integrating the data collector with the ITCAM Agent for WebSphere Applications.

   You can integrate the data collector with ITCAM Agent for WebSphere Applications, or with the ITCAM for Application Diagnostics Managing Server, or with both.

   ```
   Do you want to integrate with an ITCAM Agent for WebSphere Applications?
    [1 - YES, 2 - NO]
   [default is: 2]: 1
   ```

   You must install and configure the ITCAM Agent for WebSphere Applications and its application support files to complete the installation and configuration of the ITCAM Agent for WebSphere Applications. For more information about installing and configuring the ITCAM Agent for WebSphere Applications, see *IBM Tivoli Composite Application Manager Agent for WebSphere Applications Installation and Configuration Guide*.

9. Enter 1 to integrate the data collector with the ITCAM Agent for WebSphere Applications. Otherwise, enter 2 and skip to step 12.

   You are prompted to enter the host name of the ITCAM Agent for WebSphere Applications.

   ```
   Enter the host name or IP address of the ITCAM Agent for WebSphere Applications TEMA:
   [default is: 127.0.0.1]: 127.0.0.1
   ```

10. Enter the fully qualified host name or IP address of the ITCAM Agent for WebSphere Applications monitoring agent. The monitoring agent is on the local host, so the default is correct.

    You are prompted for the port number of the ITCAM Agent for WebSphere Applications monitoring agent.

    ```
    Enter the port number of the ITCAM Agent for WebSphere Application TEMA:
    [default is: 63335]: 63335
    ```

    You can change the port that is used for communication between the data collector and the ITCAM Agent for WebSphere Applications monitoring agent. This communication is on the local host; the default port is 63335.

11. Enter the port number of the monitoring agent.

12. In the **Integration with ITCAM for Application Diagnostics Managing Server** section, the utility provides an option for integrating the data collector with the ITCAM Application Diagnostics Managing Server, installed on a separate UNIX or Windows server, for deep-dive diagnostics. For information about installing the Managing Server, see *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

    You are prompted to specify whether you want to integrate the data collector with a Managing Server.

    ```
    Do you want to integrate with an MS? [1 - YES, 2 - NO]
    [default is: 2]: 1
    ```

Note: To integrate with ITCAM for Application Diagnostics Managing Server for deep-dive analysis, you must have ITCAM for Application Diagnostics 7.1 installed.

Note: If you decide not to configure the Managing Server at this time, you can still configure the data collector to communicate with the Managing Server later.

13. Enter 1 to integrate with the Managing Server. Otherwise, enter 2 and skip to step 16.

    You are prompted to specify the host name of the Managing Server:

    ```
    Enter the host name  or IP address of the  MS
    [default is: 127.0.0.1]: 127.0.0.1
    ```

14. Enter the fully qualified host name of the Managing Server.

    You are prompted to specify the port number of the Managing Server:

    ```
    Enter the code base port number of the MS
    [default is: 9122]: 9122
    ```

    The port number is codebase port on which the Managing Server is listening.

    Tip: The port number is defined as the value of the key "PORT_KERNEL_CODEBASE01" in the .ITCAM61_MS_CONTEXT.properties file located under the Managing Server Home directory. See *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

    The configuration tool attempts to connect to the Managing Server and retrieve the value for the *MS_home* directory. If successful, the tools displays a message similar to the following message:

    ```
    MS home directory is: /opt/IBM/itcam/WebSphere/MS
    ```

15. If the connection to the Managing Server is *not* successful, you are prompted to enter the value for the *MS_home* directory:

    ```
    Enter ITCAM Managing Server Install Directory [default is C:\IBM\itcam\WebSphere\MS]:
    ```

    If prompted, enter the value of the *MS_home* directory.

16. The utility prompts you to specify whether you want to configure advanced settings for the Managing Server.

    ```
    Do you want to configure advanced settings for the MS? [1 - Yes, 2 - No]
    [default is: 2]: 1
    ```

    Enter 1 to configure advanced settings. Otherwise, enter 2 and skip to step 20 on page 64.

17. You are prompted to enter the range of RMI port numbers that the data collector uses to accept incoming connections from the Managing Server:

    ```
    Enter the RMI port numbers
    [default is: 8200-8299] 8200-8299
    ```

    Note: Make sure that the ports are not being blocked by the firewall or other applications.

    Enter the RMI port numbers.

18. You are prompted to enter the RFS port number of the Managing Server:

    ```
    Enter the RFS port number of the MS:  [default is: 9120]:
    ```

    Enter the RFS port number.

19. You are prompted to enter the range of Controller RMI port numbers:

```
Enter the range of Controller RMI port numbers
[default is: 8300-8399]: 8300-8399
```

Enter the RMI Controller port numbers.

20. In the **Integration with ITCAM for Transactions** section, the utility provides an option for integrating the data collector with ITCAM for Transactions.

    Note: To integrate the data collector with ITCAM for Transactions, you must install ITCAM for Transactions within an IBM Tivoli Monitoring environment. You are prompted to specify whether you want to integrate with ITCAM for Transactions:

    ```
    Do you want to integrate with ITCAM for TT? [1 - YES, 2 - NO]
    [default is: 2]: 1
    ```

21. After you have configured the data collector to support ITCAM for Transactions, you then must perform some additional configuration. For details of further configuration options and how to view the aggregated transaction information, see *IBM Tivoli Composite Application Agent for WebSphere Applications Configuring and Using TTAPI*.
22. Enter 1 to integrate the data collector with ITCAM for Transactions. Otherwise, enter 2 and skip to step 27.
23. You are prompted to specify the host name or IP address of the Transaction Collector, which is the component of ITCAM from Transactions that gathers metrics from multiple agents:

    ```
    Enter the host name or IP address for the Transaction Collector:
    [default is: 127.0.0.1]: 127.0.0.1
    ```

24. Enter the fully qualified host name or IP address of the Transaction Collector.
25. You are prompted to specify the port number of the interface to the Transaction Collector:

    ```
    Enter the port number for the Transaction Collector:
    [default is: 5455]: 5455
    ```

26. Enter the port number for the interface to the Transaction Collector.
27. In the **Integration with Tivoli Performance Viewer** section, the utility provides an option for integrating the data collector with Tivoli Performance Viewer (TPV).

    ```
    Do you want to integrate with Tivoli Performance Viewer? [1 - YES, 2 - NO]
    [default is: 2]
    ```

    ITCAM for WebSphere Application Server version 7.2 can be used to monitor the performance of the WebSphere Application Server. Performance monitoring infrastructure (PMI) metrics are gathered using the ITCAM Data Collector for WebSphere and are displayed in the Tivoli Performance Viewer (TPV). The TPV is accessible from the WebSphere Application Server administrative console. ITCAM for WebSphere Application Server is installed separately from the WebSphere Application Server. For more information about installing ITCAM for WebSphere Application Server, see *IBM Tivoli Composite Application Manager for WebSphere Application Server version 7.2 Support for WebSphere Application Server version 8.5 Installation and User Guide*.

    ITCAM for WebSphere Application Server 7.2 support for WebSphere Application Server 8.5 includes the ITCAM Data Collector for WebSphere. Enter 1 to integrate the ITCAM Data Collector for WebSphere with the Tivoli Performance Viewer. Otherwise, enter 2 and skip to step 28.
28. In the **Integration with ITCAM diagnostics tool** section, the utility provides an option for integrating the data collector with the ITCAM diagnostics tool.

    ```
    Do you want to integrate with ITCAM diagnostics tool? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

ITCAM Diagnostics Tool is a tool that is built on Eclipse. The tool is used for diagnostic investigation of applications that are running on WebSphere Application Server. Using this tool, you can analyze data in real time or you can save diagnostic information to a file for later analysis. For more information about installing the ITCAM Diagnostics Tool, see *ITCAM Diagnostic Tool Installation Guide*.

Enter 1 to integrate the ITCAM Data Collector for WebSphere with the ITCAM diagnostics tool. Otherwise, enter 2 and skip to step 29.

29. In the **Advanced Settings** section, the utility provides options for performing advanced configuration of the data collector. The utility prompts you to specify whether to change the garbage collection log path:

    ```
    Do you want to specify a Garbage Collection log path? [1 - YES, 2 - NO]
    [default is: 2]: 2
    ```

    Enter 1 to select a garbage collection log path. Otherwise, enter 2 and skip to step 65.

30. You are prompted to specify the garbage collection log path:

    ```
    Enter the GC log path:
    ```

    Enter a file name with its full path. The data collector automatically modifies the log file name, adding the server instance information to it. For example, if you specify `gc.log` as the file name, the actual name is set to *`profile_name.cell_name.node_name.server_name`*`.gc.log` for every configured application server instance.

    Important: In the garbage collection log path, you can use WebSphere variables such as`${SERVER_LOG_ROOT}`. However, do not use templates, such as `%pid`.

31. You are prompted to specify whether you want to increase the heap size:

    ```
    Do you want to add 128M to the heap size? [1 - YES, 2 - NO]
    [default is: 2]: 2
    ```

    Enter 2 to retain the existing heap size. Otherwise, enter 1.

32. In the **Data collector configuration summary** section, the utility provides a summary of the data collector configuration that will be applied to the specified application server instances:

    ```
     1) List of servers selected

       - WAS server: co098170Node01Cell.co098170Node01.server1(AppSrv01)
           WAS cell: co098170Node01Cell
            WAS node: co098170Node01

           WebSphere Profile home    :
              C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01

           wsadmin location          :
             C:\Program Files\IBM\WebSphere\AppServer\bin\wsadmin.bat

                        WAS version : 8.0.0.0
                         Deployment : Standalone
                           JVM mode : 32
                  Configuration home : C\IBM\ITM\dchome


     2) Integrate with ITCAM for SOA Agent : Yes

     3) Integrate with ITCAM Agent for WebSphere Applications : Yes
    ```

```
      TEMA hostname or IP address : 127.0.0.1
               TEMA port number : 63335
                     Monitor GC : No

 4) Integrate with ITCAM for AD Managing Server : No

      MS hostname or IP address : 127.0.0.1
        MS codebase port number : 9122
              MS home directory : /opt/IBM/itcam/WebSphere/MS

 5) Integrate with ITCAM for Transactions : Yes

      Transaction Collector hostname : 127.0.0.1
      Transaction Collector port number : 5455

 6) Integrate with Tivoli Performance Viewer : No

 7) Integrate with ITCAM diagnostics tool : No

 8) Advanced settings :

      Set Garbage Collection log path : No
      Added 128M to the heap size : No

You may accept or update your configuration choices for the following actions:
 1) List of servers selected
 2) Integrate with ITCAM for SOA Agent
 3) Integrate with ITCAM Agent for WebSphere Applications
 4) Integrate with ITCAM for AD Managing Server
 5) Integrate with ITCAM for Transactions
 6) Integrate with Tivoli Performance Viewer
 7) Integrate with ITCAM diagnostics tool
 8) Advanced settings

To modify a section, enter the number. To modify all sections, enter '*'. To accept you
configuration without modifying, enter 'a'.
To quit the selection, enter 'q':
```

The summary section provides options to change parts of the data collector configuration before applying the changes and an option to exit the configuration tool without applying your changes. Enter the number that represents the section you want to edit. Enter an asterisk (*) to reconfigure all sections. Enter a to accept your changes. Enter q to exit the ITCAM Data Collector for WebSphere Reconfiguration Utility.

33. When you enter a to accept your changes, you are prompted to specify whether you want to create a backup of your current WebSphere Application Server configuration:

    ```
    Do you want to backup current WebSphere configuration? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

34. Enter 1 to create a backup of the current configuration. Otherwise, enter 2.
35. The changes are applied and a status message is presented to indicate that the configuration of the data collector for the profile is complete:

    ```
    Successfully executed config for Cell: co098170Node01Cell
    Node: co098170Node01 Profile: AppSrv01.
    ```

Important: After reconfiguring the data collector to monitor application server instances, you must restart the application server instances. The data collector configuration takes effect when the application server instances are restarted.

Migrating data collectors to the ITCAM Data Collector for WebSphere

The ITCAM Data Collector for WebSphere Migration Utility is a menu driven command-line utility for migrating older version of the data collector to the ITCAM Data Collector for WebSphere.

You can upgrade the data collector to use the ITCAM Data Collector for WebSphere if your application server instances are being monitoring by any of the following products or components:

- ITCAM for WebSphere version 6.1 (fix pack 4 or later)
- WebSphere Data Collector version 6.1 (fix pack 4 or later) included in ITCAM for Web Resources version 6.2
- ITCAM Agent for WebSphere Applications version 7.1 included in ITCAM for Applications Diagnostics 7.1
- ITCAM for WebSphere Application Server version 7.2
- ITCAM for SOA version 7.1.1

For the procedure for migrating the ITCAM for SOA 7.1.1 data collector to version 7.2, see "Migrating ITCAM for SOA version 7.1.1 data collector to the ITCAM Data Collector for WebSphere" on page 72.

To upgrade monitoring of server instances to the ITCAM Data Collector for WebSphere, complete the following procedure:

1. Set the location of the Java home directory before you run the utility.

   ```
   set JAVA_HOME=/opt/IBM/AppServer80/java
   ```

2. Run the following command to start the ITCAM Data Collector for WebSphere Migration Utility.

   DC_home/bin/migrate.sh

3. The utility displays the IP addresses of all network cards that are found on the local computer system and prompts you to specify the interface to use for the data collector:

   ```
   List of TCP/IP interfaces discovered:
     1. 9.111.98.108
   Enter a number [default is: 1]:
   ```

4. Enter the number that corresponds to the IP address to use.

   The utility prompts you to specify from the type of agent that you want to upgrade to ITCAM Data Collector for WebSphere version 7.2.

   ```
   List of ITCAM agents whose data collector can be upgraded to the
   ITCAM Data Collector for WebSphere 7.2:

   1. ITCAM for WebSphere 6.1 (fix pack 4 or later)
   2. ITCAM WebSphere Agent 6.2 (fix pack 4 or later) [ITCAM for Web Resources 6.2]
   3. ITCAM Agent for WebSphere Applications 7.1 [ITCAM for Application Diagnostics 7.1]
   4. ITCAM for WebSphere Application Server 7.2
   5. ITCAM for SOA 7.1.1
   Enter the number [default is: 1]:
   ```

   Enter the number that represents the agent.

   For the procedure for migrating the ITCAM for SOA version 7.1.1 data collector to version 7.2, see "Migrating ITCAM for SOA version 7.1.1 data collector to the ITCAM Data Collector for WebSphere" on page 72.

5. The utility prompts you to specify the home directory of the previous version of the data collector.

   ```
   Enter the home directory of the data collector to be upgraded:
   ```

6. Enter the home directory of the previous version of the data collector. For example, `C:\IBM\ITM\TMAITM6\wasdc\7.1.0.2` on Windows systems or `/opt/IBM/ITM/li6263/yn/wasdc/7.1.0.2` on Linux or UNIX systems.

   If you are migrating ITCAM for WebSphere Application Server version 7.2, skip to step 9.

7. If the data collector was integrated with the ITCAM Agent for WebSphere monitoring agent, you are prompted to reenter the host name and port of the monitoring agent. If more than one version of the monitoring agent is available, you can connect the data collector to the correct version. (On Linux and UNIX systems, you can install several versions of the monitoring agent on the same host, using different ports).

   ```
   Enter the host name or IP address of the ITCAM Agent for WebSphere Applications TEMA:
   [default is: 127.0.0.1]:
   ```

8. Enter the fully qualified host name or IP address of the ITCAM Agent for WebSphere Applications monitoring agent. It is on the local host, so the default is correct.

   You are prompted for the port number of the ITCAM Agent for WebSphere Applications monitoring agent.

   ```
   Enter the port number of the ITCAM Agent for WebSphere Application TEMA:
   [default is: 63335]:
   ```

   Enter the port number of the monitoring agent.

9. The utility searches for the list of application server instances that are configured by the specified data collector installation.

   The utility prompts you to select one or more application server instances from the list. The instances might be under different profiles.

   ```
   Choose a Server or Servers to be migrate
    1. x336r1s37-vn01Cell01.x336r1s36-vn01Node03.server3
    2. x336r1s37-vn01Cell01.x336r1s36-vn01Node03.server5
    3. x336r1s37-vn01Cell01.x336r1s36-vn01Node03.server1
   Enter a number or numbers separated by a comma, enter '*' to select all
   servers listed, or enter 'q' to quit the selection.
   ```

   Tip: If several instances under one profile are monitored, you must select them all for migrating at the same time.

   Remember:

   - For a stand-alone environment, application server instances must be running during the configuration.
   - For a Network Deployment or Extended Deployment environment, the node agent and deployment manager must be running.

10. Enter the number that corresponds to the application server instance whose data collector is to be migrated or enter an asterisk (`*`) to migrate the data collector of all application server instances. To specify a subset of servers, enter the numbers, separated by commas, that represents the servers. For example: `1,2,3`.
11. The utility determines whether WebSphere Global Security was enabled for each of the profiles that are impacted by the migration task.
12. If WebSphere Global Security is enabled on one or more profiles, the utility prompts you to specify whether to retrieve security settings from a client properties file:

    ```
    Do you want to retrieve security settings from a client properties file
    (soap.client.props or sas.client.props)?
    [1 - YES, 2 - NO] [default is: 2]:
    ```

The data collector communicates with the WebSphere Administrative Services using the Remote Method Invocation (RMI) or the SOAP protocol. If global security is enabled for a profile, you must specify the user ID and password of a user who is authorized to log in to the IBM WebSphere Application Server administrative console for the profile. Alternatively, you can encrypt the user name and password and store them in client properties files before configuring the data collector. You must use the `sas.client.props` file for an RMI connection, or the `soap.client.props` file for an SOAP connection.

Enter `1` to allow the utility to retrieve the user name and password from the appropriate client properties file and skip to step 13. Otherwise, enter `2` to enter the user name and password.

```
CFG1018I Enter WebSphere admin user name:
CFG1019I Enter WebSphere admin password:
```

Important: It may take some time to log in to the WebSphere Application Server administrative console.
The utility prompts you for the user name and password for each profile whether WebSphere Global Security is enabled.

13. The utility migrates data collection for each selected application server instance and displays a status message that indicates whether the migration of each server completed successfully.

When the utility completes the migration of all application server instances configured by the previous version of the data collector, it displays the following message:

```
Migration of the Data Collector has successfully completed with return code 0.
```

Important: After migrating the data collector, you must restart the application server instances. The data collector configuration takes effect when the application server instances are restarted.

Remember: For server instances that were migrated, do not use the configuration utility for the old data collector version.

You can also configure or reconfigure integration with ITCAM for SOA, ITCAM Agent for WebSphere Applications monitoring agent, ITCAM for Application Diagnostics Managing Server, Tivoli Performance Viewer, and ITCAM diagnostics tool for the application server instances. For more information, see "Reconfiguring the ITCAM Data Collector for WebSphere" on page 22.

Migrating the ITCAM Data Collector for WebSphere in silent mode

A previous version of the ITCAM Data Collector for WebSphere can be migrated interactively with the ITCAM Data Collector for WebSphere Migration Utility. Alternatively, to migrate many application server instances to use the latest version of the data collector, you can migrate the data collectors in silent mode.

When you migrate the data collector in silent mode, you first specify configuration options in a properties file. A sample properties file, `sample_silent_migrate.txt`, is packaged with the ITCAM Data Collector for WebSphere Migration Utility. The file is available in the following location:

DC_home`/bin`

A sample of a properties file is available in "Sample properties file" on page 71.

Complete the following steps to perform a silent migration:

1. Specify configuration options in the properties file.
2. Go to the *DC_home*/bin directory.
3. Run the following command:

   ```
   migrate.sh -silent [dir_path]/silent_file
   ```

While you are performing a silent migration, you can also configure or reconfigure integration with: ITCAM for SOA, ITCAM Agent for WebSphere Applications monitoring agent, ITCAM for Application Diagnostics Managing Server, ITCAM for WebSphere Application Server, and ITCAM Diagnostics Tool. To do this, use the silent configuration parameters for these components, as described in Table 11.

To migrate ITCAM for SOA version 7.1.1 using the ITCAM Data Collector for WebSphere Migration Utility in silent mode, see "Migrating ITCAM for SOA version 7.1.1 to the ITCAM Data Collector for WebSphere in silent mode" on page 37.

Properties file

When you create your silent response properties file, keep in mind these considerations:

- A line in the file that starts with a number sign (#) is treated as a comment, and is not processed. If the number sign is used elsewhere in the line, it is not considered to be the start of a comment. This means that you can use the number sign in passwords or for other uses.
- Each property is described on a separate line, in the following format: *property* = *value*.

  property
  : This is the name of property. The list of valid properties that you can configure is shown in Table 11.

  value
  : This is the value of the property. Default values for some properties are already provided. You can delete default values to leave property values blank, or empty. An empty value is treated as if the property is not specified, as opposed to using the default value. If you want to use default values, you can comment out the property in the file.

- Passwords are in plain text.
- Properties and their values are case-sensitive.
- The following table describes the available properties for running the migration utility in silent mode:

Table 11. Available properties for running the ITCAM Data Collector for WebSphere Migration Utility in silent mode

Property	Comment
default.hostip	If the computer system uses multiple IP addresses, specify the IP address for the data collector to use.
migrate.type	Type of agent whose data collector you want to migrate to the ITCAM Data Collector for WebSphere version 7.2. The value must be set to *AD*.
Location of data collector to be migrated	
itcam.migrate.home	Specifies the data collector home directory of the old version of the data collector. The directory is not deleted as part of the migration.

Table 11. Available properties for running the ITCAM Data Collector for WebSphere Migration Utility in silent mode (continued)

Property	Comment
ITCAM Agent for WebSphere Applications monitoring agent settings	
temaconnect	Specifies whether the data collector connects to the ITCAM Agent for WebSphere Applications monitoring agent. Set this property to *False* if you do not want to connect the ITCAM Agent for WebSphere Applications with the monitoring agent, if you plan to connect the ITCAM Agent for WebSphere Applications with the Managing Server only, or if you do not have the ITCAM Agent for WebSphere Applications installed. Valid values are *True* and *False*. **Remember:** The Managing Server is not a component of ITCAM for Applications.
tema.host	Specifies the fully qualified host name or IP address of the ITCAM for Agent for WebSphere Applications monitoring agent.
tema.port	Specifies the port number of the ITCAM for Agent for WebSphere Applications monitoring agent.
WebSphere Application Server connection settings	
was.wsadmin.connection.host	Specifies the name of the host to which the wsadmin tool is connecting.
WebSphere Application Server global security settings	
was.wsadmin.username	Specifies the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server.
was.wsadmin.password	Specifies the password that corresponds to the user specified in the `was.wsadmin.username` property.
WebSphere Application Server settings	
was.appserver.profile.name	Specifies the name of the application server profile you want to configure.
was.appserver.home	Specifies the WebSphere Application Server home directory.
was.appserver.cell.name	Specifies the WebSphere Application Server cell name.
was.appserver.node.name	Specifies the WebSphere Application Server node name.
WebSphere Application Server runtime instance settings	
was.appserver.server.name	Specifies the application server instance within the application server profile to migrate to the new version of the data collector. **Tip:** The silent response file can have multiple instances of this property.

Sample properties file

When you run the **migrate** script in silent mode, the configuration parameters are read from a simple text properties file, `silent_file`, that you create in advance. A typical properties file might look similar to the following example:

```
################################################################################
#
#Comments:
#Locate the ITCAM Data Collector for WebSphere Migration Utility (migrate.sh|bat) in <dc_home>/bin.
#Run migrate.sh|bat -silent [dir_path]/<properties_file> to migrate an older version of the data collector silently.
#This file is a sample properties file.
#
#This file has 2 sections; [DEFAULT SECTION] and [SERVER].
```

```
#You can have one instance of [DEFAULT].
#You can have multiple instances of [SERVER].
#
#Use this sample file to migrate the data collector of any of the following products:
#  ITCAM for WebSphere 6.1 (fix pack 4 or later)
#  WebSphere Data Collector 6.1 (fix pack 4 or later)
#  ITCAM Agent for WebSphere Applications 7.1
#  ITCAM for WebSphere Application Server 7.2
#
#Considerations:
#IP address to use:
#Uncomment and specify an IP address to use, if the system has multiple IP addresses.
#
#Migration type:
#Important: Do not modify this value.
#
#Servers:
#You can migrate the data collector for multiple servers in the same profile.
#Uncomment the second [SERVER] and add the server name.
#Repeat for each additional server.
#
#
################################################################################################

[DEFAULT SECTION]

#  IP address to use:
#default.hostip=9.9.9.9

#Migration type:
migrate.type=AD

#  Old data collector home directory:
itcam.migrate.home=c:\ibm\itm\tmaitm6\wasdc\71

#  ITCAM Agent for WebSphere Applications monitoring agent:
temaconnect=True
tema.host=127.0.0.1
tema.port=63335

#  Connect to WebSphere Administrative Services:
was.wsadmin.connection.host=127.0.0.1
was.wsadmin.username=username
was.wsadmin.password=password

#  WebSphere Application Server details:
was.appserver.profile.name=AppSrv01
was.appserver.home=/opt/IBM/WebSphere/AppServer
was.appserver.cell.name=yourCellName
was.appserver.node.name=yourNodeName

#Note: As of now, was.appserver.server.name is the only supported parameter in this section
[SERVER]
was.appserver.server.name=server1


#Note: As of now, was.appserver.server.name is the only supported parameter in this section
##[SERVER]
#was.appserver.server.name=server2
```

Migrating ITCAM for SOA version 7.1.1 data collector to the ITCAM Data Collector for WebSphere

If your application server instances are being monitored by ITCAM for SOA version 7.1.1, you can upgrade the data collector to use the ITCAM Data Collector for WebSphere.

The ITCAM Data Collector for WebSphere Migration Utility is a menu driven command-line utility for migrating previous versions of the ITCAM Data Collector for WebSphere.

For the procedure for migrating the following data collector components to the ITCAM Data Collector for WebSphere, see "Migrating data collectors to the ITCAM Data Collector for WebSphere" on page 67:

- ITCAM for WebSphere version 6.1 (fix pack 4 or later)
- WebSphere Data Collector version 6.1 (fix pack 4 or later) included in ITCAM for Web Resources version 6.2
- ITCAM for WebSphere Application Server version 7.1 included in ITCAM for Applications Diagnostics version 7.1
- ITCAM for WebSphere Application Server version 7.2. Data Collector

To upgrade monitoring of server instances from the ITCAM for SOA version 7.1.1 data collector to the ITCAM Data Collector for WebSphere, complete the following procedure:

1. Set the location of the Java home directory before you run the utility:

   ```
   set JAVA_HOME=/opt/IBM/AppServer80/java
   ```

2. Run the following command to start the ITCAM Data Collector for WebSphere Migration Utility:

   DC_home>/bin/migrate.sh

3. The utility displays the IP addresses of all network cards found on the local computer system and prompts you to specify the interface to use for the data collector:

   ```
   List of TCP/IP interfaces discovered:
     1. 9.111.98.108
   Enter a number [default is: 1]:
   ```

4. Enter the number that corresponds to the IP address to use.

   The utility prompts you to specify the type of agent that you want to upgrade to ITCAM Data Collector for WebSphere 7.2.

   ```
   List of ITCAM agents whose data collector can be upgraded to the
   ITCAM Data Collector for WebSphere 7.2:

     1. ITCAM for WebSphere 6.1.0.4 or later
      2. ITCAM WebSphere Agent 6.2.0.4 or later [ITCAM for Web Resources 6.2]
      3. ITCAM Agent for WebSphere Applications 7.1 [ITCAM for Application Diagnostics 7.1]
      4. ITCAM for WebSphere Application Server 7.2
      5. ITCAM for SOA 7.1 or later Enter the number [default is: 1]:
   ```

   Enter 5 to migrate ITCAM for SOA version 7.1.1.

5. The utility prompts you to specify the WebSphere Application Server home directory where the previous version of the ITCAM for SOA version 7.1.1 data collector is configured.

   ```
   Specify SOA Websphere Home Directory:
   ```

6. The utility searches for WebSphere Application Server home directories on the computer system and prompts you to select a home directory:

   ```
   List of WebSphere Application Server home directories discovered:
     1. /opt/IBM/WebSphere/AppServer
   Enter a number or enter the full path to a home directory
   [default is: 1]:
   ```

7. Enter the number that corresponds to a WebSphere Application Server home directory.

The utility searches for all profiles under the specified home directory and prompts you to select a profile:

```
List of WebSphere profiles discovered:
  1. AppSrv01
Enter a number [default is: 1]:
```

8. Enter the number that corresponds to the WebSphere Application Server profile you want to configure.

   The utility indicates whether WebSphere Global Security is enabled for the WebSphere Application profile you have specified:

   ```
   WebSphere Global Security is enabled.
   ```

   If global security is not enabled, skip to step 10.

9. The utility prompts you to specify whether to retrieve security settings from a client properties file:

   ```
   Do you want to retrieve security settings from a client properties file
   (soap.client.props or sas.client.props)?
   [1 - YES, 2 - NO] [default is: 2]:
   ```

   The data collector communicates with the WebSphere Administrative Services using the Remote Method Invocation (RMI) or the SOAP protocol. If global security is enabled for a profile, you must specify the user ID and password of a user who is authorized to log in to the IBM WebSphere Application Server administrative console for the profile. Alternatively, you can encrypt the user name and password and store them in client properties files before configuring the data collector. You must use the `sas.client.props` file for an RMI connection, or the `soap.client.props` file for a SOAP connection.

   Enter 1 to allow the utility to retrieve the user name and password from the appropriate client properties file and skip to step 10. Otherwise, enter 2 to enter the user name and password.

   ```
   CFG1018I Enter WebSphere admin user name:
   CFG1019I Enter WebSphere admin password:
   ```

10. The utility searches for all application server instances under the specified profile. The utility displays all servers that have not been configured yet for data collection and all servers that have been configured to use the current version of the ITCAM Data Collector for WebSphere.

    The utility prompts you to select one or more application server instances from the list:

    ```
    Choose one or more servers to configure for data collection:
    Application servers not yet configured:
     1. co098170Node01Cell.co098170Node01.server1(AppSrv01)
    Enter a number or numbers separated by commas, or enter * to select all:
    ```

    Important:

    - For a Network Deployment or Extended Deployment environment, the Node Agent and Deployment Manager must be running. For a stand-alone environment, application server instances must be running during the configuration of the data collector.
    - Ensure that the application server instances that you select are the actual nodes that host the BPM applications or services that you want to monitor.

11. Enter the number that corresponds to the application server instance to configure for data collection or enter an asterisk `*` to configure all application server instances for data collection. To specify a subset of servers, enter the numbers, separated by commas, that represents the servers. For example: `1,2,3`.

The utility displays a summary list. By default, it configures the migrated instances to integrate with ITCAM for SOA only. You can specify other configuration.

```
+-------------------------------------------------------------------------+
|                                                                         |
|  Data collector configuration summary                                   |
|                                                                         |
+-------------------------------------------------------------------------+

Each of the servers will be configured for data collection

 1) List of servers selected

   - WAS server: IBM-6DA7F9C6EE6Node02Cell.IBM-6DA7F9C6EE6Node02.server1(AppSrv02)
       WAS cell: IBM-6DA7F9C6EE6Node02Cell
        WAS node: IBM-6DA7F9C6EE6Node02

       WebSphere Profile home    :
         /opt/IBM/WebSphere/AppServer80/profiles/AppSrv02

       wsadmin location          :
         /opt/IBM/WebSphere/AppServer80/bin/wsadmin.bat

                    WAS version : 8.0.0.0
                     Deployment : Standalone
                       JVM mode : 32
                Configuration home : C:\NewInstall\itcam_gdc_201204122100\bin\..

 2) Integrate with ITCAM for SOA Agent : Yes

 3) Integrate with ITCAM Agent for WebSphere Applications : No

 4) Integrate with ITCAM for AD Managing Server : No

 5) Integrate with ITCAM for Transactions : No

 6) Integrate with Tivoli Performance Viewer : No

 7) DE Integrate with ITCAM diagnostics tool : No

 8) Advanced settings :

       Set Garbage Collection log path : No
       Added 128M to the heap size : No


Configuration sections:

 1) List of servers selected
 2) Integrate with ITCAM for SOA Agent
 3) Integrate with ITCAM Agent for WebSphere Applications
 4) Integrate with ITCAM for AD Managing Server
 5) Integrate with ITCAM for Transactions
 6) Integrate with Tivoli Performance Viewer
 7) DE Integrate with ITCAM diagnostics tool
 8) Advanced settings

To modify a section, enter the number. To modify all sections, enter '*'. To accept your
configuration without modifying, enter 'a'. To quit the selection, enter 'q'.:
```

12. To enable integration with products and components other than ITCAM for SOA, select the corresponding number, For details on the configuration, see "Configuring the ITCAM Data Collector for WebSphere" on page 49. Otherwise, to accept the configuration, enter `a`.

You are prompted to specify whether you want to create a backup of your current WebSphere Application Server configuration:

```
Do you want to backup current WebSphere configuration? [1 - YES, 2 - NO]
[default is: 2]:
```

13. Enter 1 to create a backup of the current configuration. Otherwise, enter 2.
14. The changes are applied and a status message is presented to indicate that the configuration of the data collector for the profile is complete:

```
Successfully executed migrate for Cell: co098170Node01Cell
Node: co098170Node01 Profile: AppSrv01.
```

Important: After migrating from the ITCAM for SOA version 7.1.1 data collector, you must restart the application server instances. The data collector configuration takes effect when the application server instances are restarted.

You can also configure or reconfigure integration with ITCAM for SOA, ITCAM Agent for WebSphere Applications monitoring agent, ITCAM for Application Diagnostics Managing Server, Tivoli Performance Viewer, and ITCAM diagnostics tool for the application server instances at the same time. For more information, see "Reconfiguring the ITCAM Data Collector for WebSphere" on page 22.

Migrating ITCAM for SOA 7.1.1 to the ITCAM Data Collector for WebSphere in silent mode

The ITCAM for SOA version 7.1.1 data collector can be migrated to the ITCAM Data Collector for WebSphere interactively with the ITCAM Data Collector for WebSphere Migration Utility. Alternatively, to migrate many application server instances to use the latest version of the data collector, you can migrate the data collector in silent mode.

When you migrate the ITCAM for SOA version 7.1.1 data collector in silent mode, you first specify configuration options in a properties file. A sample properties file, `sample_silent_migrate_soa.txt`, is packaged with the ITCAM Data Collector for WebSphere Migration Utility. The file is available in the following location:

DC_home`/bin`

A sample of a properties file is available in "Sample properties file" on page 78.

Complete the following steps to perform a silent migration:

1. Specify configuration options in the properties file.
2. Go to the *DC_home*`/bin` directory.
3. Run the following command:

```
migrate.sh -silent [dir_path]/silent file
```

While you are performing a silent migration, you can also configure or reconfigure integration with ITCAM for SOA, ITCAM Agent for WebSphere Applications monitoring agent, ITCAM for Application Diagnostics Managing Server, Tivoli Performance Monitoring, and ITCAM diagnostics tool for the application server instances at the same time. To do this, use the silent configuration parameters for these components, as described in Table 12 on page 77.

Properties file

When you create your silent response properties file, keep in mind these considerations:

- A line in the file that starts with a number sign (#) is treated as a comment, and is not processed. If the number sign is used elsewhere in the line, it is not considered to be the start of a comment. This means that you can use the number sign in passwords or for other uses.
- Each property is described on a separate line, in the following format: *property* = *value*.

  property
  This is the name of property. The list of valid properties that you can configure is shown in: Table 12.

  value This is the value of the property. Default values for some properties are already provided. You can delete default values to leave property values blank, or empty. An empty value is treated as if the property is not specified, as opposed to using the default value. To use default values, you can comment out the property in the file.
- Passwords are in plain text.
- Properties and their values are case-sensitive.

Table 12. Available properties for running the ITCAM Data Collector for WebSphere Migration Utility in silent mode

Property	Comment
default.hostip	If the computer system uses multiple IP addresses, specify the IP address for the data collector to use.
migrate.type	Type of agent whose agent you want to migrate to the ITCAM Data Collector for WebSphere version 7.2. The value must be set to *SOA*.
was.appserver.home	Location of the WebSphere Application Server home directory where the ITCAM for SOA version 7.1.1 data collector is configured. For example: `/opt/IBM/WebSphere85/AppServer`.
ms.connect	Specifies whether the data collector is configured to connect to the Managing Server in an ITCAM for Application Diagnostics environment. For a migration from ITCAM for SOA version 7.1.1, ignore this parameter.
ttapi.enable	Specifies whether the data collector communicates with ITCAM for Transactions using the Transaction Tracking API (TTAPI). Valid values are *True* and *False*.
soa.enable	Specifies whether to integrate the data collector with ITCAM for SOA. The ITCAM for SOA agent must be installed to complete the configuration.
tpv.enable	Specifies whether to integrate the data collector with the Tivoli Performance Monitoring when the data collector is included as part of ITCAM for WebSphere Application Server 8.5. Tivoli Performance Monitoring is accessed with the WebSphere Application Server administrative console. For a migration from ITCAM for SOA 7.1.1, ignore this parameter.
de.enable	Specifies whether to integrate the data collector with the ITCAM Diagnostics Tool. The ITCAM Diagnostics Tool is an Eclipse-based tool for diagnostic investigation of applications that are running on WebSphere Application Server. For a migration from ITCAM for SOA version 7.1.1, ignore this parameter.

Table 12. Available properties for running the ITCAM Data Collector for WebSphere Migration Utility in silent mode (continued)

Property	Comment
temaconnect	Specifies whether the data collector connects to the ITCAM Agent for WebSphere Applications monitoring agent (TEMA). For a migration from ITCAM for SOA version 7.1.1, ignore this parameter.
was.backup.configuration	Specifies whether to back up the current configuration of the WebSphere Application Server configuration before applying the new configuration. Valid values are *True* and *False*.
was.gc.custom.path	Specifies the path to the custom Garbage Collection log. For a migration from ITCAM for SOA version 7.1.1, ignore this parameter.
was.configure.heap	Specifies whether to add 128 MB to the heap size. Each time you run the silent configuration, 128 MB is added to the heap size if this property is set to *True*. For a migration from ITCAM for SOA version 7.1.1, ignore this parameter.
WebSphere Application Server connection settings	
was.wsadmin.connection.host	Specifies the name of the host to which the wsadmin tool is connecting.
was.wsadmin.connection.type	Specifies the connection protocol for the wsadmin tool to use.
was.wsadmin.connection.port	Specifies the port that the wsadmin tool must use to connect to the WebSphere Application Server.
WebSphere Application Server global security settings	
was.wsadmin.username	Specifies the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server.
was.wsadmin.password	Specifies the password that corresponds to the user specified in the `was.wsadmin.username` property.
WebSphere Application Server settings	
was.appserver.profile.name	Specifies the name of the application server profile you want to configure.
was.appserver.cell.name	Specifies the WebSphere Application Server cell name.
was.appserver.node.name	Specifies the WebSphere Application Server node name.
WebSphere Application Server runtime instance settings	
was.appserver.server.name	Specifies the application server instance within the application server profile to configure. **Important:** The silent response file can have multiple instances of this property.

Sample properties file

When you run the *migrate* script in silent mode, the configuration parameters are read from a simple text properties file, *silent_file*, that you create in advance. A typical properties file might look similar to the following example:

```
################################################################################
#
#Comments:
#Locate the ITCAM Data Collector for WebSphere Migration Utility (migrate.sh|bat) in <dc_home>/bin.
```

```
#Run migrate.sh|bat -silent [dir_path]/<properties_file> to migrate an older version of the data collector silently.
#This file is a sample properties file.
#
#This file has 2 sections; [DEFAULT SECTION] and [SERVER].
#You can have one instance of [DEFAULT].
#You can have multiple instances of [SERVER].
#
#Use this sample file to migrate the ITCAM for SOA 7.1.1 data collector.
#To migrate all other older versions of the data collector, use sample_silent_migrate.txt.
#
#Considerations:
#IP address to use:
#Uncomment and specify an IP address to use, if the system has multiple IP addresses.
#
#Migration type:
# Important: Do not modify this value.
#
#Connect to WebSphere Administrative Services:
#The utility determines the connection type and port automatically.
#If the utility cannot determine the values, uncomment and override the default values.
#
#Servers:
#You can migrate the data collector for multiple servers in the same profile.
#Uncomment the second [SERVER] and add the server name.
#Repeat for each additional server.
###############################################################################################


[DEFAULT SECTION]
#IP address to use:
#default.hostip=9.9.9.9

#  Migration type:
migrate.type=SOA

#  Old WebSphere Application Server home directory:
was.appserver.home=/opt/IBM/WebSphere85/AppServer

#  ITCAM for Application Diagnostics Managing Server:
ms.connect=False

#  ITCAM for Transactions:
ttapi.enable=False

#  ITCAM for SOA agent:
soa.enable=True

#  Tivoli Performance Viewer:
tpv.enable=False

#  ITCAM Diagnostics Tool:
de.enable=False

#  ITCAM Agent for WebSphere Applications monitoring agent:
temaconnect=False

#  Create a backup of WebSphere Application Server:
was.backup.configuration=False

#  Modify Garbage Collection log path:
was.gc.custom.path=False

#  Increase the JVM heap size by 128MB:
was.configure.heap=False

#Connect to WebSphere Administrative Services:
was.wsadmin.connection.host=servername.yourcompany.com
was.wsadmin.username=
was.wsadmin.password=
#was.wsadmin.connection.type=SOAP
```

```
#was.wsadmin.connection.port=8881

#  WebSphere Application Server details:
was.appserver.profile.name=AppSrv01
was.appserver.cell.name=yourITCAMCell
was.appserver.node.name=yourITCAMNode

#Note: As of now, was.appserver.server.name is the only supported parameter in this section
[SERVER]
was.appserver.server.name=server1

#Note: As of now, was.appserver.server.name is the only supported parameter in this section
#[SERVER]
#was.appserver.server.name=server2
```

Unconfiguring the ITCAM Data Collector for WebSphere

If you no longer want the data collector to monitor one or more application server instances, you can unconfigure the data collector for them.

The ITCAM Data Collector for WebSphere Unconfiguration Utility is a menu driven command-line utility for unconfiguring the ITCAM Data Collector for WebSphere.

To unconfigure the data collector, complete the following procedure:

1. From the command-line, navigate to the *DC_home*/bin directory.
2. Set the location of the Java home directory before you run the script. For example:

   ```
   export JAVA_HOME=/opt/IBM/AppServer80/java
   ```

3. Run the following command to start the ITCAM Data Collector for WebSphere Unconfiguration Utility.

   DC_home/bin/unconfig.sh

   The utility searches for all server instances monitored by the ITCAM Data Collector for WebSphere.

   Remember:

   - Application server instances must be running during the unconfiguration procedure.
   - For Network Deployment environment, the node agent and deployment manager must also be running.

   The utility prompts you to select one or more application server instances from the list of configured servers:

   ```
   Choose one or more servers to unconfigure for data collection:
   Application servers configured:
    1. co098170Node01Cell.co098170Node01.server1(AppSrv01)
   Enter a number or numbers separated by commas, or enter * to select all:
   ```

4. Enter the number that corresponds to the application server instance to unconfigure for data collection or enter an asterisk (*) to unconfigure data collection for all application server instances. To specify a subset of servers, enter the numbers, separated by commas, that represent the servers. For example: 1,2,3.
5. The utility unconfigures the data collector for the specified application server instances. A status message is presented to indicate that the data collector was successfully unconfigured:

   ```
   Unconfiguration of the Data Collector has successfully completed with return code 0.
   ```

6. After unconfiguring the data collector to monitor application server instances, you must restart the instances. The data collector unconfiguration takes effect when the application server instances are restarted.

Data collection is unconfigured for the specified application server instances.

Unconfiguring the ITCAM Data Collector for WebSphere in silent mode

The ITCAM Data Collector for WebSphere can be unconfigured interactively using the ITCAM Data Collector for WebSphere Unconfiguration Utility. Alternatively, to unconfigure data collection for many application server instances, you can unconfigure the data collectors in silent mode.

When you unconfigure the data collector in silent mode, you first specify configuration options in a properties file. A sample properties file, `sample_silent_unconfig.txt`, is packaged with the ITCAM Data Collector for WebSphere Unconfiguration Utility. The file is available in the following location:

DC_home`/bin`

The variable *DC_home* is the location where the data collector is installed. A sample of a properties file is available in "Sample properties file" on page 82.

Complete the following steps to perform a silent unconfiguration:

1. Specify configuration options in the properties file.
2. Go to the *DC_home*`/bin` directory.
3. Run the following command:

   ```
   unconfig.sh -silent [dir_path]/silent file
   ```

4. After unconfiguring the data collector to monitor application server instances, you must restart the instances. The data collector configuration takes effect when the application server instances are restarted.

Properties file

When you create your silent response properties file, keep in mind these considerations:

- A line in the file that starts with a number sign (#) is treated as a comment, and is not processed. If the number sign is used elsewhere in the line, it is not considered to be the start of a comment. This means that you can use the number sign in passwords or for other uses.
- Each property is described on a separate line, in the following format: <*property*> = *value*>.

  property
  : This is the name of property. The list of valid properties that you can configure is shown in Table 13 on page 82.

  value
  : This is the value of the property. Default values for some properties are already provided. You can delete default values to leave property values blank, or empty. An empty value is treated as if the property is not specified, as opposed to using the default value. To use default values, you can comment out the property in the file.

- Passwords are in plain text.
- Properties and their values are case-sensitive.

Table 13. Available properties for running the ITCAM Data Collector for WebSphere Unconfiguration Utility in silent mode

Property	Comment
WebSphere Application Server connecting settings	
was.wsadmin.connection.host	Specifies the name of the host to which the wsadmin tool is connecting.
WebSphere Application Server global security settings	
was.wsadmin.username	Specifies the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server.
was.wsadmin.password	Specifies the password that corresponds to the user specified in the `was.wsadmin.username` property.
WebSphere Application Server settings	
was.appserver.profile.name	Specifies the name of the application server profile you want to unconfigure.
was.appserver.home	Specifies the WebSphere Application Server home directory.
was.appserver.cell.name	Specifies the WebSphere Application Server cell name.
was.appserver.node.name	Specifies the WebSphere Application Server node name.
Backup of the WebSphere Application Server configuration	
was.backup.configuration	Specifies whether to back up the current configuration of the WebSphere Application Server data collector configuration before unconfiguring the data collector. Valid values are *True* and *False*.
was.backup.configuration.dir	Specifies the location of the backup directory.
WebSphere Application Server runtime instance settings	
was.appserver.server.name	Specifies an application server instance within the application server profile for which you want to unconfigure the data collector. **Tip:** The silent response file can have multiple instances of this property.

Sample properties file

```
#############################################################################################
#
#Comments:
#Locate the ITCAM Data Collector for WebSphere Unconfiguration Utility (unconfig.sh|bat) in <dc_home>/bin.
#Run unconfig.sh|bat -silent [dir_path]/<properties_file> to unconfigure the data collector silently.
#This file is a sample properties file.
#
#This file has 2 sections; [DEFAULT SECTION] and [SERVER].
#You can have one instance of [DEFAULT].
#You can configure multiple [SERVER] sections, one for each server to be configured within the profile.
#Uncomment the second [SERVER] and add the server name.
#Repeat for each additional server.
#
#############################################################################################

[DEFAULT SECTION]

#Connect to WebSphere Administrative Services:
was.wsadmin.connection.host=servername.yourcompany.com
was.wsadmin.username=
was.wsadmin.password=
```

```
#  WebSphere Application Server details:
was.appserver.profile.name=AppSrv02
was.appserver.home=C:\Program Files\IBM\WebSphere\AppServer
was.appserver.cell.name=yourITCAMCell
was.appserver.node.name=yourITCAMNode

#  Create a backup of WebSphere Application Server:
was.backup.configuration=False
was.backup.configuration.dir=/opt/IBM/ITM/dchome/data

[SERVER]
was.appserver.server.name=server1

#[SERVER]
#was.appserver.server.name=server2
```

Chapter 5. Installing and configuring ITCAM for WebSphere Application Server on IBM i

ITCAM for WebSphere Application Server is an optional component that can be installed on:

- WebSphere Application Server Network Deployment, Version 8.5
- WebSphere Application Server Express, Version 8.5
- WebSphere Application Server, Version 8.5

Checklist for installation and configuration on IBM i

About this task

Use the following high-level checklist to install and configure ITCAM for WebSphere Application Server:

Procedure

1. Obtain the installation images from Integrated Service Management Library.
2. Verify that your computer meets the system and software prerequisites, and complete any tasks that are needed before installation. See "Prerequisites and preinstallation tasks for ITCAM for WebSphere Application Server on IBM i."
3. Complete the following steps to install and configure ITCAM for WebSphere Application Server.
   - "Installation and configuration of ITCAM for WebSphere Application Server on IBM i" on page 87

Prerequisites and preinstallation tasks for ITCAM for WebSphere Application Server on IBM i

There are some prerequisites and preinstallation tasks for ITCAM for WebSphere Application Server on IBM i.

System and software prerequisites

The following prerequisites are the hardware and software requirements for being able to install and use the ITCAM for WebSphere Application Server on IBM i.

Hardware prerequisites for the ITCAM for WebSphere Application Server

The installation image requires 170 MB. The installation requires 330 MB.

Supported operating system and application server combinations

ITCAM for WebSphere Application Server supports IBM WebSphere Application Server Version 8.5 on IBM i 6.1 (i5/OS® V6R1) or higher.

Supported JDKs for the ITCAM for WebSphere Application Server

The minimum supported JDKs for the ITCAM for WebSphere Application Server on IBM i is JDK16.

Additional requirements for the operating system

The ITCAM for WebSphere Application Server must be installed on the same computer as the application server you are monitoring. The set of supported operating systems is further limited by the supported operating systems for the application server you are monitoring.

For the operating system requirements for the IBM WebSphere Application Server 8.5, see:

http://www-01.ibm.com/software/webservers/appserv/doc/latest/prereq.html.

Permissions

The user who installs ITCAM for WebSphere Application Server must have at least *SYSADMIN privileges.

If you are performing a remote installation, the IBM i user running the installation should have the *ALLOBJ authority.

Use the command-prompt to add the following privileges for the application server user:

```
GRTOBJAUT OBJ(QSYS/STRDBG) OBJTYPE(*CMD) USER(QEJBSVR) AUT(*USE)
GRTOBJAUT OBJ(QSYS/ENDSRVJOB) OBJTYPE(*CMD) USER(QEJBSVR) AUT(*USE)
GRTOBJAUT OBJ(QSYS/STRSRVJOB) OBJTYPE(*CMD) USER(QEJBSVR) AUT(*USE)
GRTOBJAUT OBJ(QSYS/DMPJVM) OBJTYPE(*CMD) USER(QEJBSVR) AUT(*USE)
GRTOBJAUT OBJ(QSYS/ANZJVM) OBJTYPE(*CMD) USER(QEJBSVR) AUT(*USE)
```

Make sure that the umask is set to 022. To verify the umask setting, issue the following command:

```
umask
```

To set the umask setting to 022, issue the following command in QShell:

```
umask 022
```

Restrictions on the installation path

Make sure the installation path for ITCAM for WebSphere Application Server on the IBM i system does not exist in the IFS before the installation. The default installation path is `DC_home`. Make sure that this path does not exist before the installation.

Checking the heap size

About this task

Ensure that the JVM heap size is sufficient. The default value is enough, but if the heap size was configured in WebSphere Application Server, make sure that it is not less than 384 MB. Complete the following steps for each server that you want to configure for ITCAM for WebSphere Application Server:

Procedure

1. Log on to the WebSphere Application Server administrative console.
2. Go to the area for specifying the heap size in the administrative console by completing the following steps:
   a. Click **Servers >Server Types>WebSphere Application Servers** and select the *server_name*.
   b. In the **Configuration** tab, go to **Server Infrastructure > Java and Process Management > Process Definition > Additional Properties: Java Virtual Machine**.
3. If the value in the **Maximum Heap Size** field is less than 384, set it to 384.

Adjusting ports for firewalls or for use with other applications

About this task

During the configuration, specify port numbers or accept the defaults for port numbers that are used by ITCAM for WebSphere Application Server to communicate with the application server using SOAP or RMI. Make sure that you record the correct port, and that the firewall does not prevent communication on this port from ITCAM for WebSphere Application Server to the application server.

For a Network Deployment environment, ITCAM for WebSphere Application Server uses the SOAP or RMI port to communicate with the Deployment Manager, which is usually located on a different host. In this case, take special care that the firewall does not block communication on this port.

Information to know before the installation

The following notes provide information about installation and configuration:

1. If a WebSphere Application Server installation has multiple profiles, all application servers in a single profile must run the same version of the ITCAM for WebSphere Application Server.
2. For a Network Deployment environment, you need to supply the host name of the Deployment Manager to configure ITCAM for WebSphere Application Server for a node. It is not necessary to install or configure ITCAM for WebSphere Application Server on the Deployment Manager itself.
3. To install on a cluster, run the installer on each node that you want to install upon. Create a response file and use the silent installer mode if you must install across multiple nodes in a cluster.
4. The installation and configuration programs do not accept values for directory paths if the following special characters are included:
   `\u ~!@#$*()+=[]{}|:;'"<>,?`
5. The installation and configuration programs do not accept values for user names or passwords if the following special characters are included:
   `\u ~!@#$*()+[]{}|\:;'"<>,?/`

Installation and configuration of ITCAM for WebSphere Application Server on IBM i

Install ITCAM for WebSphere Application Server on IBM i using a silent install.

Installing ITCAM for WebSphere Application Server

About this task

Complete the following procedure if you are performing the silent installation on a local IBM i machine:

Procedure

1. Create a directory called `DC_home`.
2. Copy the data collector tar file to `DC_home`, it is available here: Integrated Service Management Library.
3. Untar the tar file using the QOpenSys tar command.

Results

Log files are created in: *DC_home*`/logs`

Configuring ITCAM for WebSphere Application Server

Using the new ITCAM Data Collector for WebSphere Configuration Utility, you can connect the common ITCAM Data Collector for WebSphere to the following components:

- Tivoli Performance Viewer - (this is ITCAM for WebSphere Application Server)
- ITCAM Agent for WebSphere Applications monitoring agent
- ITCAM for Application Diagnostics Managing Server
- ITCAM for Transactions Transaction

If you have any of the following product versions installed and configured for the same WebSphere profile, you must migrate them to use the ITCAM Data Collector for WebSphere before configuring ITCAM for WebSphere Application Server:

- ITCAM for WebSphere 6.1.0.4 or later
- ITCAM Agent for WebSphere Applications 7.1 [ITCAM for Application Diagnostics 7.1]
- ITCAM for WebSphere Application Server 7.2

Configure ITCAM for WebSphere Application Server for data collection using the ITCAM Data Collector for WebSphere Configuration Utility.

Configuring in a profile where there are no other ITCAM products configured in the same WebSphere Profile

If you are configuring the ITCAM for WebSphere Application in an environment where there are no other ITCAM products configured for application servers within the same profile, you can integrate the data collector with the Tivoli Performance Viewer and accept the default values.

Configuring the ITCAM Data Collector for WebSphere

You must configure the data collector for each application server instance that you want to monitor.

The ITCAM Data Collector for WebSphere Configuration Utility is a menu driven command-line utility for configuring the ITCAM Data Collector for WebSphere.

Important: In an ITCAM for Application Diagnostics deployment, do not configure the data collector to monitor an instance of WebSphere Application Server that hosts the Managing Server Virtualization Engine (MSVE). However, you can use the data collector to monitor any other WebSphere Application Server instances that are on the same node.

To configure the data collector to monitor one or more server instances, complete the following procedure:

1. Log on to the computer on which you want to install ITCAM for WebSphere Application Server as a user with the appropriate permissions. For information about permissions, see "Permissions" on page 86.
2. Enter the QSH environment by running the STRQSH command in the IBM i main menu.
3. Go to the *DC_home*/bin directory.
4. Start the ITCAM Data Collector for WebSphere Configuration Utility by running the config_i5.sh script.
5. The utility starts and displays the IP addresses of all network cards found on the local computer system and prompts you to specify the interface to use for the data collector:

   ```
   List of TCP/IP interfaces discovered:
    1. 9.156.47.144/NC047144
   Enter a number [default is: 1]:
   ```

   Enter the number that corresponds to the IP address to use.
6. As part of the configuration some SRVPGMs need to be installed (if they were not installed before). The utility displays the following message:

   ```
   SRVPGM Installation
   Data collection for ITCAM for i5 requires the
   installation of some Service programs
   ```

   When the SRVPGMs are successfully installed, the following message is displayed:

   ```
   CFG1105I Service programs successfully installed
   ```
7. The utility prompts to specify the WebSphere Application Server home directory with the following message:

   ```
   Enter WebSphere home directory:
   ```

   Enter the WebSphere Application Server home directory, for example: /QIBM/UserData/WebSphere/AppServer/V85/ND
8. The utility searches for all profiles under the specified home directory and prompts you to select a profile:

   ```
   List of WebSphere profiles discovered:
     1. AppSrv01
   Enter a number [default is: 1]:
   ```
9. Enter the number that corresponds to the WebSphere Application Server profile you want to configure.

   The utility indicates whether WebSphere Global Security is enabled for the WebSphere Application profile you have specified:

   ```
   WebSphere Global Security is enabled.
   ```

   If global security is not enabled, skip to step 11 on page 90.
10. The utility prompts you to specify whether to retrieve security settings from a client properties file:

```
Do you want to retrieve security settings from a client properties file
(soap.client.props or sas.client.props)?
[1 - YES, 2 - NO] [default is: 2]:
```

The Data Collector communicates with the WebSphere Administrative Services using the Remote Method Invocation (RMI) or the SOAP protocol. If global security is enabled for a profile, you must specify the user ID and password of a user who is authorized to log in to the IBM WebSphere Application Server administrative console for the profile. Alternatively, you can encrypt the user name and password and store them in client properties files before configuring the data collector. You must use the `sas.client.props` file for an RMI connection, or the `soap.client.props` file for a SOA connection.

Enter *1* to allow the utility to retrieve the user name and password from the appropriate client properties file and skip to step 11. Otherwise, enter *2* to enter the user name and password.

```
CFG1018I Enter WebSphere admin user name:
CFG1019I Enter WebSphere admin password:
```

11. The utility searches for all application server instances under the specified profile. The utility displays all servers that have not been configured yet for data collection and all servers that have been configured to use the current version of the ITCAM Data Collector for WebSphere.

    The utility prompts you to select one or more application server instances from the list:

    ```
    Choose one or more servers to configure for data collection:
    Application servers not yet configured:
     1. co098170Node01Cell.co098170Node01.server1(AppSrv01)
    Enter a number or numbers separated by commas, or enter * to select all:
    ```

    Note: For a Network Deployment or Extended Deployment environment, the Node Agent and Deployment Manager must be running. For a stand-alone environment, application server instances must be running during the configuration of the data collector.

    Note: Ensure that the application server instances you select are the actual nodes that host the applications or services you want to monitor.

12. Enter the number that corresponds to the application server instance to configure for data collection or enter an astericks (*) to configure all application server instances for data collection. To specify a subset of servers, enter the numbers that represent the servers separated by commas. For example: `1,2,3`.

13. In the **Integration with ITCAM Agent for WebSphere Applications** section, the utility provides an option for integrating the data collector with the ITCAM Agent for WebSphere Applications.

    You can integrate the data collector with ITCAM Agent for WebSphere Applications, or with the ITCAM for Application Diagnostics Managing Server, or with both.

    ```
    Do you want to integrate with an ITCAM Agent for WebSphere Applications?
     [1 - YES, 2 - NO]
    [default is: 2]:
    ```

    You must install and configure the ITCAM Agent for WebSphere Applications and its application support files to complete the installation and configuration of the ITCAM Agent for WebSphere Applications. For more information about installing and configuring the ITCAM Agent for WebSphere Applications, see *IBM Tivoli Composite Application Manager Agent for WebSphere Applications Installation and Configuration Guide*.

14. Enter *1* to integrate the data collector with the ITCAM Agent for WebSphere Applications. Otherwise, enter *2* and skip to step 17.

    You are prompted to enter the host name of the ITCAM Agent for WebSphere Applications.

    ```
    Enter the host name or IP address of the ITCAM Agent for WebSphere Applications TEMA:
    [default is: 127.0.0.1]:
    ```

15. Enter the fully qualified host name or IP address of the ITCAM Agent for WebSphere Applications Monitoring Agent.

    You are prompted for the port number of the ITCAM Agent for WebSphere Applications Monitoring Agent.

    ```
    Enter the port number of the ITCAM Agent for WebSphere Application TEMA:
    [default is: 63335]:
    ```

    You can change the port that is used for communication between the data collector and the ITCAM Agent for WebSphere Applications Monitoring Agent. The default port is 63335. You can change the port at a later time, but it is normally most convenient to set it when initially configuring the data collector.

16. Enter the port number of the Monitoring Agent.
17. In the **Integration with ITCAM for Application Diagnostics Managing Server** section, the utility provides an option for integrating the data collector with the ITCAM for Application Diagnostics Managing Server, installed on a separate Windows, Linux, or UNIX server, for deep-dive diagnostics. For information about installing the Managing Server, see *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

    You are prompted to specify whether you want to integrate the data collector with a Managing Server.

    ```
    Do you want to integrate with an MS? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

    Note: To integrate with ITCAM for Application Diagnostics Managing Server for deep-dive analysis, you must have ITCAM for Application Diagnostics 7.1 installed.

    Note: If you decide not to configure the Managing Server at this time, you can still configure the data collector to communicate with the Managing Server later.

18. Enter *1* to integrate with the Managing Server. Otherwise, enter *2* and skip to step 21 on page 92.

    You are prompted to specify the host name of the Managing Server:

    ```
    Enter the host name  or IP address of the  MS
    [default is: 127.0.0.1]:
    ```

19. Enter the fully qualified host name of the Managing Server.

    You are prompted to specify the port number of the Managing Server:

    ```
    Enter the code base port number of the MS
    [default is: 9122]:
    ```

    The port number is codebase port on which the Managing Server is listening.

    Note: The port number is defined as the value of the key "PORT_KERNEL_CODEBASE01" in the .ITCAM61_MS_CONTEXT.properties file located under the Managing Server Home directory. See *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

The configuration tool attempts to connect to the Managing Server and retrieve the value for the *MS_home* directory. If successful, it produces a message similar to the following message:

```
MS home directory is: /opt/IBM/itcam/WebSphere/MS
```

20. If the connection to the Managing Server is *not* successful, you are prompted to enter the value for the *MS_home* directory:

    ```
    Enter ITCAM Managing Server install directory [default is C:\IBM\itcam\WebSphere\MS]:
    ```

    If prompted, enter the value of the *MS_home* directory.

21. The utility prompts you to specify whether you want to configure advanced settings for the Managing Server.

    ```
    Do you want to configure advanced settings for the MS? [1 - Yes, 2 - No]
    [default is: 2]:
    ```

    Enter *1* to configure advanced settings. Otherwise, enter *2* and skip to step 24.

22. You are prompted to enter the range of RMI port numbers that the data collector uses to accept incoming connections from the Managing Server:

    ```
    Enter the RMI port numbers [default is: 8200-8299]:
    ```

    Note: Make sure that the ports are not being blocked by the firewall or other applications.

    Enter the RMI port numbers.

23. You are prompted to enter the range of Controller RMI port numbers:

    ```
    Enter the range of Controller RMI port numbers
    [default is: 8300-8399]:
    ```

    Enter the RMI Controller port numbers.

24. In the **Integration with Tivoli Performance Viewer** section, the utility provides an option for integrating the data collector with Tivoli Performance Viewer (TPV).

    ```
    Do you want to integrate with Tivoli Performance Viewer? [1 - YES, 2 - NO]
    [default is: 2]
    ```

    This is the step that configures ITCAM for WebSphere Application Server 7.2 support for WebSphere Application Server 8.5. Following configuration. metrics are visible in the WebSphere Application Server administrative console in the Tivoli Performance Viewer.

    Enter *1* to integrate the ITCAM Data Collector for WebSphere with the Tivoli Performance Viewer. Otherwise, enter *2*.

25. In the **Advanced Settings** section, the utility provides options for performing advanced configuration of the data collector. The utility prompts you to specify whether to change the garbage collection log path:

    ```
    Do you want to specify a Garbage Collection log path? [1 - YES, 2 - NO] [default is: 2]:
    ```

    Enter *1* to select a garbage collection log path. Otherwise, enter *2* and skip to step 28 on page 93.

26. You are prompted to specify the garbage collection log path:

    ```
    Enter the GC log path:
    ```

    Enter a file name with full path. The Data Collector automatically modifies the log file name, adding the server instance information to it. For example, if you specify `gc.log` as the file name, the actual name is set to *`profile_name.cell_name.node_name.server_name`*`.gc.log` for every configured application server instance.

Important: In the garbage collection log path, you can use WebSphere variables such as${SERVER_LOG_ROOT}. However, do not use templates, such as %pid.

27. You are prompted to specify whether you want to increase the heap size:

```
Do you want to add 128M to the heap size? [1 - YES, 2 - NO]
[default is: 2]:
```

    Enter *2* to retain the existing heap size. Otherwise, enter *1*.

28. In the **Data collector configuration summary** section, the utility provides a summary of the data collector configuration that will be applied to the specified application server instances:

```
1) List of servers selected

  - WAS server: NC047144_AppSrv.NC047144_AppSrv.AppSrv(AppSrv)
      WAS cell: NC047144_AppSrv
       WAS node: NC047144_AppSrv

      WebSphere Profile home    :
        /QIBM/UserData/WebSphere/AppServer/V85/ND/profiles/AppSrv

      wsadmin location          :
        /QIBM/UserData/WebSphere/AppServer/V85/ND/profiles/AppSrv/bin/wsadmin

                   WAS version : 8.5.0.0
                    Deployment : Standalone
                      JVM mode : 32
              Configuration home : /QIBM/ProdData/itcam72/AppSrv/bin/..

2) Integrate with ITCAM Agent for WebSphere Applications : No

3) Integrate with ITCAM for AD Managing Server : Yes

      MS hostname or IP address : nc006008.romelab.it.ibm.com
        MS codebase port number : 9122
              MS home directory : /opt/IBM/itcam/WebSphere/MS

4) Integrate with ITCAM for Transactions : No

5) Integrate with Tivoli Performance Viewer : No

6) Advanced settings :

       Set Garbage Collection log path : No
       Added 128M to the heap size : No


Configuration sections:

 1) List of servers selected
 2) Integrate with ITCAM Agent for WebSphere Applications
 3) Integrate with ITCAM for AD Managing Server
 4) Integrate with ITCAM for Transactions
 5) Integrate with Tivoli Performance Viewer
```

    The summary section provides options to reconfigure parts of the data collector configuration before applying the changes and an option to exit the configuration tool without applying your changes. Enter the number that represents the section you want to edit. Enter * to reconfigure all sections. Enter *a* to accept your changes. Enter *q* to exit the ITCAM Data Collector for WebSphere Configuration Utility without configuring the data collector.

29. When you enter *a* to accept your changes, you are prompted to specify whether you want to create a backup of your current WebSphere Application Server configuration:

```
Do you want to backup current WebSphere configuration? [1 - YES, 2 - NO]
[default is: 2]:
```

30. Enter *1* to create a backup of the current configuration. Otherwise, enter *2*.
31. The changes are applied and a status message is presented to indicate that the configuration of the data collector for the profile is complete:

```
Successfully executed config for Cell: co098170Node01Cell
Node: co098170Node01 Profile: AppSrv01.
```

Important: After configuring the data collector to monitor application server instances, you must restart the instances. The Data Collector configuration takes effect when the application server instances are restarted.

Configuring the ITCAM for WebSphere Applications Data Collector in silent mode

The common ITCAM Data Collector for WebSphere can be configured interactively using the ITCAM Data Collector for WebSphere Configuration Utility. Alternatively, if you want to configure many application server instances, the ITCAM for WebSphere Applications Data Collector can be configured in silent mode.

When you configure the data collector in silent mode, you first specify configuration options in a properties file. A sample properties file, `sample_silent_config.txt`, is packaged with the ITCAM Data Collector for WebSphere Configuration Utility. A sample of a properties file is available here: "Configuration response file" on page 98

Complete the following steps to perform a silent configuration:

1. Log on to the computer on which you want to configure ITCAM for WebSphere Application Server as a user with the appropriate permissions. See "Permissions" on page 86.
2. Use the Start TCP/IP (STRTCP) command to start TCP/IP.
3. Use the Start Host Servers (STRHOSTSVR) command to start Host Servers.
4. Enter the QSH environment by running the STRQSH command in the IBM i main menu.
5. To verify that the instance of the application server that will be monitored by ITCAM for WebSphere Application Server is running, complete the following steps:
   a. Change to the following directory: *AppServer_home*`/profiles/`*profile_name*`/bin`
   b. Run the following command:

      ```
      serverStatus server_name
      ```

      Important: In a Network Deployment environment make sure that the Deployment Manager and the Node Agent are running, and network communication with the Deployment Manager is available.
   c. If the instance of the application server is not started, start the application server.
6. Specify configuration options in the properties file.
7. In the *DC_home*`/bin` directory, run the following command:

   ```
   config_i5 silent &{response_file}
   ```

   For example, `./config_i5.sh -silent silent_config.txt`

8. After configuring the data collector to monitor application server instances, you must restart the instances. The Data Collector configuration takes effect when the application server instances are restarted.

Properties file

When you create your properties file, keep in mind the following considerations:

- A line in the file that starts with the # character is treated as a comment, and is not processed. If the # character is used elsewhere in the line, it is not considered to be the start of a comment.
- Each property is described on a separate line, in the following format: *<property> = value>*.

  <property>
  This is the name of property. The list of valid properties that you can configure is shown in Table 14.

  <value>
  This is the value of the property. Default values for some properties are already provided. You can erase default values to leave property values blank, or empty. Note that an empty value is treated as if the property is not specified, as opposed to using the default value. If you want to use default values, you can simply comment out the property in the file.
- Passwords are in plain text.
- Properties and their values are case sensitive.
- A sample response file, `sample_silent_config.txt`, is available in the *DC_home*`/bin` directory.
- The following table describes the properties that are available when configuring the data collector in silent mode:

Table 14. Silent Configuration Properties

Property	Comment
default.hostip	If the computer system uses multiple IP addresses, specify the IP address for the data collector to use.
Integration of the data collector with the ITCAM for Application Diagnostics Managing Server	
ms.connect	Specifies whether the data collector is configured to connect to the Managing Server in an ITCAM for Application Diagnostics environment. Valid values are *True* and *False*.
ms.kernel.host	Specifies the fully qualified host name of the Managing Server.
ms.kernel.codebase.port	Specifies the codebase port on which the Managing Server is listening.
ms.am.home	Specifies the *MS_home* directory on the Managing Server.
ms.am.socket.bindip	Specifies the IP address or host name to be used by the data collector to communicate with the Managing Server. If more than one network interface or IP address is configured on Data Collector computer system, choose one of them.
ms.firewall.enabled	Specifies whether a firewall is enabled on the data collector host or you have special requirements to change the RMI ports for the data collector. Valid values are *true* and *False*.

Table 14. Silent Configuration Properties (continued)

Property	Comment
ms.probe.controller.rmi.port	If the data collector is behind a firewall or you have special requirements to change the RMI port of Data Collector, set this port number range. Configure this port number as permitted by the firewall for the data collector host. For example: ms.probe.controller.rmi.port=8300-8399 or ms.probe.controller.rmi.port=8300.
ms.probe.rmi.port	If the data collector is behind a firewall, or you have special requirements to change the RMI Port of Data Collector, set this port number range. Configure this port number as permitted by the firewall for the data collector host. For example: ms.probe.rmi.port=8200-8299 or ms.probe.rmi.port=8200.
Integration of the data collector with the Tivoli Performance Monitoring	
tpv.enable	Specifies whether to integrate the data collector with the Tivoli Performance Monitoring when the data collector is included as part of ITCAM for WebSphere Application Server 8.5. Tivoli Performance Monitoring is accessed with the WebSphere Application Server administrative console. Valid values are *True* and *False*.
Integration of the data collector with the ITCAM Agent for WebSphere Applications Monitoring Agent	
temaconnect	Specifies whether the data collector connects to the ITCAM Agent for WebSphere Applications Monitoring Agent (TEMA). Set this property to *False* if you do not want to connect the ITCAM Agent for WebSphere Applications with the Monitoring Agent, if you plan to connect the ITCAM Agent for WebSphere Applications with the Managing Server only, or if you do not have the ITCAM Agent for WebSphere Applications installed. Valid values are *True* and *False*.
tema.host	Specifies the fully qualified host name or IP address of the ITCAM Agent for WebSphere Applications Monitoring Agent.
tema.port	Specifies the port number of the ITCAM Agent for WebSphere Applications Monitoring Agent.
WebSphere Application Server backup	
was.backup.configuration	Specifies whether to back up the current configuration of the WebSphere Application Server configuration before applying the new configuration. Valid values are *True* and *False*.
Advanced configuration settings	
was.gc.custom.path	Specifies whether to set a custom path for the Garbage Collection log.
was.gc.file	Specifies the path to the custom Garbage Collection log. Set this value to a file name with full path. The Data Collector automatically modifies the log file name, adding the server instance information to it. For example, if you specify `gc.log` as the file name, the actual name is set to *`profile_name`*`.`*`cell_name`*`.`*`node_name`*`.`*`node_name`*`.gc.log` for every configured application server instance. **Important:** In the Garbage Collection log path, you can use WebSphere variables, such as ${SERVER_LOG_ROOT}. However, do not use templates, such as %pid.
was.configure.heap	Specifies whether to add 128 MB to the heap size. Each time you run the silent configuration, 128 MB is added to the heap size if this property is set to *true*. Possible values are *True* and *False*.

Table 14. Silent Configuration Properties (continued)

Property	Comment
WebSphere Application Server global security settings	
was.wsadmin.connection.host	Specifies the name of the host to which wsadmin is connecting.
was.wsadmin.connection.type	Specifies the connection protocol for wsadmin to use.
was.wsadmin.connection.port	Specifies the port that wsadmin must use to connect to the WebSphere Application Server.
was.wsadmin.username	Specifies the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server.
was.wsadmin.password	Specifies the password that corresponds to the user specified in the `was.wsadmin.username` property.
WebSphere Application Server settings	
was.appserver.profile.name	Specifies the name of the application server profile you want to configure.
was.appserver.home	Specifies the WebSphere Application Server home directory.
was.appserver.cell.name	Specifies the WebSphere Application Server cell name.
was.appserver.node.name	Specifies the WebSphere Application Server node name.
WebSphere Application Server connection settings	
was.wsadmin.connection.host	Specifies the name of the host to which the wsadmin tool is connecting.
was.wsadmin.connection.type	Specifies the connection protocol for the wsadmin tool to use.
was.wsadmin.connection.port	Specifies the port that the wsadmin tool must use to connect to the WebSphere Application Server.
WebSphere Application Server global security settings	
was.wsadmin.username	Specifies the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server.
was.wsadmin.password	Specifies the password that corresponds to the user specified in the `was.wsadmin.username` property.
was.client.props	Specifies whether to retrieve security settings from a client properties file. Possible values are *True* and *False*.
WebSphere Application Server settings	
was.appserver.profile.name	Specifies the name of the application server profile that you want to configure.
was.appserver.home	Specifies the WebSphere Application Server home directory.
was.appserver.cell.name	Specifies the WebSphere Application Server cell name.
was.appserver.node.name	Specifies the WebSphere Application Server node name.
WebSphere Application Server runtime instance settings	
was.appserver.server.name	Specifies the application server instance within the application server profile to configure. **Tip:** The silent response file can have multiple instances of this property.

Configuration response file

The configuration response file is available in the following location:
DC_home/bin/sample_silent_config.txt

```
################################################################################################
#
#Comments:
#Infrastructure can handle more than 1 server now.
#This file has 2 sections - [DEFAULT SECTION] which is fixed and exists once only
# [SERVER] which will be repeated as many times as there are servers
#
################################################################################################

[DEFAULT SECTION]

#Only to be used if there are Multiple IP Addresses for the machine
#Please use ONLY ip address
#default.hostip=9.9.9.9

#Possible Values are True or False
ms.connect=False
ms.kernel.host=msservername.yourcompany.com
ms.kernel.codebase.port=9122
ms.am.home=/opt/IBM/itcam/WebSphere/MS
ms.am.socket.bindip=servername.yourcompany.com
#ms.firewall.enabled=
ms.probe.controller.rmi.port=8300-8399
ms.probe.rmi.port=8200-8299

#Possible Values are True or False
ttapi.enable=False
ttapi.host=ttservername.yourcompany.com
ttapi.port=5455

#Possible Values are True or False
soa.enable=False

#Possible Values are True or False
tpv.enable=True
```

Reconfiguring the ITCAM Data Collector for WebSphere

If you configured the data collector to monitor one ore more application server instances, you can reconfigure it using the ITCAM Data Collector for WebSphere Reconfiguration Utility.

You can change the data collector connection to the following products or components:

- ITCAM Agent for WebSphere Monitoring Agent
- ITCAM for Application Diagnostics Managing Server
- ITCAM for WebSphere Application Server

You can also reconfigure garbage collection settings and add to the heap size.

To reconfigure data collection for one or more monitored application server instances, complete the following procedure:

1. From the *DC_home*/bin directory, run the `reconfig_i5.sh` script to start the ITCAM Data Collector for WebSphere Reconfiguration Utility.
2. The utility starts and displays the IP addresses of all network cards found on the local computer system and prompts you to specify the interface to use for the data collector:

```
List of TCP/IP interfaces discovered:
  1. 9.111.98.108
Enter a number [default is: 1]:
```

3. Enter the number that corresponds to the IP address to use.

   The utility searches for all application server instances for which the data collector is configured on this host, and prompts you to select one or more application server instances from the list:

   ```
   Choose one or more servers to configure for data collection:
   Application servers not yet configured:
    1. co098170Node01Cell.co098170Node01.server1(AppSrv01)
   Enter a number or numbers separated by commas, or enter * to select all:  1
   ```

   Important: For a Network Deployment or Extended Deployment environment, the Node Agent and Deployment Manager must be running. For a stand-alone environment, application server instances must be running during the configuration of the data collector.

4. Enter the number that corresponds to the application server instance to configure for data collection or enter * to configure all application server instances for data collection. To specify a subset of servers, enter the numbers that represent the servers separated by commas. For example: `1,2,3`. If global security is enabled, userid/password must be set.

5. In the **Integration with ITCAM Agent for WebSphere Applications** section, the utility provides an option for integrating the data collector with the ITCAM Agent for WebSphere Applications.

   You can integrate the data collector with ITCAM Agent for WebSphere Applications, or with the ITCAM for Application Diagnostics Managing Server, or with both. To integrate with ITCAM for Application Diagnostics Managing Server for deep-dive analysis, you must have ITCAM for Application Diagnostics installed.

   ```
   Do you want to integrate with an ITCAM Agent for WebSphere Applications?
    [1 - YES, 2 - NO]
   [default is: 2]: 1
   ```

6. Enter *1* to integrate the data collector with the ITCAM Agent for WebSphere Applications. Otherwise, enter *2* and skip to step 9.

   You are prompted to enter the host name of the ITCAM Agent for WebSphere Applications.

   ```
   Enter the host name or IP address of the ITCAM Agent for WebSphere Applications TEMA:
   [default is: 127.0.0.1]: 127.0.0.1
   ```

7. Enter the fully qualified host name or IP address of the ITCAM Agent for WebSphere Applications Monitoring Agent.

   You are prompted for the port number of the ITCAM Agent for WebSphere Applications Monitoring Agent.

   ```
   Enter the port number of the ITCAM Agent for WebSphere Application TEMA:
   [default is: 63335]: 63335
   ```

   You can change the port that is used for communication between the data collector and the ITCAM Agent for WebSphere Applications Monitoring Agent. The default port is 63335.

8. Enter the port number of the Monitoring Agent.

9. In the **Integration with ITCAM for Application Diagnostics Managing Server** section, the utility provides an option for integrating the data collector with the ITCAM Application Diagnostics Managing Server, installed on a separate UNIX or Windows server, for deep-dive diagnostics.

   You are prompted to specify whether you want to integrate the data collector with a Managing Server.

```
Do you want to integrate with an MS? [1 - YES, 2 - NO]
[default is: 2]: 1
```

Note: If you decide not to configure the Managing Server at this time, you can still configure the data collector to communicate with the Managing Server later.

10. Enter *1* to integrate with the Managing Server. Otherwise, enter *2* and skip to step 13.

    You are prompted to specify the host name of the Managing Server:

    ```
    Enter the host name  or IP address of the  MS
    [default is: 127.0.0.1]: 127.0.0.1
    ```

11. Enter the fully qualified host name of the Managing Server.

    You are prompted to specify the port number of the Managing Server:

    ```
    Enter the code base port number of the MS
    [default is: 9122]: 9122
    ```

    The port number is codebase port on which the Managing Server is listening.

    Note: The port number is defined as the value of the key "PORT_KERNEL_CODEBASE01" in the .ITCAM61_MS_CONTEXT.properties file located under the Managing Server Home directory. See *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

    The configuration tool attempts to connect to the Managing Server and retrieve the value for the *MS_home* directory. If successful, it produces a message similar to the following:

    ```
    MS home directory is: /opt/IBM/itcam/WebSphere/MS
    ```

12. If the connection to the Managing Server is *not* successful, you are prompted to enter the value for the *MS_home* directory:

    ```
    Enter ITCAM Managing Server Install Directory [default is C:\IBM\itcam\WebSphere\MS]:
    ```

    If prompted, enter the value of the *MS_home* directory.

13. The utility prompts you to specify whether you want to configure advanced settings for the Managing Server.

    ```
    Do you want to configure advanced settings for the MS? [1 - Yes, 2 - No]
    [default is: 2]: 1
    ```

    Enter *1* to configure advanced settings. Otherwise, enter *2* and skip to step 18 on page 101.

14. You are prompted to enter the range of RMI port numbers that the data collector uses to accept incoming connections from the Managing Server:

    ```
    Enter the RMI port numbers
    [default is: 8200-8299] 8200-8299
    ```

    Note: Make sure that the ports are not being blocked by the firewall or other applications.

    Enter the RMI port numbers.

15. You are prompted to enter the range of Controller RMI port numbers:

    ```
    Enter the range of Controller RMI port numbers
    [default is: 8300-8399]: 8300-8399
    ```

    Enter the RMI Controller port numbers.

16. You are prompted to enter the RFS port number of the Managing Server:

    ```
    Enter the RFS port number of the MS:  [default is: 9120]:
    ```

Enter the RFS port number.

17. Enter the port number for the interface to the Transaction Collector.
18. In the **Integration with Tivoli Performance Viewer** section, the utility provides an option for integrating the data collector with Tivoli Performance Viewer (TPV).

    ```
    Do you want to integrate with Tivoli Performance Viewer? [1 - YES, 2 - NO]
    [default is: 2]
    ```

    This is the step that configures ITCAM for WebSphere Application Server 7.2 support for WebSphere Application Server 8.5. Following configuration. metrics are visible in the WebSphere Application Server administrative console in the Tivoli Performance Viewer. Enter *1* to integrate the ITCAM Data Collector for WebSphere with the Tivoli Performance Viewer.
19. In the **Advanced Settings** section, the utility provides options for performing advanced configuration of the data collector. The utility prompts you to specify whether to change the garbage collection log path:

    ```
    Do you want to specify a Garbage Collection log path? [1 - YES, 2 - NO]
    [default is: 2]: 2
    ```

    Enter *1* to select a garbage collection log path. Otherwise, enter *2* and skip to step 101.
20. You are prompted to specify the garbage collection log path:

    ```
    Enter the GC log path:
    ```

    Enter a file name with full path. The Data Collector automatically modifies the log file name, adding the server instance information to it. For example, if you specify `gc.log` as the file name, the actual name is set to *`profile_name`*`.`*`cell_name`*`.`*`node_name`*`.`*`server_name`*`.gc.log` for every configured application server instance.

    Important: In the garbage collection log path, you can use WebSphere variables such as`${SERVER_LOG_ROOT}`. However, do not use templates, such as `%pid`.
21. You are prompted to specify whether you want to increase the heap size:

    ```
    Do you want to add 128M to the heap size? [1 - YES, 2 - NO]
    [default is: 2]: 2
    ```

    Enter *2* to retain the existing heap size. Otherwise, enter *1*.
22. In the **Data collector configuration summary** section, the utility provides a summary of the data collector configuration that will be applied to the specified application server instances:

    ```
     1) List of servers selected

       - WAS server: co098170Node01Cell.co098170Node01.server1(AppSrv01)
           WAS cell: co098170Node01Cell
            WAS node: co098170Node01

           WebSphere Profile home    :
              C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01

           wsadmin location          :
             C:\Program Files\IBM\WebSphere\AppServer\bin\wsadmin.bat

                        WAS version : 8.0.0.0
                         Deployment : Standalone
                           JVM mode : 32
                 Configuration home : C\IBM\ITM\dchome
    ```

```
 2) Integrate with ITCAM for SOA Agent : Yes

 3) Integrate with ITCAM Agent for WebSphere Applications : Yes

       TEMA hostname or IP address : 127.0.0.1
                TEMA port number : 63335
                      Monitor GC : No

 4) Integrate with ITCAM for AD Managing Server : No

       MS hostname or IP address : 127.0.0.1
         MS codebase port number : 9122
               MS home directory : /opt/IBM/itcam/WebSphere/MS

 5) Integrate with ITCAM for Transactions : Yes

       Transaction Collector hostname : 127.0.0.1
       Transaction Collector port number : 5455

 6) Integrate with Tivoli Performance Viewer : No

 7) Integrate with ITCAM diagnostics tool : No

 8) Advanced settings :

       Set Garbage Collection log path : No
       Added 128M to the heap size : No

You may accept or update your configuration choices for the following actions:
 1) List of servers selected
 2) Integrate with ITCAM for SOA Agent
 3) Integrate with ITCAM Agent for WebSphere Applications
 4) Integrate with ITCAM for AD Managing Server
 5) Integrate with ITCAM for Transactions
 6) Integrate with Tivoli Performance Viewer
 7) Integrate with ITCAM diagnostics tool
 8) Advanced settings

To modify a section, enter the number. To modify all sections, enter '*'. To accept you
configuration without modifying, enter 'a'.
To quit the selection, enter 'q':
```

The summary section provides options to change parts of the data collector configuration before applying the changes and an option to exit the configuration tool without applying your changes. Enter the number that represents the section you want to edit. Enter * to reconfigure all sections. Enter *a* to accept your changes. Enter *q* to exit the ITCAM Data Collector for WebSphere Reconfiguration Utility.

23. When you enter *a* to accept your changes, you are prompted to specify whether you want to create a backup of your current WebSphere Application Server configuration:

    ```
    Do you want to backup current WebSphere configuration? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

24. Enter *1* to create a backup of the current configuration. Otherwise, enter *2*.
25. The changes are applied and a status message is presented to indicate that the configuration of the data collector for the profile is complete:

    ```
    Successfully executed config for Cell: co098170Node01Cell
    Node: co098170Node01 Profile: AppSrv01.
    ```

Important: After reconfiguring the data collector to monitor an application server instance, you must restart the application server instances. The Data Collector configuration takes effect when the application server instances are restarted.

Migrating Data Collectors to the ITCAM Data Collector for WebSphere 7.2

The ITCAM Data Collector for WebSphere Migration Utility is a menu driven command-line utility for migrating previous versions of the ITCAM Data Collector for WebSphere to version 7.2.

You can upgrade the data collector to use the ITCAM Data Collector for WebSphere 7.2 if your application server instances are being monitoring by any of the following products or components:

- ITCAM for WebSphere 6.1.0.4 or later
- ITCAM Agent for WebSphere Applications 7.1 [ITCAM for Application Diagnostics 7.1]
- ITCAM for WebSphere Application Server 7.2

Note: Before you migrate, ensure that the JAVA_HOME property is cleared.

To migrate monitoring of server instances to the data collector version 7.2, complete the following procedure:

1. Run the following command to start the **ITCAM Data Collector for WebSphere Migration Utility**:

   ```
   migrate_i5.sh
   ```

2. The utility displays the IP addresses of all network cards found on the local computer system and prompts you to specify the interface to use for the data collector:

   ```
   List of TCP/IP interfaces discovered:
     1. 9.111.98.108
   Enter a number [default is: 1]:
   ```

3. Enter the number that corresponds to the IP address to use.

   The utility prompts you to specify from the type of agent that you want to upgrade to ITCAM Data Collector for WebSphere 7.2.

   ```
   List of ITCAM agents whose data collector can be upgraded to the
   ITCAM Data Collector for WebSphere 7.2:

   1. ITCAM for WebSphere 6.1.0.4 or later
   2. ITCAM Agent for WebSphere Applications 7.1 [ITCAM for Application Diagnostics 7.1]
   3. ITCAM for WebSphere Application Server 7.2
   Enter the number [default is: 1]:
   ```

   Enter the number that represents the agent.

4. The utility prompts you to specify the home directory of the previous version of the data collector.

   ```
   Enter the home directory of the data collector to be upgraded:
   ```

5. Enter the home directory of the previous version of the data collector. For example, `/QIBM/ProdData/ecam85mg`

   If you are migrating ITCAM for WebSphere Application Server 7.2, skip to step 6.

6. The utility searches for the list of application server instances configured by the specified Data Collector installation.

   The utility prompts you to select one or more application server instances from the list. The instances might be under different profiles.

   ```
   Choose a Server or Servers to be migrate
    1. x336r1s37-vn01Cell01.x336r1s36-vn01Node03.server3
    2. x336r1s37-vn01Cell01.x336r1s36-vn01Node03.server5
   ```

```
 3. x336r1s37-vn01Cell01.x336r1s36-vn01Node03.server1
Enter a number or numbers separated by a comma, enter '*' to select all
servers listed, or enter 'q' to quit the selection.
```

Attention: If several instances under one profile are monitored, you must select them all for migrating at the same time.

Important:

- For a stand-alone environment, application server instances must be running during the configuration.
- For a Network Deployment or Extended Deployment environment, the node agent and deployment manager must be running.

7. Enter the number that corresponds to the application server instance whose Data Collector is to be migrated or enter * to migrate the data collector of all application server instances. To specify a subset of servers, enter the numbers that represents the servers separated by commas. For example: `1,2,3`.
8. If the data collector was integrated with the ITCAM Agent for WebSphere Monitoring Agent, you are prompted to reenter the host name and port of the Monitoring Agent. In this way, if more than one version of the Monitoring Agent is available, you can connect the data collector to the correct version.

   ```
   Enter the host name or IP address of the ITCAM Agent for WebSphere Applications TEMA:
   [default is: 127.0.0.1]:
   ```
9. Enter the fully qualified host name or IP address of the ITCAM Agent for WebSphere Applications Monitoring Agent. It is on the local host, so the default is correct.

   You are prompted for the port number of the ITCAM Agent for WebSphere Applications Monitoring Agent.

   ```
   Enter the port number of the ITCAM Agent for WebSphere Application TEMA:
   [default is: 63335]:
   ```

   Enter the port number of the Monitoring Agent.
10. The utility determines whether WebSphere Global Security has been enabled for each of the profiles impacted by the migration task.
11. If WebSphere Global Security is found to be enabled on one or more profiles, the utility prompts you to specify whether to retrieve security settings from a client properties file:

    ```
    Do you want to retrieve security settings from a client properties file
    (soap.client.props or sas.client.props)?
    [1 - YES, 2 - NO] [default is: 2]:
    ```

    The Data Collector communicates with the WebSphere Administrative Services using the Remote Method Invocation (RMI) or the SOAP protocol. If global security is enabled for a profile, you must specify the user ID and password of a user who is authorized to log in to the IBM WebSphere Application Server administrative console for the profile. Alternatively, you can encrypt the user name and password and store them in client properties files before configuring the data collector. You must use the `sas.client.props` file for an RMI connection, or the `soap.client.props` file for a SOA connection.

    Enter *1* to allow the utility to retrieve the user name and password from the appropriate client properties file and skip to step 12 on page 105. Otherwise, enter *2* to enter the user name and password.

    ```
    CFG1018I Enter WebSphere admin user name:
    CFG1019I Enter WebSphere admin password:
    ```

Important: It may take some time to log in to the WebSphere Application Server administrative console.
The utility prompts you for the user name and password for each profile whether WebSphere Global Security is enabled.

12. The utility migrates data collection for each application server instance selected and presents a status message that indicates whether the migration of each server completed successfully.
13. When the utility completes the migration of all application server instances configured by the previous version of the data collector, it presents the following message:

    ```
    Migration of the Data Collector has successfully completed with return code 0.
    ```

Important: After migrating the data collector, you must restart the application server instances. The Data Collector configuration takes effect when the application server instances are restarted.
Attention: For instances that were migrated, do not use the configuration utility for the old Data Collector version.

Migrating the ITCAM for WebSphere Applications Data Collector in silent mode

A previous version of the ITCAM Data Collector for WebSphere can be migrated to version 7.2 interactively using the **ITCAM Data Collector for WebSphere Migration Utility**. Alternatively, if you want to migrate many application server instances to use the latest version of the data collector, you can migrate the Data Collectors in silent mode.

When you migrate the data collector in silent mode, you first specify configuration options in a properties file. A sample properties file, `sample_silent_migrate.txt`,is available in the `DC_home/bin` directory. A sample of a completed response file is available here: "Migration response file" on page 107

Note: Before you migrate, ensure that the JAVA_HOME property is cleared.

Complete the following steps to perform a silent migration:

1. Specify configuration options in the properties file.
2. Run the following command:

   ```
   migrate_i5.sh -silent &{response_file}
   ```

3. After configuring the data collector to monitor application server instances, you must restart the instances. The Data Collector configuration takes effect when the application server instances are restarted.

While you are performing a silent migration, you can also configure or reconfigure integration with: ITCAM Agent for WebSphere Applications Monitoring Agent, ITCAM for Application Diagnostics Managing Server, and ITCAM for WebSphere Application Server. To do this, use the silent configuration parameters for these components, as described in "Configuring the ITCAM for WebSphere Applications Data Collector in silent mode" on page 94.

Properties file

When you create the silent response properties file, keep in mind these considerations:

- A line in the file that starts with the # character is treated as a comment, and is not processed. If the # character is used elsewhere in the line, it is not considered to be the start of a comment.
- Each property is described on a separate line, in the following format: *<property> = value*.

  <property>
  This is the name of property. The list of valid properties that you can configure is shown in Table 15.

  <value>
  This is the value of the property. Default values for some properties are already provided. You can erase default values to leave property values blank, or empty. An empty value is treated as if the property is not specified, as opposed to using the default value. If you want to use default values, you can simply comment out the property in the file.
- Passwords are in plain text.
- Properties and their values are case-sensitive.
- A sample response file, `sample_silent_migrate.txt`, is available in the under *DC_home*`/bin` directory.
- The following table describes the available properties for running the migration utility in silent mode:

Table 15. Available properties for running the ITCAM Data Collector for WebSphere Migration Utility in silent mode

Property	Comment
default.hostip	If the computer system uses multiple IP addresses, specify the IP address for the data collector to use.
migrate.type	Type of agent whose Data Collector you want to migrate to the ITCAM Data Collector for WebSphere 7.2. The value must be set to *AD*.
Location of Data Collector to be migrated	
itcam.migrate.home	Specifies the data collector home directory of the old version of the data collector. The directory is not deleted as part of the migration.
ITCAM Agent for WebSphere Applications Monitoring Agent settings	
temaconnect	Specifies whether the data collector connects to the ITCAM Agent for WebSphere Applications Monitoring Agent (TEMA). Set this property to *False* if you do not want to connect the ITCAM Agent for WebSphere Applications with the Monitoring Agent, if you plan to connect the ITCAM Agent for WebSphere Applications with the Managing Server only, or if you do not have the ITCAM Agent for WebSphere Applications installed. Valid values are *true* and *False*. **Note:** The Managing Server is not a component of ITCAM for Applications.
tema.host	Specifies the fully qualified host name or IP address of the ITCAM for Agent for WebSphere Applications Monitoring Agent.
tema.port	Specifies the port number of the ITCAM for Agent for WebSphere Applications Monitoring Agent.
WebSphere Application Server runtime instance settings	

Table 15. Available properties for running the ITCAM Data Collector for WebSphere Migration Utility in silent mode (continued)

Property	Comment
was.appserver.server.name	Specifies the application server instance within the application server profile to migrate to the new version of the data collector. **Note:** The silent response file can have multiple instances of this property.
WebSphere Application Server settings	
was.appserver.profile.name	Specifies the name of the application server profile that you want to configure.
was.appserver.home	Specifies the WebSphere Application Server home directory.
was.appserver.cell.name	Specifies the WebSphere Application Server cell name.
was.appserver.node.name	Specifies the WebSphere Application Server node name.
WebSphere Application Server global security settings	
was.wsadmin.username	Specifies the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server.
was.wsadmin.password	Specifies the password that corresponds to the user specified in the `was.wsadmin.username` property.
WebSphere Application Server connection settings	
was.wsadmin.connection.host	Specifies the name of the host to which the wsadmin tool is connecting.

Migration response file

The migration response file is available in the following location:
DC_home/bin/sample_silent_unconfig.txt

```
################################################################
# Licensed Materials - Property of IBM
#
# 5724-L62
#
# (C) Copyright IBM Corp. 2012 All Rights Reserved.
#
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
#
################################################################

#############################################################################################
#
#Comments:
#Infrastructure can handle more than 1 Application server or 1 ND Server now.
#This file has 2 sections - [DEFAULT SECTION] which is fixed and exists once only
# [SERVER] which will be repeated as many times as there are servers
#
#############################################################################################

[DEFAULT SECTION]

#Only to be used if there are Multiple IP Addresses for the machine
#Please use ONLY ip address
#default.hostip=9.9.9.9

#This has ONLY 1 permitted value as set
#Do not change this
migrate.type=AD
```

```
itcam.migrate.home=c:\ibm\itm\tmaitm6\wasdc\71

#Possible Values are True or False
temaconnect=True
tema.host=127.0.0.1
tema.port=63335

was.wsadmin.connection.host=127.0.0.1
was.wsadmin.username=username
was.wsadmin.password=password

was.appserver.profile.name=AppSrv01
was.appserver.home=/opt/IBM/WebSphere/AppServer
was.appserver.cell.name=yourCellName
was.appserver.node.name=yourNodeName

#Note: As of now, was.appserver.server.name is the only supported parameter in this section
[SERVER]
was.appserver.server.name=server1


#Note: As of now, was.appserver.server.name is the only supported parameter in this section
#If you have multiple servers in the same profile,don't comment out the following lines and
replace with the right server name.
#[SERVER]
#was.appserver.server.name=server2
```

Unconfiguring the WebSphere Application Server Data Collector

If you no longer want the data collector to monitor one or more application server instances, you can unconfigure the data collector for them.

The **ITCAM Data Collector for WebSphere Unconfiguration Utility** is a menu driven command-line utility for unconfiguring the ITCAM Data Collector for WebSphere.

To unconfigure the data collector, complete the following procedure:

1. Run the following command to start the **ITCAM Data Collector for WebSphere Unconfiguration Utility**.

   ```
   unconfig_i5.sh
   ```

   The utility searches for all server instances monitored by the ITCAM Data Collector for WebSphere.

   Important:

   - Application server instances must be running during the unconfiguration procedure.
   - For Network Deployment environment, the node agent and deployment manager must also be running.

   The utility prompts you to select one or more application server instances from the list of configured servers:

   ```
   Choose one or more servers to unconfigure for data collection:
   Application servers configured:
    1. co098170Node01Cell.co098170Node01.server1(AppSrv01)
   Enter a number or numbers separated by commas, or enter * to select all:
   ```

2. If global security is enabled, you must enter a valid username and password.
3. Enter the number that corresponds to the application server instance to unconfigure for data collection or enter * to unconfigure data collection for all application server instances. To specify a subset of servers, enter the numbers that represent the servers separated by commas. For example: `1,2,3`.

4. The utility unconfigures the data collector for the specified application server instances. A status message is presented to indicate that the data collector was successfully unconfigured:

   ```
   Unconfiguration of the Data Collector has successfully completed with return code 0.
   ```

5. After unconfiguring the data collector to monitor application server instances, you must restart the instances. The data collector unconfiguration takes effect when the application server instances are restarted.

Data collection is unconfigured for the specified application server instances.

Unconfiguring the ITCAM for WebSphere Applications Data Collector in silent mode

The ITCAM for WebSphere Applications Data Collector can be unconfigured interactively using the **ITCAM Data Collector for WebSphere Unconfiguration Utility**. Alternatively, if you want to unconfigure data collection for many application server instances, you can unconfigure the Data Collectors in silent mode.

When you run the *unconfig* script in silent mode, the configuration parameters are read from a simple text properties file, that you create in advance. For a sample of the unconfiguration script, see. "The unconfiguration response file" on page 110

Perform the following steps to unconfigure the data collector:

1. Specify configuration options in the properties file.
2. In the *DC_home*/bin directory, run the following command:

   ```
   unconfig_i5.sh -silent &{response_file}
   ```

3. After unconfiguring the data collector to monitor application server instances, you must restart the instances. The data collector unconfiguration takes effect when the application server instances are restarted.

When you create the silent response properties file, keep in mind these considerations:

- A line in the file starting with the # character is treated as a comment, and is not processed. If the # character is used elsewhere in the line, it is not considered to be the start of a comment.
- Each property is described on a separate line, in the following format: *<property> = value>*.

  <property>
  : This is the name of property. The list of valid properties that you can configure is shown in Table 6 on page 18.

  <value>
  : This is the value of the property. Default values for some properties are already provided. You can erase default values to leave property values blank, or empty. An empty value is treated as if the property is not specified, as opposed to using the default value. If you want to use default values, you can simply comment out the property in the file.

- Passwords are in plain text.
- Properties and their values are case-sensitive.
- A sample response file, sample_silent_unconfig.txt, is available in *DC_home*/bin.

Table 16. Available properties for running the ITCAM Data Collector for WebSphere Unconfiguration Utility in silent mode

Property	Comment
WebSphere Application Server global security settings	
was.wsadmin.connection.host	Specifies the name of the host to which wsadmin is connecting.
was.wsadmin.username	Specifies the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server.
was.wsadmin.password	Specifies the password that corresponds to the user specified in the `was.wsadmin.username` property.
WebSphere Application Server settings	
was.appserver.profile.name	Specifies the name of the application server profile you want to unconfigure.
was.appserver.home	Specifies the WebSphere Application Server home directory.
was.appserver.cell.name	Specifies the WebSphere Application Server cell name.
was.appserver.node.name	Specifies the WebSphere Application Server node name.
Backup of the WebSphere Application Server configuration	
was.backup.configuration	Specifies whether to back up the current configuration of the WebSphere Application Server Data Collector configuration before unconfiguring the data collector. Valid values are *true* and *False*.
was.backup.configuration.dir	Specifies the location of the backup directory.
WebSphere Application Server runtime instance settings	
was.appserver.server.name	Specifies an application server instance within the application server profile for which you want to unconfigure the data collector. **Note:** The silent response file can have multiple instances of this property.

The unconfiguration response file

The unconfiguration response file is available in the following location:
DC_home/bin/sample_silent_unconfig_.txt

```
#####################################################################
# Licensed Materials - Property of IBM
#
# 5724-L62
#
# (C) Copyright IBM Corp. 2012 All Rights Reserved.
#
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
#
#####################################################################

#############################################################################################
#
#Comments:
#Infrastructure can handle more than 1 server now.
#This file has 2 sections - [DEFAULT SECTION] which is fixed and exists once only
# [SERVER] which will be repeated as many times as there are servers
#
#############################################################################################

[DEFAULT SECTION]
```

```
was.wsadmin.connection.host=servername.yourcompany.com
was.wsadmin.username=
was.wsadmin.password=

was.appserver.profile.name=AppSrv02
was.appserver.home=C:\Program Files\IBM\WebSphere\AppServer
was.appserver.cell.name=yourITCAMCell
was.appserver.node.name=yourITCAMNode

#Possible Values are True or False
was.backup.configuration=False
was.backup.configuration.dir=/opt/IBM/ITM/dchome/data


#Note: As of now, was.appserver.server.name is the only supported parameter in this section
[SERVER]
was.appserver.server.name=server1


#Note: As of now, was.appserver.server.name is the only supported parameter in this section
#If you have multiple servers in the same profile,don't comment out the following lines and
replace with the right server name.
#[SERVER]
#was.appserver.server.name=server2
```

Chapter 6. Installing and Configuring ITCAM for WebSphere Application Server on z/OS

ITCAM for WebSphere Application Server is an optional component that can be installed after the installation of WebSphere Application Server 8.5.

ITCAM for WebSphere Application Server is composed of a data collector - the ITCAM Data Collector for WebSphere.

You can connect the data collector to any of the following products or components:

- ITCAM for SOA Monitoring Agent
- ITCAM Agent for WebSphere Applications Monitoring Agent
- ITCAM for AD Managing Server
- Tivoli Performance Viewer
- ITCAM for Transactions

The installation files are available in: Integrated Service Management Library.

Installing ITCAM for WebSphere Application Server

1. Download or copy the downloaded pax archive into a directory. This will result in a pax archive, for example :

   ```
   /u/itcam72/downloads/ITCAM72.zOS.DC.pax.Z
   ```

   The installation files are available in Integrated Service Management Library.
2. Create an installation directory, for example: `/u/itcam72`
3. Execute the pax commands to extract the downloaded archive into the installation directory, for example:

   ```
   cd /u/itcam72
   pax-ppx -rvf  /u/itcam72/downloads/ITCAM72.zOS.DC.pax.Z
   ```

   This will result in two directories:

   - `cynzsamp` - sample JCL directory
   - `WebSphere` - ITCAM installation directory

   The user ID used to execute this pax command needs at least read access to the BPX.FILEATTR.PROGCTL FACILITY class profile.
4. Optionally, remount the WebSphere directory as read-only at this point.

To verify the installation was successful, see “Verifying the installation was successful” on page 115.

Overview of the configuration environment

The configuration root directory contains subdirectories that contain configuration files for the server and, symbolic links for the executable files to the target files in *install_home*. All of the executable files are symbolically linked.

When you run the ITCAM Data Collector for WebSphere Configuration Utility (`config.sh`) in prompt mode, you are prompted for the WebSphere Application

Server configuration root directory. The configuration utility discovers the application server instances in the configuration root directory and prompts you to select one of those instances.

For example, if you are using the default configuration root directory and configuring an instance of WebSphere Application Server 8.5 on a node called node1 and a server called server1, the configuration script creates a directory called *config_home*/runtime/was85.node1.server1/.

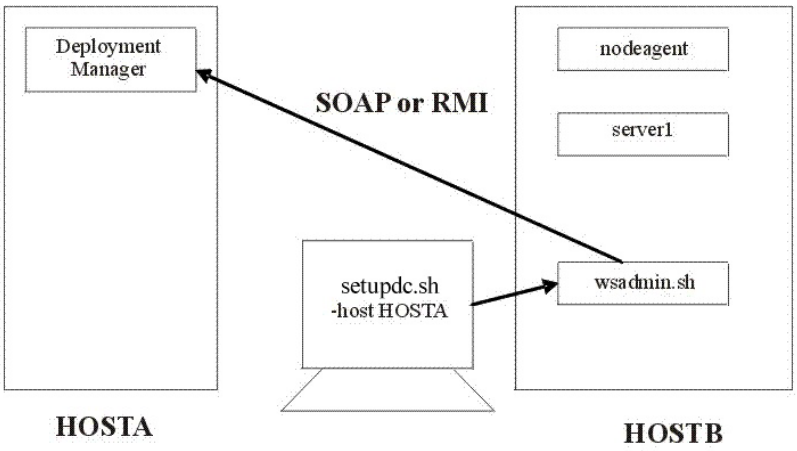
To monitor several application server instances, configure ITCAM for WebSphere Application Server for each instance using the config.sh script. As long as the instances are on the same LPAR, you can use the same configuration directory for all instances. However, you can choose to use different configuration directories to separate test and production environments.

The installation files are read-only after they are loaded up so they can be remounted as standalone.

Configuration in a stand-alone or Network Deployment environment

If you are installing and configuring ITCAM for WebSphere Application Server in a Network Deployment or stand-alone environment, perform the ITCAM for WebSphere Application Server setup for a server on the server host. The configuration utility starts the wsadmin.sh script for the necessary application server configuration changes. The default value for the host name is the local host.

Any local wsadmin.sh script in the server node can be used to configure the application server. For network deployment, communication must be established with the Deployment Manager. In contrast, for stand-alone mode when there is no Deployment Manager, communication is established with the application server. If the wsadmin.properties file specifies a default host name which is the Deployment Manager host name, you do not need to specify the host name.



In the diagram, the user configures server1 on host HOSTB, which is in a node in the cell that is controlled by the deployment manager on HOSTA. The ITCAM config.sh task is performed on HOSTB, but the -host parameter specifies the host name (or IP address) of the deployment manager host. The cell configuration repository is on HOSTA. The config.sh script issues an application server node

synchronization when it is completed and the deployment manager pushes the configuration out to the managed node using the node agent. In stand-alone mode, changes are made directly on the configured server and no synchronization is necessary.

Preconfiguration Steps

Purpose

Before you run the configuration script, perform preconfiguration tasks. Some of the pre-configuration tasks are optional, depending on your environment. The following table provides details of the pre-configuration tasks and the roles required to complete those tasks:

Table 17. Pre-configuration tasks

Task	Role Required
"Verifying the installation was successful"	NA
"Creating a configuration directory" on page 116	System programmer
Optional: "Optional: Enabling user ID and password input from sas.client.props for RMI connector types:" on page 119	Application Server administrator, Security administrator
Optional: "Optional: Enabling user ID and password input from soap.client.props for SOAP connector types:" on page 120	Application Server administrator, Security administrator
"Optional: Update wsadmin.properties with connection details for the deployment manager" on page 120	Application Server administrator
"Verifying the connection to the wsadmin.sh tool" on page 120	Application Server administrator
"Verify prerequisite settings and information before running the configuration script" on page 121	NA
ITCAM for Transactions prerequisites	
"Verify that ITCAM for Transactions contains `cytapi4j.jar`" on page 122	NA

Verifying the installation was successful

About this task

To verify that the installation was successful, complete the following steps:

Procedure

1. In the *Install_home* directory, observe that the folder structure is as follows:

   ```
   bin
   itcamdc
   license
   plugins
   soadc
   toolkit
   ```

2. In the *Install_home*/cynzsamp directory observe the following files: CYNZISRT, CYNZSETU, CYNZUCFG

Creating a configuration directory

After installing ITCAM for WebSphere Application Server, create an ITCAM configuration home directory using the `createcfg.sh` script. This directory will be used by the configuration utility. The default path for this directory is: `/u/itcam72`. This directory is referred to as *config_home*.

The configuration directory is required for configuring the ITCAM for WebSphere Application Server to monitor single or multiple application server instances. Optionally, you can also create an additional configuration directory for a different environment or LPAR.

A Java SDK 1.5 or higher defined (JAVA_HOME defined and in the PATH variable) for the user running the utility.

We recommend running the `createcfg.sh` utility using a WebSphere administrator user ID. If you are running `createcfg.sh` as a root user or a user ID with root privileges, you can specify file and directory ownership. Configuration options for `createcfg.sh` are available here: "Createfg.sh Options" on page 118.

The directory under which `createcfg.sh` utility will create the configuration directory should be owned by a WebSphere Application Server group.

Complete the following steps to create a configuration directory:

1. Determine the name and location of the configuration directory, for example: `/u/itcam72/CONFIG`.

   Note: We recommend that you create a distinct installation and configuration home directory.
2. Launch `createcfg.sh` from the installation directory, for example:

   ```
   cd /u/itcam72/WebSphere/DC/bin
   ./createcfg.sh
   ```
3. The launch page is displayed, for example:

   ```
   ------------------------------------------------------------------------
   -         Create Configuration for z/OS Data Collector                 -
   -                                                                      -
   -  ITCAM Data Collector for WebSphere Create Configuration Utility     -
   -                                                                      -
   -  Create the configuration home directories for ITCAM for AD.         -
   -  At each prompt,enter 'q' to quit the utility or '?' for help.       -
   ------------------------------------------------------------------------

   You only need to run this script once.
    All Data Collectors can share the same configuration home.

           Sun  May 20 16:39:06 EDT 2012

           uid=2403(B8ADMIN) gid=2500(B8CFG) groups=1400(ITGROUP)

   For the installation directory path you should enter
    the logical path (symbolic link) instead of the physical path
    (canonical path name). Doing this will provide flexibility
    for cloning and service migration.
   ```
4. The following message is displayed:

   ```
   Enter installation directory path:  [default is: /u/itcam72/WebSphere/DC]:
   ```

   Enter the installation path, for example: `/install/ITCAM`
5. The following message is displayed:

```
Enter directory name in which to create the ITCAM configuration root:
[default is: /u/itcam72]:
```

Enter the configuration home.

6. The following message is displayed:

```
You may set a new owner for the configuration
 home files and directories.

 The owner may be entered as 'user' or 'user:group'.
 An owner of 'none' will bypass setting the owner.
 **IMPORTANT** Root access is required to change owner.


Enter owner for the configuration home:  [default is: none]:
```

Enter ownership if userid has root capability.

7. The following message is displayed:

```
You may set permissions for the configuration
 home files and directories.

 Permissions are entered in chmod format, which may be either
 numeric, like 664, or symbolic, like: 'a+rX,u+w,g+w,o-w'
 Permissions specified as 'none' will bypass setting permissions.


Enter permissions for the configuration home:  [default is: none]:
```

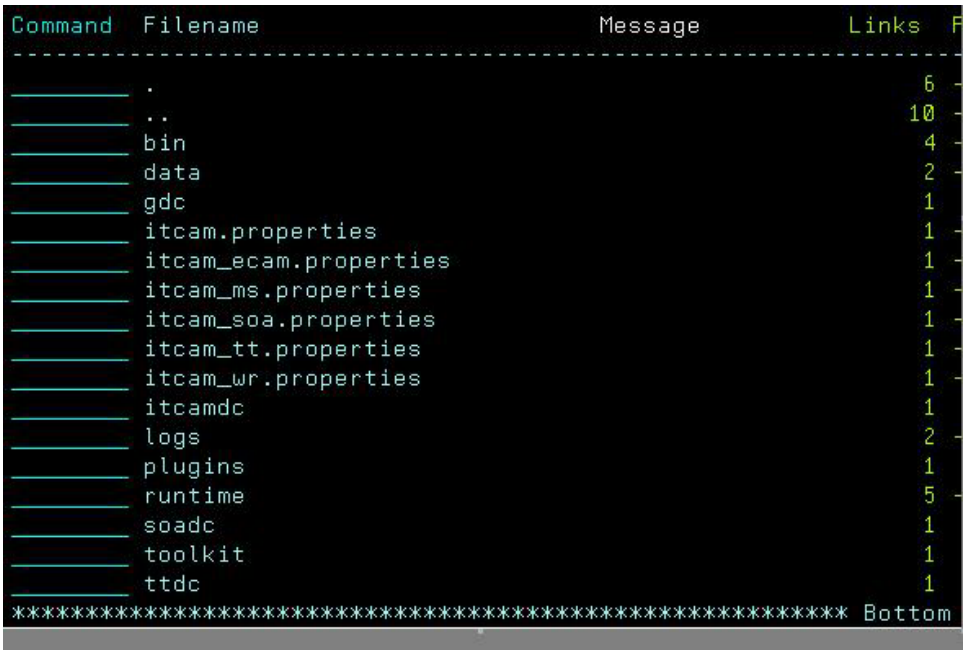
The owner and permissions must be such that the WebSphere application servant region user ID may create and update files in the *config_home* directories.

8. The following message is displayed:

```
Summary of chosen configuration parameters

ITCAM will create an ITCAM for Application Diagnostics configuration home
with the following parameters:

   1)   SMP/E install path : /u/itcam72/WebSphere/DC

   2)     Config home path : /u/itcam72/CONFIG

   3)    Owner will remain : [B8ADMIN:B8CFG]

   4)       Access will be : 775


Type 'a' to accept, and continue to build the configuration home, - or -
 type 'r' to respecify, or -
 type 'q' to quit:
```

Enter a to continue.

9. Verify the configuration home directory was created successfully, observe the following structure:



Createfg.sh Options

The parameters for `createcfg.sh` are described in the following table:

Command-prompt option	Description	Equivalent environment variable and value
`-batch`	Turns off prompting so that the script runs to completion with no user interaction. This parameter is required when running the background, as in the CYEZISRT job. The default is to prompt for all optional values.	`ITCAM_BATCH=y`
`-config` *`config_home`*	Specifies the full path of the configuration home directory. The default is `/u/itcam72`.	`ITCAM_CONFIG=config_home`
`-install` *`install_home`*	Specifies the full path of the *`install_home`* directory. You can specify a path containing a symbolic link for flexibility. The default is the current directory where the `createcfg.sh` script is being executed.	`ITCAM_INSTALL=`*`install_home`*
`-owner` *`user[:group]`*	Sets the owner of the files and directories in *`config_home`*. A user or group can also be specified using the `chown` command. If the current user does not have superuser privilege, this parameter is ignored. The default is to leave the ownership of the files and directories in *`config_home`* unchanged.	`ITCAM_OWNER=`*`user[:group]`*

Command-prompt option	Description	Equivalent environment variable and value
`-access permissions`	Sets the access permissions for the files and directories in the *config_home* directory. The permissions are specified in the same format as for chmod, and can be either numeric format, such as, `664` or symbolic format, such as, `a+Xr,u+w,g+w,o-w`. The default is to leave the access permissions of the files and directories in *config_home* unchanged.	`ITCAM_ACCESS=permissions`

Security Considerations

You must login as a WebSphere administrator who has permission to administer the application server configuration before you run the `./createcfg.sh` or `./config.sh` script.

There are two optional steps you can perform in advance of running the configuration utility:

1. **Encrypt the user name and password and store them in client properties files**: The data collector communicates with the WebSphere Administrative Services using the Remote Method Invocation (RMI) or the SOAP protocol. When you run the configuration script, if global security is enabled for a profile, you must specify the user ID and password of a user who is authorized to log in to the IBM WebSphere Application Server administrative console for the profile. Alternatively, before running the configuration script, you can encrypt the user name and password and store them in client properties files. You must use the `sas.client.props` file for an RMI connection, or the `soap.client.props` file for a SOAP connection. See

   RMI connector type
   SOAP connector type
2. **Update the `wsadmin.properties` file with the connection details for the deployment manager**: If you update the `wsadmin.properties` file with the connection details for the deployment manager, then you will not have to specify details for the deployment manager when you execute the configuration script. See "Optional: Update wsadmin.properties with connection details for the deployment manager" on page 120

Optional: Enabling user ID and password input from sas.client.props for RMI connector types:

About this task

When you use an RMI connection to WebSphere Application Server and global security is enabled, you can use the configuration script to retrieve the user ID and password from the `sas.client.props` file. When you retrieve the user ID and password from the `sas.client.props` file, you do not have to specify the -user option (or the ITCAM_USER environment variable) and the -password option (or the ITCAM_PASSWORD environment variable). Complete the following procedure:

Procedure

1. Set the following properties in the `sas.client.props` file:

```
com.ibm.CORBA.loginSource=properties
com.ibm.CORBA.securityEnabled=true
com.ibm.CORBA.loginUserid=user_ID
com.ibm.CORBA.loginPassword=password
```

2. To encrypt the password, run the following command from the directory that contains the `wsadmin.sh` script:

```
./PropFilePasswordEncoder.sh path_to_props_file/sas.client.props com.ibm.CORBA.loginPassword
```

Optional: Enabling user ID and password input from soap.client.props for SOAP connector types:

About this task

When you use a SOAP connection to WebSphere Application Server and global security is enabled, you can use the configuration script to retrieve the user ID and password from the `soap.client.props` file. When you retrieve the user ID and password from the `soap.client.props` file, you do not have to specify the -user option (or the ITCAM_USER environment variable) and the -password option (or the ITCAM_PASSWORD environment variable). Complete the following procedure:

Procedure

1. Set the following properties in the `soap.client.props` file:

```
com.ibm.SOAP.securityEnabled=true
com.ibm.SOAP.loginUserid=user_ID
com.ibm.SOAP.loginPassword=password
```

2. To encrypt the password, run the following command from the directory that contains the `wsadmin.sh` script:

```
./PropFilePasswordEncoder.sh path_to_props_file/soap.client.props com.ibm.SOAP.loginPassword
```

Optional: Update wsadmin.properties with connection details for the deployment manager

If you update the `wsadmin.properties` file with the connection details for the deployment manager, then you will not have to specify details for the deployment manager when you execute the configuration script.

Procedure

1. Open the `wsadmin.properties` file and update as follows.

```
-host
com.ibm.ws.scripting.host=dmgrhost

-conntype
com.ibm.ws.scripting.connectionType=conntype

-port
com.ibm.ws.scripting.port=port
```

2. Save and close the `wsadmin.properties` file.

Verifying the connection to the wsadmin.sh tool

About this task

The configuration utility must be able to connect to the WebSphere Application Server `wsadmin.sh` tool.

Procedure

1. Ensure that the region size is sufficient, particularly if you are running under TSO using OMVS. The `wsadmin.sh` tool starts a JVM and uses a significant amount of memory.

2. If you are in a stand-alone environment, ensure that the instance of the application server that is being monitored by ITCAM for WebSphere Application Server is running. If you are in a Network Deployment environment, ensure that the Deployment Manager is running.
3. Run `wsadmin.sh` tool from the directory in which it is located:

   ```
   ./wsadmin.sh -conntype SOAP|RMI -port port -host hostname -user
     user_ID -password password
   ```

Results

If you connect successfully to the `wsadmin.sh` tool, a message similar to the following is displayed:

```
WASX7209I: Connected to process "dmgr" on node node1  using SOAP connector;
The type of process is: DeploymentManager
WASX7029I: For help, enter: "$Help help"
```

What to do next

If you cannot connect successfully to the `wsadmin.sh` tool, a message similar to the following is displayed:

```
WASX7246E: Cannot establish "SOAP" connection to host "SOMEHOST"...
```

If you cannot connect successfully to the `wsadmin.sh` tool, there might be a problem with your installation or configuration of IBM WebSphere Application Server. Contact IBM Software Support. Correct the problem before attempting to proceed; it is not possible to run the configuration script if a successful connection can't be made to the `wsadmin.sh` tool.

Verify prerequisite settings and information before running the configuration script

Some prerequisite settings and information must be verified before you run the configuration script.

512 MB of virtual storage

You need at least 512 MB on the ASSIZEMAX parameter in the RACF® OMVS segment for the user to run the configuration script. It is recommended that you run the configuration script using a z/OS UNIX System Services telnet session, but if you use OMVS under TSO, make sure that the TSO procedure you use has a large enough REGION size to support running the configuration script.

Adjusting ports for firewalls or for use with other applications

During the configuration, specify port numbers or accept the defaults. Make sure that you record the port numbers. Make sure and that the firewall does not prevent communication on the specified ports.

For a Network Deployment environment, ITCAM for WebSphere Application Server uses the SOAP or RMI port to communicate with the Deployment Manager, which is usually located on a different host. In this case, take special care that the firewall does not block communication on this port.

Application Server instances must be running

For a Network Deployment or Extended Deployment environment, the Node Agent and the Deployment Manager must be running. For a stand-alone WebSphere configuration, application server instance must be running during the configuration of the data collector.

Verify that ITCAM for Transactions contains `cytapi4j.jar`

About this task

Before you configure communication with ITCAM for Transactions, verify that ITCAM for Transactions contains a directory with the `cytapi4j.jar` file, and the `libcytapi64.so` and `libcytapi.so` external links.

Procedure

1. Run the following command from the Transactions Tracking directory by running the following UNIX System Services command: `ls -la`.
2. The results should be displayed as follows:

```
41200 Aug 11 15:00 cytapi4j.jar
8 Aug 25 23:06 libcytapi64.so -> CYTATJ64
8 Aug 25 23:06 libcytapi.so -> CYTATJAV
```

3. Add hlq.SCYTLOAD to LINKLIST or specify hlq.SCYTLOAD in the STEPLIB of the WebSphere Application Server servant region started task (STC) procedure.

Execute the configuration script

To configure the ITCAM Data Collector for WebSphere use the ITCAM Data Collector for WebSphere Configuration Utility. Start the utility with `./config.sh` located here: *`config_home`*`/bin`.

The configuration script includes default configuration values. You can run the configuration script in prompt mode or in batch mode.

If you run the configuration script in prompt mode, you can change the default configuration values using either of the following methods:

- Specify options in the command-prompt before running the script.
- Export the equivalent environment variables before running the configuration script. The configuration script will then use the exported environment variables as the default values. When you are prompted for a value, press **Enter** and the exported equivalent environment variable is used. Command-prompt arguments override exported environmental variables. For details on running the configuration script in prompt mode, see "Executing the configuration script in prompt mode" on page 123.

If you run the configuration script in batch mode, you are not prompted for values. Before running the configuration script, set the values using one of the following methods:

- Specify options at a command-prompt that runs `config.sh` in batch mode
- Export the equivalent environment variable before running `config.sh` in batch mode. For details on running the configuration script in batch mode, see "Executing the configuration script in prompt mode" on page 123.

If you are configuring the ITCAM for WebSphere Application in an environment where there are no other ITCAM products configured for application servers

within the same profile, you can integrate the data collector with the Tivoli Performance Viewer and accept the default values.

Executing the configuration script in prompt mode

You must configure the data collector for each application server instance that you want to monitor.

The ITCAM Data Collector for WebSphere Configuration Utility referred to here as the *configuration script* is a menu driven command-line utility for configuring the ITCAM Data Collector for WebSphere.

When you run the configuration script in prompt mode, when you are prompted for values, the applicable default value is displayed in brackets at the end of the prompt. If you enter no value, the script uses the default value. The default value also provides an example of the format of the value that is required.

The default location for the configuration setup script is: `/u/itcam72/bin`. For a list of the options for running the script command, see "Configuration Options" on page 130.

You must login as a WebSphere administrator who has permission to administer the application server configuration before you run the `config.sh` script.

To configure the data collector to monitor one or more server instances, complete the following procedure:

1. Log in as a WebSphere administrator with permission to administer the application server configuration. You may use "su -s userid" if you have the appropriate permission.
2. Complete one of the following procedures:
   a. If you are running the application server in a Network Deployment environment, make sure that the Deployment Manager and the node agent are running.
   b. If you are running the application server in a stand-alone environment, ensure that the instance of the application server that is being monitored by ITCAM for WebSphere Application Server is running.
3. To set any of the configuration options as environment variables before running the configuration script, export the environment variables. By setting options in the command-prompt, the `config.sh` script uses them as the new default values. Defaults on the command-prompt override defaults that are set by exported environment variables. Here are examples of how to export an environment variable from a command-prompt:

   ```
   export ITCAM_CONNTYPE=RMI
   export ITCAM_USER=b8admin
   ```

4. When you export these variables, the `config.sh` script uses them as the default values. When prompted, you do not need to enter a value, instead just press Enter.
5. To run the configuration script, run the following command:

   ```
   ./config.sh [options]
   ```

6. The utility starts and displays the IP addresses of all network cards found on the local computer system and prompts you to specify the interface to use for the data collector:

```
List of TCP/IP interfaces discovered:
  1. 9.111.98.108
Enter a number [default is: 1]:
```

7. Enter the number that corresponds to the IP address to use.

   The utility prompts you to enter the WebSphere Application Server configuration home directory:

   ```
   Enter WebSphere home directory [default is: /u/WAS80]:
   ```

8. Enter the HFS path name of *AppServer_home*, for example, `/u/WAS800B/beta/tvt7006/AppServer` and press Enter. The configuration script uses this path to search for the `wsadmin.sh` script. The `wsadmin.sh` script is used to configure the target application server for ITCAM for WebSphere Application Server monitoring. If the path is a valid, the utility issues the following message:

   ```
   Searching for wsadmin locations under WAS configuration home:
   /u/WAS800B/beta/tvt7006/AppServer
   ```

   If the path is not a valid WebSphere Application Server configuration home directory, the utility issues a message, for example

   ```
   Searching for wsadmin locations under directory: /u/WAS800B/beta/tvt7006
   ```

9. The utility prompts you to select which of the listed `wsadmin.sh` scripts to use

   ```
   Choose WebSphere wsadmin.sh to use
   1. /u/WAS800B/beta/tvt7006/AppServer/bin/wsadmin.sh
   2. /u/WAS800B/beta/tvt7006/AppServer/profiles/default/bin/wsadmin.sh
   Enter a number [default is: 2]:
   ```

   Note: The list should not include Deployment Manager or Node Manager servers. Any application server `wsadmin.sh` script will work, but we recommend the `wsadmin.sh` script in the *AppServer_home*`/profiles/default/bin` directory because the `wsadmin.sh` script uses the `wsadmin.properties` file associated with it.

10. Enter the number that corresponds to the `wsadmin.sh` that you want to use. The utility then returns the value of the WebSphere Application Server profile home:

    ```
    WebSphere Home: /u/WAS800B/beta/tvt7006/AppServer WebSphere Profile: default
    ```

11. The utility indicates whether WebSphere Global Security is enabled for the WebSphere Application profile you have specified:

    ```
    WebSphere Global Security is enabled.
    ```

    If global security is not enabled, skip to step 14 on page 125.

12. The utility prompts you to specify whether to retrieve security settings from a client properties file:

    ```
    Do you want to retrieve security settings from a client properties file
    (soap.client.props or sas.client.props)?
    [1 - YES, 2 - NO] [default is: 2]:
    ```

    The Data Collector communicates with the WebSphere Administrative Services using the Remote Method Invocation (RMI) or the SOAP protocol. If global security is enabled for a profile, you must specify the user ID and password of a user who is authorized to log in to the IBM WebSphere Application Server administrative console for the profile. Alternatively, you can encrypt the user name and password and store them in client properties files before configuring the data collector. You must use the `sas.client.props` file for an RMI connection, or the `soap.client.props` file for a SOAP connection.

Enter *1* to allow the utility to retrieve the user name and password from the appropriate client properties file and skip to step 14. Otherwise, enter *2* to enter the user name and password.

```
CFG1018I Enter WebSphere admin user name:
CFG1019I Enter WebSphere admin password:
```

13. While the search is executing the utility displays an updating status:

```
Searching for servers under profile: default
Connecting to profile.....................
Start finding servers for profile default
Installing or upgrading IBM Tivoli Composite Application Manager for SOA on Windows 3
Processing default.............
Finding servers done successfully for profile default
Finished finding servers for profile default
Successfully executed searching servers for Profile: default
```

14. The utility searches for all application server instances under the default profile. The utility displays all servers that have not been configured yet for data collection and all servers that have been configured to use the current version of the ITCAM Data Collector for WebSphere.

    The utility prompts you to select one or more application server instances from the list:

```
Choose one or more servers to configure/unconfigure for data collection:
Application servers not yet configured:
1. beta.tvt7006.b8sr00f(default)
Application Servers configured by the current version:
2. beta.tvt7006.b8sr00a(default)
3. beta.tvt7006.b8sr00b(default)
Enter a number or numbers separated by commas, or enter * to select all:
```

    Note: For a Network Deployment or Extended Deployment environment, the Node Agent and Deployment Manager must be running. For a stand-alone environment, application server instances must be running during the configuration of the data collector.

    Note: Ensure that the application server instances you select are the actual nodes that host the applications or services you want to monitor.

15. Enter the number that corresponds to the application server instance to configure for data collection or enter * to configure all application server instances for data collection. To specify a subset of servers, enter the numbers that represent the servers separated by commas. For example: `1,2,3`.

16. In the **Integration with ITCAM for SOA Agent** section, the utility provides an option for integrating the data collector with the ITCAM for SOA agent.

```
Do you want to integrate with an ITCAM for SOA Agent? [1 - YES, 2 - NO]
[default is: 2]:
```

    You must install and configure the ITCAM for SOA Agent and its application support files, and optionally configure topology support to complete the installation and configuration of the ITCAM for SOA Agent. For more information about installing and configuring the ITCAM for SOA Agent, see *IBM Tivoli Composite Application Manager for SOA Installation Guide* 7.1.1.

    Enter *1* to integrate the data collector with the ITCAM for SOA Agent. Otherwise, enter *2*.

17. In the **Integration with ITCAM Agent for WebSphere Applications** section, the utility provides an option for integrating the data collector with the ITCAM Agent for WebSphere Applications.

    You can integrate the data collector with ITCAM Agent for WebSphere Applications, or with the ITCAM for Application Diagnostics Managing Server, or with both.

```
Do you want to integrate with an ITCAM Agent for WebSphere Applications?
 [1 - YES, 2 - NO]
[default is: 2]:
```

You must install and configure the ITCAM Agent for WebSphere Applications and its application support files to complete the installation and configuration of the ITCAM Agent for WebSphere Applications. For more information about installing and configuring the ITCAM Agent for WebSphere Applications, see *IBM Tivoli Composite Application Manager Agent for WebSphere Applications Installation and Configuration Guide*.

18. Enter *1* to integrate the data collector with the ITCAM Agent for WebSphere Applications. Otherwise, enter *2* and skip to step 21.

    You are prompted to enter the host name of the ITCAM Agent for WebSphere Applications.

    ```
    Enter the host name or IP address of the ITCAM Agent for WebSphere Applications TEMA:
    [default is: 127.0.0.1]:
    ```

19. Enter the fully qualified host name or IP address of the ITCAM Agent for WebSphere Applications Monitoring Agent. The Monitoring Agent is located on the local host, so you do not need to change the default.

    You are prompted for the port number of the ITCAM Agent for WebSphere Applications Monitoring Agent.

    ```
    Enter the port number of the ITCAM Agent for WebSphere Application TEMA:
    [default is: 63335]:
    ```

    You can change the port that is used for communication between the data collector and the ITCAM Agent for WebSphere Applications Monitoring Agent. This communication is on the local host; the default port is 63335. You can change the port at a later time, but it is normally most convenient to set it when initially configuring the data collector.

20. Enter the port number of the Monitoring Agent.

21. In the **Integration with ITCAM for Application Diagnostics Managing Server** section, the utility provides an option for integrating the data collector with the ITCAM for Application Diagnostics Managing Server, installed on a separate Windows, Linux, or UNIX server, for deep-dive diagnostics. For information about installing the Managing Server, see *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

    You are prompted to specify whether you want to integrate the data collector with a Managing Server.

    ```
    Do you want to integrate with an MS? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

    Note: To integrate with ITCAM for Application Diagnostics Managing Server for deep-dive analysis, you must have ITCAM for Application Diagnostics 7.1 installed.

    Note: If you decide not to configure the Managing Server at this time, you can still configure the data collector to communicate with the Managing Server later.

22. Enter *1* to integrate with the Managing Server. Otherwise, enter *2* and skip to step 25 on page 127.

    You are prompted to specify the host name of the Managing Server:

    ```
    Enter the host name  or IP address of the  MS
    [default is: 127.0.0.1]:
    ```

23. Enter the fully qualified host name of the Managing Server.

You are prompted to specify the port number of the Managing Server:

```
Enter the code base port number of the MS
[default is: 9122]:
```

The port number is codebase port on which the Managing Server is listening.

Note: The port number is defined as the value of the key "PORT_KERNEL_CODEBASE01" in the .ITCAM61_MS_CONTEXT.properties file located under the Managing Server Home directory. See *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

The configuration tool attempts to connect to the Managing Server and retrieve the value for the *MS_home* directory. If successful, it produces a message similar to the following message:

```
MS home directory is: /opt/IBM/itcam/WebSphere/MS
```

24. If the connection to the Managing Server is *not* successful, you are prompted to enter the value for the *MS_home* directory:

    ```
    Enter ITCAM Managing Server install directory [default is C:\IBM\itcam\WebSphere\MS]:
    ```

    If prompted, enter the value of the *MS_home* directory.

25. The utility prompts you to specify whether you want to configure advanced settings for the Managing Server.

    ```
    Do you want to configure advanced settings for the MS? [1 - Yes, 2 - No]
    [default is: 2]:
    ```

    Enter *1* to configure advanced settings. Otherwise, enter *2* and skip to step 29.

26. You are prompted to enter the range of RMI port numbers that the data collector uses to accept incoming connections from the Managing Server:

    ```
    Enter the RMI port numbers [default is: 8200-8299]:
    ```

    Note: Make sure that the ports are not being blocked by the firewall or other applications.

    Enter the RMI port numbers.

27. You are prompted to enter the range of Controller RMI port numbers:

    ```
    Enter the range of Controller RMI port numbers
    [default is: 8300-8399]:
    ```

    Enter the RMI Controller port numbers.

28. You are prompted to enter the RFS port number of the Managing Server:

    ```
    Enter the RFS port number of the MS: [default is: 9120]:
    ```

    Enter the RFS port number.

29. In the **Integration with ITCAM for Transactions** section, the utility provides an option for integrating the data collector with ITCAM for Transactions.

    Note: To integrate the data collector with ITCAM for Transactions, you must install ITCAM for Transactions within an IBM Tivoli Monitoring environment. You are prompted to specify whether you want to integrate with ITCAM for Transactions:

    ```
    Do you want to integrate with ITCAM for TT? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

    After you have configured the data collector to support ITCAM for Transactions, you then must perform some additional configuration. For details of further configuration options and how to view the aggregated

transaction information, see *IBM Tivoli Composite Application Agent for WebSphere Applications Configuring and Using TTAPI*.

30. Enter *1* to integrate the data collector with ITCAM for Transactions. Otherwise, enter *2* and skip to step 34.
31. You are prompted to specify the ITCAM for Transactions z/OS subsystem name:

    ```
    Enter the ITCAM for Transactions z/OS subsystem name [default is: CYTZ]:
    ```

32. Enter the ITCAM for Transactions z/OS subsystem name.
33. You are prompted to specify the ITCAM for Transactions z/OS directory path:

    ```
    Enter the ITCAM for Transactions z/OS directory path [default is: /usr/lpp/cyt/jar/IBM ]
    ```

34. In the **Integration with Tivoli Performance Viewer** section, the utility provides an option for integrating the data collector with Tivoli Performance Viewer (TPV).

    ```
    Do you want to integrate with Tivoli Performance Viewer? [1 - YES, 2 - NO]
    [default is: 2]
    ```

    This is the step that configures ITCAM for WebSphere Application Server 7.2 support for WebSphere Application Server 8.5. Following configuration. metrics are visible in the WebSphere Application Server administrative console in the Tivoli Performance Viewer.

    ITCAM for WebSphere Application Server 7.2 support for WebSphere Application Server 8.5 includes the ITCAM Data Collector for WebSphere. Enter *1* to integrate the ITCAM Data Collector for WebSphere with the Tivoli Performance Viewer. Otherwise, enter *2*.
35. In the **Advanced Settings** section, the utility provides options for performing advanced configuration of the data collector. The utility prompts you to specify whether to change the garbage collection log path:

    ```
    Do you wish GC log data included in output? [1 - YES, 2 - NO] [default is: 2]:
    Enter 1 to include verbose GC output in the WebSphere output.
    Otherwise, enter 2..
    ```

36. In the **Data collector configuration summary** section, the utility provides a summary of the data collector configuration that will be applied to the specified application server instances:

    ```
    1) List of servers selected

       - WAS server: beta.tvt7006.b8sr00a(default)
           WAS cell: beta
            WAS node: tvt7006

           WebSphere Profile home    :
             /u/WAS800B/beta/tvt7006/AppServer/profiles/default

           wsadmin location          :
             /u/WAS800B/beta/tvt7006/AppServer/profiles/default/bin/wsadmin.sh

                        WAS version : 8.0.0.1
                          Deployment : Network deployment
                            JVM mode : 64bit
                 Configuration home : /u/itcam72/CONFIG

     2) Integrate with ITCAM for SOA Agent : Yes

     3) Integrate with ITCAM Agent for WebSphere Applications : Yes

           TEMA hostname or IP address : 127.0.0.1
                    TEMA port number : 37275
                          Monitor GC : No

     4) Integrate with ITCAM for AD Managing Server : Yes
    ```

```
      MS hostname or IP address : devapp-lnx-s06.usca.ibm.com
        MS codebase port number : 9122
              MS home directory : /opt/bvt/IBM/itcam/WebSphere/MS

 5) Integrate with ITCAM for Transactions : Yes

                    TT subsystem : CYTZ
                    TT directory : /u/itt72/smpe/usr/lpp/cyt/jar/IBM

 6) Integrate with Tivoli Performance Viewer : Yes

 7) Advanced settings :

                 Collect SMF data : Leave
              GC output to sysout : No


Configuration sections:
 1) List of servers selected
 2) Integrate with ITCAM for SOA Agent
 3) Integrate with ITCAM Agent for WebSphere Applications
 4) Integrate with ITCAM for AD Managing Server
 5) Integrate with ITCAM for Transactions
 6) Integrate with Tivoli Performance Viewer
 7) Advanced settings
```

The summary section provides options to reconfigure parts of the data collector configuration before applying the changes and an option to exit the configuration tool without applying your changes. Enter the number that represents the section you want to edit. Enter * to reconfigure all sections. Enter *a* to accept your changes. Enter *q* to exit the ITCAM Data Collector for WebSphere Configuration Utility without configuring the data collector.

Up to this point, no configuration changes have been made, which means, it is safe to exit without affecting the WebSphere Application Server configuration.

37. When you enter *a* to accept your changes, you are prompted to specify whether you want to create a backup of your current WebSphere Application Server configuration:

    ```
    Do you want to backup current WebSphere configuration? [1 - YES, 2 - NO]
    [default is: 2]:
    ```

38. Enter *1* to create a backup of the current configuration. Otherwise, enter *2*.
39. The changes are applied and a status message is presented to indicate that the configuration of the data collector for the profile is complete:

    ```
    Successfully executed Configuring for Cell: beta Node: tvt7006 Profile: default
    ```

40. After configuring the data collector to monitor application server instances, you must restart the instances. The Data Collector configuration takes effect when the application server instances are restarted.

The ITCAM Data Collector for WebSphere Configuration Utility creates a log of all the configuration operations, including any error conditions. You might be requested to provide the log contents to IBM software support. The log file is located here: *config_home*/data/config-trace.log

Executing the configuration script in batch mode

Executing the configuration script in batch (auto-run) mode eliminates the need for command-prompt-execution prompting.

About this task

Complete the following procedure to run the configuration script in batch (auto-run) mode by running the `config.sh` script through a command-prompt:

Procedure

1. Log in as a WebSphere administrator who has permission to perform the application server configuration.
2. Complete one of the following procedures:
   - If you are running the application server in a Network Deployment environment, ensure that the Deployment Manager and the node agent are running.
   - If you are running the application server in a non-Network Deployment environment, ensure that the instance of the application server that is being monitored by ITCAM for WebSphere Application Server is running.
3. Run `config.sh` from a command-prompt. Complete the same procedure you use to run `config.sh` in prompt mode, but indicate all the options you want to specify at the command-prompt (or by exporting the corresponding environment variable before running `config.sh`). Be sure to indicate options that are required for running in batch mode. See "Executing the configuration script in prompt mode" on page 123, and .

Results

The configuration script creates a log of all the configuration operations that it performs. You can review the log for any error conditions, and you might be requested to provide the log contents to IBM software support for problem diagnosis. The log file is called `config.log` and is located in the runtime directory under *config_home*, for example, `/u/itcam72/runtime/config.log`.

For successful configuration, look for messages similar to the following message:

```
Successfully configured data collector for server server1
```

For a sample of a batch mode script, see "Sample batch mode script" on page 137

Configuration Options

Standard Configuration Options

The following table describes the options in the configuration script. These are the standard options required to configure a WebSphere Application Server instance for data collection.

Table 18. Standard Configuration Options

Command-prompt option	Description	Equivalent environment variable and value	Default
`-log` *`logfile_name`* | `-nolog`	Indicates whether you want to create a log of the configuration operations. If you indicate `-log`, you can specify a location. The default location is: *`config_home`*`/data/config-trace.log`. For example: `/u/itcam72/data/config-trace.log`.	ITCAM_LOG	*`config_home`*`/data`
`-help`	Provides help on the options.	ITCAM_HELP	
`-batch`	Indicates whether you want to run the configuration script in batch mode. For details about batch mode.	`ITCAM_BATCH=y`	The default is to run in prompt mode.

Table 18. Standard Configuration Options (continued)

Command-prompt option	Description	Equivalent environment variable and value	Default
`-config config_home`	Indicates the ITCAM for WebSphere Application Server configuration directory, for example: `/u/itcam72` The value for this option is generated automatically. To override the automatically generated value, specify a path to be used in the configuration process. This path must resolve to the actual ITCAM for WebSphere Application Server configuration home path. For example, if the *config_home* you want is `/u/itcam72`, but due to symbolic links, the physical path for this logical path is `/V1R8M0/u/itcam72`. enter `-config /u/itcam72`. This means that you can change the physical path without reconfiguring ITCAM for WebSphere Application Server. If you need to change the *config_home* value, rerun `createcfg.sh`.	`ITCAM_CONFIG=config_home`	The default is the `bin` directory.
`-conntype SOAP | RMI`	Specifies the connection type for communications with `wsadmin.sh`.	`ITCAM_CONNTYPE= connect_type`	The default is to use the connection type specified in the `wsadmin.properties` file associated with the `wsadmin.sh` script you have chosen. If `wsadmin.properties` file does not have a connection type specified then `SOAP` is the default.

`-port port`	Specifies the port number that is used by `wsadmin.sh`.
	
	In a Network Deployment environment, the specified port is the Deployment Manager SOAP or RMI port (not the application server instance SOAP or RMI port).
	
	To find the SOAP port number in the control region job log, look for:
	`BBOO0222I: ADMC0013I: The SOAP connector is available at port port`
	
	To find the RMI port number in the control region job log, look for:
	`BBOO0222I: ADMC0026I: The RMI connector is available at port port`
	
	The SOAP and RMI ports can also be found in the administration console.
		`ITCAM_PORT=port`	The default is to use the port specified in the `wsadmin.properties` file associated with the `wsadmin.sh` script you have chosen.

`-host host`	Specifies the fully qualified host name or IP address used by `wsadmin.sh`. Do not specify this option if the Deployment Manager is on the same host as the application server, if your application server is in stand-alone mode, or if the correct host name is configured in the `wsadmin.properties` file. In a Network Deployment environment, enter the value for the host for the Deployment Manager.	`ITCAM_HOST=host_name`	The default is to use the host name specified in the `wsadmin.properties` file associated with the `wsadmin.sh` script you have chosen.

Table 18. Standard Configuration Options (continued)

Command-prompt option	Description	Equivalent environment variable and value	Default
`-profile profile_script`	Specifies a profile script for running `wsadmin.sh`.	`ITCAM_PROFILE=script`	If you do not specify a profile script, then none is used.
`-user user_id`	Specifies the user ID to use for connection to `wsadmin.sh`. This ID is required if Global Security is enabled unless it set in the `sas.client.props` (RMI) or `soap.client.props` (SOAP) files. Log in as this user when you run the script. See, "Optional: Enabling user ID and password input from sas.client.props for RMI connector types:" on page 119, and "Optional: Enabling user ID and password input from soap.client.props for SOAP connector types:" on page 120	`ITCAM_USER=user_id`	N/A
`-password password`	Specifies the password to use for connection to `wsadmin.sh`. This password is required if Global Security is enabled, unless it is set in the `sas.client.props` (RMI) or `soap.client.props` (SOAP) files.	`ITCAM_PASSWORD= password`	N/A
`-server servername`	Specifies the name of the application server. This name is the name displayed in the IBM WebSphere Application Server administrative console, not the short name used to construct the z/OS started task names, for example, `server1`. This option is required if running in batch mode.	`ITCAM_SERVER=N/A servername`	N/A
`-serverfile filepath`	Specifies the path to a file containing a list of servers to be configured.	ITCAM_SERVERFILE=filepath	N/A
`-dmgrhost DeplyMgr RMI hostname`	Specifies the host name or IP address used to connect to the Deployment Manager RMI.	ITCAM_DMGRHOST= *IP_or_host*	The default is to use the local host name.
`-smf | -leavesmf`	Specify whether to activate SMF 120 records in WebSphere Application Server	ITCAM_SMF=Yes|No|Leave	
`-useclientprops`	Prevents the `config.sh` script from prompting you for the username and password. The username and password from the `wsadmin.sh` file is used instead.	ITCAM_USECLIENTPROPS=y|n	n
`-wasroot path`	Specifies the installation directory for IBM WebSphere Application Server (*AppServer_home*. It is the partial path to the `wsadmin.sh` file. For example: `/u/WAS8000/Servers/AppServer` If you specify a value for `-wsadmin`, this option is ignored. If you specify more of the path to the `wsadmin.sh` script, it is located quickly, If you specify less of the path, searching takes longer.	`ITCAM_WASROOT= AppServer _home`	`/u/WAS80`

Table 18. Standard Configuration Options (continued)

Command-prompt option	Description	Equivalent environment variable and value	Default
`-wsadmin` *path_and_file*	Specifies the full path to the `wsadmin.sh` file. For example: `/u/WAS8000/Servers/AppServer/profiles/default/bin/wsadmin.sh` This option is required if running in batch mode and the default `wsadmin.sh` script that `config.sh` selects is not acceptable. You can use any local `wsadmin.sh` script. You might want to use a `wsadmin.sh` with a particular profile. Any application server `wsadmin.sh` script works, but the one under *AppServer_home*`/profiles/default/bin` for the application server instance you are configuring is recommended. The `wsadmin.sh` script has its own associated `wsadmin.properties` file, which specifies the default options for the `wsadmin.sh` script.	`ITCAM_WSADMIN=`*path_and_file*	N/A
`-defaulthostname` *IP_or_host*	Specifies the fully qualified host name or IP address that replaces the value of the local host name for all purposes during configuration of ITCAM for WebSphere Application Server, such as for the bind IP or export IP processes. The value returned by running the hostname command is usually acceptable, but in some environments this value will not work. If running the hostname command returns a value that cannot be used, you can use the `-defaulthostname` option.	`ITCAM_DEFAULTHOSTNAME=`*IP_or_host*	The default is the system default host name.
`-default hostip` *host_IP*	Specifies the default local host IP address. Using the default, which is the value returned by running the host IP command, as the host IP address is acceptable, but in some environments, this value does not work. If running the host IP command returns a value that is not usable for configuring ITCAM for WebSphere Application Server, you can use this `-defaulthostip` option. For multi-homed addresses, the IP address to use will be prompted for. In the batch mode, the first IP address will be used.	`ITCAM_DEFAULTHOSTIP=`*host_IP*	The default is the system default host IP. In prompt mode, for multi-homed addresses, you are prompted for the IP address. In batch mode, the first IP address is used.
`-localhostname` *hostname*	Specifies the local host name and IP address. This option is used by findServers.jacl to make a node match if there is a problem identifying nodes. This option is used to determine the local node. This option is only required if the WAS_NODE associated with `wsadmin.sh` file is not usable. If the `-server` option is specified, then do not specify a value for this option.	`ITCAM_LOCALHOSTNAME=`*hostname*	The default is the value entered or the default value for the `-defaulthostname` option.
`-localhostip` *IP_address*	Specifies the local IP address. This option is used by findServers.jacl to make a node match if there is a problem identifying nodes. This option is used to determine the local node. This option is only required if the WAS_NODE associated with `wsadmin.sh` file is not usable. If the `-server` option is specified, then do not specify a value for this option.	`ITCAM_LOCALIP=`*IP_address*	
`-gcoutput`	Indicates whether you want garbage collection logs enabled. The value `y` results in logs being recorded to the SYSOUT log.	ITCAM_GCOUTPUT=y	n

Managing Server options

The following table describes the options in the configuration script required to configure communication with the ITCAM for Application Diagnostics Managing Server.

Table 19. Managing Server Configuration Options

Command-prompt option	Description	Equivalent environment variable and value	Default
`msconnect`	Indicates you want to enable communication with the ITCAM for Application Diagnostics Managing Server	ITCAM_MSCONNECT	n
`-kernelip` *`kernel IP addr`*	Specifies the host name or IP address of the ITCAM for Application Diagnostics Managing Server	ITCAM_KERNELIP=IP_or_host	N/A
`-mshome` *`MS home path`*	Specifies the path to the ITCAM for Application Diagnostics Managing Server home directory.	ITCAM_MSHOME=MS_home	`/opt/IBM/itcam/WebSphere/MS`
`-rfsport01` *`RFS port 1`*	Specifies the first RFS port	ITCAM_RFSPORT01=port	9120
`-kernelport01` *`Kernel port 1`*	Specifies the first kernel port.	ITCAM_KERNELPORT01=port	9122
`-probermiport` *`port range`*	Specifies a range of RMI ports for communication between the data collector and the ITCAM for Application Diagnostics Managing Server.	ITCAM_PROBERMIPORT=range	8200-8299
`-probecontrollerrmiport`	Specifies a range of controller RMI ports for communication between the data collector and the ITCAM for Application Diagnostics Managing Server.	ITCAM_PROBECONTROLLERRMIPORT=range	8300-8399
`-nomshomeconnect`	Indicates whether you want to contact the running ITCAM for Application Diagnostics Managing Server to get the home path.	ITCAM_MSHOMECONNECT=n	n
`-mshomeconnect`	Indicates whether you want to contact the running ITCAM for Application Diagnostics Managing Server to get the home path.	ITCAM_MSHOMECONNECT=y	y
`-bindip` *`bind ip`*	Specifies the bind IP host name or IP address.	ITCAM_BINDIP=IP_or_host	The default is to use the local host name.
`-exportip` *`export ip`*	Specifies the export IP host name or IP address.	ITCAM_EXPORTIP=IP_or_host	The default is to use the local host name.

ITCAM for Transactions options

The following table describes the options in the configuration script that are required to configure communication with ITCAM for Transactions.

Note: ITCAM for Transactions is not currently supported on Itanium platforms.

Table 20. ITCAM for Transactions Configuration Options

Command-prompt option	Description	Equivalent environment variable and value	Default
`-ttapi`	Indicates you want to enable communication with ITCAM for Transactions.	ITCAM_TTAPI=y	n
`-ttapissn` *Subsystem name*	Specifies the subsystem name of the ITCAM for Transactions z/OS .	ITCAM_TTAPISSN= *subsystem name*	CYTZ
`-ttapidir` *dir path*	Specifies the path of the ITCAM for Transactions z/OS HFS directory.	ITCAM_TTAPIDIR=/usr/lpp/cyt/jar/IBM	`/usr/lpp/cyt/jar/IBM`

ITCAM for SOA options

The following table describes the options in the configuration script that are required to configure communication with ITCAM for SOA.

Table 21. ITCAM for SOA Configuration Options

Command-prompt option	Description	Equivalent environment variable and value	Default
`-soadc`	Indicates you want to enable communication with ITCAM for SOA Agent	ITCAM_SOADC=y	n

ITCAM Agent for WebSphere Applications Monitoring Agent options

The following table describes the options in the configuration script that are required to configure communication with ITCAM Agent for WebSphere Applications Monitoring Agent.

Table 22. Monitoring Agent Configuration Options

Command-prompt option	Description	Equivalent environment variable and value	Default
`-temaconnect`	Indicates you want to enable communication with the monitoring agent	ITCAM_TEMACONNECT	n
`-temahost`	Specifies the fully qualified host name or IP address of the monitoring agent host	ITCAM_TEMAHOST	127.0.0.1
`-temaport`	Specifies the port number for the monitoring agent host	ITCAM_TEMAPORT	63335

Tivoli Performance Viewer options

The following table describes the options in the configuration script that are required to configure communication with Tivoli Performance Viewer.

Table 23. Tivoli Performance Viewer Options

Command-prompt option	Description	Equivalent environment variable and value	Default
`-tpv`	Integrate with ITCAM Tivoli Performance Viewer	ITCAM_TPV	n

Backup WebSphere Application Server options

The following table describes the options in the configuration script that are required to configure communication with Tivoli Performance Viewer.

Table 24. Backup WebSphere Application Server Configuration Options

Command-prompt option	Description	Equivalent environment variable and value	Default
`-backup`	Specifies whether to create a backup of the WebSphere Application Server configuration.	ITCAM_BACKUP	n
`-backupdir`	Backup directory name	ITCAM_BACKUPDIR	NA
`-backupsuffix`	Backup suffix	ITCAM_BACKUPSUFFIX	NA

Examining the log files

Standard Configuration Options

The following table describes log files generated before and during the configuration process;

Table 25. Log files generated before and during the configuration process

File path name	Description
config_home`/data/config-console.log`	User input while `config.sh` script is running
config_home`/data/config-message.log`	Messages generated while the `config.sh` script is running
config_home`/data/config-trace.log`	Debug messages generate while the `config.sh` script is running
config_home`/data/unconfig-console.log`	User input while the `unconfig.sh` script is running
config_home`/data/unconfig-message.log`	Messages generated while the `unconfig.sh` script is running
config_home`/data/unconfig-trace.log`	Debug messages generated while the `unconfig.sh` script is running
`config_home/data/createcfg.log`	Debug messages generated while the `createcfg.sh` script is running
profile`.`*cell*`.`*node*`.configdatacollector.log` For example `default.beta85.tvt6080.configdatacollector.log`	Log written by the wsadmin script (`configDataCollector.py`) during configuration updates to WebSphere Application Server
profile`.`*cell*`.`*node*`.unconfigdatacollector.log` For example `default.beta85.tvt6080.unconfigdatacollector.log`	Log written by the wsadmin script (`unconfigDataCollector.py`) during unconfiguration updates to WebSphere Application Server

Table 25. Log files generated before and during the configuration process (continued)

File path name	Description
profile.findservers.logFor example:default.findservers.log	Log generated by findSevers.py - used for diagnosing problems with the find servers process
node.*server*_valCheck.log For example: tvt6080_rd-test_valCheck.log	Log generated by WebSphere Application Sever validity checking

Additional configuration tasks

About this task

Complete the tasks described in each of the following sections, if applicable.

Increasing the heap size

About this task

Increase the heap-size configuration to 128 MB above the current configuration.

Procedure

1. Log on to the IBM WebSphere Application Server administrative console.
2. Navigate to specifying heap size in the WebSphere Application Server administrative console:
   a. Click **Server** > **Application Servers** and select the *server_name*.
   b. In the **Configuration** tab, navigate to **Server Infrastructure** > **Java and Process Management** > **Process Definition** > **Servant** > **Additional Properties: Java Virtual Machine**.
3. Edit the field **Maximum Heap Size**. If the default is not specified, then it assumes 256. Enter a value of 384.

Sample batch mode script

```
------------------------------------------------------------------------
-  ITCAM Data Collector for WebSphere Configuration Utility            -
-                                                                      -
-  The utility guides you through the steps involved in                -
-  configuring the data collector:                                     -
-  1.Select one or more application servers                            -
-  2.Integrate the data collector with one or more components:         -
-    a. ITCAM for SOA Agent                                            -
-    b. ITCAM Agent for WebSphere Applications                         -
-    c. ITCAM for Application Diagnostics Managing Server              -
-    d. ITCAM for Transactions                                         -
-    e. Tivoli Performance Viewer                                      -
-    f. ITCAM diagnostics tool                                         -
-  3.Specify advanced data collector settings                          -
-  4.Review and modify configuration settings                          -
-  5.Apply configuration settings                                      -
-                                                                      -
-  The utility applies your data collector configuration settings      -
-  to all of the application servers you specify.                      -
-                                                                      -
-  At each prompt, enter 'q' to quit the utility or enter '?' for help.-
------------------------------------------------------------------------



Environment Variables:

  ITCAM_SERVERS=beta.tvt7004.b8srELJ beta.tvt7004.b8srELJ(default)
  ITCAM_WASROOT=/u/WAS800B/beta/tvt7004/AppServer/profiles/default
  ITCAM_WSADMIN=/u/WAS800B/beta/tvt7004/AppServer/profiles/default/bin/wsadmin.sh
  ITCAM_KERNELIP=devapp-lnx-s06.usca.ibm.com
```

```
  ITCAM_TEMACONNECT=yes
  ITCAM_SOADC=yes
  ITCAM_TPV=yes
  ITCAM_USER=b8admin
  ITCAM_PASSWORD=********
  ITCAM_MSCONNECT=yes
  ITCAM_TTAPI=yes
  ITCAM_CONFIG=/u/ejack/config
  ITCAM_BYPASSFINDSERVERS=/u/ejack/findServers.dat

Command Line Flags:

  -server b8srELJ
  -batch

Log file name: /u/ejack/config/data/config-trace.log.
Searching for wsadmin locations under directory: /u/WAS800B/beta/tvt7004/AppServer/profiles/default
WebSphere home directory located at /u/WAS800B/beta/tvt7004/AppServer

Searching for servers under profile: default
  Connecting to profile.........................
     Start finding servers for profile default
         Processing default.............
         Finding servers done successfully for profile default
     Finished finding servers for profile default
Successfully executed searching servers for Profile: default


Error occurred processing find probes - Data element WASCELLMODIFIED of PDL is not a list, superfluous index 0 specified
CFG2017E Error occurred while processing find probes - AssertionError('Data element WASCELLMODIFIED of PDL is not a list, superfluous index 0 sp

------------------------------------------------------------------------
-         [Optional] integration with ITCAM for SOA Agent              -
------------------------------------------------------------------------



------------------------------------------------------------------------
-   [Optional] integration with ITCAM Agent for WebSphere Applications -
------------------------------------------------------------------------



------------------------------------------------------------------------
-                 [Optional] integration with                          -
-           ITCAM for Application Diagnostics Managing Server          -
------------------------------------------------------------------------



MS home directory is: /opt/bvt/IBM/itcam/WebSphere/MS
------------------------------------------------------------------------
-         [Optional] integration with ITCAM for Transactions           -
-                                                                      -
-                                                                      -
-                                                                      -
- This requires a separate installation of ITCAM for                   -
- Transactions on the same host as WebSphere Application Server.       -
- You will need to supply the subsystem name and directory             -
- path of the ITCAM for Transactions container.                        -
------------------------------------------------------------------------




------------------------------------------------------------------------
-         [Optional] integration with Tivoli Performance Viewer        -
------------------------------------------------------------------------



------------------------------------------------------------------------
- JVM Garbage Collection information will be gathered.                 -
- You may eliminate the output of the GC log from.                     -
- SYSOUT in order to conserve SPOOL space                              -
------------------------------------------------------------------------


+----------------------------------------------------------------------+
```

```
|                                                                          |
|  Data collector configuration summary                                    |
|                                                                          |
+--------------------------------------------------------------------------+

Each of the servers will be configured for data collection

 1) List of servers selected

   - WAS server: beta.tvt7004.b8srELJ(default)
       WAS cell: beta
        WAS node: tvt7004

       WebSphere Profile home    :
         /u/WAS800B/beta/tvt7004/AppServer/profiles/default

       wsadmin location          :
         /u/WAS800B/beta/tvt7004/AppServer/profiles/default/bin/wsadmin.sh

                    WAS version : 8.0.0.0
                     Deployment : Network deployment
                       JVM mode : 64bit
              Configuration home : /u/ejack/config

 2) Integrate with ITCAM for SOA Agent : Yes

 3) Integrate with ITCAM Agent for WebSphere Applications : Yes

       TEMA hostname or IP address : 127.0.0.1
                TEMA port number : 63335
                      Monitor GC : No

 4) Integrate with ITCAM for AD Managing Server : Yes

       MS hostname or IP address : devapp-lnx-s06.usca.ibm.com
         MS codebase port number : 9122
               MS home directory : /opt/bvt/IBM/itcam/WebSphere/MS

 5) Integrate with ITCAM for Transactions : Yes

                    TT subsystem : CYTZ
                    TT directory : /usr/lpp/cyt/jar/IBM

 6) Integrate with Tivoli Performance Viewer : Yes

 7) Advanced settings :

                  Collect SMF data : Leave
              GC output to sysout : No

Configuring Cell: beta Node: tvt7004 Profile: default
  Connecting to profile...................
     Start Configuring b8srELJ
         Processing b8srELJ.........
         Configuration done successfully for b8srELJ
         Application server (b8srELJ) should be restarted
     Finished Configuring b8srELJ successfully
     Summary:
         b8srELJ (OK)
Successfully executed Configuring for Cell: beta Node: tvt7004 Profile: default


RC(0) from config.sh

EJACK:/u/ejack/bin ejack >
```

Chapter 7. Troubleshooting a problem

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the IBM technical-support representative know where to start to find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead you a problem resolution.

What are the symptoms of the problem?

When starting to describe a problem, the most obvious question is "What is the problem?" This question might seem straightforward; however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

- Is the problem specific to one platform or operating system, or is it common across multiple platforms or operating systems?
- Is the current environment and configuration supported?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration; many problems can be

traced back to incompatible levels of software that are not intended to run together or have not been fully tested together.

When does the problem occur?

Develop a detailed timeline of events leading up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you need to look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:

- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

Under which conditions does the problem occur?

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:

- Does the problem always occur when the same task is being performed?
- Does a certain sequence of events need to occur for the problem to surface?
- Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might have occurred around the same time, the problems are not necessarily related.

Can the problem be reproduced?

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Consequently, problems that you can reproduce are often easier to debug and solve. However, problems that you can reproduce can have a disadvantage: If the problem is of significant business impact, you do not want it to recur. If possible, re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Are multiple users or applications encountering the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

Known issues and solutions

The following are troubleshooting tips and techniques for problems that occur during installation and configuration of ITCAM for WebSphere Application Server.

Missing runtime tab

The problem: After installing and configuring ITCAM for WebSphere Application Server in a Network Deployment environment and stopping/starting the application server, there is no **Runtime** tab available in the WebSphere Application Server administration console (**Monitoring and Tuning > Performance Monitoring Infrastructure > ITCAM for WebSphere Application Server**). Ensure that the **Configuration tab** check box is selected and that there is no `CYNEC0001I IBM Tivoli Composite Application Manager for WebSphere Application Server started` message in the `msg-dc-bcm.log` file.

Important: This issue only applies to zOS configurations.

The cause: If there is no `CYNEC0001I IBM Tivoli Composite Application Manager for WebSphere Application Server started` message in the `msg-dc-bcm.log` file, this means that ITCAM for WebSphere Application Server Data Collector cannot be initialized. One of the reasons for this is that ITCAM for WebSphere Application Server is unable to establish a connection to Admin Service.

The solution: Userids associated with the started task names of DMGR and servant must use the same keyring file.

Missing runtime tab after configuration

The problem: There is no **Runtime** tab for ITCAM for WebSphere Application Server even though configuration ended successfully.

The cause: After configuration, reconfiguration, or unconfiguration of ITCAM for WebSphere Application Server, the server has to be stopped and started for changes to take effect. Be aware that on high-load machines, the initial startup of WebSphere Application Server services required by monitoring features can be more time consuming.

The solution: To restart WebSphere Application Server, go to the `WebSphere_home/profiles/`*`profile_name`*`/bin` directory. Depending on platform use the following scripts:

- `startServer.bat <server_name>/stopServer.bat <server_name>` for Windows
- `startServer.sh <server_name>/stopServer.sh <server_name>` for Linux and Unix systems

where `<profile_name>` is the name of the profile.

`<server_name>` is the name of the server on which ITCAM for WebSphere Application Server was configured, unconfigured, or reconfigured. Wait two minutes and verify if the **Runtime** tab is available on the **ITCAM for WebSphere Application Server** link.

When WebSphere Application Server Global Security is enabled, config.sh fails

The problem: While configuring the data collector using `config.sh` in a z/OS environment for a WebSphere Application Server with Global Security enabled, the connection to the Application Server fails with the following error:

```
WASX7023E: Error creating "SOAP" connection to host "localhost";
exception information: com.ibm.websphere.management.exception.ConnectorNotAvailableException:
SOAPException: faultCode=SOAP-ENV:Client;
msg=Error opening socket: javax.net.ssl.SSLException: java.lang.RuntimeException:
Unexpected error: java.security.InvalidAlgorithmParameterException: the trustAnchors parameter must be non-empty;
```

Important: This issue only applies to zOS configurations.

The cause: If WebSphere Global Security is enabled, a WebSphere administrator user ID (default is W8ADMIN) needs to be used to run `config.sh` (and the underlying `wsadmin.sh`). If a different ID is used to run `config.sh`, then this user ID needs to be connected to a WebSphere Application Server keyring and certificates in the same way as a WebSphere Application Server administrator ID.

The solution: Three examples of script execution are provided for different user ID situations:

1. When the user ID the script runs under @USER@ and the WebSphere Application Server administrative user ID @WASUSER@ are identical, run `config.sh`.
2. When the user ID the script runs under @USER@ and the WebSphere Application Server administrative user ID @WASUSER@ are different but the WebSphere Application Server administrator user ID is not root. In this case the commands are piped into an instance of the **su** command with a user ID specified:

   ```
   echo "./config.sh ..." | su -s @WASUSER@
   ```
3. When the configuration user ID is the root user, use the following command:

   ```
   echo "./setupdc.sh ..." | su
   ```

   This is not usually recommended because all directories and files created by the script will be owned by the root user. It is also unlikely that the root user will be in the keyring if WebSphere Application Server security is enabled. When the user ID @USER@ is different to the WebSphere Application Server admin user ID @WASUSER@, then the former must be permitted to issue the **su** to the latter. This is provided by giving @USER@ read access to the resource BPX.SRV.@WASUSER@ in the SURROGAT class. This can be done using TSO commands:

   ```
   rdefine surrogat bpx.srv.@WASUSER@ uacc(none)
   setr raclist(surrogat) refresh
   pe bpx.srv.@WASUSER@ cl(surrogat) acc(read) id(@USER@)
   ```

   For permission to execute the su command with no operands, issue the following TSO commands:

   ```
   rdef facility bpx.superuser
   setr raclist(facility) refresh
   pe bpx.superuser cl(facility) acc(read) id(@USER@)
   ```

Configuration of communication with ITCAM for Transactions

The Problem: Global Publishing Service (GPS) tokens are not available in ITCAM for WebSphere Application Server. Some features of ITCAM for Transaction Tracking are limited without GPS tokens. The following features are not available without GPS tokens:

- RMI/IIOP
- WebServices
- IMS™ Connect

The Solution: GPS tokens are supplied by the Common Services component, SMP/E FMID HAAD71C. The Common Services component is available in ITCAM for Applications Diagnostics 7.1 or later.

To disable the unavailable features, in the `toolkit_custom.properties` file, set the following properties to false.

```
com.ibm.tivoli.itcam.dc.ttapi.rmiiiop.enabled=false
com.ibm.tivoli.itcam.dc.ttapi.webservice.enabled=false
com.ibm.tivoli.itcam.dc.ttapi.cics.enabled=false
com.ibm.tivoli.itcam.dc.ttapi.ims.enabled=false
```

WebSphere Application Server and IMS cannot be stitched in the TEP

The problem: In ITCAM for Transactions TT reporter, WebSphere Application Server and IMS cannot be stitched in the TEP.

Problem Description: If the following conditions are met, WebSphere Application Server and IMS can be stitched in the TEP and resulting data is visible in TT reporter:

- the common data collector is connected to ITCAM for Transactions
- the common data collector is connected to a Managing Server
- the Managing Server and the ITCAM Common Services CYN1 subsystem are running. ITCAM Common Services is an ITCAM for Application Diagnostics component.

If the data collector is **not** connected to a Managing Server, WebSphere Application Server and IMS cannot be stitched in the ITCAM for Transactions TT Reporter.

Reason: IMS-TT client does not support the tokens sent in the OTMA which the common data collector sends when the Managing Server is not connected.

Solution: This is a current limitation.

Connection timeout errors to server in the trace-install.logs file

The problem: ITCAM for WebSphere Application Server cannot be configured. Errors appear regarding connection timeout to server in the install loffs. In some situations, it can happen that more time is necessary to connect to server or deployment manager. It is usually caused either by slow network connection or insufficient memory.

The solution: Change timeout values for the `wsadmin.sh` script. Default timeout values for the are:

- For the connection from the wsadmin environment to the deployment manager, the default is 180 seconds
- For the connection from the deployment manager to the node agent, the default is 600 seconds.
- For the connection from the node agent to the runtime deployment target, the default is 600 seconds.

To change these values, modify the properties in the `soap.client.props` file, or `sas.client.prop` file, and the custom properties for the deployment manager and the node agents where members of your runtime deployment target are running (in case of an ND environment). Complete the following steps:

1. Modify the com.ibm.SOAP.requestTimeout property by editing the `soap.client.props` file, located in the properties subdirectory of the `profile_root` directory.
2. Change the requestTimeout custom property using the administrative console:
   a. For servers or cluster members, click **Servers** > **Server Types** > **WebSphere Application servers** > **server_name** > **Server Infrastructure** > **Administration** > **Administration Services** > **Additional properties** > **JMX Connectors** > **SOAPConnector** > **Additional Properties** > **Custom properties**. Locate the requestTimeout custom property, and modify its value.
   b. For the deployment manager, click **System administration** > **Deployment manager** > **Additional Properties** > **Administration Services** > **Additional properties** > **JMX Connectors** > **SOAPConnector** > **Additional Properties** > **Custom properties**. Locate the requestTimeout custom property, and modify its value.
   c. For the node agents, click **System administration** > **Node agents** > *node_agent_name* > **Additional Properties** > **Administration Services** > **Additional properties** > **JMX Connectors** > **SOAPConnector** > **Additional Properties** > **Custom properties**. Locate the requestTimeout custom property, and modify its value.

Tivoli Performance Viewer reports requests as servlets not web services

The problem: If web service caching is enabled in WebSphere Application Server, Tivoli Performance Viewer reports requests as servlets not web services.

The solution: To view web service requests in Tivoli Performance Viewer, disable web service caching in WebSphere Application Server by completing the following steps:

1. In the WebSphere Application Server administrative console, click **Servers** > **WebSphere Application Servers** > *server_name* > **Web Container Settings** > **Web Container**. The configuration page opens.
2. Clear the **Enable Servlet Caching** option.
3. Click **OK**. Save the changes and restart WebSphere Application Server.

CFG2037E Could not connect to the MS error

The problem: While configuring the data collector to connect to a Managing Server, an error message similar to the following appears:

```
CFG2037E Could not connect to the MS - hostname
```

The solution: On the Managing Server, in the `kl1.properties` and `kl2.properties` files, ensure that the `codebase.http.header.enabled` property is set to true.

Tivoli Performance Monitor displays count for edge requests only

The problem: The number of requests displayed in Tivoli Performance Monitor relates only to edge requests, nested requests are not counted.

The solution: Product functions as designed.

No SOA data is collected

***The Problem*:** When you integrate the ITCAM Data Collector for WebSphere with ITCAM for SOA for applications servers within a profile where ITCAM for SOA is not already installed and configured, and you later install ITCAM for SOA 7.1.1, no SOA data is collected and no SOA metric data files are created.

The Solution: You must add additional properties to the `KD4.DC.Properties` file, complete the following steps:

1. Navigate to the *ITCAM4SOA_Home*`/KD4/config` directory.
2. Add the following properties to the `KD4.DC.Properties` file with any text editor:

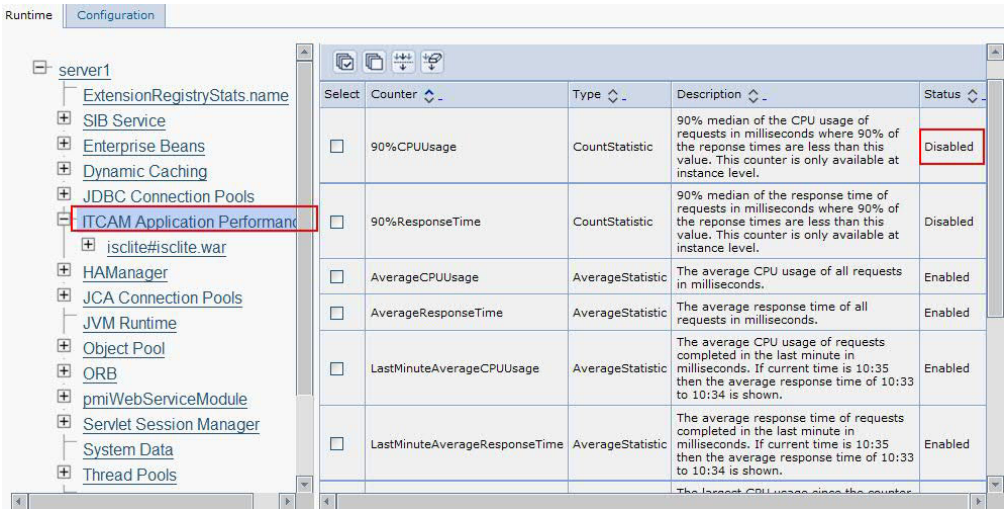
   ```
   1.server_instance.monitor=on
   1.server_instance.log=info
   1.server_instance.trace=off
   1.server_instance.monitor.control.count=1
   1.server_instance.monitor.control.1=*;*;*;*;*;none
   1.server_instance.filter.control.count=0
   ```

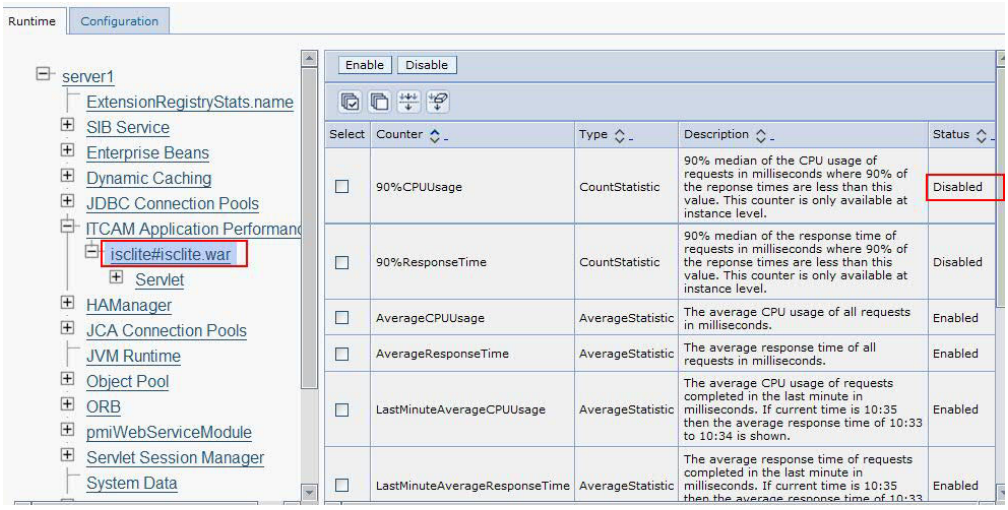
3. Save the file.

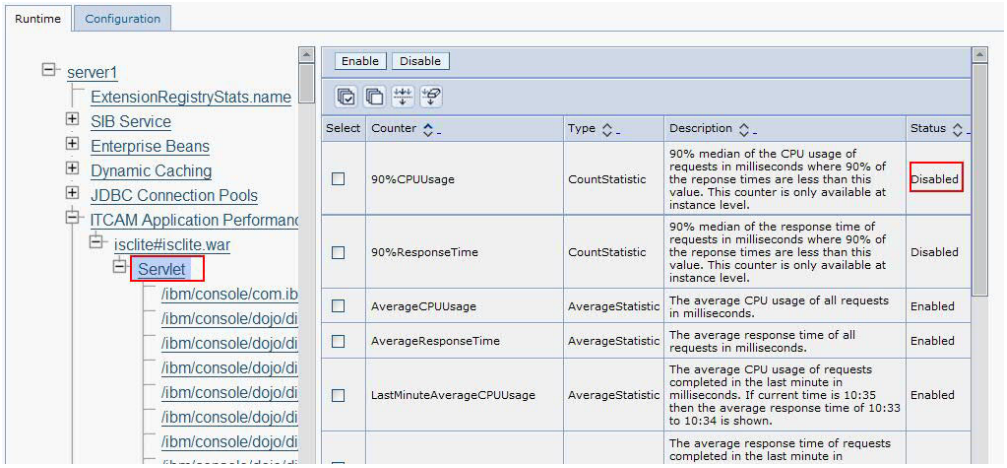
When I select instance level counters in TPV, they appear disabled

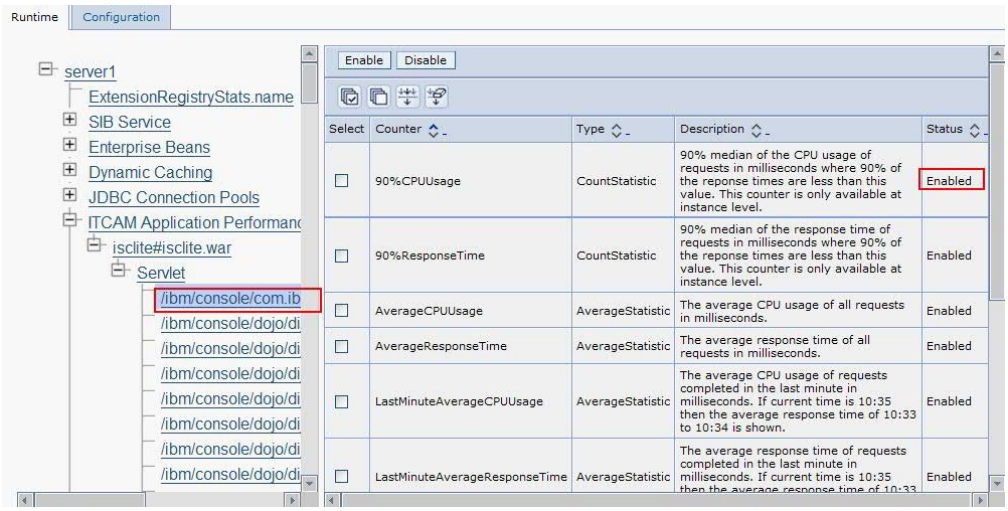
***The Problem*:** In Tivoli Performance Monitor, when I select instance level counters, they appear disabled.

Problem Description: Enable instance level counters by expanding **ITCAM Application Performance**, selecting the instance level node, and then selecting the counters you want to enable. For more information, see "Start ITCAM for WebSphere Application Server, enable counters, and view data" on page 3. When you enable instance level counters, they appear disabled at the **ITCAM Application Performance** level, but at request level, they are enabled. Also, when you view the performance graphs, the counters are enabled. The following graphics demonstrate this:


Runtime
Configuration
server1
ExtensionRegistryStats.name
SIB Service
Enterprise Beans
Dynamic Caching
JDBC Connection Pools
ITCAM Application Performanc
isclite#isclite.war
HAManager
JCA Connection Pools
JVM Runtime
Object Pool
ORB
pmiWebServiceModule
Servlet Session Manager
System Data
Thread Pools
Select
Counter
Type
Description
Status
90%CPUUsage
CountStatistic
90% median of the CPU usage of requests in milliseconds where 90% of the reponse times are less than this value. This counter is only available at instance level.
Disabled
90%ResponseTime
CountStatistic
90% median of the response time of requests in milliseconds where 90% of the reponse times are less than this value. This counter is only available at instance level.
Disabled
AverageCPUUsage
AverageStatistic
The average CPU usage of all requests in milliseconds.
Enabled
AverageResponseTime
AverageStatistic
The average response time of all requests in milliseconds.
Enabled
LastMinuteAverageCPUUsage
AverageStatistic
The average CPU usage of requests completed in the last minute in milliseconds. If current time is 10:35 then the average response time of 10:33 to 10:34 is shown.
Enabled
LastMinuteAverageResponseTime
AverageStatistic
The average response time of requests completed in the last minute in milliseconds. If current time is 10:35 then the average response time of 10:33 to 10:34 is shown.
Enabled


Runtime
Configuration
server1
ExtensionRegistryStats.name
SIB Service
Enterprise Beans
Dynamic Caching
JDBC Connection Pools
ITCAM Application Performanc
isclite#isclite.war
Servlet
HAManager
JCA Connection Pools
JVM Runtime
Object Pool
ORB
pmiWebServiceModule
Servlet Session Manager
System Data
Enable
Disable
Select
Counter
Type
Description
Status
90%CPUUsage
CountStatistic
90% median of the CPU usage of requests in milliseconds where 90% of the reponse times are less than this value. This counter is only available at instance level.
Disabled
90%ResponseTime
CountStatistic
90% median of the response time of requests in milliseconds where 90% of the reponse times are less than this value. This counter is only available at instance level.
Disabled
AverageCPUUsage
AverageStatistic
The average CPU usage of all requests in milliseconds.
Enabled
AverageResponseTime
AverageStatistic
The average response time of all requests in milliseconds.
Enabled
LastMinuteAverageCPUUsage
AverageStatistic
The average CPU usage of requests completed in the last minute in milliseconds. If current time is 10:35 then the average response time of 10:33 to 10:34 is shown.
Enabled
LastMinuteAverageResponseTime
AverageStatistic
The average response time of requests completed in the last minute in milliseconds. If current time is 10:35
Enabled


Runtime
Configuration
server1
ExtensionRegistryStats.name
SIB Service
Enterprise Beans
Dynamic Caching
JDBC Connection Pools
ITCAM Application Performanc
isclite#isclite.war
Servlet
/ibm/console/com.ib
/ibm/console/dojo/di
/ibm/console/dojo/di
/ibm/console/dojo/di
/ibm/console/dojo/di
/ibm/console/dojo/di
/ibm/console/dojo/di
Enable
Disable
Select
Counter
Type
Description
Status
90%CPUUsage
CountStatistic
90% median of the CPU usage of requests in milliseconds where 90% of the reponse times are less than this value. This counter is only available at instance level.
Disabled
90%ResponseTime
CountStatistic
90% median of the response time of requests in milliseconds where 90% of the reponse times are less than this value. This counter is only available at instance level.
Disabled
AverageCPUUsage
AverageStatistic
The average CPU usage of all requests in milliseconds.
Enabled
AverageResponseTime
AverageStatistic
The average response time of all requests in milliseconds.
Enabled
LastMinuteAverageCPUUsage
AverageStatistic
The average CPU usage of requests completed in the last minute in milliseconds. If current time is 10:35 then the average response time of 10:33 to 10:34 is shown.
Enabled
The average response time of requests completed in the last minute in



The Solution: The product functions as designed.

In MSVE, JVM CPU are always 100% while JVM CPU value is zero in TEP

***The Problem*:** In MSVE, the Server Activity Display and Recent Activity sections always display JVM CPU as 100% while JVM CPU value is zero in TEP. This occurs regardless of whether requests are loading or not. This problem occurs because the "*PUBLIC" authority for Service Program QPMLPMGT (QSYS/QPMLPMGT) is set to "*EXCLUDE"

The Solution: Set the "*PUBLIC" authority for Service Program QPMLPMGT (QSYS/QPMLPMGT) as "*USE".

In MSVE, the Last Known Action is not NA for WebService request while MOD is L1

***The Problem*:** In MSVE, In Recent Activity Display window, the Last Known Action is not NA for WebService request while MOD is L1

The Solution: Functions as designed.

Errors occur when you run configuration or migration script on IBMi

***The Problem*:** You might encounter the following issue while running either the configuration or migration utility on IBMi:

1. While running the `./config_i5.sh` or `./migrate_i5.sh` script, you receive an error message similar to the following:

   ```
   CFG2006E Migration of the Data Collector did not complete successfully with return code 1.
   ```

2. Check the logs in *DC_home*`/data`.
3. Locate the lines in the log file that relate to the wsadmin task, they will be similar to this:

```
[2012-06-04 15:31:37 DEBUG _execute_command (WsadminTask:683)]  Entry _execute_command - /qibm/userdata/websphere/apps
  erver/v7/wr71nd64/profiles/default/bin/wsadmin  -conntype SOAP -port 8879 -profileName default -wsadmin_classpath
/home/WWTING/images/ecam85/0603/bin/../toolkit/lib/jiti.jar:/home/WWTING/images/ecam85/0603/bin/../itcamdc/lib/ppe.ins
  taller.jar:/home/WWTING/images/ecam85/0603/bin/../bin/lib/installbundle.jar -lang jython -f
/home/WWTING/images/ecam85/0603/bin/../bin/lib/configDataCollector.py -javaoption "-
Dpython.path=/home/WWTING/images/ecam85/0603/bin/../bin:/home/WWTING/images/ecam85/0603/bin/../bin/lib"
```

```
 /home/WWTING/images/ecam85/0603/bin/../data/config_inputlist >
/home/WWTING/images/ecam85/0603/bin/../data/default.TIV4001Network.TIV4001.configdatacollector.log 2>&1

 [2012-06-04 15:31:37 DEBUG _execute_command (WsadminTask:687)]  wsadmin thread started
```

The next line will display the return code, you might see return code 105.

The Solution: If you see return code 105 in logs, you might need to increase the resources (job priority for the related jobs)

CFG2017E message is displayed when you run config.sh a second or subsequent time

***The Problem*:** If you configure the data collector using the configuration utility (`config.sh`) for an application server instance and then run the configuration utility a second or subsequent time to configure further application server instances which had been configured earlier, you will get the following erroneous message:

```
Error occurred processing find probes - Data element WASCELLMODIFIED of PDL is not a list, superfluou
CFG2017E Error occurred while processing find probes - AssertionError('Data element WASCELLMODIFIED o
```

The Solution: No action is required, the configuration completes successfully and everything works correctly

Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

About this task

You can find useful information by searching the information center for ITCAM for WebSphere Application Server, but sometimes you need to look beyond the information center to answer your questions or resolve problems.

Procedure

To search knowledge bases for information that you need, use one or more of the following approaches:

- Search for content by using the IBM Support Assistant (ISA).

  ISA is a no-charge software serviceability workbench that helps you answer questions and resolve problems with IBM software products. You can find instructions for downloading and installing ISA on the ISA website.
- Find the content that you need by using the IBM Support Portal.

  The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. The IBM Support Portal lets you access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the demo videos (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos) about this tool. These videos introduce you to the IBM Support Portal, explore troubleshooting and other resources, and demonstrate how you can tailor the page by moving, adding, and deleting portlets.

- Search for content about ITCAM for WebSphere Application Server by using one of the following additional technical resources:
  - Tivoli Identity Manager Version 4.3 technotes and APARs (problem reports)
  - Tivoli Identity Manager Support website
  - Tivoli support communities (forums and newsgroups)
- Search for content by using the IBM masthead search. You can use the IBM masthead search by typing your search string into the Search field at the top of any ibm.com® page.
- Search for content by using any external search engine, such as Google, Yahoo, or Bing. If you use an external search engine, your results are more likely to include information that is outside the ibm.com domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

  Tip: Include "IBM" and the name of the product in your search if you are looking for information about an IBM product.

Getting fixes

A product fix might be available to resolve your problem.

About this task

Procedure

To find and install fixes:

1. Obtain the tools required to get the fix.
2. Determine which fix you need.
3. Download the fix. Open the download document and follow the link in the "Download package" section.
4. Apply the fix. Follow the instructions in the "Installation Instructions" section of the download document.
5. Subscribe to receive weekly email notifications about fixes and other IBM Support information.

Getting fixes from Fix Central

You can use Fix Central to find the fixes that are recommended by IBM Support for a variety of products, including ITCAM for WebSphere Application Server. With Fix Central, you can search, select, order, and download fixes for your system with a choice of delivery options. An ITCAM for WebSphere Application Server product fix might be available to resolve your problem.

About this task

Procedure

To find and install fixes:

1. Obtain the tools that are required to get the fix. If not installed, obtain your product update installer. The installer can be downloaded from Fix Central. This site provides download, installation, and configuration instructions for the update installer.

2. Select ITCAM for WebSphere Application Server as the product, and select one or more check boxes that are relevant to the problem that you want to resolve.
3. Identify and select the fix that is required.
4. Download the fix.
   a. Open the download document and follow the link in the "Download Package" section.
   b. When downloading the file, ensure that the name of the maintenance file is not changed. This change might be intentional, or it might be an inadvertent change that is caused by certain web browsers or download utilities.
5. Apply the fix.
   a. Follow the instructions in the "Installation Instructions" section of the download document.
   b. For more information, see the "Installing fixes with the Update Installer" topic in the product documentation.
6. Optional: Subscribe to receive weekly email notifications about fixes and other IBM Support updates.

Contacting IBM Support

IBM Support provides assistance with product defects, answering FAQs, and performing rediscovery.

Before you begin

After trying to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before contacting IBM Support, your company must have an active IBM *maintenance contract name*, and you must be authorized to submit problems to IBM. For information about the types of available support, see the Support portfolio topic in the *Software Support Handbook*.

Procedure

Complete the following steps to contact IBM Support with a problem:

1. Define the problem, gather background information, and determine the severity of the problem. For more information, see the Getting IBM support topic in the *Software Support Handbook*.
2. Gather diagnostic information.
3. Submit the problem to IBM Support in one of the following ways:
   - Using IBM Support Assistant (ISA):
   - Online through the IBM Support Portal: You can open, update, and view all your Service Requests from the Service Request portlet on the Service Request page.
   - By phone: For the phone number to call in your region, see the Directory of worldwide contacts web page.

Results

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is

resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support website daily, so that other users who experience the same problem can benefit from the same resolution.

Exchanging information with IBM

To diagnose or identify a problem, you might need to provide IBM Support with data and information from your system. In other cases, IBM Support might provide you with tools or utilities to use for problem determination.

Sending information to IBM Support

To reduce the time that it takes to resolve your problem, you can send trace and diagnostic information to IBM Support.

Procedure

To submit diagnostic information to IBM Support:

1. Open a problem management record (PMR).
2. Collect the diagnostic data that you need. Diagnostic data helps reduce the time that it takes to resolve your PMR. You can collect the diagnostic data manually or automatically:
   - Collect the data manually.
   - Collect the data automatically.
3. Compress the files by using the ZIP or TAR format.
4. Transfer the files to IBM. You can use one of the following methods to transfer the files to IBM:
   - IBM Support Assistant
   - The Service Request tool
   - Standard data upload methods: FTP, HTTP
   - Secure data upload methods: FTPS, SFTP, HTTPS
   - Email

   All of these data exchange methods are explained on the IBM Support site.

Receiving information from IBM Support

Occasionally an IBM technical-support representative might ask you to download diagnostic tools or other files. You can use FTP to download these files.

Before you begin

Ensure that your IBM technical-support representative provided you with the preferred server to use for downloading the files and the exact directory and file names to access.

Procedure

To download files from IBM Support:

1. Use FTP to connect to the site that your IBM technical-support representative provided and log in as `anonymous`. Use your email address as the password.
2. Change to the appropriate directory:
   a. Change to the `/fromibm` directory.

      ```
      cd fromibm
      ```

b. Change to the directory that your IBM technical-support representative provided.

   ```
   cd nameofdirectory
   ```

3. Enable binary mode for your session.

   ```
   binary
   ```

4. Use the **get** command to download the file that your IBM technical-support representative specified.

   ```
   get filename.extension
   ```

5. End your FTP session.

   ```
   quit
   ```

Appendix A. Manually removing data collector configuration from an application server instance

To manually remove the data collector configuration from an application server instance, you must be able to connect to the application server using the wsadmin tool - this is only possible if you are using WebSphere Application Server Network Deployment and the Deployment Manager is running. If the WebSphere Application Server cannot start up, you must restore the WebSphere Application Server from the back up taken while running the configuration utility.

You can manually remove the data collector configuration from an application server instance, if any of the following conditions apply:

- In a non-Network Deployment, you manually added the data collector configuration to the application server instance and you want to unconfigure data collection. The application server instance must be running.
- In a Network Deployment, you manually added the data collector configuration to the application server instance and you want to unconfigure data collection. The Deployment Manager the node agent on the application server must be running.
- In a Network Deployment environment, you configured the application server instance for data collection manually and the application server fails to start. The Deployment Manager the node agent on the application server must be running.

If you configure a stand-alone application server instance for data collection either manually or with the configuration or migration utility and the application server fails to start, you must restore your WebSphere Application Server configuration with your backup configuration. For more information, see Appendix B, “Restoring the WebSphere Application Server configuration from a backup,” on page 159. If you did not create a backup, contact IBM Support.

Remember:

- You must make manual changes to the WebSphere Application Server configuration for data collectors as the WebSphere administrative user.
- Making manual changes to the WebSphere Application Server for data collection must be performed by an experience WebSphere administrator only. Any error in the manual configuration change can result in the application server not starting.
- If you manually configure the data collector to monitor application server instances, you cannot use the ITCAM Data Collector for WebSphere Unconfiguration Utility to unconfigure the data collector.

To manually remove the data collector configuration, complete the following procedure:

1. Log in to the WebSphere Administration Server Console.
2. Click **Servers**.
3. Expand **Server Type** and select **WebSphere application servers**.
4. Click the name of the server.
5. On the Configuration tab, under Server Infrastructure, expand **Java and Process Management** and select **Process Definition**.
6. Under the **Additional Properties** section, click **Java Virtual Machine**.

7. Under the **Additional Properties** section, click **Custom Properties**.
8. Remove any of the following JVM Custom Properties, if they are present:
   - `am.home`
   - `ITCAM.DC.ENABLED`
   - `TEMAGCCollector.gclog.path`
   - `com.ibm.tivoli.itcam.toolkit.ai.runtimebuilder.enable.rebuild`
   - `com.ibm.tivoli.jiti.injector.ProbeInjectorManagerChain.primaryInjectorFile` (if it is present)
9. Identify the JVM arguments added for the ITCAM Data Collector for WebSphere:
   a. In the Navigation Pane, click **Environment** > **WebSphere Variables**.
   b. If you configured the application server for data collection manually, locate the JVM arguments you added manually.

      If you configured the application server for data collection with the configuration utilities, compare the value of the arguments `AM_OLD_ARGS` and `AM_CONFGI_JVM_ARGS` to determine which arguments were added by the configuration utility.
10. Click **Server** > **Application Server** and select the *server_name*.
11. On the Configuration tab, navigate to **Server Infrastructure** > **Java and Process Management** > **Process Definition** > **Java Virtual Machine**.
12. In **Generic JVM Arguments**, remove the JVM arguments you identified in step 9 for the ITCAM Data Collector for WebSphere.
13. Click **Apply** or **OK**.
14. In the **Messages** dialog box, click **Save**.
15. In the **Save to Master Configuration** dialog box, complete one of the following steps:
    - If you are under a Network Deployment environment, make sure the check box **Synchronize changes with Nodes** is selected, then click **Save**.
    - If you are not under a Network Deployment environment, click **Save**.
16. Remove environment entries added for the ITCAM Data Collector for WebSphere.
    a. In the Configuration tab, go to **Server Infrastructure** > **Java and Process Management** > **Process Definition** > **Environment Entries**.
    b. Depending on the hardware platform, delete the `LIBPATH` (on AIX systems), `SHLIB_PATH` (on HP-UX systems), `LD_LIBRARY_PATH` (on Linux systems), or `PATH` (on Windows systems) environment entry.
    c. Remove the `NLSPATH` environment entry.
17. Click **Apply** or **OK**.
18. In the **Messages** dialog box, click **Save**.
19. In the **Save to Master Configuration** dialog box, complete one of the following steps:
    - If you are under a Network Deployment environment, make sure the check box **Synchronize changes with Nodes** is selected, then click **Save**.
    - If you are not under a Network Deployment environment, click **Save**.
20. In the Navigation Pane, click **Environment** > **WebSphere Variables**.
21. Delete the following variables:
    - `AM_CONFIG_JVM_ARGS`
    - `AM_OLD_JVM_ARGS`

- ITCAMDCHOME
- ITCAMDCVERSION

22. In the **Messages** dialog box, click **Save**.
23. In the **Save to Master Configuration** dialog box, complete one of the following steps:
    - If you are under a Network Deployment environment, make sure the check box **Synchronize changes with Nodes** is selected, then click **Save**.
    - If you are not under a Network Deployment environment, click **Save**.
24. If you configured the server instance for data collection with the data collector configuration tool, rather than manually, complete the following steps:
    a. Navigate to the *DC_home*/runtime directory.
    b. Rename the file $profile.$cell.$node.$server.input.properties to $profile.$cell.$node.$server.input.properties.bak
25. If you are manually removing the data collector configuration from all application server instances in a profile, perform the following steps:
    a. Navigate to the $appserverhome/bin directory.
    b. Run the command osgiCfgInit.sh/bat -all on Windows or osgiCfgInit.sh -all on UNIX or Linux.
26. Restart the application server instance that was monitored by the data collector.

Appendix B. Restoring the WebSphere Application Server configuration from a backup

If you configured a stand-alone application server instance for data collection either manually or with the configuration or migration utility and the application server fails to start, you must restore the application server configuration with your backup configuration. If you did not create a backup, contact IBM Support.

In a Network Deployment environment, if you configured an application server instance for data collection manually or with the configuration or migration utility and the application server fails to start, you have the following options:

- You can restore the application server configuration from a backup configuration. If you did not create a backup, contact IBM Support.
- You can manually unconfigure the data collector. The Deployment Manager and the node agent on the application server must be running. For more information, see Appendix A, "Manually removing data collector configuration from an application server instance," on page 155.

This section applies only to the Windows, UNIX, and Linux platforms.

To apply the backup configuration using the **restoreConfig** command, complete one of the following procedures:

- In a non-Network Deployment environment:
  1. Locate your backup configuration file. The default directory is *DC_home*/data. If several backup files are present, check the modification date and time of the file. It must be the date and time of the failed configuration. If you did not complete any other data collector configurations on the same host after the failed one, use the most recent file in the directory.
  2. Stop all instances of the application server.
  3. Run the **restoreConfig** command from the *Appserver_home*/profiles/*profile_name*/bin directory. The syntax is:

Table 26. Syntax of the restoreConfig command in a non-Network Deployment environment

Operating system	Syntax	Example
Windows	restoreConfig.bat *full_path_to_backup_file*	restoreConfig.bat "C:\Program Files\IBM\ITM\dchome \data\ WebSphereConfig_2006-04-22.zip"
UNIX or **Linux**	./restoreConfig.sh *full_path_to_backup_file*	./restoreConfig.sh /opt/IBM/ITM /dchome/data/ WebSphereConfig_2006-04-22.zip

     For more information about the arguments of the **restoreConfig** command, see the WebSphere Application Server v8.5 infocenter at the following URL: http://pic.dhe.ibm.com/infocenter/wasinfo/beta/index.jsp.
  4. Start the instance of the application server.
- In a Network Deployment environment:
  1. Locate your backup configuration file. The default directory is *DC_home*/data. If several backup files are present, check the modification date and time of the file; it must be the date and time of the failed configuration. If you did

not complete any other data collector configurations on the same host after the failed one, use the most recent file in the directory.

2. Stop all instances of the application server..
3. Create a temporary directory in any convenient path (*temp_directory*). On a UNIX or Linux host, create it under `/tmp`.
4. Run the `restoreConfig` command from the *Appserver_home*`/profiles/`*profile_name*`/bin` directory. The syntax is:

Table 27. Syntax of restoreConfig command, Network Deployment environment

Operating system	Syntax	Example
Windows	`restoreConfig.bat` *full_path_to_backup_file*	`restoreConfig.bat "C:\Program Files\IBM\itcam\WebSphere \DC\config_dc\backup\ WebSphereConfig_2006-04-22.zip" -location` *temp_directory*
UNIX or **Linux**	`./restoreConfig.sh` *full_path_to_backup_file*	`./restoreConfig.sh /opt/IBM/itcam/WebSphere/DC/config_dc /backup/WebSphereConfig_2006-04-22.zip -location` *temp_directory*

Running the `restoreConfig` command restores the original application server configuration to the temporary directory.

5. Copy the `server.xml`, `variables.xml`, and `pmi-config.xml` files from the following path:

   temp_directory`/`*restored_configuration_home*`/cells/`*cell_name*`/ nodes/`*node_name*`/servers/`*server_name*

   to the following path on the **Deployment Manager** host:

   Appserver_home`/profiles/`*profile_name*`/config/cells/`*cell_name*`/ nodes/`*node_name*`/servers/`*server_name*
6. Complete a node sync from the Deployment Manager administrative console for the node.
7. In the Deployment Manager administrative console, save changes to the master configuration.
8. Start the instance of the application server. .

Appendix C. Setting up security

Setting up optional security for IBM Tivoli Composite Application Manager for WebSphere Application Server (ITCAM for WebSphere Application Server) is described in this appendix.

Setting up the user ID and password for ITCAM for WebSphere Application Server on z/OS with global security enabled

About this task

Installing, configuring, and running ITCAM for WebSphere Application Server on z/OS with Global Security turned on might require additional steps, depending on your security configuration.

If WebSphere Global Security has been turned on, perform the following steps before running the `config.sh` script:

Procedure

1. Make sure the user ID you use to log on to UNIX System Services (z/OS UNIX System Services) and to run the `config.sh` script has read and write access to the IBM WebSphere Application Server configuration files. This user ID must also have permission to run the WebSphere Scripting Client script (`wsadmin.sh`).
2. Make sure the user ID you use to run `config.sh` is a member of the same UNIX group as the servant user ID. Since this user ID creates the ITCAM for WebSphere Application Server runtime directories for the server, the servant user ID must also have read and write access to these directories.
3. Make sure the user ID you use to run `config.sh` fulfills the requirements for Secure Sockets Layer (SSL) security.

   Background information:

   When Global Security is enabled, SSL security is always used by the administrative subsystem to secure administrative commands, the IBM WebSphere Application Server administrative console, and communications between IBM WebSphere Application Server processes (which includes the `wsadmin.sh` scripting facility). SSL support always provides a mechanism by which the server proves its identity.

   In addition, SSL support on IBM WebSphere Application Server for z/OS allows the following ways for a client to prove its identity:

   - Basic authentication (also known as SSL Type 1 authentication), in which a client proves its identity to the server by passing a user identity and password known by the target server
   - Client certificate support, in which both the server and client supply digital certificates to prove their identities to each other

   For the client to authenticate the server, the server (actually, the controller user ID) must possess a signed certificate created by a certificate authority. The server passes the signed certificate to prove its identity to the client. The client must possess the CA certificate from the same certificate authority that issued the server certificate. The IBM WebSphere Application Server customization dialogs generate jobs that, among other things, define the user IDs for the various IBM WebSphere Application Server regions (Deployment Manager,

Node Agent, Server Controller, and Servant tasks). These jobs also specify user IDs that can be used to log on to the IBM WebSphere Application Server administrative console. The RACF customization jobs create key rings for each of these user IDs and connect certificates to them. You can use one of these user IDs to perform the ITCAM for WebSphere Application Server setup if it also has the necessary permissions to access the IBM WebSphere Application Server configuration root files mentioned in step 1 on page 161.

If you do not already have a user ID with the necessary permissions and certificates for SSL security, you can define one. Complete the following procedure:

a. Find the following information:
   1) The user ID and group of the IBM WebSphere Application Server servant started task.
   2) The name of the CA certificate that was used to sign the controller user ID server certificate. (If configuring a server in a Network Deployment, find the name of the CA certificate that was used to sign the Deployment Manager server certificate).

   If you do not know the group ID of the servant ID, issue the TSO RACF command LISTUSER (LU) for servant task owner. For example:

```
LU WSSR1

USER=ASCR1  NAME=WAS APPSVR CR         OWNER=IBMUSER   CREATED=05.043
 DEFAULT-GROUP=WSCFG1    PASSDATE=N/A     PASS-INTERVAL=N/A
 ATTRIBUTES=PROTECTED
 REVOKE DATE=NONE   RESUME DATE=NONE
```

   This shows that the group default group name for the ID is `WSCFG1`.

b. Define a user ID you use exclusively for running the ITCAM for WebSphere Application Server setup configuration using the TSO RACF command ADDUSER (AU). For example:

```
AU ITCAMWS NAME('ITCAM for WAS USER') PASSWORD(password) -
      OWNER(IBMUSER) DFLTGRP(WSCFG1) UACC(READ) -
   TSO(ACCTNUM(ACCT#) PROC(GENERAL) -
      SIZE(200000) MAXSIZE(200000)) -
   OMVS(HOME(/u/itcamws) PROGRAM(/bin/sh) UID(00001234))
```

   The TSO segment for this user profile is required if you intend to run the ITCAM for WebSphere Application Server setup from TSO OMVS. This same user ID is used for the ITCAM for WebSphere Application Server JMX client (see step 8 on page 163 for information about how to manually define the user ID and password for the ITCAM for WebSphere Application Server JMX client).

c. Create a keyring for this user ID, and have the cell signing CA certificate placed on it, as follows:

```
RACDCERT ID(ITCAMWS) CONNECT -
(RING(WASKeyring) LABEL('WebSphereCA') CERTAUTH)
```

   Access to keyrings and certificates is protected by RACF by a set of profiles in the FACILITY class. Although the keyring is associated with the user ID, the user must have read authority to the IRR.DIGTCERT.LISTRING profile in order to access its keyring. The user must also have read access to the IRR.DIGTCERT.LIST profile to be able to access its certificate.

4. If you selected Use SAF EJBROLE profiles to enforce J2EE roles during security domain setup in the IBM WebSphere Application Server Customization Dialogs,

make sure the user ID you use to run `config.sh` has read access to the EJBROLE administrator profile. The following administrative roles were defined by the customization jobs:

```
RDEFINE EJBROLE (optionalSecurityDomainName.) administrator UACC(NONE)
RDEFINE EJBROLE (optionalSecurityDomainName.) monitor       UACC(NONE)
RDEFINE EJBROLE (optionalSecurityDomainName.) configurator  UACC(NONE)
RDEFINE EJBROLE (optionalSecurityDomainName.) operator      UACC(NONE)
```

Ideally, your user ID will be a member of the servant ID group, which is already granted permission to these profiles.

5. For any RACF classes whose profiles have been added or modified, refresh the RACF cache. To do this, an authorized RACF administrator must issue the following command:

   ```
   SETROPTS RACLIST(classname) GENERIC(classname) REFRESH
   ```

6. Use the WebSphere Scripting Client directly to see if the user ID is set up correctly. From a z/OS UNIX System Services session, change to the bin directory of IBM WebSphere Application Server and issue the following command:

   ```
   ./wsadmin.sh –user itcamws –password itcamws
   ```

   If the user ID is set up correctly, a messages similar to the following is displayed:

   ```
   WASX7209I: Connected to process "dmgr" on node PLEX1Manager using SOAP
    connector;  The type of process is: DeploymentManager WASX7029I: For
    help, enter: "$Help help"
   ```

7. Enter `quit` to terminate the WebSphere Scripting Client.
8. If needed, change the user ID and password used by the ITCAM for WebSphere Application Server JMX client. The `config.sh` script configures the ITCAM for WebSphere Application Server JMX client security using the user ID and password that you supply in the `config.sh` script.

Enabling privacy filtering

About this task

When the `secure.filter.on` property is set to `true`, SQL, cookie, and HTTP Request query strings are filtered out. These strings are not collected by ITCAM for WebSphere Application Server.

Procedure

1. Stop the application server instance that is being monitored by ITCAM for WebSphere Application Server.
2. Set the following property definition in the *install_home*`/runtime/`*appserver_version.node_name.server_name*`/`*appserver_version.node_name.server_name*`.datacollector.properties`: file

   ```
   secure.filter.on=true
   ```

3. Start the application server instance that is being monitored by ITCAM for WebSphere Application Server.

Results

The following statement is printed out to the ITCAM for WebSphere Application Server log when privacy filtering is properly configured:

```
Privacy Filter is On. Http Request Query String, SQL String and Http Cookie data is
not trasmitted.
```

Appendix D. Install and configure the ITCAM Data Collector for WebSphere on a remote system

You can install and configure the ITCAM Data Collector for WebSphere to a remote system from the command prompt of the monitoring server.

You can use **tacmd executecommand** to install the data collector and configure it in silent mode. To use the **tacmd executecommand** command, the hub and remote monitoring servers must be at version 6.2.2 fix pack 2 or later. The target machine must have a ITM 6.2.2 fix pack 2 or later versions of agent deployed. For details about using `tacmd` commands, see *IBM Tivoli Monitoring Command Reference*.

All configured servers within a profile must run with the same version of the data collector. Having different versions of the data collector within one profile is not supported. Therefore, when you install the ITCAM Data Collector for WebSphere on the remote system, if an older version of the data collector exists, you will need to firstly run the migration utility (`migrate.sh`) before you configure the data collector. However, you do not need to configure all servers under one profile. For more information, see the *IBM Tivoli Composite Application Manager for Applications: Planning an Installation Guide*.

To install the ITCAM Data Collector for WebSphere from the command-line, complete the following procedure on the monitoring server:

1. Change to *ITM_HOME*\bin directory on Windows systems or *ITM_HOME*/bin on Linux or UNIX systems.
2. Use the following command to log in to the monitoring server:

   ```
   tacmd login -s TEMS hostname -u userid -p password
   ```

   Use the SYSADMIN user of IBM Tivoli Monitoring and password. For example:

   ```
   tacmd login -s machine01.raleigh.ibm.com -u user01 -p a1b2c3d4
   ```
3. Copy the installation tar file or compressed file to the remote system:

   On Windows systems:

   ```
   tacmd putfile -m System -s local_dir_path\archive_file
    -d remote_dir_path\archive_file -t bin
   ```

   On UNIX or Linux systems:

   ```
   ./tacmd putfile -m System -s local_dir_path/archive_file
    -d remote_dir_path/archive_file -t bin
   ```

   where:

   -m | --system
   Specifies on which managed system to execute the command.

   -s | --source
   Specifies the local file name.

   -d | --destination
   Specifies the remote file name.

   -t | --text
   Specifies the mode of transfer.
4. Create the data collector home directory on the remote system.

   On Windows systems:

   ```
   tacmd executecommand -m System -c "mkdir "DC_home"
   ```

On UNIX or Linux systems:

```
./tacmd executecommand -m System -c "mkdir DC_home"
```

where

-m|--system
Specifies on which managed system to execute the command.

-c|--commandstring
Specifies the command to run.

5. Extract the data collector installation files to the data collector home directory.

   On Windows systems, firstly ensure a compression utility is installed, the following command uses WinZip, but any Windows compatible compression utility will work. Run the following command:

   ```
   tacmd executecommand -m System -c "unzip.exe archive_file -d "DC_home""
   ```

   On UNIX or Linux systems:

   ```
   tacmd executecommand -m System -c "tar xvf  archive_file -C DC_home"
   ```

6. Specify the data collector configuration in a properties file on your local computer system. A sample properties file, `sample_silent_config.txt`, is available from the following location on the local system:

   On Windows systems: *DC_home*\bin
   On Linux and UNIX: *DC_home*/bin

7. Copy the *silent_file* to the remote system using the **tacmd putfile** command.

   On Windows systems:

   ```
   tacmd putfile -m System -s local_dir_path\silent_file
    -d remote_dir_path\silent_file -t text
   ```

   On UNIX or Linux systems:

   ```
   ./tacmd putfile -m System -s local_dir_path/silent_file
    -d remote_dir_path/silent_file -t text
   ```

8. Set the location of the Java home directory:

   On Windows systems:

   ```
   tacmd executecommand -m System -c "set JAVA_HOME=path_to_java_home& config.bat
   -silent path_to_silent_file\silent_file.txt"
   ```

   On UNIX or Linux systems:

   ```
   ./tacmd executecommand -m System -c "export JAVA_HOME=/opt/path_to_java_home; ./config.sh
   -silent /path_to_silent_file/silent_file.txt" -w path_to_dc_home/bin
   ```

   On Solaris systems:

   ```
   ./tacmd executecommand -m System -c "JAVA_HOME=path_to_java_home; export JAVA_HOME; ./config.sh
   -silent /path_to_silent_file/silent_file.txt" -w path_to_dc_home/bin
   ```

9. Restart the application server instances.
   a. Stop the application server.

      On Windows systems:

      ```
      tacmd executecommand -m System -c "stopServer.bat server_name" -w profile_home\bin
      ```

      On UNIX or Linux systems:

      ```
      ./tacmd executecommand -m System -c "./stopServer.sh server_name" -w profile_home/bin
      ```

   b. Start the application server:

      On Windows systems:

      ```
      tacmd executecommand -m System -c "startServer.bat server_name -w profile_home\bin"
      ```

      On UNIX or Linux systems:

      ```
      ./tacmd executecommand -m System -c "./startServer.sh server_name" -w profile_home\bin
      ```

For more information about remote deployment, see the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Appendix E. Using regular expressions

Regular expressions are sets of symbols and characters that are used to match patterns of text. You can use regular expressions to search specific IP addresses across your web environment. Regular expressions also enable you to search a simple, fixed URI or a complex URI pattern that matches one or more groups of transactions.

This appendix contains the following sections:

Regular expressions library

An extensive library of regular expression characters and operators is available for your URI filters and IP address specifications. The International Components for Unicode (ICU) open-source development project provides this library for your use. For a full description of the ICU regular expression library and an explanation of how to use the characters and operators for complex expressions, see: http://oss.software.ibm.com/icu/userguide/regexp.html.

Frequently used regular expressions

The following list highlights characters and operators most frequently used in regular expressions:

\ Quotes the character that follows it, which treats that character as a literal character or operator (not a regular expression). When you want the following characters to be treated as literal, precede them with a backslash:

```
* ? + [ ( ) { } ^ $ | \ . /
```

In other words, use a backslash followed by a forward slash (\/) to include a forward slash in a URI filter. Use a backslash followed by a period (\.) to include a period in a URI filter.

Example: to specify the URI pattern `http://www.ibm.com/`, use the following regular expression:

```
http:\/\/www\.ibm\.com\/
```

To specify all URIs that begin with `http://www.ibm.com/`, use the following regular expression:

```
http:\/\/www\.ibm\.com\/.*
```

. Matches any one character.

Example: to match both `ibm2` and `ibm3` within a string, use `ibm.` such as in the following example: **`http:\/\/www\.ibm.\.com\/`**

(?: ...)

Non-capturing parentheses. Groups the included pattern, but does not provide capturing of matching text. Somewhat more efficient than capturing parentheses.

Example: you can use the non-capturing parenthesis to group expressions to form more complicated regular expressions. To match a URI that starts with one of the following: `http://www.ibm.com/marketing/` or `http://www.ibm.com/sales/`, do a grouping with a pipe sign (`|`) (represents *or*):

```
http://www.ibm.com/(?:marketing)|(?:sales)/
```

* Matches the preceding element zero or more times. Quote this character:

Example: the expression, **`ca*t`**, matches `cat`, `caat`, `ct`, and `caaaaat`. The term `cabt`, would not return as a match.

Specifying exclusions with the bang (!) operator (Quality of Service listening policies only)

You can use an exclamation point (**!**), also called the *bang* operator, to filter out transactions that might match the regular expressions already entered, but that should not be considered valid transactions for this listening policy. These exclusions are considered negative filters. You can enter these exclusions as additional URI or client IP filters. The formatting of these additional filters is as follows:

URI Filter Exclusions

Use only fixed strings. For example, you can use the following strings:

!http://www.ibm.com/
!http://www.ibm.com/hr/index.html
!http://www.ibm.com/it/errorpage.html

Client IP Exclusions

The following options are valid:

!*.24.45.46
!12.*.45.56
!12.24.*.56
!12.24.45.*
!12.24.45.56

You can replace any "octet" (there are four in an IP address: octet . octet . octet . octet) with a wildcard (*). Note that this is not the regular expression wildcard (.*) from the positive filters.

Appendix F. Accessibility

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. These are the major accessibility features you can use with ITCAM for WebSphere Application Server when accessing it through the *IBM Personal Communications* terminal emulator:

- You can operate all features using the keyboard instead of the mouse.
- You can read text through interaction with assistive technology.
- You can use system settings for font, size, and color for all user interface controls.
- You can magnify what is displayed on your screen.

For more information about viewing PDFs from Adobe, go to the following website: http://www.adobe.com/accessibility/index.html.

Trademarks

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

Adobe is either a registered trademark or a trademark of Adobe Systems Incorporated in the United States, other countries, or both.

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

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

Windows is a trademarks of Microsoft Corporation in the United States, other countries, or both.

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

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

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

Notices

This information was developed for products and services offered in the U.S.A. IBM might 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 might 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 IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY 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 or changes in the product(s) or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites 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 want to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information might 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 might vary significantly. Some measurements might 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 might have been estimated through extrapolation. Actual results might 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.

COPYRIGHT LICENSE:

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

Readers' Comments — We'd Like to Hear from You

IBM Tivoli Composite Application Manager for WebSphere Application Server 7.2 support for WebSphere Application Server 8.5
Installation and User Guide

Publication No. GC23-9701-01

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

Comments:

Thank you for your support.

Submit your comments using one of these channels:
- Send your comments to the address on the reverse side of this form.
- Send a fax to the following number: 800-555-1213
- Send your comments via email to: phred@us.ibm.com
- Send a note from the web page: http://w3-03.ibm.com/ids/page/636

If you would like a response from IBM, please fill in the following information:

Name	Address
Company or Organization	
Phone No.	Email address

Readers' Comments — We'd Like to Hear from You
GC23-9701-01

IBM

Cut or Fold
Along Line

Fold and Tape | **Please do not staple** | Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM
ATTN: Dept 542
3905 37th Street NW
Rochester, MN
USA
55901-6666

Fold and Tape | **Please do not staple** | Fold and Tape

GC23-9701-01

Cut or Fold
Along Line

Product Number:

Printed in USA

GC23-9701-01