IBM Tivoli Composite Application Manager
Version 6.1.0.4

# *Agent for J2EE Data Collector Installation and Configuration Guide*

SC27-2823-02

IBM Tivoli Composite Application Manager
Version 6.1.0.4

# *Agent for J2EE Data Collector Installation and Configuration Guide*

SC27-2823-02

**Note:**

Before using this information and the product it supports, read the information in “Notices” on page 243.

# Contents

# Figures

# Tables

# About this publication

This publication provides information about installing, customizing, starting, and maintaining ITCAM Agent for J2EE Data Collector on Windows, Linux, and UNIX systems.

**Important:** The version of the Data Collector is the same as was shipped with ITCAM for J2EE 6.1 fix pack 4. The product name "ITCAM for J2EE" is still used in the user interface and in this document.

## Intended audience

This publication is for administrators or advanced users wanting to install or modify the configuration of ITCAM Agent for J2EE. The publication assumes that readers are familiar with maintaining operating systems, administering Web servers, 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
- Web servers, such as IBM® HTTP Server and Apache HTTP Server
- Application servers, such as WebLogic, NetWeaver, JBoss, Oracle, and Tomcat, and J2SE applications
- Internet protocols such as HTTP, HTTPS, TCP/IP, Secure Sockets Layer (SSL), and Transport Layer Security (TLS)
- Digital certificates for secure communication

## Publications

This section lists publications in the product library and related documents. It also describes how to access Tivoli® publications online and how to order Tivoli publications.

### ITCAM for Application Diagnostics library

The following publications are included in the ITCAM for Application Diagnostics library, available at http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/topic/com.ibm.itcamfad.doc_7101/ic-homepage.html:

- *IBM Tivoli Composite Application Manager for Application Diagnostics: Prerequisites*

  Provides the hardware and software requirements for installing ITCAM for Application Diagnostics components.
- *IBM Tivoli Composite Application Manager for Application Diagnostics: User's Guide*

  Provides the user overview, user scenarios, and Helps for every ITCAM for Application Diagnostics component.
- *IBM Tivoli Composite Application Manager for Application Diagnostics: Planning an Installation*

  Provides the user with a first reference point for a new ITCAM for Application Diagnostics installation or upgrade.
- ITCAM Agent for WebSphere® Applications Installation and Configuration Guides:

  - *IBM Tivoli Composite Application Manager: Agent for WebSphere Applications Installation and Configuration Guide*
  - *IBM Tivoli Composite Application Manager: Agent for WebSphere Applications Installation and Configuration Guide for z/OS*
  - *IBM Tivoli Composite Application Manager: Agent for WebSphere Applications Data Collector Installation and Configuration Guide for IBM i*

  Provide installation instructions for setting up and configuring ITCAM Agent for WebSphere Applications on distributed, z/OS®, and IBM i systems.
- ITCAM Agent for J2EE Applications Installation and Configuration Guides:
  - *IBM Tivoli Composite Application Manager: Agent for J2EE Data Collector Installation and Configuration Guide*
  - *IBM Tivoli Composite Application Manager: Agent for J2EE Monitoring Agent Installation and Configuration Guide*

  Provide installation instructions for setting up and configuring ITCAM Agent for J2EE.
- *IBM Tivoli Composite Application Manager: Agent for HTTP Servers Installation and Configuration Guide*

  Provides installation instructions for setting up and configuring ITCAM Agent for HTTP Servers.
- *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*

  Provides installation instructions for setting up and configuring ITCAM for Application Diagnostics Managing Server.
- *IBM Tivoli Composite Application Manager for Application Diagnostics: Troubleshooting Guide*

  Provides instructions on problem determination and troubleshooting for ITCAM for Application Diagnostics.
- *IBM Tivoli Composite Application Manager for Application Diagnostics: Messaging Guide*

  Provides information about system messages received when installing and using ITCAM for Application Diagnostics.

## Related publications

The following documentation also provides useful information:

- IBM Tivoli Documentation Central:

  Information about IBM Tivoli Documentation is provided on the following Web site:

  https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli Documentation Central
- IBM DB2®:

  Information about IBM DB2 is provided on the following Web site:

  http://www.ibm.com/software/data/sw-library/
- IBM Tivoli Enterprise Console®:

  Information about IBM Tivoli Enterprise Console is provided on the following Web site:

  http://submit.boulder.ibm.com/tividd/td/EnterpriseConsole3.9.html
- IBM Tivoli Data Warehouse:

  Information about IBM Tivoli Data Warehouse is provided on the following Web site:

https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Documentation%20Central/page/Tivoli%20Data%20Warehouse

- IBM Tivoli Change and Configuration Management Database:

  Information about IBM Tivoli Change and Configuration Management Database is provided on the following Web site:

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

- IBM Support Assistant:

  Information about IBM Support Assistant is provided on the following Web site:

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

## Accessing terminology online

The *Tivoli Software Glossary* includes definitions for many of the technical terms related to Tivoli software. The *Tivoli Software Glossary* is available at the following Tivoli software library Web site:

http://publib.boulder.ibm.com/tividd/glossary/tivoliglossarymst.htm

The IBM Terminology Web site consolidates the terminology from IBM product libraries in one convenient location. You can access the Terminology Web site at the following Web address:

http://www.ibm.com/software/globalization/terminology

## Accessing publications online

The documentation CD contains the publications that are in the product library. The format of the publications is PDF, HTML, or both.

IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli software information center Web site. Access the Tivoli documentation center at the following Web address:

https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli Documentation Central

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

The IBM Software Support Web site provides the latest information about known product limitations and workarounds in the form of technotes for your product. You can view this information at the following Web site:

http://www.ibm.com/software/support

## Ordering publications

You can order many Tivoli publications online at the following Web site:

http://www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi

You can also 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 Tivoli publications. To locate the telephone number of your local representative, perform the following steps:

1. Go to the following Web site:

   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 panel 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 J, "Accessibility," on page 235.

## Application Performance Management community on Service Management Connect

Connect, learn, and share with Service Management professionals: product support technical experts who provide their perspectives and expertise.

Access Service Management Connect at https://www.ibm.com/developerworks/servicemanagement/apm/index.html. Use Service Management Connect in the following ways:

- Become involved with transparent development, an ongoing, open engagement between other users and IBM developers of Tivoli products. You can access early designs, sprint demonstrations, product roadmaps, and prerelease code.
- Connect one-on-one with the experts to collaborate and network about Tivoli and the (enter your community name here) community.
- Read blogs to benefit from the expertise and experience of others.
- Use wikis and forums to collaborate with the broader user community.

## Tivoli technical training

For Tivoli technical training information, refer to the following IBM Tivoli Education Web site:

http://www.ibm.com/software/tivoli/education/

## Support information

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

**Online**

Go to the IBM Software Support at the following Web site:

http://www.ibm.com/software/support/

Follow the instructions.

**IBM Support Assistant**
The IBM Support Assistant (ISA) is a free local software serviceability workbench that helps you resolve questions and problems with IBM software products. The ISA provides quick access to support-related information and serviceability tools for problem determination. To install the ISA software, see the instructions for installing ISA in the Data Collector installation guide.

**Troubleshooting Guide**
For more information about resolving problems, see the corresponding part in *IBM Tivoli Composite Application Manager for Application Diagnostics: Troubleshooting Guide*.

# Conventions used in this publication

This publication uses several conventions for special terms and actions, operating system-dependent commands and paths, and margin graphics.

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

## Operating-system-dependent variables and paths

This document uses the UNIX convention for specifying environment variables and for directory notation.

When using the Windows command line, replace **$***variable* with **%***variable***%** for environment variables and replace each forward slash (**/**) with a backslash (\) in directory paths. The names of environment variables are not always the same on Windows and UNIX systems. For example, %TEMP% on Windows is equivalent to $tmp on UNIX systems.

**Note:** If you are using a UNIX shell on a Windows system, you can use the UNIX conventions.

## 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 xiii. 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 ITCAM Agent for J2EE Data Collector is installed. The following table shows the default locations:

*Table 1. Default locations for DC_home*

| | |
|---|---|
| **UNIX** or **Linux** | `/opt/IBM/itcam/J2EE/DC` |
| **Windows** | `C:\Program Files\IBM\itcam\J2EE\DC` |

- *AppServer_home*: the directory where the application server's core product files are installed.
- *instance_runtime_directory*: the directory where Data Collector stores the files controlling the instrumentation of a particular application server instance. This location depends on the application server type.

*Table 2. Locations for instance_runtime_directory*

| | |
|---|---|
| WebLogic | If the monitored server instance is represented by a WebLogic machine:<br>*DC_home*/runtime/wls*app_server_version*.*domain_name*.*machine_name*.*instance_name*<br>else:<br>*DC_home*/runtime/wls*app_server_version*.*domain_name*.*host_name*.*instance_name* |
| Tomcat | *DC_home*/runtime/tomcat*app_server_version*.*host_name*.*instance_name* |
| Sun Java™ System Application Server (JSAS) | *DC_home*/runtime/sjsas*app_server_version*.*domain_name*.*node_name*.*instance_name* |
| JBoss | *DC_home*/runtime/jboss*app_server_version*.*host_name*.*instance_name* |
| NetWeaver | *DC_home*/runtime/netweaver*app_server_version*.*sap_node_ID_host_name*.*sap_instance_number* |
| Oracle | *DC_home*/runtime/oracle*app_server_version*.*host_name*.*node_name*.*instance_name* |
| J2SE | *DC_home*/runtime/j2se.*application_name*.*host_name*.*instance_name* |

**Note:** The paths are provided here with UNIX style slashes, /; for Windows, use backslashes \.

- *custom_directory*: the directory where Data Collector custom properties files are located. These files contain values specific to a particular configuration. The location of this directory is *instance_runtime_directory*/custom .

# Chapter 1. Overview of ITCAM Agent for J2EE Data Collector

IBM Tivoli Composite Application Manager (ITCAM) Agent for J2EE Data Collector monitors applications in the J2EE environment. It can communicate monitoring information to the Managing Server and the Monitoring Agent.

**Important:** The version of the Data Collector is the same as was shipped with ITCAM for J2EE 6.1 fix pack 4. The product name "ITCAM for J2EE" is still used in the user interface and in this document.

**Important:** IBM Tivoli Composite Application Manager Agent for J2EE is a component of ITCAM for Application Diagnostics, Version 7.1. It is also a component of ITCAM for Applications, Version 6.2.3. If you are using ITCAM for Applications the Managing Server (deep dive) functionality is not available; please ignore all references to this functionality in this document.

## Overview of the monitoring process

### Data Collector

A Data Collector runs on each monitored J2EE application server, and communicates essential operational data to the Managing Server and the Monitoring Agent. Unique sampling algorithms maintain low CPU and network overhead while providing application specific performance information.

Many Data Collectors can work with a single Managing Server. The communication between Data Collectors and the Managing Server is independent of platforms.

### Managing Server

The Managing Sever is an application that is configured within a J2EE application server. The Managing Server is shared by all of the monitoring software's components and servers as the control center. The Managing Server collects information from, and provides services to, the Data Collectors in your environment.

### Monitoring Agent

The Monitoring Agent collects information from the Data Collector, as well as J2EE application server log messages and garbage collection activity records. It passes the information to a Tivoli Enterprise Monitoring Server, for use in the IBM Tivoli Monitoring infrastructure.

A Monitoring Agent can communicate with many Data Collectors. Typically, install the Monitoring Agent on every monitored host, so that every Data Collector communicates with a local Monitoring Agent.

## System and software prerequisites

The software and hardware requirements are available from the software product compatibility reports website.

**Note:** For Data Collector installation on Oracle 9i, ensure you have bc installed on your server before starting the installation process. The version should be bc-1.06-5 or higher.

# Chapter 2. Installing the ITCAM for J2EE Data Collector on Windows

This chapter provides complete instructions for installing the ITCAM for J2EE Data Collector (DC) on Windows XP and 2003 for the supported application servers. For advanced users who prefer to input installation information once through a response file instead of repeatedly inputting data, the ITCAM for J2EE Data Collector provides a silent installation. For specific application servers, you need to perform the steps for pre-installation or post-installation. Perform the steps in the following sections:

- "Permission requirements to install Data Collector"
- If applicable, "Prerequisites for NetWeaver Data Collector installation"
- If applicable, "Three installation types of ITCAM for J2EE Data Collector for NetWeaver" on page 4
- Either "Installing the DC by InstallShield Wizard" on page 5 or "Performing a silent installation and configuration" on page 12

**Note:** Use only English characters and Arabic numbers for entering names and directories.

Note that all the screen captures in this chapter are taken from Data Collector installation on Tomcat for illustration purpose. Actual screen displays may vary by platform.

## Prerequisites for installing ITCAM for J2EE Data Collector

After installing the Data Collector, several options will be added to the application server startup command. But on windows, there is a limitation on the length of the command line. The overall command length should be less than 8191 characters on windows XP/2003 and less than 2047 characters for windows 2000. Thus it is recommended to use a path with short length for the Data Collector installation. For example, for Oracle application server on Windows, it is recommended to use C:\DC as the Data Collector installation path.

### Permission requirements to install Data Collector

Depending on the version of the J2EE application server and the type of J2EE Data Collector to be installed, there are requirements on the file and directory permissions. When using a non-root user to install Data Collector, the user should check and make sure that the requirements are followed. For detailed information on file and directory permission requirements, refer to Appendix D, "Summary of permissions required for installing and configuring the Data Collector," on page 207

### Prerequisites for NetWeaver Data Collector installation

#### Pre-installation steps for NetWeaver server

1. Manually backup your NetWeaver database. Use the database admin user, such as db2j2e.
2. Make sure the NetWeaver system is running.

3. You need to gather the information of the directories of the **Server Home**, the **Central Instance Home**, and the **Central Instance Network Home**. For detailed information about the directories described, please refer to "Three installation types of ITCAM for J2EE Data Collector for NetWeaver."
4. Make sure you have got the system ID and the instance name.
5. For silent installation, use the configtool to get the server ID to be monitored.
6. You should know the Java Naming and Directory Interface (JNDI) port. The JNDI port is a P4 port of the NetWeaver server to be monitored.
7. If distributed dialog instance installation is selected as the installation type, mount the *Central instance home* on central instance computer to a local directory (For example, the absolute path of *Central instance home* on central instance computer on is C:\usr\sap\J2E\JC00, You should map or mount it to a local directory, such as \\<*hostname*>\usr\sap\J2E\JC00 or Y:\usr\sap\J2E\JC00), and make sure you have the writing rights. Where <hostname> is the IP address or qualified host name of the central instance computer.

**Note:** Be sure to use backslash at all time on Windows platform.

## Three installation types of ITCAM for J2EE Data Collector for NetWeaver

The ITCAM for J2EE Data Collector supports three types of installation. Before introducing the three types of installation, be familiar with the following parameters:

- *Server home*: The absolute path of directory wherein the instance is monitored.
- *Central instance home*: The absolute path of central instance home directory.
- *Central instance network home*: A local path mounted from central instance home directory.

### 1. Central instance installation

Install the ITCAM for J2EE Data Collector to monitor the NetWeaver server on the central instance. Specify the *Server home* for this installation type.

**Server home**: The absolute path of Central instance home directory (for example, C:\usr\sap\J2E\JC00).

**Note:** For the silent installation, the value of *Central instance home* and *Central instance network home* should be identical with the value of *Server home*.

### 2. Local dialog instance installation

Install ITCAM for J2EE DC to monitor the NetWeaver server on the dialog instance which is located on the same server as the central instance is. Specify the *Server home* and *Central instance home* for this installation type.

**Server home**: The absolute path of local dialog instance home directory (for example, C:\usr\sap\J2E\J01).

**Central instance home**: The absolute path of central instance home directory (for example, C:\usr\sap\J2E\JC00).

**Note:** For the silent installation, the value of *Central instance network home* should be identical with *Central instance home*.

### 3. Distributed dialog instance installation

Install ITCAM for J2EE DC on the dialog instance computer. The central instance is not installed on the same computer as the dialog instance. Specify *Server home*, *Central instance home*, and *Central instance network home* for this installation type.

**Server home**: The absolute path of distributed dialog instance home directory (for example, C:\usr\sap\J2E\J01).

**Central instance home**: The absolute path of central instance home directory (for example, C:\usr\sap\J2E\JC00).

**Central instance network home**: A local path mounted from central instance home directory (for example, Y:\usr\sap\J2E\JC00. This directory is the location where you mounted from the central instance home).

## Installing the DC by InstallShield Wizard

This section guides you through the DC installation process with a graphical user interface. Follow the proceeding instructions to perform the installation.

1. "Step 1: Launch the InstallShield Wizard"
2. "Step 2: Accept the product license agreement" on page 7
3. "Step 3: Choose the installation directory" on page 7
4. "Step 4: Generate a response file" on page 8
5. "Step 5: Review the installation summary" on page 9
6. "Step 6: Configure servers for data collection" on page 10
7. "Step 7: Finalize the installation" on page 11

### Step 1: Launch the InstallShield Wizard

Begin the installation by invoking the setup file. Load the ITCAM for J2EE Data Collector CD or open the directory with downloaded installation files, and double click to open the file setup_DC_w32.exe to begin the InstallShield Wizard.

If you insert the Data Collector installation CD, a Launch Pad window may be shown automatically. Select "Install ITCAM" in this window.

The log path window opens.


*Figure 1. The Log path window of the InstallShield Wizard*

If necessary, modify the path where the log files will be written. (The current user must have write access to the log path). Then click OK.

The Welcome window opens.

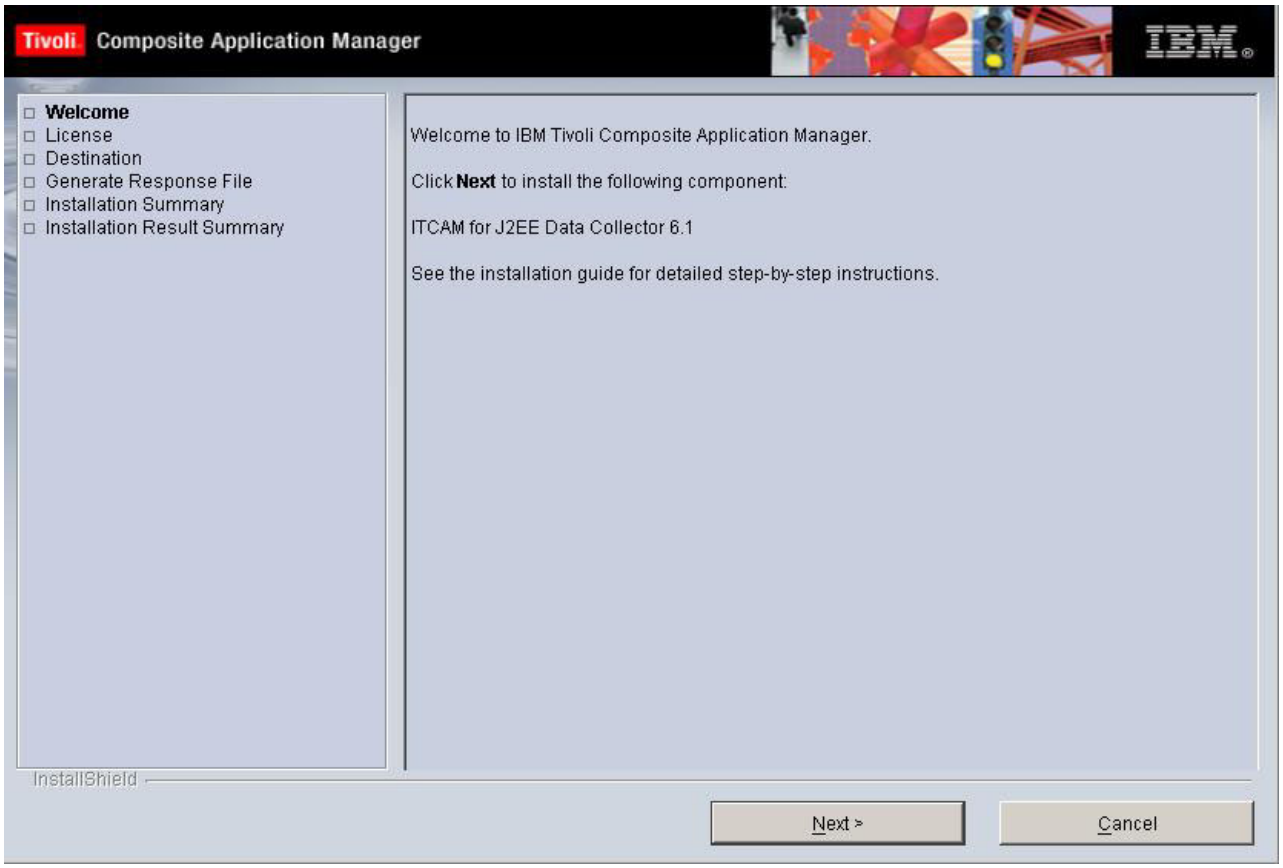



*Figure 2. The Welcome window of the InstallShield Wizard*

Click **Next**. You may exit the InstallShield Wizard at any time, and cancel the installation by clicking **Cancel**.

## Step 2: Accept the product license agreement

By clicking **Next** in the initial Welcome window to arrive at the product license agreement:

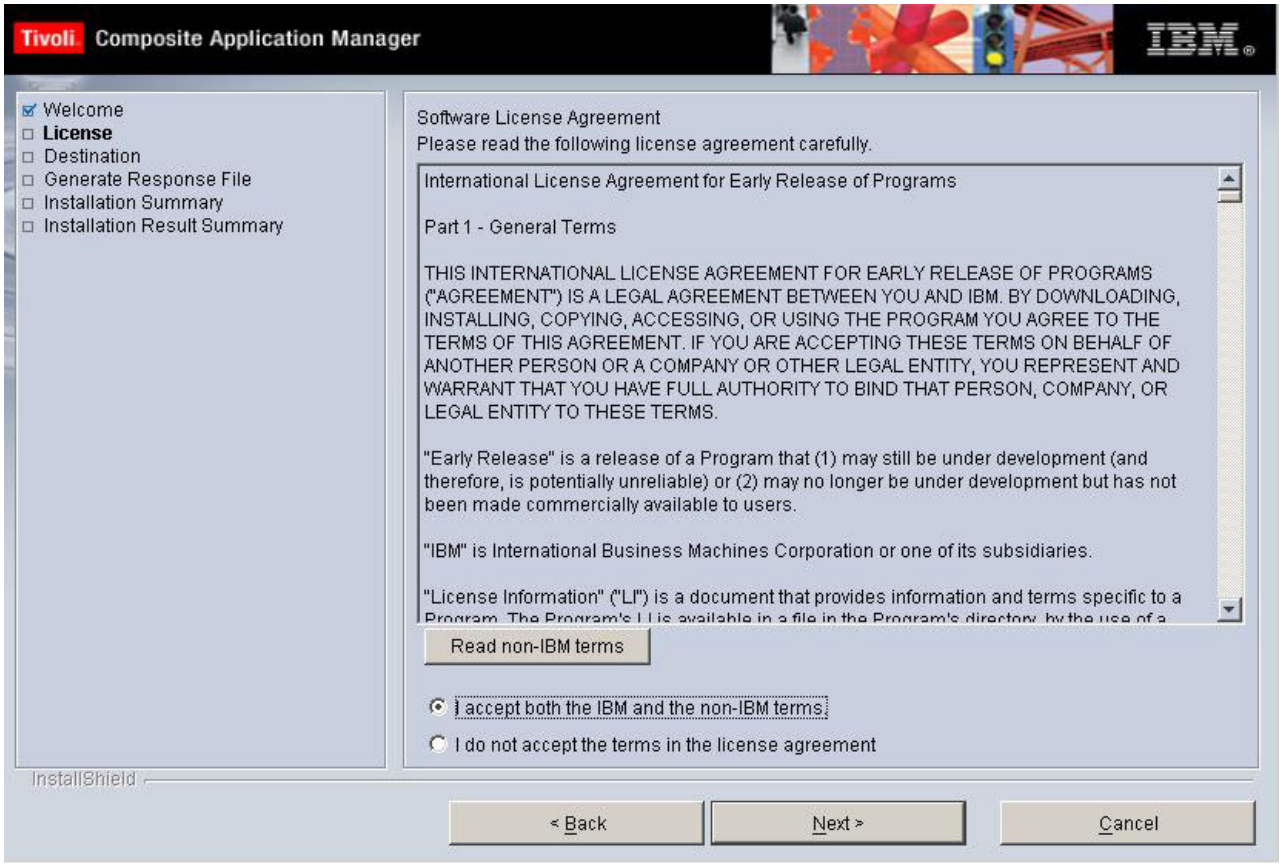



*Figure 3. Product license agreement*

Read through the product license agreement, and then click **I accept both the IBM and the non-IBM terms**. You must accept the product license in order to continue with the installation. Click **Next** .

## Step 3: Choose the installation directory

After accepting the product license you are prompted to select the destination in which the DC will be installed.

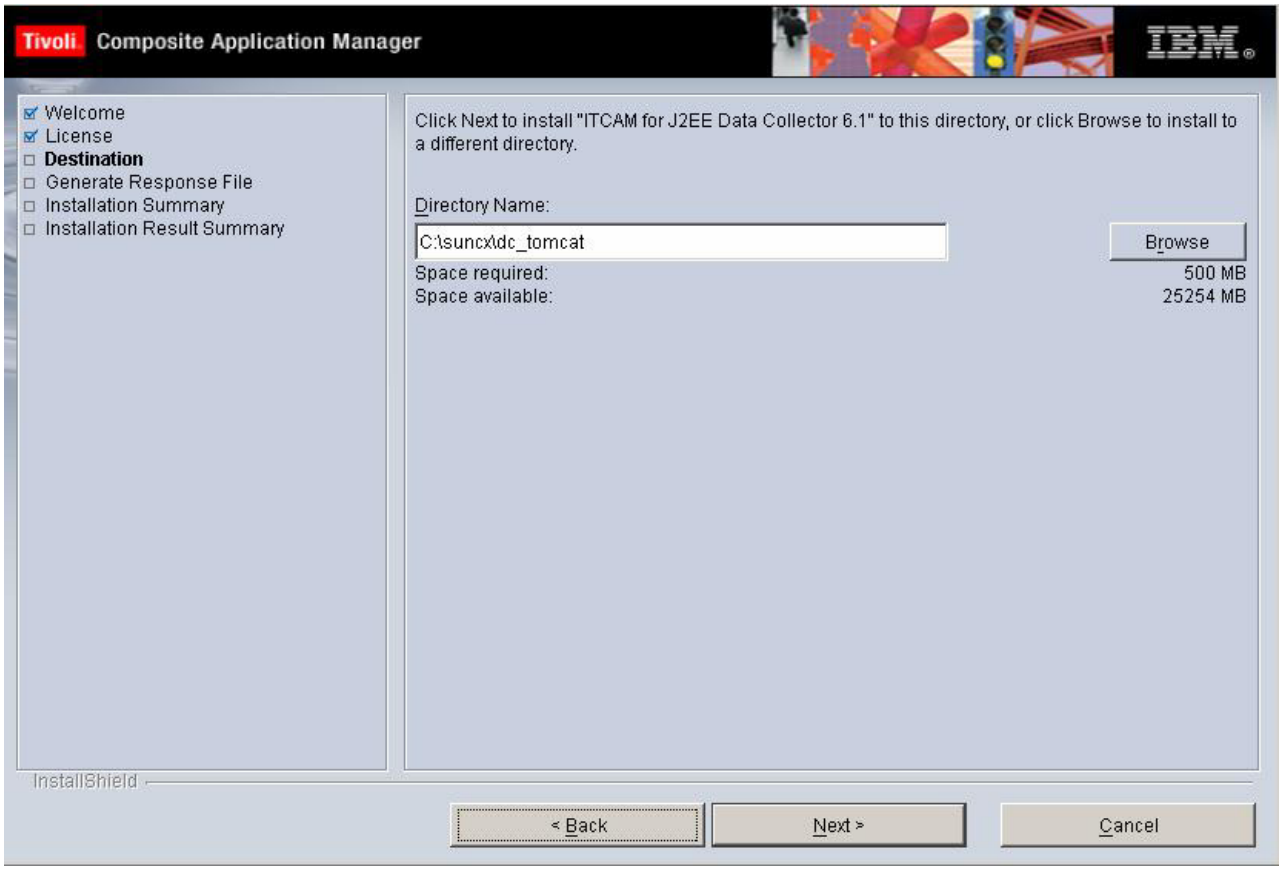



*Figure 4. Installation directory*

Either use the default directory *C:\IBM\itcam\J2EE\DC*, or click **Browse** to change the directory destination. If you are using an existing directory, make sure the directory is empty.

**Note:** You cannot install the Data Collector on an application server instance in a directory path (including profile, cell, node, and server names) that includes the following types of characters:

- Traditional Chinese
- Simplified Chinese
- Japanese
- Korean
- Spanish special characters
- German special characters
- Portuguese Brazilian special characters
- French special characters
- Italian special characters

Click **Next**.

## Step 4: Generate a response file

You can choose to generate a response file to save all your settings. It enables you to have the same installation settings when you want to install the Data Collector later again on this computer or on another computer by silent installation.

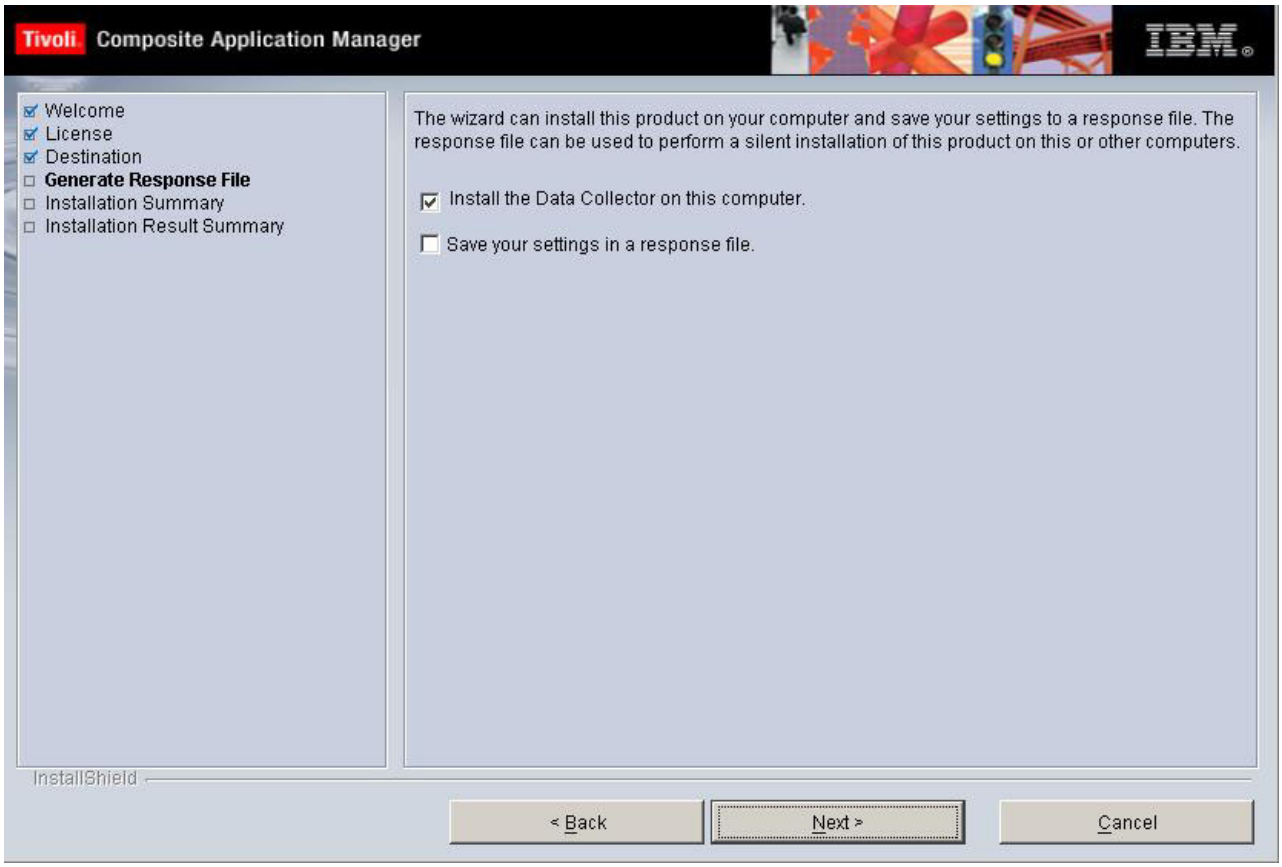



*Figure 5. Choose to save your settings in a response file*

**Install the Data Collector on this computer** is selected by default. If you wish to create a response file with all the settings in this installation, select **Save your settings in a response file**, and choose a location for the response file to generate.

Click **Next** to proceed.

## Step 5: Review the installation summary

A review summary is shown before the Data Collector is installed.

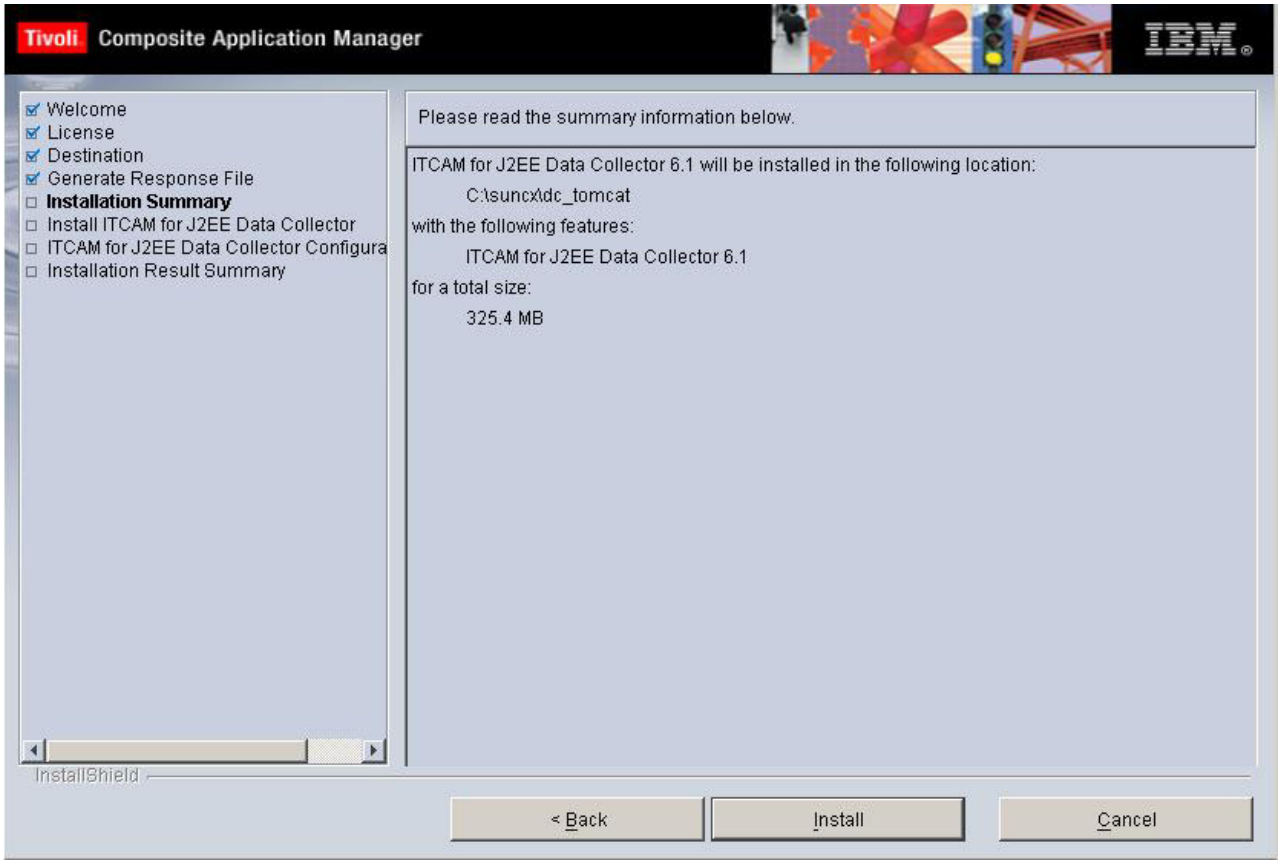



*Figure 6. Install summary preview*

Read through the summary of information, and ensure that your computer meets the prerequisite space requirements. To change the install location, click **Back** and select another destination directory. Click **Install**.

## Step 6: Configure servers for data collection

After the Data Collector is installed, the InstallShield Wizard prompts you to either configure servers for data collection, or to defer the configuration until a later time.

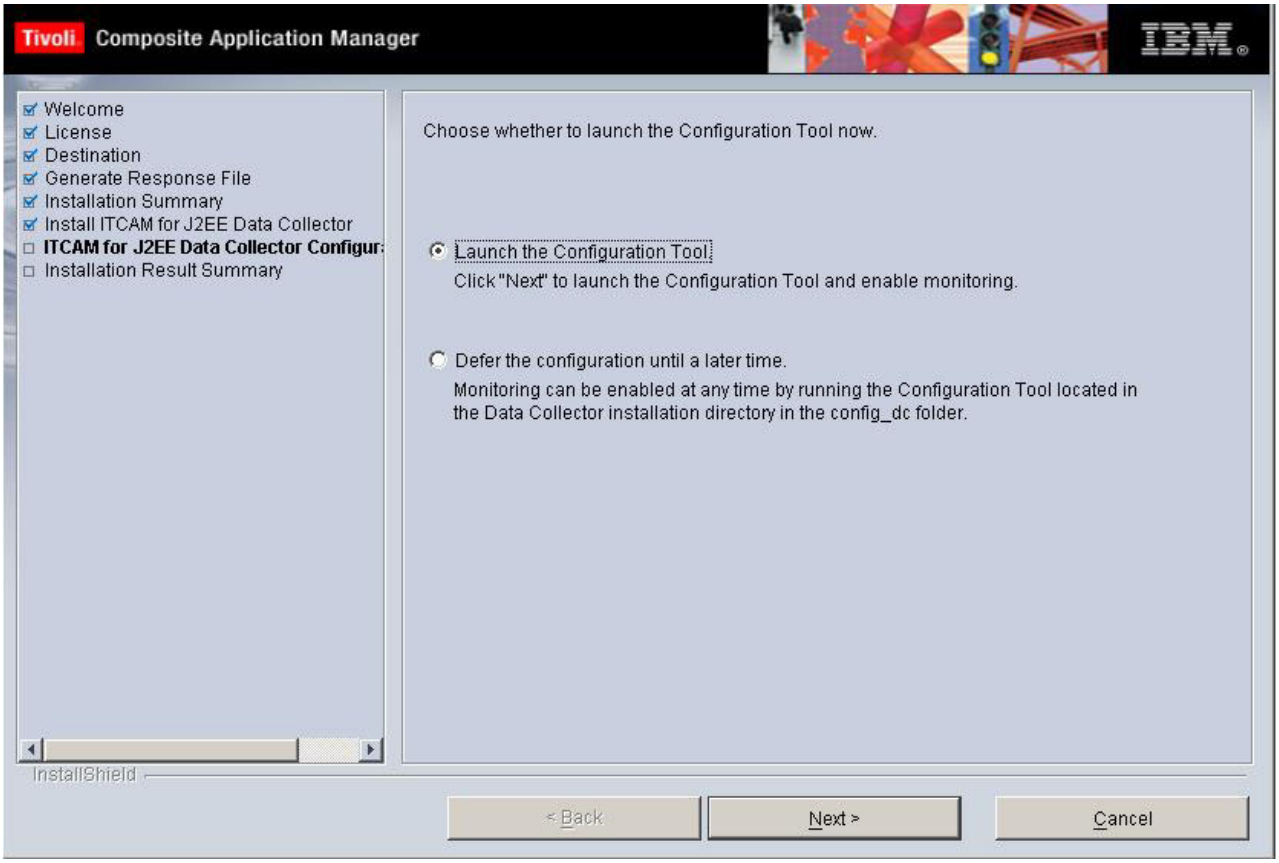



*Figure 7. Configuration Tool launch prompt*

Click **Launch the Configuration Tool** to open up the Configuration Tool and follow the Wizard through the configuration process, otherwise click **Defer the configuration until a later time**. The Configuration Tool can be invoked by **installer > config_dc> config_dc.bat** in the DC install directory.

For detailed information about configuring the DC to the Managing Server, refer to Chapter 4, “Configuring the ITCAM for J2EE Data Collector,” on page 83.

Click **Next** to proceed to the final installation summary.

## Step 7: Finalize the installation

A final summary of the results is shown after the DC is installed.

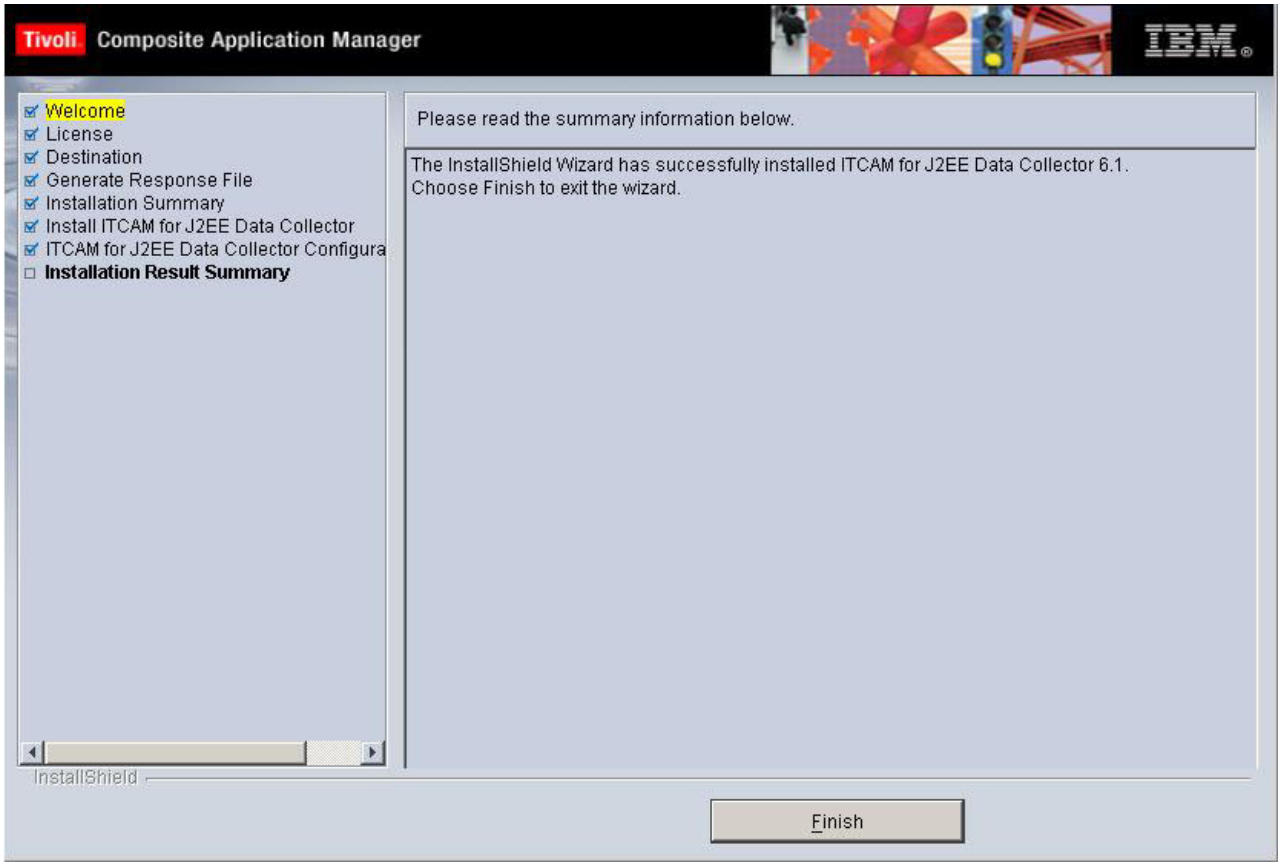



*Figure 8. Installation result summary*

Review the information, and then click **Finish** to finalize the installation and exit the InstallShield Wizard.

## Performing a silent installation and configuration

The ITCAM for J2EE Data Collector supports silent installation and configuration. In a silent installation/configuration, predefined parameters replace user interface interactions. Silent installation and configuration is useful for advanced users who prefer to input installation and configuration information once through a response file instead of repeatedly inputting data in an installation procedure.

Before editing the response file, note the following syntax rules:

- Comment lines begin with a number sign (#).
- Blank lines are ignored.
- Parameter lines are PARAMETER=value.
- Do not use a space before the parameter; you can use a space before or after an equal sign (=)
- Do not use any of the following characters in any parameter value:
  - Dollar sign ($)
  - Equal sign (=)
  - Pipe sign (|)

The following notes apply to silent installation and configuration:

**Note:**

1. By default, the installer will create log files in the following directory: C:\Program Files\IBM\tivoli\common\CYN\logs.
2. By default, the configuration program will create the garbage collection logs in the file *DC_home*/*ServerTypeServerVersion*-gc-log.log.*InstanceName*.
3. If you are using a startup script, the configuration program will produce a copy of the script as it was before the configuration. If a failure occurs after the configuration, you can use this copy of the script to switch back to the configuration of the application server before it was modified by the installer. The copy of the startup script will be named with a .orig extension. If the Data Collector configuration fails, no copy of the startup script gets produced, because the installer will not modify the original file.

You have the option to only install the Data Collector, both install and configure the Data Collector, or only configure the Data Collector using this procedure. If you only want to configure the Data Collector, perform this procedure after the Data Collector has been installed.

Perform the following procedure to run the silent installation command:

1. Log on to the computer on which you want to install and configure the Data Collector as a user with the proper permissions (see Appendix D, "Summary of permissions required for installing and configuring the Data Collector," on page 207).
2. Start the instance of the application server that will be monitored by the Data Collector.
3. If Terminal Services is enabled on **Windows 2000** or **Windows 2003 Server**: put the server into installation mode. Run the following command:

   ```
   change user /install
   ```

   **Note:** Ignore the message:

   ```
   Install mode does not apply to a Terminal server configured for remote
   administration.
   ```
4. Check the following Web site to see if the latest level of maintenance (such as fix packs or interim fixes) needs to be applied:

   http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliCompositeApplicationManagerforJ2EE.html

   If there is no maintenance you need to apply, you have the option to perform both the installation and configuration by running the executable file once and using one response file.

   If there is maintenance you need to apply, you must run the installation and configuration separately. After you perform the silent installation and before you perform the silent configuration, apply the latest level of maintenance.
5. If you will be configuring, or installing and configuring, the Data Collector, perform the applicable pre-configuration steps for the application server:

*Table 3. Pre-configuration steps for application servers*

| Application server type | Pre-configuration steps |
|---|---|
| WebLogic | If a customized script is used for starting the server, see "Pre-configuration steps for supporting customized startup script for WebLogic" on page 84 |
| NetWeaver | No pre-configuration steps required |

*Table 3. Pre-configuration steps for application servers (continued)*

| Application server type | Pre-configuration steps |
|---|---|
| JBoss | See "Pre-configuration steps for Tomcat users" on page 88<br><br>If a customized script is used for starting the server, also see "Pre-configuration steps for supporting customized startup script for JBoss" on page 85<br><br>If the Java Wrapper Service for Tomcat is used, also see "Pre-configuration steps for supporting Java Service Wrapper for Tomcat" on page 89 |
| Tomcat | If a customized script is used for starting the server, see "Pre-configuration steps for supporting customized startup script for Tomcat" on page 85 |
| Oracle | No pre-configuration steps required |
| J2SE | See "Pre-configuration steps for J2SE users" on page 90 |

6. Specify configuration options in one of the following response file templates and save the file:

*Table 4. Response file templates*

| Application server type | Sample response file |
|---|---|
| WebLogic | DC61_weblogic.opt |
| NetWeaver | DC61_netweaver.opt |
| JBoss | DC61_jboss.opt |
| Tomcat | DC61_tomcat.opt |
| Oracle | DC61_oracle.opt |
| J2SE | DC61_j2se.opt |

The file is located in *installation_image_directory*/silent. See the following sections for guidance on how to modify the file:

*Table 5. Application server specific configuration optionsfor Windows*

| Application Server | Silent Installation Response File Settings |
|---|---|
| WebLogic | "Silent installation and configuration settings for WebLogic" on page 16 |
| WebLogic Portal Server | "Silent installation and configuration settings for WebLogic Portal Server" on page 21 |
| NetWeaver | "Silent installation and configuration settings for NetWeaver" on page 26 |
| JBoss | "Silent installation and configuration settings for JBoss" on page 29 |
| Tomcat | "Silent installation and configuration for Tomcat" on page 32 |
| Oracle | "Silent installation and configuration for Oracle" on page 35 |
| J2SE | "Silent installation and configuration for J2SE" on page 38 |

**Note:**

a. If you are performing only the installation, options for the configuration will be ignored when running the silent installation.
b. If you are performing only the configuration, options for the installation will be ignored when running the silent configuration.
c. Optionally, you can use response files created by the GUI installation and configuration programs. Perform the following steps to make one response file from two generated response files:
   1) In both the Installation program and the Configuration tool, when the **Save settings to the response file** option is shown, select it and enter a file path name.
   2) With a text editor, copy and paste the contents of the response file generated from the installation program into the response file generated by the configuration program.
   3) Save the newly created response file with a unique name or in another location. Enter the name of this response file in in Step 8.

7. Complete one of the following steps:

*Table 6. Whether to use setup_DC_w32.exe or config_dc.bat*

| If you want to install or install and configure the Data Collector | If you only want to configure the Data Collector |
|---|---|
| Use the command-line interface to access the directory that contains the installation executable file. The setup_DC_w32.exe file is located in this directory. | Go to the *DC_home*/installer/config_dc directory. The config_dc.bat file is located in this directory. |

8. Type the following command and press **Enter**:

   ```
   executable_file -silent [-is:log [log_file_name]] [configuration_option...]
     -options response_file
   ```

   The *executable_file* specifies either setup_DC_w32.exe or config_dc.bat.

   The *log_file_name* specifies the path and name of the log file that the silent installer will write to. The file will be created even if it does not yet exist or if no name is specified. Wrap the path in double-quotes if it contains spaces.

   The *configuration_option* specifies one or more configuration options not included in the response file.

   The *response_file* specifies the response file you configured in Step 6 on page 14. Indicate the path and name of the file. Wrap the path in double-quotes if it contains spaces.

   For example:

   ```
   setup_DC_w32.exe -silent -is:log "C:\log\DClog.txt" -V DC_ASL_SOAPPORT="8885"
     -options C:\itcam\images\silent\DC6.opt
   ```

   ```
   config_dc.bat -silent -V DC_ASL_SOAPPORT="8885" -options
     C:\itcam\images\silent\DC6.opt
   ```

   **Note:**

   a. Configuration options specified in the response file take precedence over those entered in the command line. For a particular command-line configuration option to take effect, you must first nullify that option in the response file by commenting it out with a number sign (#).
   b. If you are performing a silent configuration (after the Data Collector has been installed), you cannot use the -is option. Instead run the command in the following way:

      ```
      config_dc.bat -silent [configuration_option...] -options response_file
      ```

For example:

```
config_dc.bat -silent -V DC_ASL_SOAPPORT="8885" -options
  C:\itcam\images\silent\DC6.opt
```

9. If you have performed only a silent installation (you indicated `LAUNCH_CONFIG="false"`), check the C:\Program Files\IBM\tivoli\common\CYN\logs\trace-install.log file to find out whether the installation was successful.
10. If you have just performed a silent installation (and are about to perform configuration) and there is maintenance you need to apply, do so from the following Web site:

    http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliCompositeApplicationManagerforJ2EE.html
11. If you have performed a silent configuration, or instalation and configuration, perform the applicable post-configuration steps for the application server:
    - See "Post-configuration steps for ITCAM for J2EE Data Collector" on page 147
    - If the application server uses Sun JDK 1.5 or HP JDK 1.5, see "Post-configuration steps for all application servers using Sun JDK 1.5 or HP JDK 1.5" on page 147
    - If the application server uses any version of the Sun JDK, see "Post-configuration steps for all application servers using Sun JDK" on page 148
    - Server-specific steps as per the folowing table:

*Table 7. Post-configuration steps for application servers*

| Application server type | Pre-configuration steps |
|---|---|
| WebLogic | See "Post-configuration steps for WebLogic users" on page 149 |
| NetWeaver | See "Post-configuration steps for NetWeaver" on page 151 |
| JBoss | No post-configuration steps required |
| Tomcat | See "Post-configuration steps for Tomcat users" on page 148 |
| Oracle | See "Post-configuration steps for Oracle users" on page 148 |
| J2SE | See "Post-configuration steps for J2SE" on page 150 |

    - See "Additional post-configuration tasks" on page 155
12. Start the Application Monitor interface of the Managing Server and verify that you can see the monitored data.

## Silent installation and configuration settings for WebLogic

*Table 8. WebLogic silent install parameter definitions for Windows*

| Parameter | Definition |
|---|---|
| LICENSE_ACCEPT_BUTTON | License agreement. You must specify this parameter to begin the product installation. Default setting is *true*. |

*Table 8. WebLogic silent install parameter definitions for Windows (continued)*

| Parameter | Definition |
|---|---|
| installLocation | The location where you intend to install the product. The default location for installation is: C:\Program Files\IBM\tivoli\itcam\ J2EE\DC |
| LAUNCH_CONFIG | This parameter launches the Configuration Tool. Specifying this parameter begins the process of configuring the DC to the Managing Server after installation. The default setting is *true*. |
| LOGSETTING.LOGLEVEL | The log level for the installation and configuration process. Possible values are: ALL / DEBUG_MAX / DEBUG_MID / INFO / WARN / ERROR / FATAL / OFF. |
| LOGSETTING.LOGCONSOLEOUT | This parameter controls whether the output message is printed to console or not. Possible values are true or false. |
| **DC Configuration** | |
| UNCONFIGURE_SERVERS | Specifying this parameter will cancel the configuration process after the installation is complete. The default setting is *false*. |
| J2EE_SELECTED | ITCAM for J2EE's Application Monitor interface. Specifying this parameter will configure monitored data to be accessed through ITCAM for J2EE's Application Monitor interface. To use the Application Monitor interface, the Managing Server must be available in your environment. The default is *true*. |
| TEMA_SELECTED | ITCAM for J2EE Tivoli Enterprise Portal . Specifying this parameter will configure monitored data to be accessed using the portal. To use the portal interface, ITCAM for J2EE and its components must be fully installed. The default is *false*. |
| SERVER_HOME | WebLogic directory location. Enter the root directory location in which WebLogic is located on the host server |
| SERVER_VERSION | WebLogic version number. Enter the version number of WebLogic that you are currently running |
| JAVA_HOME | The location of the JDK. Enter the directory location of the JDK that supports WebLogic. |
| IS64UNIXJVM | The flag for 64 bit model. The default value is *false*. If you are running a 64 bit OS using 64 bit JVM on a UNIX or Linux platform, change the parameter to*true*. Ignore this parameter on Windows. |

*Table 8. WebLogic silent install parameter definitions for Windows (continued)*

| Parameter | Definition |
|---|---|
| DC_OFFLINE_ALLOW | This is for you to decide whether offline configuration is allowed. If you enter "true", the program will skip the verification of the connection to Managing Server (MS) during configuration, and use the entered value of MS_AM_HOME; if you enter "false", the program will connect to MS and detect the MS home directory on MS server. The default value is *false*. |
| TEMA_OFFLINE_ALLOW | The option indicates whether offline configuration type is allowed during the configuation. The program will skip the monitoring agent connection test if it is set to be *true*. Set it to *false* when you don't want to allow the offline configuration for the monitoring agent. |
| AM_SOCKET_BINDIP | This is the DC side IP address or full qualified Host name. The IP or Host name will be used by DC to communicate with MS. If there are more then one NIC or multiple IP address configured on DC server, choose one of them. For example: -V AM_SOCKET_BINDIP=9.181.93.95 or -V AM_SOCKET_BINDIP=dc.cn.ibm.com or -V AM_SOCKET_BINDIP=<*value*> |
| FIREWALL_ENABLED | For DC side if the firewall is enabled, set the value to be *true*; otherwise, set the value to be *false*. |
| PROBE_RMI_POR | If the DC is behind firewall, set this port number. This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8200" to "8299". |
| PROBE_CONTROLLER_RMI_PORT | If the DC is behind firewall, set this port number. This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8300" to "8399". |
| **Managing-Server Specific Options** | |
| RECOLLECT_MSINFO | Specifying this parameter prompts the DC to recollect data from the Managing Server. The default is *true*. |
| MS_AM_HOME | The location of the Managing Server. Enter the directory location where the Managing Server is located. This parameter correlates the *DC_OFFLINE_ALLOW*. Refer to *DC_OFFLINE_ALLOW* for more detailed information. |
| KERNEL_HOST01 | Primary kernel server name. Enter full-qualified host name of the primary kernel server hosting the Managing Server. |
| PORT_KERNEL_CODEBASE01 | Primary kernel codebase port. The default is 9122. |

*Table 8. WebLogic silent install parameter definitions for Windows (continued)*

| Parameter | Definition |
|---|---|
| **Application Server Specific Options** | |
| WLHOST | WebLogic Server host name. Enter the IP or domain name of the host location of the WebLogic server. |
| WLPORT | WebLogic server port number. The default is 7001. |
| WLUSER | User name. This parameter is optional. Enter a user ID name to match your current security settings; otherwise, leave this blank. |
| WLPSWD | Password. This parameter is optional. Enter a password to match your current security settings; otherwise, leave this blank. |
| WLJNDI_TYPE | WebLogic admin server connection method. If you choose connect to the WebLogic admin server using plain socket or HTTP, set WLJNDI_TYPE to *t3* and ignore WL_SSL_* parameters. If you choose connect to the WebLogic admin server using SSL, set WLJNDI_TYPE to *t3s_oneway* for SSL one way connection or *t3s_twoway* for SSL two way connection. |
| WL_SSL_TRUST__KEYSTORE | SSL client CA trust keystore file. It is a *.jks* file. This parameter is for t3s_oneway and t3s_twoway. |
| WL_SSL_CERT_TYPES | SSL Certificate types. This parameter is for SSL two way connection only. The valid file format types are *DER* and *PEM*. Types of multiple certificates should be separated by a vertical bar ("\|"). Note that the certificate type should be corresponding to the certificate file in terms of sequence. |
| WL_SSL_CERT_FILES | SSL Certificate Files. This parameter is for SSL two way connection only. Set WL_SSL_CERT_FILES to RSA private key and chain of X.509 certificates for SSL client authentication. Multiple files are separated by a vertical bar ("\|"). Note that the sequence of the certificates matters. The SSL Client private key should be put as the first certificate. All but the first certificate are issuer certificates for the previous certificate. Example: *WL_SSL_CERT_FILES="C:\temp\testkey\client3.prv\|C:\temp\testkey\client3.pub\|C:\temp\testkey\netca_test_individual.cer"* |
| WL_SSL_KEY_PSWD | SSL client private key password. If the SSL client private key file is encrypted, set WL_SSL_KEY_PSWD to be the RSA private key's password; otherwise, leave it blank. |

*Table 8. WebLogic silent install parameter definitions for Windows (continued)*

| Parameter | Definition |
|---|---|
| WL_MANAGED | Managed Server instance. WebLogic supports two server instance types, managed and admin. Specifying this parameter as false indicates that the server instance is an admin type. True indicates that the server instance is a managed server. Default setting is *false*. |
| WLINST | WebLogic instances. Enter the names of the Managing Server instances that will be configured for data collection. Multiple instances should be separated by a comma (",") |
| WL_STARTSH | WebLogic startup script. This is the startup script containing the necessary commands to call the application server. Ignore this value if CUSTOM_SCRIPT_ENABLED is set to be *false*. Multiple startup files should be separated by a comma (","). Check "Table for WebLogic/WebLogic Portal server startup script locations" on page 108 for details. |
| CUSTOM_SCRIPT_ENABLED | Enable custom startup script. If this parameter is selected, the WebLogic Startup Script is ignored. The custom startup script adds certain JVM properties to the WebLogic Startup command line, which enables the DC for testware when WebLogic is launched. |
| INST_WLHOST | WebLogic server host. Enter the host name or IP address of the computer that has WebLogic installed. Multiple value should be separated by a comma (",") |
| INST_WLPORT | WebLogic server port number. Enter the port number of the computer that has WebLogic installed. Default is 7001. Multiple value should be separated by a comma (",") |
| INST_WLJNDI_TYPE | WebLogic admin server instance connection method. If you choose connect to the WebLogic admin server using plain socket or HTTP, set INST_WLJNDI_TYPE to *t3* and ignore INST_WL_SSL_* parameters. If you choose connect to the WebLogic admin server using SSL, set INST_WLJNDI_TYPE to *t3s_oneway* for SSL one way connection or *t3s_twoway* for SSL two way connection. Multiple value should be separated by a comma (",") |
| INST_WL_SSL_TRUST_CA_KEYSTORE | SSL client CA trust keystore file. It is a *.jks* file. Multiple value should be separated by a comma (","). This parameter is for t3s_oneway and t3s_twoway. |

*Table 8. WebLogic silent install parameter definitions for Windows (continued)*

| Parameter | Definition |
|---|---|
| INST_WL_SSL_CERT_TYPES | SSL Certificate types. This parameter is for SSL two way connection only. The valid file format types are *DER* and *PEM*. Types of multiple certificates should be separated by a vertical bar ("\|"). Note that the certificate type should be corresponding to the certificate file in terms of sequence. Multiple value should be separated by a comma (",") |
| INST_WL_SSL_CERT_FILES | SSL Certificate Files. This parameter is for SSL two way connection only. Set INST_WL_SSL_CERT_FILES to RSA private key and chain of X.509 certificates for SSL client authentication. Multiple files are separated by a vertical bar ("\|"). Note that the sequence of the certificates matters. The SSL Client private key should be put as the first certificate. All but the first certificate are issuer certificates for the previous certificate. Example: *INST_WL_SSL_CERT_FILES="C:\temp\testkey\client3.prv\|C:\temp\testkey\client3.pub\|C:\temp\testkey\netca_test_individual.cer"*. Multiple value should be separated by a comma (",") |
| INST_WL_SSL_KEY_PSWD | SSL client private key password. If the SSL client private key file is encrypted, set INST_WL_SSL_KEY_PSWD to be the RSA private key's password; otherwise, leave it blank. Multiple value should be separated by a comma (",") |

## Silent installation and configuration settings for WebLogic Portal Server

*Table 9. WebLogic Portal Server silent install parameter definitions for Windows*

| Parameter | Definition |
|---|---|
| LICENSE_ACCEPT_BUTTON | License agreement. You must specify this parameter to begin the product installation. Default setting is *true*. |
| installLocation | The location where you intend to install the product. The default location for installation is: C:\Program Files\IBM\tivoli\itcam\J2EE\DC |
| LAUNCH_CONFIG | This parameter launches the Configuration Tool. Specifying this parameter begins the process of configuring the DC to the Managing Server after installation. The default setting is *true*. |
| LOGSETTING.LOGLEVEL | The log level for the installation and configuration process. Possible values are: ALL / DEBUG_MAX / DEBUG_MID / INFO / WARN / ERROR / FATAL / OFF. |

*Table 9. WebLogic Portal Server silent install parameter definitions for Windows (continued)*

| Parameter | Definition |
|---|---|
| LOGSETTING.LOGCONSOLEOUT | This parameter controls whether the output message is printed to console or not. Possible values are true / false. |
| **DC Configuration** | |
| UNCONFIGURE_SERVERS | Specifying this parameter will cancel the configuration process after the installation is complete. The default setting is *false*. |
| J2EE_SELECTED | ITCAM for J2EE's Application Monitor interface. Specifying this parameter will configure monitored data to be accessed through ITCAM for J2EE's Application Monitor interface. To use the Application Monitor interface, the Managing Server must be available in your environment. The default is *true*. |
| TEMA_SELECTED | ITCAM for J2EE Tivoli Enterprise Portal. Specifying this parameter will configure monitored data to be accessed using the portal. To use the portal interface, ITCAM for J2EE and its components must be fully installed. The default is *false*. |
| SERVER_HOME | WebLogic directory location. Enter the root directory location in which WebLogic is located on the host server |
| SERVER_VERSION | WebLogic version number. Enter the version number of WebLogic that you are currently running |
| JAVA_HOME | The location of the JDK. Enter the directory location of the JDK that supports WebLogic. |
| IS64UNIXJVM | The flag for 64 bit model. The default value is *false*. If you are running a 64 bit OS using 64 bit JVM on a UNIX or Linux platform, change the parameter to*true*. Ignore this parameter on Windows. |
| DC_OFFLINE_ALLOW | This is for you to decide whether offline configuration is allowed. If you enter "true", the program will skip the verification of the connection to the Managing Server (MS) during configuration, and use the entered value of MS_AM_HOME; if you enter "false", the program will connect to MS and detect the MS home directory on MS server. The default value is *false*. |
| TEMA_OFFLINE_ALLOW | The option indicates whether offline configuration type is allowed during the configuation. The program will skip the monitoring agent connection test if it is set to be *true*. Set it to *false* when you don't want to allow the offline configuration for the monitoring agent. |

*Table 9. WebLogic Portal Server silent install parameter definitions for Windows (continued)*

| Parameter | Definition |
|---|---|
| AM_SOCKET_BINDIP | This is the DC side IP address or full qualified Host name. The IP or Host name will be used by DC to communicate with MS. If there are more then one NIC or multiple IP address configured on DC server, choose one of them. For example: -V AM_SOCKET_BINDIP=9.181.93.95 or -V AM_SOCKET_BINDIP=dc.cn.ibm.com or -V AM_SOCKET_BINDIP=<*value*> |
| FIREWALL_ENABLED | For DC side if the firewall is enabled, set the value to be *true*; otherwise, set the value to be *false*. |
| PROBE_RMI_POR | If the DC is behind firewall, set this port number. This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8200" to "8299". |
| PROBE_CONTROLLER_RMI_PORT | If the DC is behind firewall, set this port number. This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8300" to "8399". |
| **Managing-Server Specific Options** | |
| RECOLLECT_MSINFO | Specifying this parameter prompts the DC to recollect data from the Managing Server. The default is *true*. |
| MS_AM_HOME | The location of the Managing Server. Enter the directory location where the Managing Server is located. This parameter correlates the *DC_OFFLINE_ALLOW*. Refer to *DC_OFFLINE_ALLOW* for more detailed information. |
| KERNEL_HOST01 | Primary kernel server name. Enter full-qualified host name of the primary kernel server hosting the Managing Server. |
| PORT_KERNEL_CODEBASE01 | Primary kernel codebase port. The default is 9122. |
| **Application Server Specific Options** | |
| WLHOST | WebLogic Server host name. Enter the IP or domain name of the host location of the WebLogic server. |
| WLPORT | WebLogic server port number. The default is 7001. |
| WLUSER | User name. This parameter is optional. Enter a user ID name to match your current security settings; otherwise, leave this blank. |
| WLPSWD | Password. This parameter is optional. Enter a password to match your current security settings; otherwise, leave this blank. |

*Table 9. WebLogic Portal Server silent install parameter definitions for Windows (continued)*

| Parameter | Definition |
|---|---|
| WLJNDI_TYPE | WebLogic admin server connection method. If you choose connect to the WebLogic admin server using plain socket or HTTP, set WLJNDI_TYPE to *t3* and ignore WL_SSL_* parameters. If you choose connect to the WebLogic admin server using SSL, set WLJNDI_TYPE to *t3s_oneway* for SSL one way connection or *t3s_twoway* for SSL two way connection. |
| WL_SSL_TRUST_CA_KEYSTORE | SSL client CA trust keystore file. It is a *.jks* file. This parameter is for t3s_oneway and t3s_twoway. |
| WL_SSL_CERT_TYPES | SSL Certificate types. This parameter is for SSL two way connection only. The valid file format types are *DER* and *PEM*. Types of multiple cetificates should be separated by a vertical bar ("\|"). Note that the certificate type should be corresponding to the certificate file in terms of sequence. |
| WL_SSL_CERT_FILES | SSL Certificate Files. This parameter is for SSL two way connection only. Set WL_SSL_CERT_FILES to RSA private key and chain of X.509 certificates for SSL client authentication. Multiple files are separated by a vertical bar ("\|"). Note that the sequence of the certificates matters. The SSL Client private key should be put as the first certificate. All but the first certificate are issuer certificates for the previous certificate. Example: *WL_SSL_CERT_FILES="C:\temp\testkey\client3.prv\|C:\temp\testkey\client3.pub\|C:\temp\testkey\netca_test_individual.cer"* |
| WL_SSL_KEY_PSWD | SSL client private key password. If the SSL client private key file is encrypted, set WL_SSL_KEY_PSWD to be the RSA private key's password; otherwise, leave it blank. |
| WL_MANAGED | Managed Server instance. WebLogic supports two server instance types, managed and admin. Specifying this parameter as false indicates that the server instance is an admin type. True indicates that the server instance is a managed server. Default setting is *false*. |
| WLINST | WebLogic instances. Enter the names of the Managing Server instances that will be configured for data collection. Multiple instances should be separated by a comma (",") |

*Table 9. WebLogic Portal Server silent install parameter definitions for Windows (continued)*

| Parameter | Definition |
|---|---|
| WL_STARTSH | WebLogic startup script. This is the startup script containing the necessary commands to call the application server. Ignore this value if CUSTOM_SCRIPT_ENABLED is set to be *false*. Multiple startup files should be separated by a comma (","). Check "Table for WebLogic/WebLogic Portal server startup script locations" on page 108 for details. |
| CUSTOM_SCRIPT_ENABLED | Enable custom startup script. If this parameter is selected, the WebLogic Startup Script is ignored. The custom startup script adds certain JVM properties to the WebLogic Startup command line, which enables the DC for testware when WebLogic is launched. |
| INST_WLHOST | WebLogic server host. Enter the host name or IP address of the computer that has WebLogic installed. Multiple value should be separated by a comma (",") |
| INST_WLPORT | WebLogic server port number. Enter the port number of the computer that has WebLogic installed. Default is 7001. Multiple value should be separated by a comma (",") |
| INST_WLJNDI_TYPE | WebLogic admin server instance connection method. If you choose connect to the WebLogic admin server using plain socket or HTTP, set INST_WLJNDI_TYPE to *t3* and ignore INST_WL_SSL_* parameters. If you choose connect to the WebLogic admin server using SSL, set INST_WLJNDI_TYPE to *t3s_oneway* for SSL one way connection or *t3s_twoway* for SSL two way connection. Multiple value should be separated by a comma (",") |
| INST_WL_SSL_TRUST_CA_KEYSTORE | SSL client CA trust keystore file. It is a *.jks* file. Multiple value should be separated by a comma (","). This parameter is for t3s_oneway and t3s_twoway. |
| INST_WL_SSL_CERT_TYPES | SSL Certificate types. This parameter is for SSL two way connection only. The valid file format types are *DER* and *PEM*. Types of multiple certificates should be separated by a vertical bar ("\|"). Note that the certificate type should be corresponding to the certificate file in terms of sequence. Multiple value should be separated by a comma (",") |

*Table 9. WebLogic Portal Server silent install parameter definitions for Windows (continued)*

| Parameter | Definition |
|---|---|
| INST_WL_SSL_CERT_FILES | SSL Certificate Files. This parameter is for SSL two way connection only. Set INST_WL_SSL_CERT_FILES to RSA private key and chain of X.509 certificates for SSL client authentication. Multiple files are separated by a vertical bar ("\|"). Note that the sequence of the certificates matters. The SSL Client private key should be put as the first certificate. All but the first certificate are issuer certificates for the previous certificate. Example: *INST_WL_SSL_CERT_FILES="C:\temp\testkey\client3.prv\|C:\temp\testkey\client3.pub\|C:\temp\testkey\netca_test_individual.cer"*. Multiple value should be separated by a comma (",") |
| INST_WL_SSL_KEY_PSWD | SSL client private key password. If the SSL client private key file is encrypted, set INST_WL_SSL_KEY_PSWD to be the RSA private key's password; otherwise, leave it blank. Multiple value should be separated by a comma (",") |

## Silent installation and configuration settings for NetWeaver

*Table 10. NetWeaver silent install parameter definitions for Windows*

| Parameter | Definition |
|---|---|
| LICENSE_ACCEPT_BUTTON | License agreement. You must specify this parameter to begin the product installation. Default setting is *true*. |
| installLocation | The location where you intend to install the product. The default location for installation is: C:\Program Files\IBM\itcam\J2EE\DC |
| LAUNCH_CONFIG | This parameter launches the Configuration Tool. Specifying this parameter begins the process of configuring the DC to the Managing Server after installation. The default setting is *true*. |
| LOGSETTING.LOGLEVEL | The log level for the installation and configuration process. Possible values are: ALL / DEBUG_MAX / DEBUG_MID / INFO / WARN / ERROR / FATAL / OFF. |
| LOGSETTING.LOGCONSOLEOUT | This parameter controls whether the output message is printed to console or not. Possible values are true / false. |
| **DC Configuration** | |
| UNCONFIGURE_SERVERS | Specifying this parameter will cancel the configuration process after the installation is complete. The default setting is *false*. |

*Table 10. NetWeaver silent install parameter definitions for Windows (continued)*

| Parameter | Definition |
|---|---|
| J2EE_SELECTED | ITCAM for J2EE's Application Monitor interface. Specifying this parameter will configure monitored data to be accessed through ITCAM for J2EE's Application Monitor interface. To use the Application Monitor interface, the Managing Server must be available in your environment. The default is *true*. |
| TEMA_SELECTED | ITCAM for J2EE Tivoli Enterprise Portal. Specifying this parameter will configure monitored data to be accessed using the ITCAM for J2EE's portal. To use the portal interface, ITCAM for J2EE and its components must be fully installed. The default is *false*. |
| DC_OFFLINE_ALLOW | This is for you to decide whether offline configuration is allowed. If you enter "true", the program will skip the verification of the connection to the Managing Server (MS) during configuration, and use the entered value of MS_AM_HOME; if you enter "false", the program will connect to MS and detect the MS home directory on MS server. The default value is *false*. |
| TEMA_OFFLINE_ALLOW | The option indicates whether offline configuration type is allowed during the configuation. The program will skip the monitoring connection test if it is set to be *true*. Set it to *false* when you don't want to allow the offline configuration for the monitoring agent. |
| AM_SOCKET_BINDIP | This is the DC side IP address or full qualified Host name. The IP or Host name will be used by DC to communicate with MS.If there are more then one NIC or multiple IP address configured on DC server, choose one of them. For example: -V AM_SOCKET_BINDIP=9.181.93.95 or -V AM_SOCKET_BINDIP=dc.cn.ibm.com or -V AM_SOCKET_BINDIP=<*value*> |
| FIREWALL_ENABLED | For DC side if the firewall is enabled, set the value to be *true*; otherwise, set the value to be *false*. |
| PROBE_RMI_POR | If the DC is behind firewall, set this port number. This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8200" to "8299". |
| PROBE_CONTROLLER_RMI_PORT | If the DC is behind firewall, set this port number. This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8300" to "8399". |
| **Managing-Server Specific Options** | |

*Table 10. NetWeaver silent install parameter definitions for Windows (continued)*

| Parameter | Definition |
|---|---|
| RECOLLECT_MSINFO | Specifying this parameter prompts the DC to recollect data from the Managing Server. The default is *true*. |
| MS_AM_HOME | The location of the Managing Server. Enter the directory location where the Managing Server was installed. This parameter correlates the *DC_OFFLINE_ALLOW*. Refer to *DC_OFFLINE_ALLOW* for more detailed information. |
| KERNEL_HOST01 | Primary kernel server name. Enter full-qualified host name of the primary kernel server hosting the Managing Server. |
| PORT_KERNEL_CODEBASE01 | Primary kernel codebase port. The default is 9122. |
| **Application Server Specific Options** | |
| INSTALL_TYPE | NetWeaver installation type. Choose from the three installation types: central instance (denoted as 1), local dialog instance (denoted as 2), and distributed dialog instance (denoted as 3). Enter the number value representing your installation type.<br>The 3 DC installation types are:<br>1. Central instance installation: Install DC to monitor the server on Central instance;<br>2. Local dialog instance installation: Dialog instance and central instance are installed on one computer and the DC is installed to monitor the server on the dialog instance;<br>3. Distributed dialog instance installation: Dialog instance and central instance are not installed on the same computer, and the DC is installed to monitor the server on the dialog instance. |
| SERVER_HOME | NetWeaver directory location. The absolute path of directory wherein the instance is monitored. |
| CENTRAL_INSTANCE_HOME | NetWeaver central instance directory. Enter the directory location of the NetWeaver central server instance. For central instance installation, its value is the same as the *Server home*. |

*Table 10. NetWeaver silent install parameter definitions for Windows (continued)*

| Parameter | Definition |
|---|---|
| CENTRAL_INSTANCE_NETWORK_HOME | NetWeaver central instance network directory. A local path mounted from *Central instance home* directory. For central instance installation, its value is the same as the *Server home*. For local dialog instance installation, its value is the same as the *Central instance home*. For distributed dialog instance installation, mount the *Central instance home* on central instance computer to a local directory, and the value of *Central instance network home* should be the mounted local directory. You can use the remote path of the *Central instance home* on Windows platforms (for example, \\9.181.25.46\usr\sap\J2E\JC00). |
| SERVER_VERSION | NetWeaver version number. Enter the current version number of NetWeaver that you are running. |
| JAVA_HOME | JDK location. Enter the directory location of the JDK supporting NetWeaver. |
| IS64UNIXJVM | The flag for 64 bit model. The default value is *false*. If you are running a 64 bit OS using 64 bit JVM on a UNIX or Linux platform, change the parameter to*true*. Ignore this parameter on Windows. |
| SAPNW64HOST | The qualified host name of local server. |
| SAPNW64PORT | The P4 port of the NetWeaver instance. |
| SAPNW64USER | The required user name used to get the Java Management Extensions (JMX) Data from MBean Server. Usually, this user ID is the same as you log on the Visual Administrator tool. For example, Administrator. |
| SAPNW64PSWD | The required password used to get the JMX Data from MBean Server. Usually, this password is the same as you log on the Visual Administrator tool. |
| SAPNW64_SVRS | Server instance names. Enter the names of the Managing Server instances to be configured for data collection. If multiple instances are monitored, separate them by semicolons. |

## Silent installation and configuration settings for JBoss

*Table 11. JBoss silent install parameter definitions for Windows*

| Parameter | Definition |
|---|---|
| LICENSE_ACCEPT_BUTTON | License agreement. You must specify this parameter to begin the product installation. Default setting is *true*. |

*Table 11. JBoss silent install parameter definitions for Windows (continued)*

| Parameter | Definition |
|---|---|
| installLocation | The location where you intend to install the product. The default location for installation is: C:\Program Files\IBM\itcam\J2EE\DC |
| LAUNCH_CONFIG | This parameter launches the Configuration Tool. Specifying this parameter begins the process of configuring the DC to the Managing Server after installation. The default setting is *true*. |
| LOGSETTING.LOGLEVEL | The log level for the installation and configuration process. Possible values are: ALL / DEBUG_MAX / DEBUG_MID / INFO / WARN / ERROR / FATAL / OFF. |
| LOGSETTING.LOGCONSOLEOUT | This parameter controls whether the output message is printed to console or not. Possible values are true / false. |
| **DC Configuration** | |
| UNCONFIGURE_SERVERS | Specifying this parameter will cancel the configuration process after the installation is complete. The default setting is *false*. |
| J2EE_SELECTED | ITCAM for J2EE's Application Monitor interface. Specifying this parameter will configure monitored data to be accessed through ITCAM for J2EE's Application Monitor interface. To use the Application Monitor interface, the Managing Server must be available in your environment. The default is *true*. |
| TEMA_SELECTED | ITCAM for J2EE Tivoli Enterprise Portal. Specifying this parameter will configure monitored data to be accessed using the portal. To use the portal interface, ITCAM for J2EE and its components must be fully installed. The default is *false*. |
| SERVER_HOME | JBoss directory location. Enter the root directory location in which JBoss is located. |
| SERVER_VERSION | JBoss version number. Enter the version number of JBoss that you are currently running. |
| JAVA_HOME | The location of the JDK. Enter the directory location of the JDK supporting JBoss. |
| IS64UNIXJVM | The flag for 64 bit model. The default value is *false*. If you are running a 64 bit OS using 64 bit JVM on a UNIX or Linux platform, change the parameter to*true*. Ignore this parameter on Windows. |

*Table 11. JBoss silent install parameter definitions for Windows (continued)*

| Parameter | Definition |
|---|---|
| DC_OFFLINE_ALLOW | This is for you to decide whether offline configuration is allowed. If you enter "true", the program will skip the verification of the connection to the Managing Server (MS) during configuration, and use the entered value of MS_AM_HOME; if you enter "false", the program will connect to MS and detect the MS home directory on MS server. The default value is *false*. |
| TEMA_OFFLINE_ALLOW | The option indicates whether offline configuration type is allowed during the configuation. The program will skip the monitoring agent connection test if it is set to be *true*. Set it to *false* when you don't want to allow the offline configuration for the monitoring agent. |
| AM_SOCKET_BINDIP | This is the DC side IP address or full qualified Host name. The IP or Host name will be used by DC to communicate with MS.If there are more then one NIC or multiple IP address configured on DC server, choose one of them. For example: -V AM_SOCKET_BINDIP=9.181.93.95 or -V AM_SOCKET_BINDIP=dc.cn.ibm.com or -V AM_SOCKET_BINDIP=*<value>* |
| FIREWALL_ENABLED | For DC side if the firewall is enabled, set the value to be *true*; otherwise, set the value to be *false*. |
| PROBE_RMI_POR | If the DC is behind firewall, set this port number. This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8200" to "8299". |
| PROBE_CONTROLLER_RMI_PORT | If the DC is behind firewall, set this port number. This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8300" to "8399". |
| **Managing-Server Specific Options** | |
| RECOLLECT_MSINFO | Specifying this parameter prompts the DC to recollect data from the Managing Server. The default is *true*. |
| MS_AM_HOME | The location of the Managing Server. Enter the directory location where the Managing Server was installed. This parameter correlates the *DC_OFFLINE_ALLOW*. Refer to *DC_OFFLINE_ALLOW* for more detailed information. |
| KERNEL_HOST01 | Primary kernel server name. Enter full-qualified host name of the primary kernel server hosting the Managing Server. |
| PORT_KERNEL_CODEBASE01 | Primary kernel codebase port. The default is 9122. |

*Table 11. JBoss silent install parameter definitions for Windows (continued)*

| Parameter | Definition |
|---|---|
| **Application Server Specific Options** | |
| JBOSSHOST | JBoss server host name. Enter the IP or domain name of the JBoss server host server. |
| JBOSSPORT | JBoss server port number. The default is 1099. |
| SECURITY_ENABLE | The parameters, JBOSSUSER and JBOSSPSWD, are ignored if SECURITY_ENABLE is false. The default value is *false*. |
| JBOSSUSER | User name. This parameter is optional. Enter a user ID name to match your current security settings; otherwise, leave this blank. |
| JBOSSPSWD | Password. This parameter is optional. Enter a password to match your current security settings; otherwise, leave this blank. |
| JBOSSINST | JBoss instances. Enter the Managing Server instances that will be configured for data collection. |
| JBOSS_SERVER_DIR | JBoss Server instance directory. The directory location of JBoss server that will be configured for the data collector, for example: C:\jboss4.0.3SP1\server\default. |
| JBOSSSTARTSH | JBoss server startup script. This is the file containing the necessary commands to launch JBoss. The script can be found within the location in which you installed JBoss, for example: C:\jboss-4.0.3SP1\bin\run.bat. |

## Silent installation and configuration for Tomcat

*Table 12. Tomcat silent install parameter definitions for Windows*

| Parameter | Definition |
|---|---|
| LICENSE_ACCEPT_BUTTON | License agreement. You must specify this parameter to begin the product installation. Default setting is *true*. |
| installLocation | The location where you intend to install the product. The default location for installation is: C:\Program Files\IBM\itcam\J2EE\DC |
| LAUNCH_CONFIG | This parameter launches the Configuration Tool. Specifying this parameter begins the process of configuring the DC to the Managing Server after installation. The default setting is *true*. |
| LOGSETTING.LOGLEVEL | The log level for the installation and configuration process. Possible values are: ALL / DEBUG_MAX / DEBUG_MID / INFO / WARN / ERROR / FATAL / OFF. |
| LOGSETTING.LOGCONSOLEOUT | This parameter controls whether the output message is printed to console or not. Possible values are true / false. |
| **DC Configuration** | |

*Table 12. Tomcat silent install parameter definitions for Windows (continued)*

| Parameter | Definition |
|---|---|
| UNCONFIGURE_SERVERS | Specifying this parameter will cancel the configuration process after the installation is complete. The default setting is *false*. |
| J2EE_SELECTED | ITCAM for J2EE's Application Monitor interface. Specifying this parameter will configure monitored data to be accessed through ITCAM for J2EE's Application Monitor interface. To use the Application Monitor interface, the Managing Server must be available in your environment. The default is *true*. |
| TEMA_SELECTED | ITCAM for J2EE Tivoli Enterprise Portal. Specifying this parameter will configure monitored data to be accessed using the portal. To use the portal interface, ITCAM for J2EE and its components must be fully installed. The default is *false*. |
| SERVER_HOME | Tomcat server directory location. Enter the root directory location in which Tomcat is located on. |
| SERVER_VERSION | Tomcat server version number. Enter the version of the Tomcat server that you are currently running. For example, if the Tomcat version is 5.0, SERVER_VERSION should be set as 50; if the version is 5.5, SERVER_VERSION should be set as 55. |
| JAVA_HOME | The location of the JDK. Enter the directory location of the JDK supporting Tomcat. |
| IS64UNIXJVM | The flag for 64 bit model. The default value is *false*. If you are running a 64 bit OS using 64 bit JVM on a UNIX or Linux platform, change the parameter to *true*. Ignore this parameter on Windows. |
| DC_OFFLINE_ALLOW | This is for you to decide whether offline configuration is allowed. If you enter "true", the program will skip the verification of the connection to the Managing Server (MS) during configuration, and use the entered value of MS_AM_HOME; if you enter "false", the program will connect to MS and detect the MS home directory on MS server. The default value is *false*. |
| TEMA_OFFLINE_ALLOW | The option indicates whether offline configuration type is allowed during the configuation. The program will skip the monitoring agent connection test if it is set to be *true*. Set it to *false* when you don't want to allow the offline configuration for the monitoring agent. |

*Table 12. Tomcat silent install parameter definitions for Windows (continued)*

| Parameter | Definition |
|---|---|
| AM_SOCKET_BINDIP | This is the DC side IP address or full qualified Host name. The IP or Host name will be used by DC to communicate with MS. If there are more then one NIC or multiple IP address configured on DC server, choose one of them. For example: -V AM_SOCKET_BINDIP=9.181.93.95 or -V AM_SOCKET_BINDIP=dc.cn.ibm.com or -V AM_SOCKET_BINDIP=<*value*> |
| FIREWALL_ENABLED | For DC side if the firewall is enabled, set the value to be *true*; otherwise, set the value to be *false*. |
| PROBE_RMI_POR | If the DC is behind firewall, set this port number.This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8200" to "8299". |
| PROBE_CONTROLLER_RMI_PORT | If the DC is behind firewall, set this port number. This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8300" to "8399". |
| **Managing-Server Specific Options** | |
| RECOLLECT_MSINFO | Specifying this parameter prompts the DC to recollect data from the Managing Server. The default is *true*. |
| MS_AM_HOME | The location of the Managing Server. Enter the directory location where the Managing Server was installed. This parameter correlates the *DC_OFFLINE_ALLOW*. Refer to *DC_OFFLINE_ALLOW* for more detailed information. |
| KERNEL_HOST01 | Primary kernel server name. Enter full-qualified host name of the primary kernel server hosting the Managing Server. |
| PORT_KERNEL_CODEBASE01 | Primary kernel codebase port. The default is 9122. |
| **Application Server Specific Options** | |

*Table 12. Tomcat silent install parameter definitions for Windows (continued)*

| Parameter | Definition |
|---|---|
| APPSERVER | Tomcat application server instance. Enter the Tomcat Server instance names that you wish to configure for data collection.<br><br>If you are editing the Tomcat Server instance name for the Tomcat configurator, check whether the instance name exists.<br>• If you are configuring a new Tomcat server, make sure there is no existing instance name. Use a different instance name.<br>• If you are reconfiguring an existing Tomcat server, you do not need to check the instance name.<br><br>**Note:** The instance name information can be found in the directory, <*DC_HOME*>/runtime/. If there is an existing Tomcat Server instance name, you can find a child directory under this directory. The child directory takes the form as <Server Name>.<Node Name>.<Instance Name>. For example, tomcat_55_1029_1 is the instance name in the <*DC_HOME*>/runtime/tomcat55.tiv147.cn.ibm.com.tomcat_55_1029_1 directory. |
| STARTUP_FILE | Server startup script. The startup script is a batch or command file containing the necessary command lines required to startup the application server. Enter the full file path of the startup script here. On Windows, the startup script is <*Tomcat Home*>\bin\catalina.bat. Where <*Tomcat Home*> is the root directory where you installed the Tomcat server. |

## Silent installation and configuration for Oracle

*Table 13. Oracle silent install parameter definitions for Windows*

| Parameter | Definition |
|---|---|
| LICENSE_ACCEPT_BUTTON | License agreement. You must specify this parameter to begin the product installation. Default setting is *true*. |
| installLocation | The location where you intend to install the product. The default location for installation is: C:\Program Files\IBM\itcam\J2EE\DC |
| LAUNCH_CONFIG | This parameter launches the Configuration Tool. Specifying this parameter begins the process of configuring the DC to the Managing Server after installation. The default setting is *true*. |
| LOGSETTING.LOGLEVEL | The log level for the installation and configuration process. Possible values are: ALL / DEBUG_MAX / DEBUG_MID / INFO / WARN / ERROR / FATAL / OFF. |

*Table 13. Oracle silent install parameter definitions for Windows (continued)*

| Parameter | Definition |
|---|---|
| LOGSETTING.LOGCONSOLEOUT | This parameter controls whether the output message is printed to console or not. Possible values are true / false. |
| **DC Configuration** | |
| UNCONFIGURE_SERVERS | Specifying this parameter will cancel the configuration process after the installation is complete. The default setting is *false*. |
| J2EE_SELECTED | ITCAM for J2EE's Application Monitor interface. Specifying this parameter will configure monitored data to be accessed through ITCAM for J2EE's Application Monitor interface. To use the Application Monitor interface, the Managing Server must be available in your environment. The default is *true*. |
| TEMA_SELECTED | ITCAM for J2EE Tivoli Enterprise Portal. Specifying this parameter will configure monitored data to be accessed using the ITCAM for J2EE's portal. To use the portal interface, ITCAM for J2EE and its components must be fully installed. The default is *false*. |
| SERVER_HOME | Oracle server directory location. Enter the root directory location in which Oracle is located (for example, *C:/OraHome_1*). |
| SERVER_VERSION | Oracle server version number. Enter the version of the Oracle server that you are currently running. |
| JAVA_HOME | The location of the JDK. Enter the directory location of the JDK supporting Oracle (for example, C:/OraHome/jdk). |
| IS64UNIXJVM | The flag for 64 bit model. The default value is *false*. If you are running a 64 bit OS using 64 bit JVM on a UNIX or Linux platform, change the parameter to*true*. Ignore this parameter on Windows. |
| DC_OFFLINE_ALLOW | This is for you to decide whether offline configuration is allowed. If you enter "true", the program will skip the verification of the connection to the Managing Server (MS) during configuration, and use the entered value of MS_AM_HOME; if you enter "false", the program will connect to MS and detect the MS home directory on MS server. The default value is *false*. |
| TEMA_OFFLINE_ALLOW | The option indicates whether offline configuration type is allowed during the configuation. The program will skip the monitoring agent connection test if it is set to be *true*. Set it to *false* when you don't want to allow the offline configuration for the monitoring agent. |

*Table 13. Oracle silent install parameter definitions for Windows (continued)*

| Parameter | Definition |
|---|---|
| AM_SOCKET_BINDIP | This is the DC side IP address or full qualified Host name. The IP or Host name will be used by DC to communicate with MS.If there are more then one NIC or multiple IP address configured on DC server, choose one of them. For example: -V AM_SOCKET_BINDIP=9.181.93.95 or -V AM_SOCKET_BINDIP=dc.cn.ibm.com or -V AM_SOCKET_BINDIP=<*value*> |
| FIREWALL_ENABLED | For DC side if the firewall is enabled, set the value to be *true*; otherwise, set the value to be *false*. |
| PROBE_RMI_POR | If the DC is behind firewall, set this port number.This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8200" to "8299". |
| PROBE_CONTROLLER_RMI_PORT | If the DC is behind firewall, set this port number. This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8300" to "8399". |
| **Managing-Server Specific Options** | |
| RECOLLECT_MSINFO | Specifying this parameter prompts the DC to recollect data from the Managing Server. The default is *true*. |
| MS_AM_HOME | The location of the Managing Server. Enter the directory location where the Managing Server was installed. This parameter correlates the *DC_OFFLINE_ALLOW*. Refer to *DC_OFFLINE_ALLOW* for more detailed information. |
| KERNEL_HOST01 | Primary kernel server name. Enter full-qualified host name of the primary kernel server hosting the Managing Server. |
| PORT_KERNEL_CODEBASE01 | Primary kernel codebase port. The default is 9122. |
| **Application Server Specific Options** | |
| OAS_INST | Oracle application server instance. The instances that you chose to have configured must be defined in this parameter. |
| ORA_ADMIN_USER | The admin username of the Oracle application server. Required only when configuring Oracle 10.1.3. |
| ORA_ADMIN_PSWD | The password of ORA_ADMIN_USER. |

## Silent installation and configuration for J2SE

*Table 14. J2SE silent install parameter definitions for Windows*

| Parameter | Definition |
|---|---|
| LICENSE_ACCEPT_BUTTON | License agreement. You must specify this parameter to begin the product installation. Default setting is *true*. |
| installLocation | The location where you intend to install the product. The default location for installation is: C:\Program Files\IBM\itcam\J2EE\DC |
| LAUNCH_CONFIG | This parameter launches the Configuration Tool. Specifying this parameter begins the process of configuring the DC to the Managing Server after installation. The default setting is *true*. |
| LOGSETTING.LOGLEVEL | The log level for the installation and configuration process. Possible values are: ALL / DEBUG_MAX / DEBUG_MID / INFO / WARN / ERROR / FATAL / OFF. |
| LOGSETTING.LOGCONSOLEOUT | This parameter controls whether the output message is printed to console or not. Possible values are true / false. |
| **DC Configuration** | |
| UNCONFIGURE_SERVERS | Specifying this parameter will cancel the configuration process after the installation is complete. The default setting is *false*. |
| J2EE_SELECTED | ITCAM for J2EE's Application Monitor interface. Specifying this parameter will configure monitored data to be accessed through ITCAM for J2EE's Application Monitor interface. To use the Application Monitor interface, the Managing Server must be available in your environment. The default is *true*. |
| TEMA_SELECTED | ITCAM for J2EE Tivoli Enterprise Portal. Specifying this parameter will configure monitored data to be accessed using the portal. To use the portal interface, ITCAM for J2EE and its components must be fully installed. The default is *false*. |
| SERVER_HOME | J2SE directory location. Enter the root directory location in which J2SE is located |
| SERVER_VERSION | J2SE version number. Enter the version number of J2SE that you are currently running |
| JAVA_HOME | The location of the JDK. Enter the directory location of the JDK supporting J2SE |
| IS64UNIXJVM | The flag for 64 bit model. The default value is *false*. If you are running a 64 bit OS using 64 bit JVM on a UNIX or Linux platform, change the parameter to*true*. Ignore this parameter on Windows. |

*Table 14. J2SE silent install parameter definitions for Windows (continued)*

| Parameter | Definition |
|---|---|
| DC_OFFLINE_ALLOW | This is for you to decide whether offline configuration is allowed. If you enter "true", the program will skip the verification of the connection to the Managing Server (MS) during configuration, and use the entered value of MS_AM_HOME; if you enter "false", the program will connect to MS and detect the MS home directory on MS server. The default value is *false*. |
| TEMA_OFFLINE_ALLOW | The option indicates whether offline configuration type is allowed during the configuation. The program will skip the monitoring agent connection test if it is set to be *true*. Set it to *false* when you don't want to allow the offline configuration for the monitoring agent. |
| AM_SOCKET_BINDIP | This is the DC side IP address or full qualified Host name. The IP or Host name will be used by DC to communicate with MS.If there are more then one NIC or multiple IP address configured on DC server, choose one of them. For example: -V AM_SOCKET_BINDIP=9.181.93.95 or -V AM_SOCKET_BINDIP=dc.cn.ibm.com or -V AM_SOCKET_BINDIP=<*value*> |
| FIREWALL_ENABLED | For DC side if the firewall is enabled, set the value to be *true*; otherwise, set the value to be *false*. |
| PROBE_RMI_POR | If the DC is behind firewall, set this port number.This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8200" to "8299". |
| PROBE_CONTROLLER_RMI_PORT | If the DC is behind firewall, set this port number. This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8300" to "8399". |
| **Managing-Server Specific Options** | |
| RECOLLECT_MSINFO | Specifying this parameter prompts the DC to recollect data from the Managing Server. The default is *true*. |
| MS_AM_HOME | The location of the Managing Server. Enter the directory location where the Managing Server was installed. This parameter correlates the *DC_OFFLINE_ALLOW*. Refer to *DC_OFFLINE_ALLOW* for more detailed information. |
| KERNEL_HOST01 | Primary kernel server name. Enter full-qualified host name of the primary kernel server hosting the Managing Server. |
| PORT_KERNEL_CODEBASE01 | Primary kernel codebase port. The default is 9122. |

*Table 14. J2SE silent install parameter definitions for Windows (continued)*

| Parameter | Definition |
|---|---|
| **Application Server Specific Options** | |
| J2SEMAINCLASS | Class type. Enter the main class type. |
| J2SEJMXEMBEDED | Embedded MBeans. Select *yes* if MBeans are embedded in the application. Select *no* if not. |
| J2SEJMXREMOTE | If MBeans are embedded in your application, this parameter must be input. Select *yes* if the DC must be connected using remote client, otherwise select *no* |
| J2SEHOST | Host name. Input the host name or IP address of the J2SE host in the event that the DC is connected using remote client. |
| J2SEPORT | J2SE port number. Input the port number of the Managing Server's host server. |
| J2SEUSER | User name. This parameter is optional. Enter a user ID name to match your current security settings; otherwise, leave this blank. |
| J2SEPSWD | Password. This parameter is optional. Enter a password to match your current security settings; otherwise, leave this blank. |
| J2SEINST | Instance names. Input the Managing Server instance names will be configured for data collection here. |
| J2SEGENERATENEW | Generate new startup script. Select *yes* to generate a new startup script. Select *no* to use a preexisting one. |
| J2SESTARTSH | Startup script directory. Input the startup script location here, if you selected *no* to the parameter: J2SEGENERATENEW . The startup script is the command or batch file with the necessary command lines capable of running the application server. |
| J2SEJVMMACRO | JVM macro. Input the JVM macro name here, only if you selected *no* to the parameter: J2SEGENERATENEW. |
| J2SESAMPLEPATH | Sample path. Input the directory location for the new startup script if you selected *yes* to the parameter: J2SEGENERATENEW. |
| J2SEJVMARG | JVM argument. Insert your JVM argument name if you selected *yes* to the parameter: J2SEGENERATENEW. Multiple arguments must be separated by a blank ( ). |
| J2SEPROGARG | Program argument. Input the program argument name. Multiple arguments must be separated by a blank ( ). |

# Chapter 3. Installing the ITCAM for J2EE Data Collector on UNIX/Linux

This chapter provides complete instructions for installing the ITCAM for J2EE Data Collector (DC) on UNIX/Linux for the supported application servers. For advanced users who prefer to input installation information once through a response file instead of repeatedly inputting data, the ITCAM for J2EE DC provides a silent installation. For specific application servers, you need to perform the steps for pre-installation or post-installation. Perform the steps in the following sections:

- "Using non-root user to install Data Collector"
- If applicable, "HP-UX and Solaris: Kernel settings for application servers"
- Either "Installing DC by InstallShield Wizard" on page 45 or "Performing a silent installation and configuration" on page 52
- "A post-installation step for ITCAM for J2EE Data Collector" on page 81

**Note:**

1. For users of Oracle 9, ensure that you have bc-1.06-5 or higher version installed on your server if you are installing DC on Linux.
2. For DC installation on WebLogic, there is an additional post-installation step.
3. All the screen captures in this chapter are taken from DC installation on JBoss for illustration purpose. Actual screen displays may vary by platform.

## Pre-installation instruction

### Using non-root user to install Data Collector

Depending on the version of the J2EE application server and the J2EE Data Collector being installed, there are various requirements on the file and directory permissions. If you are using a non-root user to install Data Collector, see the following section for details:Appendix D, "Summary of permissions required for installing and configuring the Data Collector," on page 207

### HP-UX and Solaris: Kernel settings for application servers

If you are installing the Data Collector on HP-UX or Solaris, you need to set the operating system's kernel values to support the application server.

#### HP-UX

Several HP-UX kernel values are typically too small for the application server.

Perform the following procedure to adjust the kernel values:

1. Log into the host computer as `root`.
2. Determine the physical memory, which you must know to avoid setting certain kernel parameters above the physical capacity:
   a. Start the HP-UX System Administration Manager (SAM) utility:

      ```
      sam
      ```

      This starts a text-based GUI interface. Use tab and arrow keys to move around in the interface.
   b. Select **Performance Monitors > System Properties > Memory**.

c. Note the value for Physical Memory and click **OK**.
d. Exit from the SAM utility.

3. Set the maxfiles and maxfiles_lim parameters to at least `4096`. Table 15 shows recommended values of `8000` and `8196`, respectively. You must first edit the /usr/conf/master.d/core-hpux file, so the SAM utility can set values greater than 2048:
   a. Open the /usr/conf/master.d/core-hpux file in a text editor.
   b. Change the line, "*range maxfiles<=2048" to "*range maxfiles<=60000"
   c. Change the line, "*range maxfiles_lim<=2048" to "*range maxfiles_lim<=60000"
   d. Save and close the file. Old values might be stored in the /var/sam/boot.config file. Force the SAM utility to create a new boot.config file:
      1) Move the existing version of the /var/sam/boot.config file to another location, such as the /tmp directory.
      2) Start the SAM utility.
      3) Select Kernel Configuration > Configurable Parameters. When the Kernel Configuration window opens, a new boot.config file exists.

         Alternatively, rebuild the boot.config file with the following command:

         ```
         # /usr/sam/lbin/getkinfo -b
         ```

4. Set new kernel parameter values:
   a. Start the SAM utility.
   b. Click **Kernel Configuration > Configurable Parameters**.
   c. For each of the parameters in the following table, perform this procedure:
      1) Highlight the parameter to change.
      2) Click **Actions > Modify Configurable Parameter**.
      3) Type the new value in the Formula/Value field.
      4) Click **OK**.

   Typical kernel settings for running the application server are displayed in the following table:

*Table 15. Typical Kernel settings for Running the Application Server*

| Parameter | Value |
|---|---|
| dbc_max_pct | 25 |
| maxdsiz | 805306358 |
| maxdsiz | 2048000000 (when running multiple profiles on the same system) |
| maxfiles_lim | 8196 (Change this one before maxfiles.) |
| maxfiles | 8000 |
| maxssiz | 8388608 |
| maxswapchunks | 8192 |
| max_thread_proc | 3000 |
| maxuprc | 512 |
| maxusers | 512 |
| msgmap | 2048 |
| msgmax | 65535 |
| msgmax | 131070 (when running multiple profiles on the same system) |

*Table 15. Typical Kernel settings for Running the Application Server (continued)*

| Parameter | Value |
|---|---|
| msgmnb | 65535 |
| msgmnb | 131070 (when running multiple profiles on the same system) |
| msgmni | 50 |
| msgseg | 32767 |
| msgssz | 32 |
| msgtql | 2046 |
| nfile | 58145 |
| nflocks | 3000 |
| ninode | 60000 |
| nkthread | 7219 |
| nproc | 4116 |
| npty | 2024 |
| nstrpty | 1024 |
| nstrtel | 60 |
| sema | 1 |
| semaem | 16384 |
| semmap | 514 |
| semmni | 2048 |
| semmns | 16384 |
| semmnu | 1024 |
| semume | 200 |
| semvmx | 32767 |
| shmmax | 2147483647 |
| shmem | 1 |
| shmmni | 1024 |
| shmseg | 1024 |
| STRMSGSZ | 65535 |

**Note:** When the application server and DB2 are on the same server, some kernel values are higher than those shown in the preceding table.

5. Click **Actions > Process New Kernel**.
6. Click **Yes** on the information window to confirm your decision to restart the server. Follow the on-screen instructions to restart your server and to enable the new settings.
7. If you plan to redirect displays to non-HP servers, complete the following steps before running the application server installation wizard:
   a. Issue the following command to obtain information about all the public locales that are accessible to your application:

      ```
      # locale -a
      ```

   b. Choose a value for your system from the output that is displayed and set the LANG environment variable to this value. Here is an example command that sets the value of LANG to en_US.iso88591:

```
# export LANG=en_US.iso8859
```

### Solaris

Several Solaris kernel values are typically too small for the application server.

Perform the following procedure to adjust the kernel values:

1. Before installing, review the server configuration:

   ```
   sysdef -i
   ```

   The kernel values are set in the /etc/system file, as shown in the following example.

   ```
   set shmsys:shminfo_shmmax = 4294967295
   set shmsys:shminfo_shmseg = 1024
   set shmsys:shminfo_shmmni = 1024
   set semsys:seminfo_semaem = 16384
   set semsys:seminfo_semmni = 1024
   set semsys:seminfo_semmap = 1026
   set semsys:seminfo_semmns = 16384
   set semsys:seminfo_semmsl = 100
   set semsys:seminfo_semopm = 100
   set semsys:seminfo_semmnu = 2048
   set semsys:seminfo_semume = 256
   set msgsys:msginfo_msgmap = 1026
   set msgsys:msginfo_msgmax = 65535
   set rlim_fd_cur=1024
   ```

2. Change kernel values by editing the /etc/system file then rebooting the operating system.

   For more information about setting up the Solaris system, see the Solaris System Administration documentation at the following Web site: http://docs.sun.com/app/docs/prod/solaris.admin.misc

   For example, the *Solaris Tunable Parameters Reference Manual* at the following Web site: http://docs.sun.com/app/docs/doc/816-7137?q=shmsys

Queue managers are generally independent of each other. Therefore system kernel parameters, for example shmmni, semmni, semmns, and semmnu need to allow for the number of queue managers in the system.

## Prerequisites for NetWeaver DC installation

Make sure you have met the prerequisites described in “Prerequisites for NetWeaver Data Collector installation” on page 3 before you install the NetWeaver DC.

**Note:** Be sure to use forward slash at all time on UNIX/Linux platforms.

For information about the three installation types of NetWeaver DC, refer to “Three installation types of ITCAM for J2EE Data Collector for NetWeaver” on page 4

The admin users for every SAP NetWeaver instance must belong to the same group (for example, sapsys). When installing the Data Collector, run the installation program as a user belonging to the same group.

Also, make sure that the group has read and write permissions for the Tivoli logging directory (by default, `/var/ibm/tivoli/common`),

To configure each SAP NetWeaver instance that you need to monitor, run the Data Collector configuration tool using the admin user for the instance.

## Preinstallation steps for Data Collectors on Solaris 8

To install the Data Collector on Solaris 8, complete the following steps prior to the installation:

1. Navigate to the DCPrereqs.xml file.
2. Make a backup copy of the file, with a name such as DCPrereqs_original.xml.
3. In the file, locate the following line:
   *<osname Name="SunOS" Version="5" ReleaseMin="9" ReleaseMax="10">*
4. Change *ReleaseMin="9"* to *"ReleaseMin="8"*. For example:
   *<osname Name="SunOS" Version="5" ReleaseMin="8" ReleaseMax="10">*
5. Save the updated file.
6. Perform the installation.

To see what application servers are supported on Solaris 8, visit the Prerequisites pages in the Tivoli Information Center:

http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?topic=/com.ibm.itcamwas_wr.doc_6.2/welcome.htm

# Installing DC by InstallShield Wizard

This section guides you through the DC installation process with a graphical user interface. Follow the proceeding instructions to perform the installation.

1. "Step 1: Start the InstallShield Wizard"
2. "Step 2: Accept the product license agreement" on page 47
3. "Step 3: Choose the installation directory" on page 47
4. "Step 4: Generate a response file" on page 48
5. "Step 5: Review the installation summary" on page 49
6. "Step 6: Configure servers for data collection" on page 50
7. "Step 7: Finalize the installation" on page 51

## Step 1: Start the InstallShield Wizard

Start the installation by running the setup file. Load the ITCAM for J2EE Data Collector CD, and change to its root directory. Start one of the following files:

- **IBM AIX®**: **`setup_DC_aix.bin`**
- **Solaris**: **`setup_DC_sol.bin`**
- **Linux**: **`setup_DC_lin.bin`**
- **HP-UX**: **`setup_DC_hp11.bin`**

This begins the InstallShield Wizard.

The log path window opens.

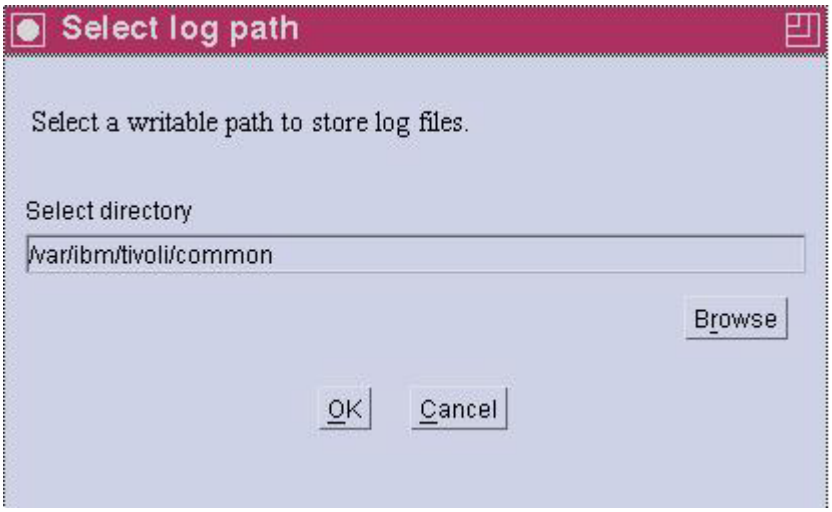



*Figure 9. The Log path window of the InstallShield Wizard*

If necessary, modify the path where the log files will be written. (The current user must have write access to the log path). Then click OK.

The Welcome window opens.

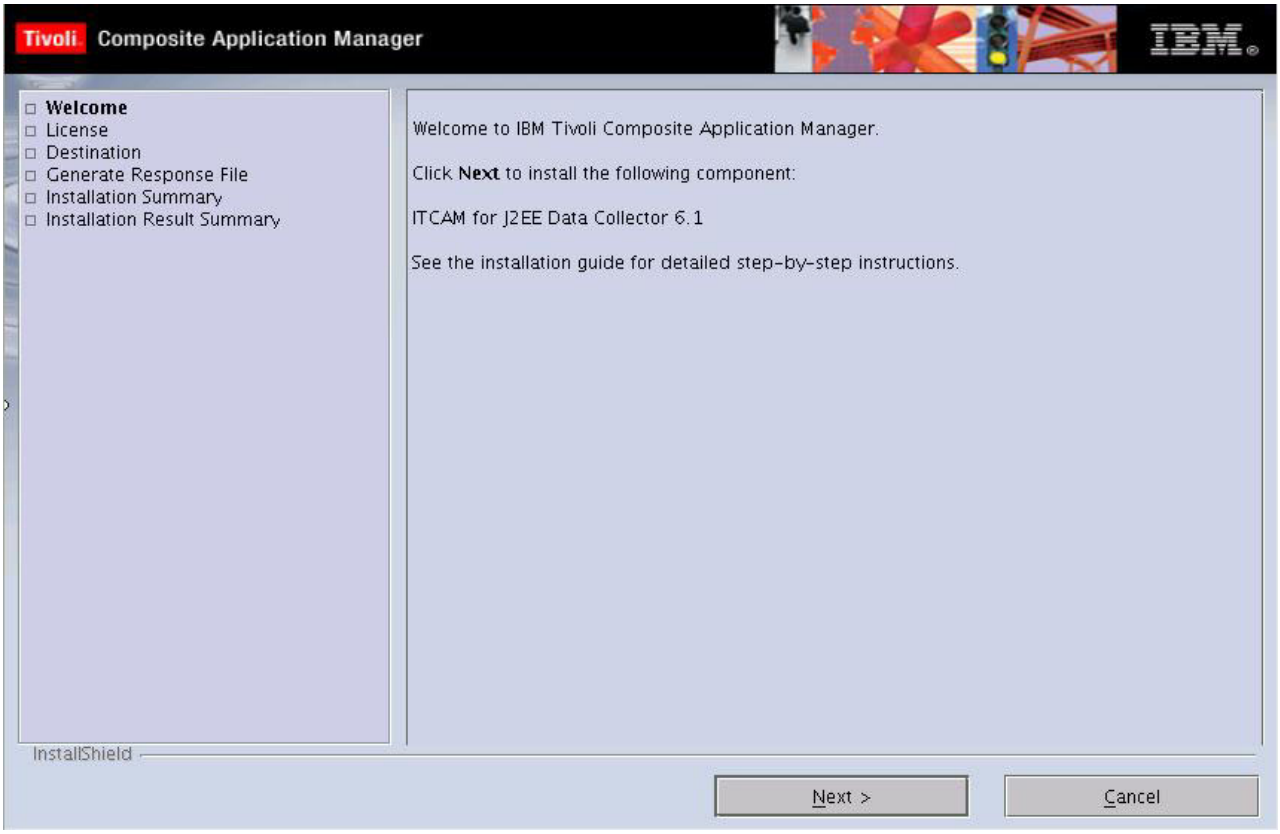



*Figure 10. The Welcome window of the InstallShield Wizard*

Proceed by clicking **Next**. You can exit the InstallShield Wizard at any time by clicking **Cancel**.

## Step 2: Accept the product license agreement

By clicking **Next** from the initial Welcome screen, you arrive at the product license agreement.

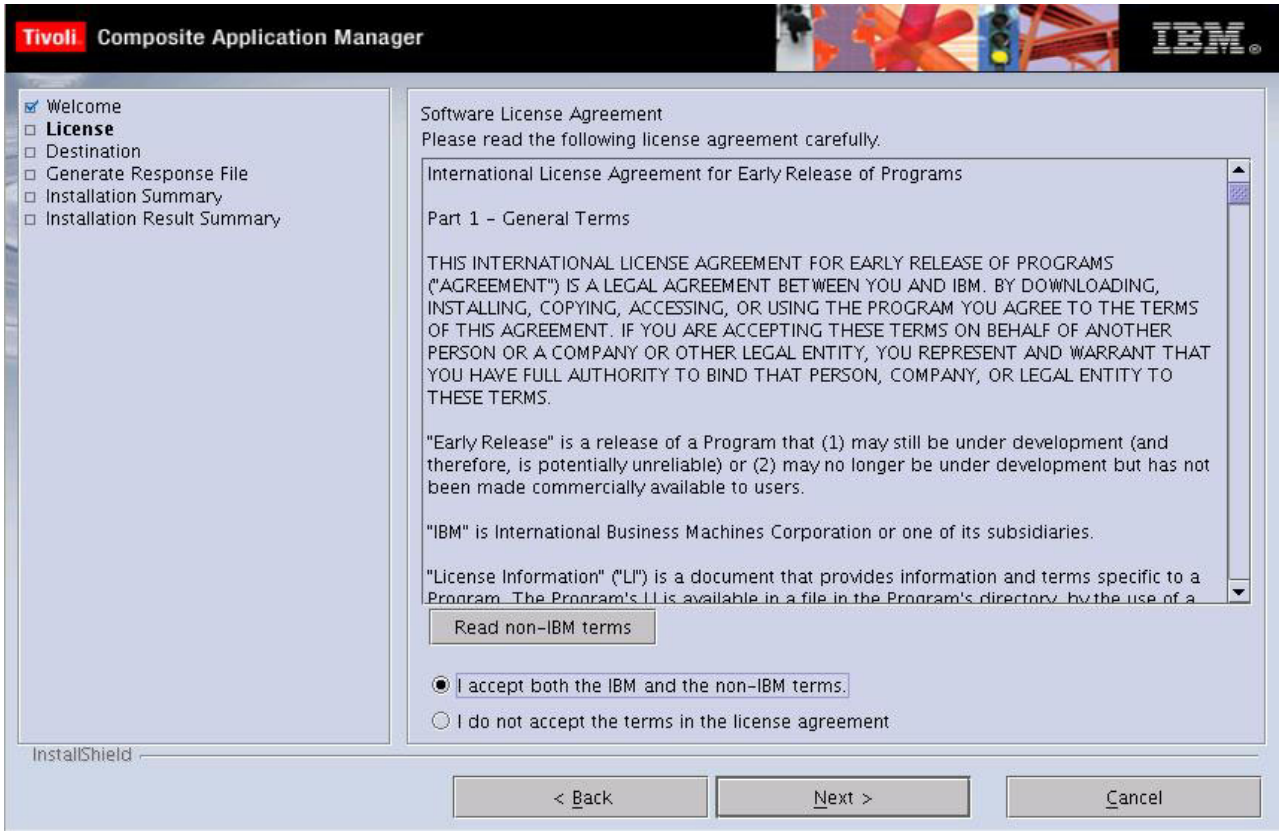



*Figure 11. Product license agreement*

Read through the product license agreement, and then select **I accept both the IBM and the non-IBM terms.**. You must accept the product license in order to continue with the installation. Continue by clicking **Next**.

## Step 3: Choose the installation directory

After accepting the product license you are prompted to select the destination in which the DC is to be installed.

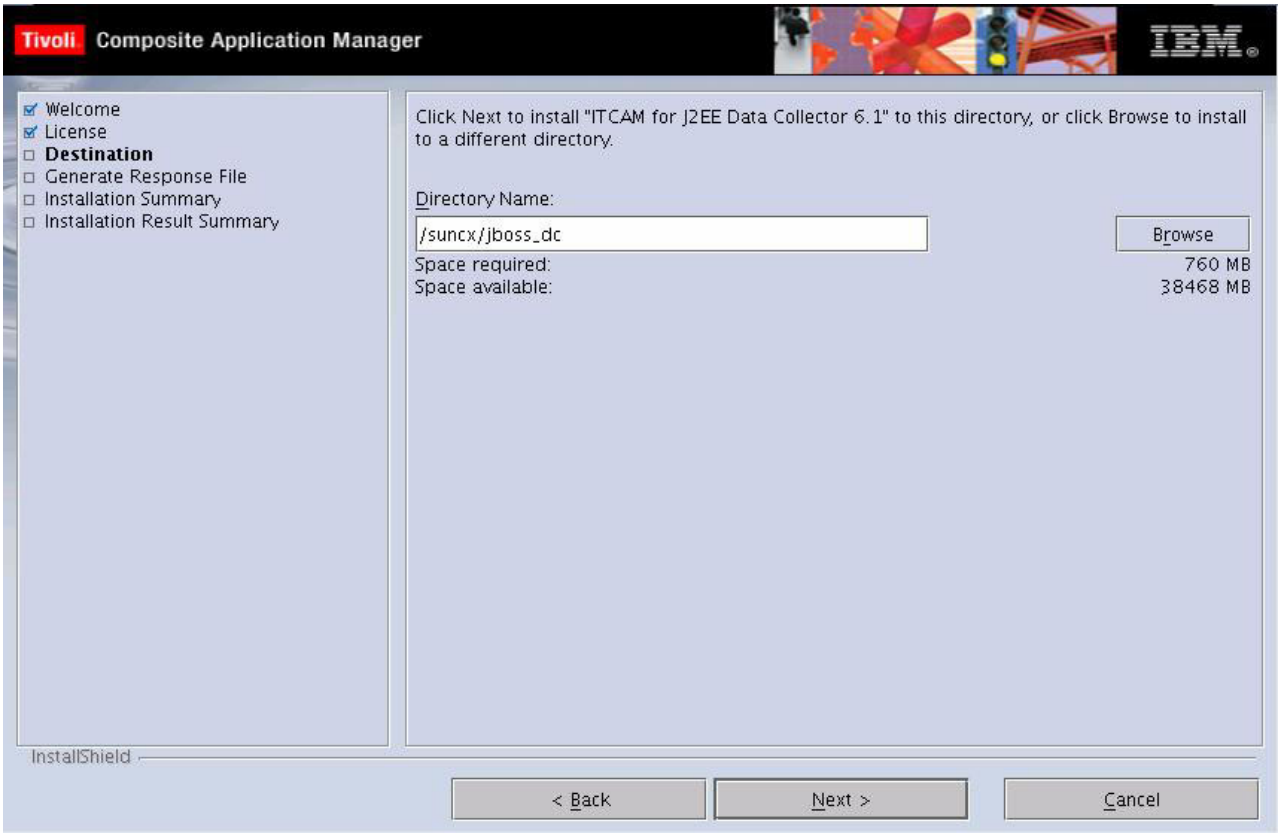



*Figure 12. Installation directory*

Click **Browse** to find a directory in which you want to install the Data Collector or create a new one if you do not wish to use the default location.

**Note:** You cannot install the Data Collector on an application server instance in a directory path (including profile, cell, node, and server names) that includes the following types of characters:

- Traditional Chinese
- Simplified Chinese
- Japanese
- Korean
- Spanish special characters
- German special characters
- Portuguese Brazilian special characters
- French special characters
- Italian special characters

Proceed by clicking **Next**.

## Step 4: Generate a response file

You can choose to generate a response file to save all your settings. It enables you to have the same installation settings when you want to install the Data Collector later again on this computer or on another computer by silent installation.

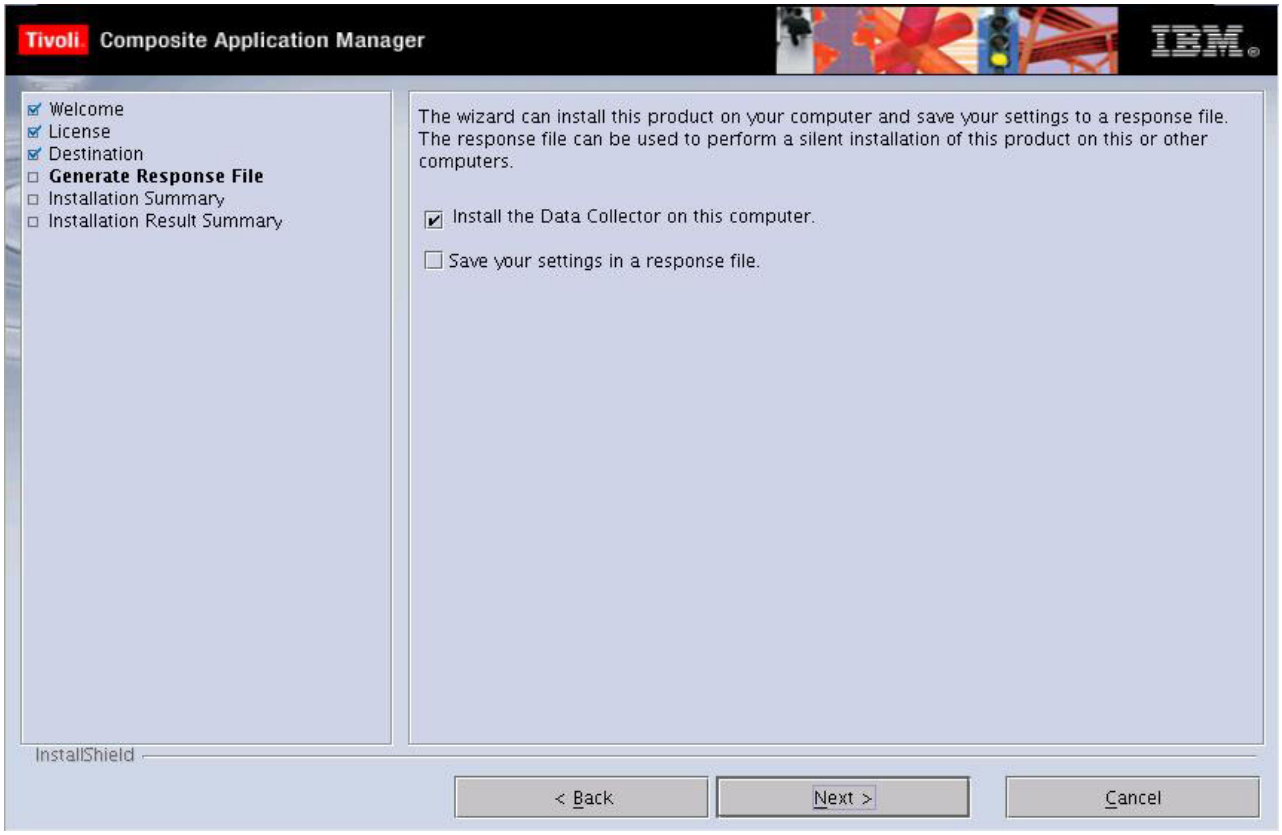



*Figure 13. Choose to save your settings in a response file*

**Install the Data Collector on this computer** is selected by default. If you wish to create a response file with all the settings in this installation, select **Save your settings in a response file**, and choose a location for the response file to generate.

Click **Next** to proceed.

## Step 5: Review the installation summary

A review summary is presented before the Data Collector is installed.

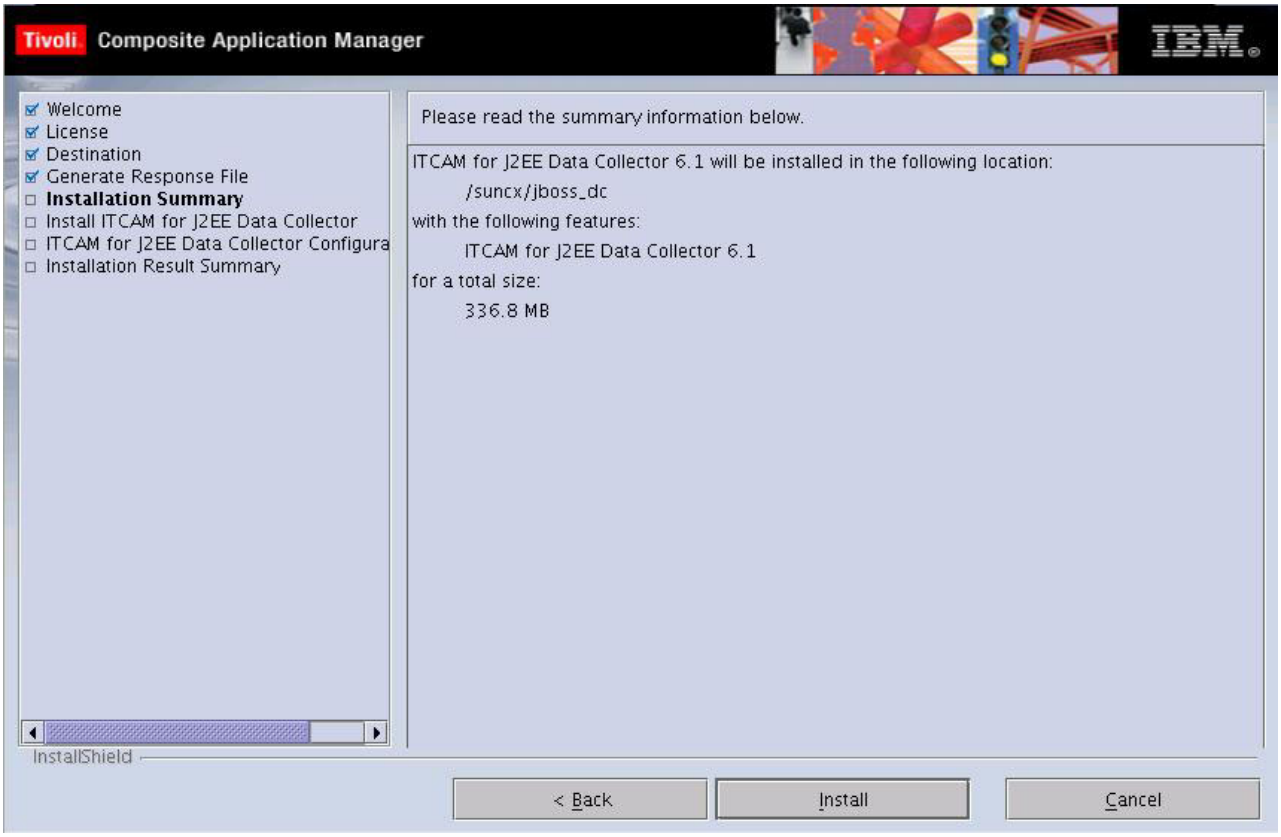



*Figure 14. Install summary preview*

Read through the summary of information, and ensure that your computer meets the prerequisite space requirements. If you wish to change the install location, click **Back** and select another destination directory. Click **Install** to proceed. This will install the DC.

## Step 6: Configure servers for data collection

After the Data Collector is installed, the InstallShield Wizard prompts you to either configure servers for data collection, or to defer the configuration until a later time.

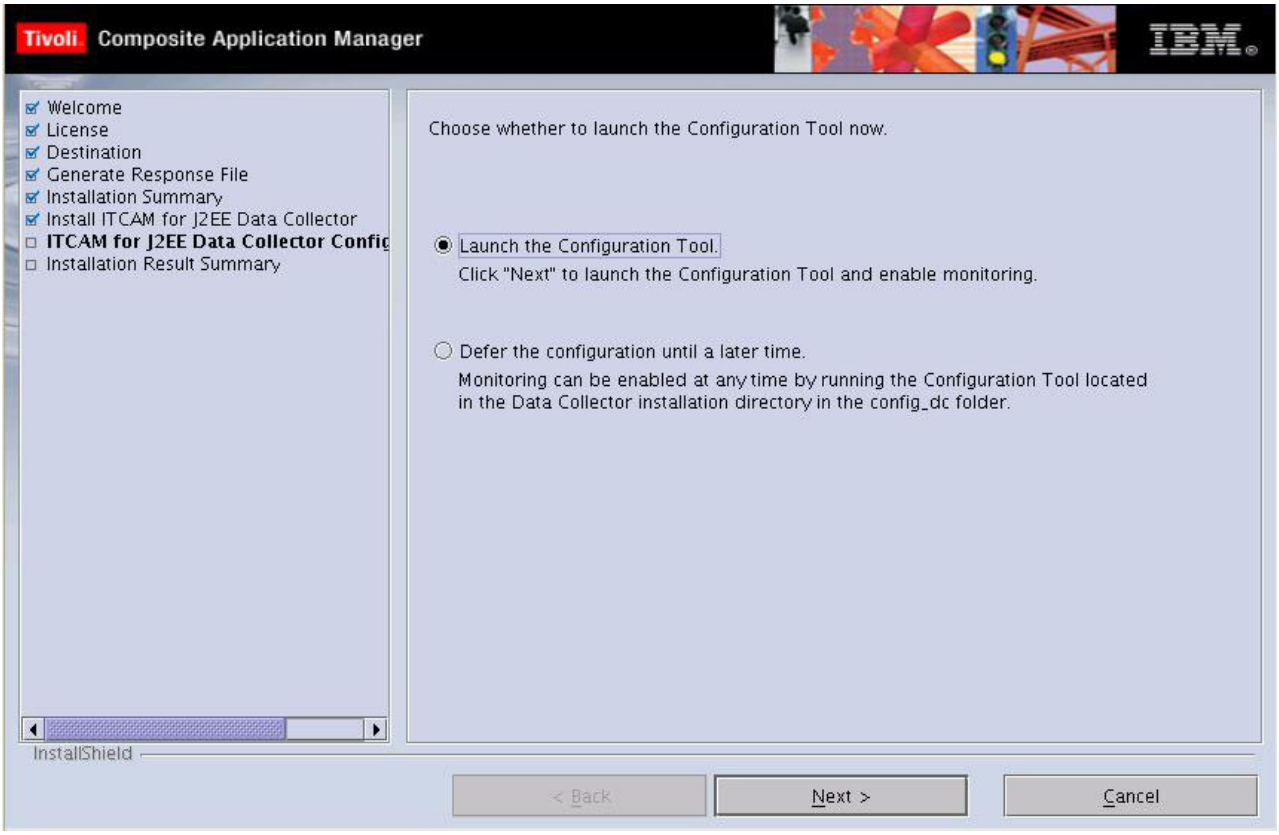



*Figure 15. Configuration Tool launch panel*

Choose **Launch the Configuration Tool** to open up the Configuration Tool and follow the Wizard through the configuration process. If you wish not to do this, select **Defer the configuration until a later time**. The Configuration Tool can be invoked by **installer > config_dc> config_dc.sh** located in the DC install directory.

For detailed information about configuring the DC to the Managing Server, refer to Chapter 4, “Configuring the ITCAM for J2EE Data Collector,” on page 83.

Click **Next** to proceed to the final installation summary.

## Step 7: Finalize the installation

A final summary of the installation process is displayed when DC is installed in your computer.

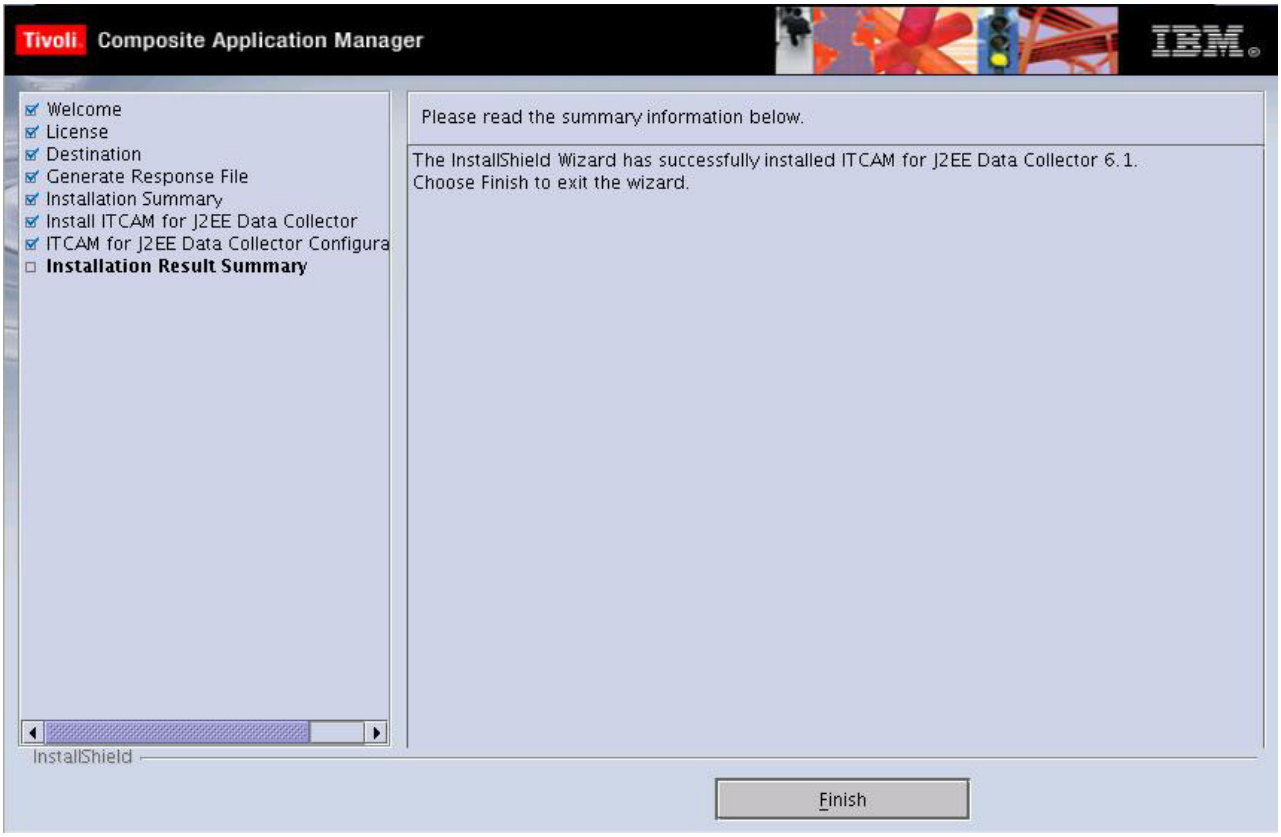



*Figure 16. Final installation summary*

Review the information, and then click **Finish** to finalize the installation and exit the InstallShield Wizard.

## Performing a silent installation and configuration

The ITCAM for J2EE Data Collector supports the silent installation. In a silent installation, predefined parameters are used to replace user interface interactions. Silent installation is useful for advanced users. Users who prefer to input installation information once through a response file instead of repeatedly inputting data in an installation procedure.

The following notes apply to silent installation and configuration:

**Note:**

1. By default, the installer creates log files in the following directory: /var/ibm/tivoli/common/CYN/logs.
2. By default, the configuration program creates the garbage collection logs in the file *DC_home*/*ServerTypeServerVersion*-gc-log.log.*InstanceName*.
3. If you are using a startup script, the configuration program produces a copy of the script as it was before the configuration. If a failure occurs after the configuration, use this copy of the script. Switch back to the configuration of the application server before it was modified by the installer. The copy of the startup script is named with a .orig extension. If the Data Collector configuration fails, no copy of the startup script gets produced, because the installer does not modify the original file.

You have the option to; install, install and configure, or configure theData Collector using this procedure. If you only want to configure the Data Collector, perform this procedure after the Data Collector has been installed.

Perform the following procedure to run the silent installation command:

1. Log on to the computer on which you want to install and configure the Data Collector as a user with the proper permissions (see Appendix D, "Summary of permissions required for installing and configuring the Data Collector," on page 207).
2. Start the instance of the application server that is monitored by the Data Collector.
3. Check the following Web site to see if the latest level of maintenance (such as fix packs or interim fixes) needs to be applied:

   http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliCompositeApplicationManagerforJ2EE.html

   If there is no maintenance you need to apply, you can perform both the installation and configuration. Run the executable file once and use one response file.

   If there is maintenance you need to apply, run the installation and configuration separately. After you perform the silent installation and before you perform the silent configuration, apply the latest level of maintenance.
4. If you are configuring, or installing and configuring, the Data Collector, perform the applicable pre-configuration steps for the application server:

*Table 16. Pre-configuration steps for application servers*

| Application server type | Pre-configuration steps |
|---|---|
| WebLogic | If a customized script is used for starting the server, see "Pre-configuration steps for supporting customized startup script for WebLogic" on page 84 |
| NetWeaver | No pre-configuration steps required |
| JBoss | See "Pre-configuration steps for Tomcat users" on page 88<br><br>If a customized script is used for starting the server, also see "Pre-configuration steps for supporting customized startup script for JBoss" on page 85<br><br>If the Java Wrapper Service for Tomcat is used, also see "Pre-configuration steps for supporting Java Service Wrapper for Tomcat" on page 89 |
| Tomcat | If a customized script is used for starting the server, see "Pre-configuration steps for supporting customized startup script for Tomcat" on page 85 |
| Oracle | No pre-configuration steps required |
| J2SE | See "Pre-configuration steps for J2SE users" on page 90 |
| Sun Java System Application Server (JSAS) | No pre-configuration steps required |

5. Specify configuration options in one of the following response file templates and save the file:

*Table 17. Response file templates*

| Application server type | Sample response file |
|---|---|
| WebLogic | DC61_weblogic.opt |

*Table 17. Response file templates (continued)*

| Application server type | Sample response file |
|---|---|
| NetWeaver | DC61_netweaver.opt |
| JBoss | DC61_jboss.opt |
| Tomcat | DC61_tomcat.opt |
| Oracle | DC61_oracle.opt |
| J2SE | DC61_j2se.opt |
| Sun Java System Application Server (JSAS) | DC61_jsas.opt |

The file is located in *installation_image_directory*/silent. See each of the following for guidance on how to modify the file:

*Table 18. Application server-specific silent installation settings for UNIX/Linux*

| Application Server | Silent Installation Steps |
|---|---|
| WebLogic | "Silent installation and configuration settings for WebLogic" on page 56 |
| WebLogic Portal Server | "Silent installation and configuration settings for WebLogic Portal Server" on page 61 |
| NetWeaver | "Silent installation and configuration settings for NetWeaver" on page 66 |
| JBoss | "Silent installation and configuration settings for JBoss" on page 69 |
| Tomcat | "Silent installation and configuration settings for Tomcat" on page 72 |
| Oracle | "Silent installation and configuration settings for Oracle" on page 74 |
| J2SE | "Silent installation and configuration settings for J2SE" on page 77 |
| Sun Java System Application Server (JSAS) | "Silent installation and configuration settings for JSAS" on page 80 |

**Note:**

a. If you are performing only the installation, options for the configuration are ignored when running the silent installation.

b. If you are performing only the configuration, options for the installation are ignored when running the silent configuration.

c. Optionally, you can use response files created by the GUI installation and configuration programs. If you are performing an installation and configuration, perform the following steps to make one response file from two generated response files:

   1) In both the Installation program and the Configuration tool, select the **Save your settings in a response file** option when shown. Enter a file path name.

   2) With a text editor, copy the contents of the response file generated from the installation program. Paste the contents into the response file generated by the configuration program.

   3) Save the newly created response file with a unique name or in another location. Enter the name of this response file in Step 7 on page 55.

d. If you save the response file in a location other than *installation_image_directory*/silent, make sure that directory is readable by the user performing the silent installation.

6. Do one of the following:

*Table 19. Whether to use the installation executable file or config_dc.sh*

| If you want to install or install and configure the Data Collector | If you want to only configure the Data Collector |
|---|---|
| Use the command-line interface to access the directory that contains the installation executable file. One of the following files is located in this directory:<br>• **IBM AIX**: **setup_DC_aix.bin**<br>• **Solaris**: **setup_DC_sol.bin**<br>• **Linux**: **setup_DC_lin.bin**<br>• **HP-UX**: **setup_DC_hp11.bin** | Go to the *DC_home*/installer/config_dc directory. The config_dc.sh file is located in this directory. |

7. Type the following command and press **Enter**:

   ```
   ./executable_file -silent [-is:log [log_file_name]] [configuration_option...]
     -options response_file
   ```

   The *executable_file* specifies the installation executable file, or the config_dc.sh file, mentioned in Step 6.

   The *log_file_name* specifies the path and name of the log file that the silent installer writes to. The file is created even if it does not yet exist or if no name is specified.

   The *configuration_option* specifies one or more configuration options not included in the response file.

   The *response_file* specifies the response file you configured in Step 5 on page 53. Indicate the path and name of the file.

   Examples:

   ```
   ./setup_DC_lin.bin -silent -is:log /opt/tmp/DClog.txt -V DC_ASL_SOAPPORT="8885"
     -options /opt/silent/DC6.opt
   ./config_dc.sh -silent -V DC_ASL_SOAPPORT="8885" -options /opt/silent/DC6.opt
   ```

   **Note:**

   a. Configuration options specified in the response file take precedence over options entered in the command line. For a particular command-line configuration option to take effect, nullify that option in the response file. Comment out the option with a number sign (#).

   b. If you are performing a silent configuration (after the Data Collector has been installed), you cannot use the -is option. Instead run the command in the following way:

      ```
      ./config_dc.sh -silent [configuration_option...] -options response_file
      ```

      For example:

      ```
      ./config_dc.sh -silent -V DC_ASL_SOAPPORT="8885" -options
        /opt/silent/DC6.opt
      ```

   r

8. If you have performed only a silent installation (you indicated `LAUNCH_CONFIG="false"`), check the /var/ibm/tivoli/common/CYN/trace-install.log file to find out whether the installation was successful.

9. If you performed a silent installation (and are about to perform configuration) and there is maintenance to apply, go to the following Web site:

http://www-947.ibm.com/support/entry/portal/Overview/Software/Tivoli/Tivoli_Composite_Application_Manager_for_J2EE

10. If you have performed a silent configuration, or installation and configuration, perform the applicable post-configuration steps for the application server:
    - See "Post-configuration steps for ITCAM for J2EE Data Collector" on page 147
    - If the application server uses Sun JDK 1.5 or HP JDK 1.5, see "Post-configuration steps for all application servers using Sun JDK 1.5 or HP JDK 1.5" on page 147
    - If the application server uses any version of the Sun JDK, see "Post-configuration steps for all application servers using Sun JDK" on page 148
    - Server-specific steps as per the following table:

*Table 20. Post-configuration steps for application servers*

| Application server type | Pre-configuration steps |
|---|---|
| WebLogic | See "Post-configuration steps for WebLogic users" on page 149 |
| NetWeaver | See "Post-configuration steps for NetWeaver" on page 151 |
| JBoss | No post-configuration steps required |
| Tomcat | See "Post-configuration steps for Tomcat users" on page 148 |
| Oracle | See "Post-configuration steps for Oracle users" on page 148 |
| J2SE | See "Post-configuration steps for J2SE" on page 150 |
| Sun Java System Application Server (JSAS) | See "Post-configuration steps for JSAS" on page 150 |

    - See "Additional post-configuration tasks" on page 155
11. Start the Application Monitor interface of the Managing Server and verify that you can see the monitored data.

## Silent installation and configuration settings for WebLogic

*Table 21. WebLogic silent install parameter definitions for UNIX/Linux*

| Parameter | Definition |
|---|---|
| LICENSE_ACCEPT_BUTTON | License agreement. You must specify this parameter to begin the product installation. Default setting is *true*. |
| installLocation | The location where you intend to install the product. |
| LAUNCH_CONFIG | This parameter launches the Configuration Tool. Specifying this parameter begins the process of configuring the DC to the Managing Server after installation. The default setting is *true*. |
| LOGSETTING.LOGLEVEL | The log level for the installation and configuration process. Possible values are: ALL / DEBUG_MAX / DEBUG_MID / INFO / WARN / ERROR / FATAL / OFF. |

*Table 21. WebLogic silent install parameter definitions for UNIX/Linux (continued)*

| Parameter | Definition |
|---|---|
| LOGSETTING.LOGCONSOLEOUT | This parameter controls whether the output message is printed to console or not. Possible values are true or false. |
| **DC Configuration** | |
| UNCONFIGURE_SERVERS | Specifying this parameter will cancel the configuration process after the installation is complete. The default setting is *false*. |
| J2EE_SELECTED | ITCAM for J2EE's Application Monitor interface. Specifying this parameter will configure monitored data to be accessed through ITCAM for J2EE's Application Monitor interface. To use the Application Monitor interface, the Managing Server must be available in your environment. The default is *true*. |
| TEMA_SELECTED | ITCAM for J2EE Tivoli Enterprise Portal. Specifying this parameter will configure monitored data to be accessed using the portal. To use the portal interface, ITCAM for J2EE and its components must be fully installed. The default is *false*. |
| SERVER_HOME | WebLogic directory location. Enter the root directory location in which WebLogic is located on the host computer. |
| SERVER_VERSION | WebLogic version number. Enter the version number of WebLogic that you are currently running. |
| JAVA_HOME | The location of the JDK. Enter the directory location of the JDK that supports WebLogic. |
| IS64UNIXJVM | The flag for 64 bit model. The default value is *false*. If you are running a 64 bit OS using 64 bit JVM on a UNIX or Linux platform, change the parameter to*true*. Ignore this parameter on Windows. |
| DC_OFFLINE_ALLOW | This is for you to decide whether offline configuration is allowed. If you enter "true", the program will skip the verification of the connection to the Managing Server (MS) during configuration, and use the entered value of MS_AM_HOME; if you enter "false", the program will connect to MS and detect the MS home directory on MS server. The default value is *false*. |
| TEMA_OFFLINE_ALLOW | The option indicates whether offline configuration type is allowed during the configuation. The program will skip the monitoring agent connection test if it is set to be *true*. Set it to *false* when you don't want to allow the offline configuration for the monitoring agent. |

*Table 21. WebLogic silent install parameter definitions for UNIX/Linux (continued)*

| Parameter | Definition |
|---|---|
| AM_SOCKET_BINDIP | This is the DC side IP address or full qualified Host name. The IP or Host name will be used by DC to communicate with MS. If there are more then one NIC or multiple IP address configured on DC server, choose one of them. For example: -V AM_SOCKET_BINDIP=9.181.93.95 or -V AM_SOCKET_BINDIP=dc.cn.ibm.com or -V AM_SOCKET_BINDIP=<*value*> |
| FIREWALL_ENABLED | For DC side if the firewall is enabled, set the value to be *true*; otherwise, set the value to be *false*. |
| PROBE_RMI_POR | If the DC is behind firewall, set this port number. This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8200" to "8299". |
| PROBE_CONTROLLER_RMI_PORT | If the DC is behind firewall, set this port number. This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8300" to "8399". |
| **Managing-Server Specific Options** | |
| RECOLLECT_MSINFO | Specifying this parameter prompts the DC to recollect data from the Managing Server. The default is *true*. |
| MS_AM_HOME | The location of the Managing Server. Enter the directory location where the Managing Server is located. This parameter correlates the *DC_OFFLINE_ALLOW*. Refer to *DC_OFFLINE_ALLOW* for more detailed information. |
| KERNEL_HOST01 | Primary kernel server name. Enter full-qualified host name of the primary kernel server hosting the Managing Server. |
| PORT_KERNEL_CODEBASE01 | Primary kernel codebase port. The default is 9122. |
| **Application Server Specific Options** | |
| WLHOST | WebLogic Server host name. Enter the IP or domain name of the host location of the WebLogic server. |
| WLPORT | WebLogic server port number. The default is 7001. |
| WLUSER | User name. This parameter is optional. Enter a user ID name to match your current security settings; otherwise, leave this blank. |
| WLPSWD | Password. This parameter is optional. Enter a password to match your current security settings; otherwise, leave this blank. |

*Table 21. WebLogic silent install parameter definitions for UNIX/Linux (continued)*

| Parameter | Definition |
|---|---|
| WLJNDI_TYPE | WebLogic admin server connection method. If you choose connect to the WebLogic admin server using plain socket or HTTP, set WLJNDI_TYPE to *t3* and ignore WL_SSL_* parameters. If you choose connect to the WebLogic admin server using SSL, set WLJNDI_TYPE to *t3s_oneway* for SSL one way connection or *t3s_twoway* for SSL two way connection. |
| WL_SSL_TRUST_CA_KEYSTORE | SSL client CA trust keystore file. It is a *.jks* file. This parameter is for t3s_oneway and t3s_twoway. |
| WL_SSL_CERT_TYPES | SSL Certificate types. This parameter is for SSL two way connection only. The valid file format types are *DER* and *PEM*. Types of multiple cetificates should be separated by a vertical bar ("\|"). Note that the certificate type should be corresponding to the certificate file in terms of sequence. |
| WL_SSL_CERT_FILES | SSL Certificate Files. This parameter is for SSL two way connection only. Set WL_SSL_CERT_FILES to RSA private key and chain of X.509 certificates for SSL client authentication. Multiple files are separated by a vertical bar ("\|"). Note that the sequence of the certificates matters. The SSL Client private key should be put as the first certificate. All but the first certificate are issuer certificates for the previous certificate. Example: *WL_SSL_CERT_FILES="C:\temp\testkey\client3.prv\|C:\temp\testkey\client3.pub\|C:\temp\testkey\netca_test_individual.cer"* |
| WL_SSL_KEY_PSWD | SSL client private key password. If the SSL client private key file is encrypted, set WL_SSL_KEY_PSWD to be the RSA private key's password; otherwise, leave it blank. |
| WL_MANAGED | Managed Server instance. WebLogic supports two server instance types, managed and admin. Specifying this parameter as false indicates that the server instance is an admin type. True indicates that the server instance is a managed server. Default setting is *false*. |
| WLINST | WebLogic instances. Enter the names of the Managing Server instances that will be configured for data collection. Multiple instances should be separated by a comma (",") |

*Table 21. WebLogic silent install parameter definitions for UNIX/Linux (continued)*

| Parameter | Definition |
|---|---|
| WL_STARTSH | WebLogic startup script. This is the startup script containing the necessary commands to call the application server. Ignore this value if CUSTOM_SCRIPT_ENABLED is set to be *false*. Multiple startup files should be separated by a comma (","). Check "Table for WebLogic/WebLogic Portal server startup script locations" on page 108 for details. |
| CUSTOM_SCRIPT_ENABLED | Enable custom startup script. If this parameter is selected, the WebLogic Startup Script is ignored. The custom startup script adds certain JVM properties to the WebLogic Startup command line, which enables the DC for testware when WebLogic is launched. |
| INST_WLHOST | WebLogic server host. Enter the host name or IP address of the computer that has WebLogic installed. Multiple value should be separated by a comma (",") |
| INST_WLPORT | WebLogic server port number. Enter the port number of the computer that has WebLogic installed. Default is 7001. Multiple value should be separated by a comma (",") |
| INST_WLJNDI_TYPE | WebLogic admin server instance connection method. If you choose connect to the WebLogic admin server using plain socket or HTTP, set INST_WLJNDI_TYPE to *t3* and ignore INST_WL_SSL_* parameters. If you choose connect to the WebLogic admin server using SSL, set INST_WLJNDI_TYPE to *t3s_oneway* for SSL one way connection or *t3s_twoway* for SSL two way connection. Multiple value should be separated by a comma (",") |
| INST_WL_SSL_TRUST_CA_KEYSTORE | SSL client CA trust keystore file. It is a *.jks* file. Multiple value should be separated by a comma (","). This parameter is for t3s_oneway and t3s_twoway. |
| INST_WL_SSL_CERT_TYPES | SSL Certificate types. This parameter is for SSL two way connection only. The valid file format types are *DER* and *PEM*. Types of multiple certificates should be separated by a vertical bar ("\|"). Note that the certificate type should be corresponding to the certificate file in terms of sequence. Multiple value should be separated by a comma (",") |

*Table 21. WebLogic silent install parameter definitions for UNIX/Linux (continued)*

| Parameter | Definition |
|---|---|
| INST_WL_SSL_CERT_FILES | SSL Certificate Files. This parameter is for SSL two way connection only. Set INST_WL_SSL_CERT_FILES to RSA private key and chain of X.509 certificates for SSL client authentication. Multiple files are separated by a vertical bar ("\|"). Note that the sequence of the certificates matters. The SSL Client private key should be put as the first certificate. All but the first certificate are issuer certificates for the previous certificate. Example: *INST_WL_SSL_CERT_FILES="C:\temp\testkey\client3.prv\|C:\temp\testkey\client3.pub\|C:\temp\testkey\netca_test_individual.cer"*. Multiple value should be separated by a comma (",") |
| INST_WL_SSL_KEY_PSWD | SSL client private key password. If the SSL client private key file is encrypted, set INST_WL_SSL_KEY_PSWD to be the RSA private key's password; otherwise, leave it blank. Multiple value should be separated by a comma (",") |

## Silent installation and configuration settings for WebLogic Portal Server

*Table 22. WebLogic Portal Server silent install parameter definitions for UNIX/Linux*

| Parameter | Definition |
|---|---|
| LICENSE_ACCEPT_BUTTON | License agreement. You must specify this parameter to begin the product installation. Default setting is *true*. |
| installLocation | The location where you intend to install the product. |
| LAUNCH_CONFIG | This parameter launches the Configuration Tool. Specifying this parameter begins the process of configuring the DC to the Managing Server after installation. The default setting is *true*. |
| LOGSETTING.LOGLEVEL | The log level for the installation and configuration process. Possible values are: ALL / DEBUG_MAX / DEBUG_MID / INFO / WARN / ERROR / FATAL / OFF. |
| LOGSETTING.LOGCONSOLEOUT | This parameter controls whether the output message is printed to console or not. Possible values are true / false. |
| **DC Configuration** | |
| UNCONFIGURE_SERVERS | Specifying this parameter will cancel the configuration process after the installation is complete. The default setting is *false*. |

*Table 22. WebLogic Portal Server silent install parameter definitions for UNIX/Linux (continued)*

| Parameter | Definition |
|---|---|
| J2EE_SELECTED | ITCAM for J2EE's Application Monitor interface. Specifying this parameter will configure monitored data to be accessed through ITCAM for J2EE's Application Monitor interface. To use the Application Monitor interface, the Managing Server must be available in your environment. The default is *true*. |
| TEMA_SELECTED | ITCAM for J2EE Tivoli Enterprise Portal. Specifying this parameter will configure monitored data to be accessed using the portal. To use the portal interface, ITCAM for J2EE and its components must be fully installed. The default is *false*. |
| SERVER_HOME | WebLogic directory location. Enter the root directory location in which WebLogic is located on the host computer |
| SERVER_VERSION | WebLogic version number. Enter the version number of WebLogic that you are currently running |
| JAVA_HOME | The location of the JDK. Enter the directory location of the JDK that supports WebLogic. |
| IS64UNIXJVM | The flag for 64 bit model. The default value is *false*. If you are running a 64 bit OS using 64 bit JVM on a UNIX or Linux platform, change the parameter to*true*. Ignore this parameter on Windows. |
| DC_OFFLINE_ALLOW | This is for you to decide whether offline configuration is allowed. If you enter "true", the program will skip the verification of the connection to the Managing Server (MS) during configuration, and use the entered value of MS_AM_HOME; if you enter "false", the program will connect to MS and detect the MS home directory on MS server. The default value is *false*. |
| TEMA_OFFLINE_ALLOW | The option indicates whether offline configuration type is allowed during the configuation. The program will skip the monitoring agent connection test if it is set to be *true*. Set it to *false* when you don't want to allow the offline configuration for the monitoring agent. |
| AM_SOCKET_BINDIP | This is the DC side IP address or full qualified Host name. The IP or Host name will be used by DC to communicate with MS.If there are more then one NIC or multiple IP address configured on DC server, choose one of them. For example: -V AM_SOCKET_BINDIP=9.181.93.95 or -V AM_SOCKET_BINDIP=dc.cn.ibm.com or -V AM_SOCKET_BINDIP=<*value*> |

*Table 22. WebLogic Portal Server silent install parameter definitions for UNIX/Linux (continued)*

| Parameter | Definition |
|---|---|
| FIREWALL_ENABLED | For DC side if the firewall is enabled, set the value to be *true*; otherwise, set the value to be *false*. |
| PROBE_RMI_POR | If the DC is behind firewall, set this port number. This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8200" to "8299". |
| PROBE_CONTROLLER_RMI_PORT | If the DC is behind firewall, set this port number. This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8300" to "8399". |
| **Managing-Server Specific Options** | |
| RECOLLECT_MSINFO | Specifying this parameter prompts the DC to recollect data from the Managing Server. The default is *true*. |
| MS_AM_HOME | The location of the Managing Server. Enter the directory location where the Managing Server is located. This parameter correlates the *DC_OFFLINE_ALLOW*. Refer to *DC_OFFLINE_ALLOW* for more detailed information. |
| KERNEL_HOST01 | Primary kernel server name. Enter full-qualified host name of the primary kernel server hosting the Managing Server. |
| PORT_KERNEL_CODEBASE01 | Primary kernel codebase port. The default is 9122. |
| **Application Server Specific Options** | |
| WLHOST | WebLogic Server host name. Enter the IP or domain name of the host location of the WebLogic server. |
| WLPORT | WebLogic server port number. The default is 7001. |
| WLUSER | User name. This parameter is optional. Enter a user ID name to match your current security settings; otherwise, leave this blank. |
| WLPSWD | Password. This parameter is optional. Enter a password to match your current security settings; otherwise, leave this blank. |
| WLJNDI_TYPE | WebLogic admin server connection method. If you choose connect to the WebLogic admin server using plain socket or HTTP, set WLJNDI_TYPE to *t3* and ignore WL_SSL_* parameters. If you choose connect to the WebLogic admin server using SSL, set WLJNDI_TYPE to *t3s_oneway* for SSL one way connection or *t3s_twoway* for SSL two way connection. |

*Table 22. WebLogic Portal Server silent install parameter definitions for UNIX/Linux (continued)*

| Parameter | Definition |
|---|---|
| WL_SSL_TRUST_CA_KEYSTORE | SSL client CA trust keystore file. It is a *.jks* file. This parameter is for t3s_oneway and t3s_twoway. |
| WL_SSL_CERT_TYPES | SSL Certificate types. This parameter is for SSL two way connection only. The valid file format types are *DER* and *PEM*. Types of multiple cetificates should be separated by a vertical bar ("\|"). Note that the certificate type should be corresponding to the certificate file in terms of sequence. |
| WL_SSL_CERT_FILES | SSL Certificate Files. This parameter is for SSL two way connection only. Set WL_SSL_CERT_FILES to RSA private key and chain of X.509 certificates for SSL client authentication. Multiple files are separated by a vertical bar ("\|"). Note that the sequence of the certificates matters. The SSL Client private key should be put as the first certificate. All but the first certificate are issuer certificates for the previous certificate. Example: *WL_SSL_CERT_FILES="C:\temp\testkey\client3.prv\|C:\temp\testkey\client3.pub\|C:\temp\testkey\netca_test_individual.cer"* |
| WL_SSL_KEY_PSWD | SSL client private key password. If the SSL client private key file is encrypted, set WL_SSL_KEY_PSWD to be the RSA private key's password; otherwise, leave it blank. |
| WL_MANAGED | Managed Server instance. WebLogic supports two server instance types, managed and admin. Specifying this parameter as false indicates that the server instance is an admin type. True indicates that the server instance is a managed server. Default setting is *false*. |
| WLINST | WebLogic instances. Enter the names of the Managing Server instances that will be configured for data collection. Multiple instances should be separated by a comma (",") |
| WL_STARTSH | WebLogic startup script. This is the startup script containing the necessary commands to call the application server. Ignore this value if CUSTOM_SCRIPT_ENABLED is set to be *false*. Multiple startup files should be separated by a comma (","). Check "Table for WebLogic/WebLogic Portal server startup script locations" on page 108 for details. |

*Table 22. WebLogic Portal Server silent install parameter definitions for UNIX/Linux (continued)*

| Parameter | Definition |
|---|---|
| CUSTOM_SCRIPT_ENABLED | Enable custom startup script. If this parameter is selected, the WebLogic Startup Script is ignored. The custom startup script adds certain JVM properties to the WebLogic Startup command line, which enables the DC for testware when WebLogic is launched. |
| INST_WLHOST | WebLogic server host. Enter the host name or IP address of the computer that has WebLogic installed. Multiple value should be separated by a comma (",") |
| INST_WLPORT | WebLogic server port number. Enter the port number of the computer that has WebLogic installed. Default is 7001. Multiple value should be separated by a comma (",") |
| INST_WLJNDI_TYPE | WebLogic admin server instance connection method. If you choose connect to the WebLogic admin server using plain socket or HTTP, set INST_WLJNDI_TYPE to *t3* and ignore INST_WL_SSL_* parameters. If you choose connect to the WebLogic admin server using SSL, set INST_WLJNDI_TYPE to *t3s_oneway* for SSL one way connection or *t3s_twoway* for SSL two way connection. Multiple value should be separated by a comma (",") |
| INST_WL_SSL_TRUST_CA_KEYSTORE | SSL client CA trust keystore file. It is a *.jks* file. Multiple value should be separated by a comma (","). This parameter is for t3s_oneway and t3s_twoway. |
| INST_WL_SSL_CERT_TYPES | SSL Certificate types. This parameter is for SSL two way connection only. The valid file format types are *DER* and *PEM*. Types of multiple certificates should be separated by a vertical bar ("\|"). Note that the certificate type should be corresponding to the certificate file in terms of sequence. Multiple value should be separated by a comma (",") |
| INST_WL_SSL_CERT_FILES | SSL Certificate Files. This parameter is for SSL two way connection only. Set INST_WL_SSL_CERT_FILES to RSA private key and chain of X.509 certificates for SSL client authentication. Multiple files are separated by a vertical bar ("\|"). Note that the sequence of the certificates matters. The SSL Client private key should be put as the first certificate. All but the first certificate are issuer certificates for the previous certificate. Example: *INST_WL_SSL_CERT_FILES="C:\temp\testkey\client3.prv\|C:\temp\testkey\client3.pub\|C:\temp\testkey\netca_test_individual.cer"*. Multiple value should be separated by a comma (",") |

*Table 22. WebLogic Portal Server silent install parameter definitions for UNIX/Linux (continued)*

| Parameter | Definition |
|---|---|
| INST_WL_SSL_KEY_PSWD | SSL client private key password. If the SSL client private key file is encrypted, set INST_WL_SSL_KEY_PSWD to be the RSA private key's password; otherwise, leave it blank. Multiple value should be separated by a comma (",") |

## Silent installation and configuration settings for NetWeaver

*Table 23. NetWeaver silent install parameter definitions for UNIX/Linux*

| Parameter | Definition |
|---|---|
| LICENSE_ACCEPT_BUTTON | License agreement. You must specify this parameter to begin the product installation. Default setting is *true*. |
| installLocation | The location where you intend to install the product. |
| LAUNCH_CONFIG | This parameter launches the Configuration Tool. Specifying this parameter begins the process of configuring the DC to the Managing Server after installation. The default setting is *true*. |
| LOGSETTING.LOGLEVEL | The log level for the installation and configuration process. Possible values are: ALL / DEBUG_MAX / DEBUG_MID / INFO / WARN / ERROR / FATAL / OFF. |
| LOGSETTING.LOGCONSOLEOUT | This parameter controls whether the output message is printed to console or not. Possible values are true / false. |
| **DC Configuration** | |
| UNCONFIGURE_SERVERS | Specifying this parameter will cancel the configuration process after the installation is complete. The default setting is *false*. |
| J2EE_SELECTED | ITCAM for J2EE's Application Monitor interface. Specifying this parameter will configure monitored data to be accessed through ITCAM for J2EE's Application Monitor interface. To use the Application Monitor interface, the Managing Server must be available in your environment. The default is *true*. |
| TEMA_SELECTED | ITCAM for J2EE Tivoli Enterprise Portal. Specifying this parameter will configure monitored data to be accessed using the portal. To use the portal interface, ITCAM for J2EE and its components must be fully installed. The default is *false*. |

*Table 23. NetWeaver silent install parameter definitions for UNIX/Linux (continued)*

| Parameter | Definition |
|---|---|
| DC_OFFLINE_ALLOW | This is for you to decide whether offline configuration is allowed. If you enter "true", the program will skip the verification of the connection to the Managing Server (MS) during configuration, and use the entered value of MS_AM_HOME; if you enter "false", the program will connect to MS and detect the MS home directory on MS server. The default value is *false*. |
| TEMA_OFFLINE_ALLOW | The option indicates whether offline configuration type is allowed during the configuation. The program will skip the monitoring agent connection test if it is set to be *true*. Set it to *false* when you don't want to allow the offline configuration for the monitoring agent. |
| AM_SOCKET_BINDIP | This is the DC side IP address or full qualified Host name. The IP or Host name will be used by DC to communicate with MS.If there are more then one NIC or multiple IP address configured on DC server, choose one of them. For example: -V AM_SOCKET_BINDIP=9.181.93.95 or -V AM_SOCKET_BINDIP=dc.cn.ibm.com or -V AM_SOCKET_BINDIP=*<value>* |
| FIREWALL_ENABLED | For DC side if the firewall is enabled, set the value to be *true*; otherwise, set the value to be *false*. |
| PROBE_RMI_POR | If the DC is behind firewall, set this port number.This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8200" to "8299". |
| PROBE_CONTROLLER_RMI_PORT | If the DC is behind firewall, set this port number. This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8300" to "8399". |
| **Managing-Server Specific Options** | |
| RECOLLECT_MSINFO | Specifying this parameter prompts the DC to recollect data from the Managing Server. The default is *true*. |
| MS_AM_HOME | The location of the Managing Server. Enter the directory location where the Managing Server was installed. This parameter correlates the *DC_OFFLINE_ALLOW*. Refer to *DC_OFFLINE_ALLOW* for more detailed information. |
| KERNEL_HOST01 | Primary kernel server name. Enter full-qualified host name of the primary kernel server hosting the Managing Server. |
| PORT_KERNEL_CODEBASE01 | Primary kernel codebase port. The default is 9122. |

*Table 23. NetWeaver silent install parameter definitions for UNIX/Linux (continued)*

| Parameter | Definition |
|---|---|
| **Application Server Specific Options** | |
| INSTALL_TYPE | NetWeaver installation type. Choose from the three installation types: central instance (denoted as 1), local dialog instance (denoted as 2), and distributed dialog instance (denoted as 3). Enter the number value representing your installation type.<br>The 3 DC installation types are:<br>1. Central instance installation: Install DC to monitor the server on Central instance;<br>2. Local dialog instance installation: Dialog instance and central instance are installed on one computer and the DC is installed to monitor the server on the dialog instance;<br>3. Distributed dialog instance installation: Dialog instance and central instance are not installed on the same computer, and the DC is installed to monitor the server on the dialog instance. |
| SERVER_HOME | NetWeaver directory location. The absolute path of directory wherein the instance is monitored. |
| CENTRAL_INSTANCE_HOME | NetWeaver central instance directory. Enter the directory location of the NetWeaver central server instance. For central instance installation, its value is the same as the *Server home*. |
| CENTRAL_INSTANCE_NETWORK_HOME | NetWeaver central instance network directory. A local path mounted from *Central instance home* directory. For central instance installation, its value is the same as the *Server home*. For local dialog instance installation, its value is the same as the *Central instance home*. For distributed dialog instance installation, mount the *Central instance home* on central instance computer to a local directory, and the value of *Central instance network home* should be the mounted local directory. |
| SERVER_VERSION | NetWeaver version number. Enter the current version number of NetWeaver that you are running. |
| JAVA_HOME | JDK location. Enter the directory location of the JDK supporting NetWeaver. |
| IS64UNIXJVM | The flag for 64 bit model. The default value is *false*. If you are running a 64 bit OS using 64 bit JVM on a UNIX or Linux platform, change the parameter to*true*. Ignore this parameter on Windows. |

*Table 23. NetWeaver silent install parameter definitions for UNIX/Linux (continued)*

| Parameter | Definition |
|---|---|
| SAPNW64HOST | The qualified host name of local computer. |
| SAPNW64PORT | The P4 port of the NetWeaver instance. |
| SAPNW64USER | The required user name used to get the Java Management Extensions (JMX) Data from MBean Server. Usually, this user ID is the same as you log on the Visual Administrator tool. For example, Administrator. |
| SAPNW64PSWD | The required password used to get the JMX Data from MBean Server. Usually, this password is the same as you log on the Visual Administrator tool. |
| SAPNW64_SVRS | Server instance names. Enter the names of the Managing Server instances to be configured for data collection. If multiple instances are monitored, separate them by semicolons. |

## Silent installation and configuration settings for JBoss

*Table 24. JBoss silent install parameter definitions for UNIX/Linux*

| Parameter | Definition |
|---|---|
| LICENSE_ACCEPT_BUTTON | License agreement. You must specify this parameter to begin the product installation. Default setting is *true*. |
| installLocation | The location where you intend to install the product. |
| LAUNCH_CONFIG | This parameter launches the Configuration Tool. Specifying this parameter begins the process of configuring the DC to the Managing Server after installation. The default setting is *true*. |
| LOGSETTING.LOGLEVEL | The log level for the installation and configuration process. Possible values are: ALL / DEBUG_MAX / DEBUG_MID / INFO / WARN / ERROR / FATAL / OFF. |
| LOGSETTING.LOGCONSOLEOUT | This parameter controls whether the output message is printed to console or not. Possible values are true / false. |
| **DC Configuration** | |
| UNCONFIGURE_SERVERS | Specifying this parameter will cancel the configuration process after the installation is complete. The default setting is *false*. |
| J2EE_SELECTED | ITCAM for J2EE's Application Monitor interface. Specifying this parameter will configure monitored data to be accessed through ITCAM for J2EE's Application Monitor interface. To use the Application Monitor interface, the Managing Server must be available in your environment. The default is *true*. |

*Table 24. JBoss silent install parameter definitions for UNIX/Linux (continued)*

| Parameter | Definition |
|---|---|
| TEMA_SELECTED | ITCAM for J2EE Tivoli Enterprise Portal. Specifying this parameter will configure monitored data to be accessed using the portal. To use the portal interface, ITCAM for J2EE and its components must be fully installed. The default is *false*. |
| SERVER_HOME | JBoss directory location. Enter the root directory location in which JBoss is located. |
| SERVER_VERSION | JBoss version number. Enter the version number of JBoss that you are currently running. |
| JAVA_HOME | The location of the JDK. Enter the directory location of the JDK supporting JBoss. |
| IS64UNIXJVM | The flag for 64 bit model. The default value is *false*. If you are running a 64 bit OS using 64 bit JVM on a UNIX or Linux platform, change the parameter to*true*. Ignore this parameter on Windows. |
| DC_OFFLINE_ALLOW | This is for you to decide whether offline configuration is allowed. If you enter "true", the program will skip the verification of the connection to the Managing Server (MS) during configuration, and use the entered value of MS_AM_HOME; if you enter "false", the program will connect to MS and detect the MS home directory on MS server. The default value is *false*. |
| TEMA_OFFLINE_ALLOW | The option indicates whether offline configuration type is allowed during the configuation. The program will skip the monitoring agent connection test if it is set to be *true*. Set it to *false* when you don't want to allow the offline configuration for the monitoring agent. |
| AM_SOCKET_BINDIP | This is the DC side IP address or full qualified Host name. The IP or Host name will be used by DC to communicate with MS.If there are more then one NIC or multiple IP address configured on DC server, choose one of them. For example: -V AM_SOCKET_BINDIP=9.181.93.95 or -V AM_SOCKET_BINDIP=dc.cn.ibm.com or -V AM_SOCKET_BINDIP=<*value*> |
| FIREWALL_ENABLED | For DC side if the firewall is enabled, set the value to be *true*; otherwise, set the value to be *false*. |
| PROBE_RMI_POR | If the DC is behind firewall, set this port number.This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8200" to "8299". |

*Table 24. JBoss silent install parameter definitions for UNIX/Linux (continued)*

| Parameter | Definition |
|---|---|
| PROBE_CONTROLLER_RMI_PORT | If the DC is behind firewall, set this port number. This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8300" to "8399". |
| **Managing-Server Specific Options** | |
| RECOLLECT_MSINFO | Specifying this parameter prompts the DC to recollect data from the Managing Server. The default is *true*. |
| MS_AM_HOME | The location of the Managing Server. Enter the directory location where the Managing Server was installed. This parameter correlates the *DC_OFFLINE_ALLOW*. Refer to *DC_OFFLINE_ALLOW* for more detailed information. |
| KERNEL_HOST01 | Primary kernel server name. Enter full-qualified host name of the primary kernel server hosting the Managing Server. |
| PORT_KERNEL_CODEBASE01 | Primary kernel codebase port. The default is 9122. |
| **Application Server Specific Options** | |
| JBOSSHOST | JBoss server host name. Enter the IP or domain name of the JBoss server host server. |
| JBOSSPORT | JBoss server port number. The default is 1099. |
| SECURITY_ENABLE | The parameters, JBOSSUSER and JBOSSPSWD, are ignored if SECURITY_ENABLE is false. The default value is *false*. |
| JBOSSUSER | User name. This parameter is optional. Enter a user ID name to match your current security settings; otherwise, leave this blank. |
| JBOSSPSWD | Password. This parameter is optional. Enter a password to match your current security settings; otherwise, leave this blank. |
| JBOSSINST | JBoss instances. Enter the Managing Server instances that will be configured for data collection. |
| JBOSS_SERVER_DIR | JBoss Server instance directory. The directory location of JBoss server that will be configured for the data collector, for example: /var/jboss4.0.3SP1/server/default. |
| JBOSSSTARTSH | JBoss server startup script. This is the file containing the necessary commands to launch JBoss. The script can be found within the location in which you installed JBoss, for example: /var/jboss-4.0.3SP1/bin/run.sh. |

## Silent installation and configuration settings for Tomcat

*Table 25. Tomcat silent install parameter definitions for UNIX/Linux*

| Parameter | Definition |
|---|---|
| LICENSE_ACCEPT_BUTTON | License agreement. You must specify this parameter to begin the product installation. Default setting is *true*. |
| installLocation | The location where you intend to install the product. |
| LAUNCH_CONFIG | This parameter launches the Configuration Tool. Specifying this parameter begins the process of configuring the DC to the Managing Server after installation. The default setting is *true*. |
| LOGSETTING.LOGLEVEL | The log level for the installation and configuration process. Possible values are: ALL / DEBUG_MAX / DEBUG_MID / INFO / WARN / ERROR / FATAL / OFF. |
| LOGSETTING.LOGCONSOLEOUT | This parameter controls whether the output message is printed to console or not. Possible values are true / false. |
| **DC Configuration** | |
| UNCONFIGURE_SERVERS | Specifying this parameter will cancel the configuration process after the installation is complete. The default setting is *false*. |
| J2EE_SELECTED | ITCAM for J2EE's Application Monitor interface. Specifying this parameter will configure monitored data to be accessed through ITCAM for J2EE's Application Monitor interface. To use the Application Monitor interface, the Managing Server must be available in your environment. The default is *true*. |
| TEMA_SELECTED | ITCAM for J2EE Tivoli Enterprise portal. Specifying this parameter will configure monitored data to be accessed using the ITCAM for J2EE's portal. To use the portal interface, ITCAM for J2EE and its components must be fully installed. The default is *false*. |
| SERVER_HOME | Tomcat server directory location. Enter the root directory location in which Tomcat is located on. |
| SERVER_VERSION | Tomcat server version number. Enter the version of the Tomcat server that you are currently running. For example, if the Tomcat version is 5.0, SERVER_VERSION should be set as 50; if the version is 5.5, SERVER_VERSION should be set as 55. |
| JAVA_HOME | The location of the JDK. Enter the directory location of the JDK supporting Tomcat. |
| IS64UNIXJVM | The flag for 64 bit model. The default value is *false*. If you are running a 64 bit OS using 64 bit JVM on a UNIX or Linux platform, change the parameter to *true*. Ignore this parameter on Windows. |

*Table 25. Tomcat silent install parameter definitions for UNIX/Linux (continued)*

| Parameter | Definition |
|---|---|
| DC_OFFLINE_ALLOW | This is for you to decide whether offline configuration is allowed. If you enter "true", the program will skip the verification of the connection to the Managing Server (MS) during configuration, and use the entered value of MS_AM_HOME; if you enter "false", the program will connect to MS and detect the MS home directory on MS server. The default value is *false*. |
| TEMA_OFFLINE_ALLOW | The option indicates whether offline configuration type is allowed during the configuation. The program will skip the monitoring agent connection test if it is set to be *true*. Set it to *false* when you don't want to allow the offline configuration for the monitoring agent. |
| AM_SOCKET_BINDIP | This is the DC side IP address or full qualified Host name. The IP or Host name will be used by DC to communicate with MS.If there are more then one NIC or multiple IP address configured on DC server, choose one of them. For example: -V AM_SOCKET_BINDIP=9.181.93.95 or -V AM_SOCKET_BINDIP=dc.cn.ibm.com or -V AM_SOCKET_BINDIP=<*value*> |
| FIREWALL_ENABLED | For DC side if the firewall is enabled, set the value to be *true*; otherwise, set the value to be *false*. |
| PROBE_RMI_POR | If the DC is behind firewall, set this port number.This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8200" to "8299". |
| PROBE_CONTROLLER_RMI_PORT | If the DC is behind firewall, set this port number. This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8300" to "8399". |
| **Managing-Server Specific Options** | |
| RECOLLECT_MSINFO | Specifying this parameter prompts the DC to recollect data from the Managing Server. The default is *true*. |
| MS_AM_HOME | The location of the Managing Server. Enter the directory location where the Managing Server was installed. This parameter correlates the *DC_OFFLINE_ALLOW*. Refer to *DC_OFFLINE_ALLOW* for more detailed information. |
| KERNEL_HOST01 | Primary kernel server name. Enter full-qualified host name of the primary kernel server hosting the Managing Server. |
| PORT_KERNEL_CODEBASE01 | Primary kernel codebase port. The default is 9122. |
| **Application Server Specific Options** | |

*Table 25. Tomcat silent install parameter definitions for UNIX/Linux (continued)*

| Parameter | Definition |
|---|---|
| APPSERVER | Tomcat application server instance. Enter the Tomcat Server instance names that you wish to configure for data collection.<br><br>If you are editing the Tomcat Server instance name for the Tomcat configurator, check whether the instance name exists.<br>• If you are configuring a new Tomcat server, make sure there is no existing instance name. Use a different instance name.<br>• If you are reconfiguring an existing Tomcat server, you do not need to check the instance name.<br><br>**Note:** The instance name information can be found in the directory, <*DC_HOME*>/runtime/. If there is an existing Tomcat Server instance name, you can find a child directory under this directory. The child directory takes the form as <Server Name>.<Node Name>.<Instance Name>. For example, tomcat_55_1029_1 is the instance name in the <*DC_HOME*>/runtime/ tomcat55.tiv147.cn.ibm.com.tomcat_55_1029_1 directory. |
| STARTUP_FILE | Server startup script. The startup script is a batch or command file containing the necessary command lines required to startup the application server. Enter the full file path of the startup script here. On UNIX/Linux, the startup script is <*Tomcat Home*>/bin/catalina.sh. Where <*Tomcat Home*> is the root directory where you installed the Tomcat server. |

## Silent installation and configuration settings for Oracle

*Table 26. Oracle silent install parameter definitions for UNIX/Linux*

| Parameter | Definition |
|---|---|
| LICENSE_ACCEPT_BUTTON | License agreement. You must specify this parameter to begin the product installation. Default setting is *true*. |
| installLocation | The location where you intend to install the product. |
| LAUNCH_CONFIG | This parameter launches the Configuration Tool. Specifying this parameter begins the process of configuring the DC to the Managing Server after installation. The default setting is *true*. |
| LOGSETTING.LOGLEVEL | The log level for the installation and configuration process. Possible values are: ALL / DEBUG_MAX / DEBUG_MID / INFO / WARN / ERROR / FATAL / OFF. |

*Table 26. Oracle silent install parameter definitions for UNIX/Linux (continued)*

| Parameter | Definition |
|---|---|
| LOGSETTING.LOGCONSOLEOUT | This parameter controls whether the output message is printed to console or not. Possible values are true / false. |
| **DC Configuration** | |
| UNCONFIGURE_SERVERS | Specifying this parameter will cancel the configuration process after the installation is complete. The default setting is *false*. |
| J2EE_SELECTED | ITCAM for J2EE's Application Monitor interface. Specifying this parameter will configure monitored data to be accessed through ITCAM for J2EE's Application Monitor interface. To use the Application Monitor interface, the Managing Server must be available in your environment. The default is *true*. |
| TEMA_SELECTED | ITCAM for J2EE Tivoli Enterprise Portal . Specifying this parameter will configure monitored data to be accessed using the portal. To use the portal interface, ITCAM for J2EE and its components must be fully installed. The default is *false*. |
| SERVER_HOME | Oracle server directory location. Enter the root directory location in which Oracle is located. |
| SERVER_VERSION | Oracle server version number. Enter the version of the Oracle server that you are currently running. |
| JAVA_HOME | The location of the JDK. Enter the directory location of the JDK supporting Oracle. |
| IS64UNIXJVM | The flag for 64 bit model. The default value is *false*. If you are running a 64 bit OS using 64 bit JVM on a UNIX or Linux platform, change the parameter to*true*. Ignore this parameter on Windows. |
| DC_OFFLINE_ALLOW | This is for you to decide whether offline configuration is allowed. If you enter "true", the program will skip the verification of the connection to the Managing Server (MS) during configuration, and use the entered value of MS_AM_HOME; if you enter "false", the program will connect to MS and detect the MS home directory on MS server. The default value is *false*. |
| TEMA_OFFLINE_ALLOW | The option indicates whether offline configuration type is allowed during the configuation. The program will skip the monitoring agent connection test if it is set to be *true*. Set it to *false* when you don't want to allow the offline configuration for the monitoring agent. |

*Table 26. Oracle silent install parameter definitions for UNIX/Linux (continued)*

| Parameter | Definition |
|---|---|
| AM_SOCKET_BINDIP | This is the DC side IP address or full qualified Host name. The IP or Host name will be used by DC to communicate with MS.If there are more then one NIC or multiple IP address configured on DC server, choose one of them. For example: -V AM_SOCKET_BINDIP=9.181.93.95 or -V AM_SOCKET_BINDIP=dc.cn.ibm.com or -V AM_SOCKET_BINDIP=<*value*> |
| FIREWALL_ENABLED | For DC side if the firewall is enabled, set the value to be *true*; otherwise, set the value to be *false*. |
| PROBE_RMI_POR | If the DC is behind firewall, set this port number.This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8200" to "8299". |
| PROBE_CONTROLLER_RMI_PORT | If the DC is behind firewall, set this port number. This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8300" to "8399". |
| **Managing-Server Specific Options** | |
| RECOLLECT_MSINFO | Specifying this parameter prompts the DC to recollect data from the Managing Server. The default is *true*. |
| MS_AM_HOME | The location of the Managing Server. Enter the directory location where the Managing Server was installed. This parameter correlates the *DC_OFFLINE_ALLOW*. Refer to *DC_OFFLINE_ALLOW* for more detailed information. |
| KERNEL_HOST01 | Primary kernel server name. Enter full-qualified host name of the primary kernel server hosting the Managing Server. |
| PORT_KERNEL_CODEBASE01 | Primary kernel codebase port. The default is 9122. |
| **Application Server Specific Options** | |
| OAS_INST | Oracle application server instance. The instances that you chose to have configured must be defined in this parameter. |
| ORA_ADMIN_USER | The admin username of the Oracle application server. Required only when configuring Oracle 10.1.3. |
| ORA_ADMIN_PSWD | The password of ORA_ADMIN_USER. |

## Silent installation and configuration settings for J2SE

*Table 27. J2SE silent install parameter definitions for UNIX/Linux*

| Parameter | Definition |
|---|---|
| LICENSE_ACCEPT_BUTTON | License agreement. You must specify this parameter to begin the product installation. Default setting is *true*. |
| installLocation | The location where you intend to install the product. |
| LAUNCH_CONFIG | This parameter launches the Configuration Tool. Specifying this parameter begins the process of configuring the DC to the Managing Server after installation. The default setting is *true*. |
| LOGSETTING.LOGLEVEL | The log level for the installation and configuration process. Possible values are: ALL / DEBUG_MAX / DEBUG_MID / INFO / WARN / ERROR / FATAL / OFF. |
| LOGSETTING.LOGCONSOLEOUT | This parameter controls whether the output message is printed to console or not. Possible values are true / false. |
| **DC Configuration** | |
| UNCONFIGURE_SERVERS | Specifying this parameter will cancel the configuration process after the installation is complete. The default setting is *false*. |
| J2EE_SELECTED | ITCAM for J2EE's Application Monitor interface. Specifying this parameter will configure monitored data to be accessed through ITCAM for J2EE's Application Monitor interface. To use the Application Monitor interface, the Managing Server must be available in your environment. The default is *true*. |
| TEMA_SELECTED | ITCAM for J2EE Tivoli Enterprise Portal. Specifying this parameter will configure monitored data to be accessed using the portal. To use the portal interface, ITCAM for J2EE and its components must be fully installed. The default is *false*. |
| SERVER_HOME | J2SE directory location. Enter the root directory location in which J2SE is located |
| SERVER_VERSION | J2SE version number. Enter the version number of J2SE that you are currently running |
| JAVA_HOME | The location of the JDK. Enter the directory location of the JDK supporting J2SE |
| IS64UNIXJVM | The flag for 64 bit model. The default value is *false*. If you are running a 64 bit OS using 64 bit JVM on a UNIX or Linux platform, change the parameter to*true*. Ignore this parameter on Windows. |

*Table 27. J2SE silent install parameter definitions for UNIX/Linux (continued)*

| Parameter | Definition |
|---|---|
| DC_OFFLINE_ALLOW | This is for you to decide whether offline configuration is allowed. If you enter "true", the program will skip the verification of the connection to the Managing Server (MS) during configuration, and use the entered value of MS_AM_HOME; if you enter "false", the program will connect to MS and detect the MS home directory on MS server. The default value is *false*. |
| TEMA_OFFLINE_ALLOW | The option indicates whether offline configuration type is allowed during the configuation. The program will skip the monitoring agent connection test if it is set to be *true*. Set it to *false* when you don't want to allow the offline configuration for the monitoring agent. |
| AM_SOCKET_BINDIP | This is the DC side IP address or full qualified Host name. The IP or Host name will be used by DC to communicate with MS.If there are more then one NIC or multiple IP address configured on DC server, choose one of them. For example: -V AM_SOCKET_BINDIP=9.181.93.95 or -V AM_SOCKET_BINDIP=dc.cn.ibm.com or -V AM_SOCKET_BINDIP=<*value*> |
| FIREWALL_ENABLED | For DC side if the firewall is enabled, set the value to be *true*; otherwise, set the value to be *false*. |
| PROBE_RMI_POR | If the DC is behind firewall, set this port number.This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8200" to "8299". |
| PROBE_CONTROLLER_RMI_PORT | If the DC is behind firewall, set this port number. This port number should be configured as allowable in firewall software on which the DC host locates. The legal values are from "8300" to "8399". |
| **Managing-Server Specific Options** | |
| RECOLLECT_MSINFO | Specifying this parameter prompts the DC to recollect data from the Managing Server. The default is *true*. |
| MS_AM_HOME | The location of the Managing Server. Enter the directory location where the Managing Server was installed. This parameter correlates the *DC_OFFLINE_ALLOW*. Refer to *DC_OFFLINE_ALLOW* for more detailed information. |
| KERNEL_HOST01 | Primary kernel server name. Enter full-qualified host name of the primary kernel server hosting the Managing Server. |
| PORT_KERNEL_CODEBASE01 | Primary kernel codebase port. The default is 9122. |

*Table 27. J2SE silent install parameter definitions for UNIX/Linux (continued)*

| Parameter | Definition |
|---|---|
| **Application Server Specific Options** | |
| J2SEMAINCLASS | Class type. Enter the main class type. |
| J2SEJMXEMBEDED | Embedded MBeans. Select *yes* if MBeans are embedded in the application. Select *no* if not. |
| J2SEJMXREMOTE | If MBeans are embedded in your application, this parameter must be input. Select *yes* if the DC must be connected using remote client, otherwise select *no* |
| J2SEHOST | Host name. Input the host name or IP address of the J2SE host in the event that the DC is connected using remote client. |
| J2SEPORT | J2SE port number. Input port number of the Managing Server's host computer. |
| J2SEUSER | User name. This parameter is optional. Enter a user ID name to match your current security settings; otherwise, leave this blank. |
| J2SEPSWD | Password. This parameter is optional. Enter a password to match your current security settings; otherwise, leave this blank. |
| J2SEINST | Instance names. Input the Managing Server instance names will be configured for data collection here. |
| J2SEGENERATENEW | Generate new startup script. Select *yes* to generate a new startup script. Select *no* to use a preexisting one. |
| J2SESTARTSH | Startup script directory. Input the startup script location here, if you selected *no* to the parameter: J2SEGENERATENEW . The startup script is the command or batch file with the necessary command lines capable of running the application server. |
| J2SEJVMMACRO | JVM macro. Input the JVM macro name here, only if you selected *no* to the parameter: J2SEGENERATENEW. |
| J2SESAMPLEPATH | Sample path. Input the directory location for the new startup script if you selected *yes* to the parameter: J2SEGENERATENEW. |
| J2SEJVMARG | JVM argument. Insert your JVM argument name if you selected *yes* to the parameter: J2SEGENERATENEW. |
| J2SEPROGARG | Program argument. Input the program argument name. |

## Silent installation and configuration settings for JSAS

*Table 28. JSAS silent install parameter definitions for UNIX/Linux*

| Parameter | Definition |
|---|---|
| LOGSETTING.LOGLEVEL | The log level for the installation and configuration process. Possible values are: ALL / DEBUG_MAX / DEBUG_MID / INFO / WARN / ERROR / FATAL / OFF. |
| LOGSETTING.LOGCONSOLEOUT | This parameter controls whether the output message is printed to console or not. Possible values are true / false. |
| SERVER_HOME | JSAS and iPlanet Application Server (IAS) home directory. Enter the root directory in which JSAS or IAS is located. For JSAS 7 and JSAS 8, the default value is /opt/SUNWappserver/appserver. For IAS 6.5, the default value is /opt/ias/iplanet/ias6/ias. |
| SERVER_VERSION | JSAS and IAS version number. Enter the version number of JSAS or IAS that you are currently running. The supported versions are IAS 6.5, JSAS 7 and 8. |
| JAVA_HOME | The Java home directory that the application server uses. For JSAS 8, the typical java home directory is /usr/jdk/entsys-j2se. For JSAS 7, the typical java home directory is /usr/java. For IAS 6.5 the typical java home directory is <SERVER_HOME>/usr/java. |
| ADMIN_HOST | For Sun JSAS 8, the value is the Java Management Extensions (JMX) connector listening IP address or the hostname of the domain admin server. For Sun JSAS 7, the value is the listening IP address or the hostname of the domain admin server. This parameter is valid for Sun JSAS 7 and 8 only. |
| ADMIN_PORT | For JSAS 8, the value is the JMX connector listening port of the domain admin server. For Sun JSAS 7, the value is the listening port of the domain admin server. This parameter is valid for JSAS 7 and 8 only. |
| ADMIN_USER | The login user ID of the domain admin server. This parameter is valid for JSAS 7 and 8 only. |
| ADMIN_PSWD | The password of the domain admin server. This parameter is valid for JSAS 7 and 8 only. |
| ADMIN_SSL | The SSL of the JMX connector listener for the domain admin server. Valid values are *true* and *false*. This parameter is valid for JSAS 7 and 8 only. |

*Table 28. JSAS silent install parameter definitions for UNIX/Linux (continued)*

| Parameter | Definition |
| --- | --- |
| ADMIN_INST | The application instance names. For JSAS 7 and 8, this parameter contains the names of application instances to be configured or unconfigured. You can logon the domain admin server to get the names of application server. If there are multiple instances to be configured, separate the instance names with commas. For IAS 6.5, specify the parameter which contains alpha or number characters only. In this situation, this parameter does not support multiple instance names. |

## A post-installation step for ITCAM for J2EE Data Collector

After the installation, the files and directories of the Data Collector are readable by all users in the system. You can enforce the security of them by using *chmod* command to change the permissions of them.

To lock Data Collector files and directories to a specific user, use the following command:

```
chmod -R 700 <DC_HOME>
```

To lock Data Collector files and directories to a specific user and allow a user group to read and execute, use the following command:

```
chmod -R 750 <DC_HOME>
```

# Chapter 4. Configuring the ITCAM for J2EE Data Collector

This chapter provides instructions for configuring your Managing Server instance using the ITCAM for J2EE Data Collector's Configuration Tool. Perform the following steps:



**Note:**

1. To configure the ITCAM for J2EE Data Collector for the WebLogic server, JBoss server, and NetWeaver server, you must ensure that the corresponding application server is already started before your configuration.
2. Data Collector (DC) configuration depends on JVM information (vendor, version and whether JVM is 32-bit or 64-bit). Make sure you have the correct JVM information before you configure the Data Collector.
3. For installation using non-root users, please read Appendix D, "Summary of permissions required for installing and configuring the Data Collector," on page 207 and follow the requirements before doing the installation.
4. All the screen captures in this section are taken from configuration toolkits running on Windows, for the purpose of illustration. Actual screen displays might vary by platform and operating system.

## Pre-configuration steps for supporting customized startup script for WebLogic

If a customized script is used for starting the WebLogic server, there are additional steps to be performed. The steps are necessary for the Configuration Tool to correctly locate the appropriate section of the script and insert the configurations of the Data Collector accordingly.

Two anchors are needed to be specified in the customized script before running the Configuration Tool. They are ***ITCAM_DC_SCRIPT*** and ***ITCAM_OPTIONS***.

1. Anchor **ITCAM_DC_SCRIPT**

   To support a customized startup script, the anchor *ITCAM_DC_SCRIPT* is needed to be specified in the script. It must be defined in a new line, immediately before the execution of the java command that starts the application server. When the Configuration Tool runs, the configuration of the Data Collector is inserted before this anchor.

   Syntax:

   ```
   <comment_tab> ITCAM_DC_SCRIPT, <VAR_SERVER_NAME>
   ```

   where:

   *<comment_tab>* is the character used for indicating a line of comment in a script. In UNIX, this character is '###'. In Windows, this character is "REM"'

   *<VAR_SERVER_NAME>* is the name of the WebLogic startup script variable that contains the server instance name. The default variable name is *SERVER_NAME*. In rare cases when the name is changed, this changed variable name must be used in the anchor. If omitted, the default value is *SERVER_NAME*.

   Examples:

   Add the following line in a customized script on Linux and UNIX systems:

   ```
   #### ITCAM_DC_SCRIPT, SERVER_NAME
   ```

   Add the following line in a customized script on Windows systems:

   ```
   REM ITCAM_DC_SCRIPT, SERVER_NAME
   ```

2. Anchor **ITCAM_OPTIONS**

   The second anchor is required to be added as the last JVM option in the customized script. User needs to find where the JVM options are and insert *$ITCAM_OPTIONS* (on UNIX) or *%ITCAM_OPTIONS%* (on Windows). Specify the*ITCAM_OPTIONS* anchor as the last JVM option, before the main class *weblogic.Server* in the WebLogic JVM startup options.

   **Note:** Any existing Garbage Collection (GC) logging argument or Java security policy is overwritten after the configuration process

   Examples:

   ```
   ${JAVA_HOME}/bin/java ${JAVA_VM} ${MEM_ARGS} ${JAVA_OPTIONS}
   -Dweblogic.Name=${SERVER_NAME}
   -Djava.security.policy=${WL_HOME}/server/lib/weblogic.policy
   ${PROXY_SETTINGS} $ITCAM_OPTIONS ${SERVER_CLASS} >"${WLS_REDIRECT_LOG}" 2>&1
   ```

## Pre-configuration steps for supporting customized startup script for Tomcat

If a customized script is used for starting the Tomcat server, there are additional steps to be performed. The steps are necessary for the Configuration Tool to correctly locate the appropriate section of the script and insert the configurations of the Data Collector accordingly.

Two anchors are needed to be specified in the customized script before running the Configuration Tool. They are ***ITCAM_DC_SCRIPT*** and ***ITCAM_OPTIONS***.

1. Anchor **ITCAM_DC_SCRIPT**

   To support a customized startup script, the anchor *ITCAM_DC_SCRIPT* is needed to be specified in the script. It must be defined in a new line, immediately before the execution of the java command that starts the application server. When the Configuration Tool runs, the configuration of the Data Collector is inserted before this anchor.

   Syntax:

   `<comment_tab> ITCAM_DC_SCRIPT`

   where:

   *<comment_tab>* is the character used for indicating a line of comment in a script. In UNIX, this character is '###'. In Windows, this character is “REM”

   Examples:

   Add the following line in a customized script on UNIX:

   ```
   #### ITCAM_DC_SCRIPT
   ```

   Add the following line in a customized script on Windows:

   ```
   REM ITCAM_DC_SCRIPT
   ```

2. Anchor **ITCAM_OPTIONS**

   The second anchor is required to be added as the last JVM option in the customized script. User needs to find where the JVM options are and insert *$ITCAM_OPTIONS* (on UNIX) or *%ITCAM_OPTIONS%* (on Windows). Specify the anchor *ITCAM_OPTIONS* as the last JVM option, before the main class *%MAINCLASS%* in the Tomcat JVM startup options.

   **Note:** Any existing GC logging argument or Java security policy will be overwritten after the configuration process

   Examples:

   ```
   %_EXECJAVA% %JAVA_OPTS% %CATALINA_OPTS% %DEBUG_OPTS%
   -Djava.endorsed.dirs="%JAVA_ENDORSED_DIRS%"
   -classpath "%CLASSPATH%"
   -Dcatalina.base="%CATALINA_BASE%"
   -Dcatalina.home="%CATALINA_HOME%"
   -Djava.io.tmpdir="%CATALINA_TMPDIR%" %ITCAM_OPTIONS%
   %MAINCLASS% %CMD_LINE_ARGS% %ACTION%
   ```

## Pre-configuration steps for supporting customized startup script for JBoss

If a customized script is used for starting the JBoss server, there are additional steps to be performed. The steps are necessary for the Configuration Tool to correctly locate the appropriate section of the script and insert the configurations of the Data Collector accordingly.

Two anchors are needed to be specified in the customized script before running the Configuration Tool. They are ***ITCAM_DC_SCRIPT*** and ***ITCAM_OPTIONS***.

1. Anchor **ITCAM_DC_SCRIPT**

   To support a customized startup script, the anchor *ITCAM_DC_SCRIPT* is needed to be specified in the script. It must be defined in a new line, immediately before the execution of the java command that starts the application server. When the Configuration Tool runs, the configuration of the Data Collector is inserted before this anchor.

   Syntax:

   ```
   <comment_tab> ITCAM_DC_SCRIPT
   ```

   where:

   *<comment_tab>* is the character used for indicating a line of comment in a script. In UNIX, this character is '###'. In Windows, this character is 'REM'

   Examples:

   Add the following line in a customized script on UNIX:

   ```
   #### ITCAM_DC_SCRIPT
   ```

   Add the following line in a customized script on Windows:

   ```
   REM ITCAM_DC_SCRIPT
   ```

2. Anchor **ITCAM_OPTIONS**

   The second anchor is required to be added as the last JVM option in the customized script. User needs to find where the JVM options are and insert *$ITCAM_OPTIONS* (on UNIX) or *%ITCAM_OPTIONS%* (on Windows). Specify the *ITCAM_OPTIONS* anchor as the last JVM option, before the main class *%MAINCLASS%* in the JBoss JVM startup options.

   **Note:** Any existing GC logging argument or Java security policy will be overwritten after the configuration process

   Examples:

   ```
   "%JAVA%" %JAVA_OPTS% %ITCAM_OPTIONS%
   "-Djava.endorsed.dirs=%JBOSS_ENDORSED_DIRS%"
   -classpath "%JBOSS_CLASSPATH%" org.jboss.Main %*
   ```

## Pre-configuration steps for ITCAM for J2EE Data Collector

The Configuration Tool supports a list of optional parameters to provide more customization when Data Collector is configured. Optional parameters include specifying Data Collector log file location, additional JVM options, and CLASSPATH. The parameters can be specified by creating a file named as *optional_config_params.properties* under the directory *<DC_home>*/installer/config_dc/. The Configuration Tool reads the content of the file and configure the Data Collector according to the value specified. The following table summarizes the parameters supported by the Configuration Tool:

**Note:** (Optional step) Default value is used unless it is specified in *optional_config_params.properties*

*Table 29. Parameters supported by the Configuration Tool*

| Parameter Name | Description |
|---|---|
| CCLOG_COMMON_DIR | User-defined global logging common directory for the Data Collector, If the parameter is set, it overwrites the default logging common directory.<br><br>Default logging common directory on Windows: C:\Program Files\ibm\tivoli\common<br><br>Default logging common directory on UNIX: /var/ibm/tivoli/common<br>**Note:** If the value of this parameter contains any shell variable or environment variable, for example, $MY_LOG_DIR (UNIX) or %MY_LOG_DIR% (Windows). The parameter EXTRA_APPEND_LOGOPTS is required to be true. |
| NEED_ITCAM_SPECIFY_GCLOG | Possible values: true or false. Default value is true.<br><br>If you have a default GC log file configured in the JVM start up script (with the -Xloggc option) prior to the DC configuration, set this parameter to "true". The Configuration Tool sends the GC log information to a new log file. From this moment on, the GC data is written to the new file but the old default log is not overwritten. The new GC log file has the following path and name format:<br><br><DC_HOME>/<ServerType><ServerVersion>-gc-log.log.<InstanceName><br><br>You can choose not to add a new log file during the DC configuration and continue with the old log file. To do that set the NEED_ITCAM_SPECIFY_GCLOG parameter to "false" before running the Configuration Tool. |
| NEED_ITCAM_SECURITY_POLICY | Possible values: true or false. Default value is false.<br><br>This parameter specifies whether the Configuration Tool specifies any Java security policy.<br><br>If the value is set to true, the Configuration Tool adds the option "-Djava.security.policy=<DC_HOME>/runtime/<InstanceDir>/<NodeName>.<InstanceName>.datacollector.policy" to the JVM start up options.<br><br>If the value is set to false, only the Java security policy file is created but no JVM start up option is added |
| EXTRA_JVM_OPTION | Additional JVM start up options to be added. If specified, the value is appended to the JVM start up options. |
| EXTRA_CLASSPATH | Additional CLASSPATH to be added. Separate multiple entries by a colon (UNIX) or semicolon (Windows). |

*Table 29. Parameters supported by the Configuration Tool (continued)*

| Parameter Name | Description |
|---|---|
| EXTRA_APPEND_LOGOPTS | Possible values: true or false. Default is false.<br><br>This parameter specifies if the Configuration Tool appends the log related Java system properties to the JVM start up options. Otherwise the system properties are saved in the dc.properties file.<br><br>The JVM system properties affected by this parameter include:<br>• CCLOG_COMMON_DIR<br>• jlog.qualDir<br>• jlog.propertyFile<br>• jlog.propertyFileDir.CYN<br>• com.ibm.tivoli.itcam.toolkit.util.logging.qualDir<br>• ibm.common.log.dir<br>• jlog.common.dir<br><br>If the value is set to true, the log related Java system properties are appended to the JVM start up options.<br><br>If the value is set to false, the log related Java system properties are saved in the file <DC_HOME>/runtime/<InstanceDir>/dc.properties. |
| EXTRA_IGNORE_UNIX_PERMISSION | Possible values: true or false. Default is false.DC<br><br>This parameter specifies whether the Configuration Tool ignores non-root permission check.<br>**Note:** This option is supported only in UNIX platform |

## Pre-configuration steps for Tomcat users

When you installed the Tomcat server using the Windows installer, you need to perform the following steps to pre-configure Tomcat DC manually. If you installed the Tomcat server using Tomcat archive build, skip the following steps.

**Note:** In the following text, <*TOMCAT_HOME*> refers to the directory where Tomcat Application Server is installed. <DC_HOME> refers to the directory where TOMCAT DC is installed

For Tomcat 5.5, there is no batch script in <*TOMCAT_HOME*>\bin. Copy the batch scripts from archive build or other locations of Tomcat 5.5.

Before starting Tomcat windows service, navigate to ***My Computer > Advanced > Environment Variables*** and find the system variable `PATH`. Set it as `<DC_HOME>\toolkit\lib\w32-ix86`.

Configure Java CLASSPATH for Tomcat in Tomcat configuration tool by invoking *tomcat5w.exe* in <*TOMCAT_HOME*>\bin. Find **Java Options** in the tab page named **Java** and append the following command lines:

```
-Xbootclasspath/p:%DC_HOME%\toolkit\
lib\jiti.jar;%DC_HOME%\itcamdc\lib\ppe.probe-bootstrap.jar
-Dam.appserver=%INSTANCE_NAME%
-Dam.nodename=%NODE_NAME%
-Djava.rmi.server.RMIClassLoaderSpi=com.ibm.tivoli.itcam.tomcat.sdc.DCRMIClass
LoaderSpi
-Dappserver.platform=%TOMCAT_SERVER%
-Dam.home=%DC_HOME%\itcamdc
```

```
-Ditcam61.home=%DC_HOME%
-Xrunam_%JDK_VENDOR%_%JDK_VERSION%:%DC_HOME%\runtime\%TOMCAT_SERVER%.%NODE_NAME%.
%INSTANCE_NAME%\jiti.properties
-Djlog.propertyFileDir.CYN=%DC_HOME%\toolkit\etc
-Djlog.propertyFile=cynlogging.properties
-DArm40.ArmTransactionFactory=com.ibm.tivoli.itcam.toolkit.arm.j2.transaction.
Arm40TransactionFactory
-Djlog.qualDir=%NODE_NAME%.%INSTANCE_NAME%
-Dcom.ibm.tivoli.itcam.toolkit.util.logging.qualDir=%NODE_NAME%.%INSTANCE_NAME%
-DITCAMfJ2=true
-DArm4EventListener.0=com.ibm.tivoli.itcam.dc.event.ARM4TransactionDataHandler
-Dcom.ibm.tivoli.transperf.instr.probes.impl.was.Globals.traceLevel=0
-Dcom.ibm.tivoli.jiti.injector.IProbeInjectorManager=com.ibm.tivoli.itcam.toolkit.
ai.bcm.bootstrap.ProbeInjectorManager
-Dorg.omg.PortableInterceptor.ORBInitializerClass.com.ibm.tivoli.itcam.dc.
orbinterpretor.Initializer
-Dibm.common.log.dir=%LOG_PATH%
-Djlog.common.dir=%LOG_PATH%
-Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
-Djava.util.logging.config.file=%TOMCAT_HOME%\conf\logging.properties
-Djava.endorsed.dirs=%TOMCAT_HOME%\common\endorsed
```

**Note:**

1. There should be no any space character at the end of each line.
2. For Tomcat 5.0, the last three properties:

   ```
   -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
   -Djava.util.logging.config.file=%TOMCAT_HOME%\conf\logging.properties
   -Djava.endorsed.dirs=%TOMCAT_HOME%\common\endorsed
   ```

   should be removed from **Java Options**.

In the above code, %DC_HOME% refers to the DC Installation home; %INSTANCE_NAME% refers to the instance name of Tomcat dc that is used to distinguish from others; %NODE_NAME% refers to host name of DC side server; %TOMCAT_SERVER% refers to the Tomcat version, which should be written as "tomcat50" or "tomcat55"; %JDK_VENDOR% refers to the JDK vendor, which should be either "sun" or "ibm"; %JDK_VERSION% refers to JDK version, which should be written as 15 when the JDK is 1.5; %TOMCAT_HOME% refers to the Tomcat installation home, and %LOG_PATH% refers to the Tomcat DC log file, whose default value should be "C:/PROGRA~1/IBM/tivoli/common". Replace the variables by their real value in your environment.

## Pre-configuration steps for supporting Java Service Wrapper for Tomcat

If you use Java Service Wrapper for starting the Tomcat server, perform these steps:

1. Make sure that Java Service Wrapper is configured to the Tomcat server before you attach the Data Collector to the Tomcat server.
2. Make sure that the wrapper property path number, for example, `wrapper.java.additional.<n>`, is sequential.
3. (Optional) Remove from the Java Service Wrapper configuration file any manually added JVM arguments.

   Perform this step only if you manually added ITCAM JVM arguments into the Java Service Wrapper configuration file to make the DC work with Java Service Wrapper. If there are such arguments in your Java Service Wrapper configuration file, remove them before running the DC configuration.

## Pre-configuration steps for J2SE users

If there is a startup script for your application server, edit the customized script before running the Configuration Tool. Specify the following two anchors in the customized script to correctly locate the appropriate section of the script and insert the configuration of the Data Collector into the startup script:

- In the startup script start a new line to define the **ITCAM_DC_SCRIPT** anchor immediately before before the execution of the Java command:
  - operating systems such as AIX or Linux: ### ITCAM_DC_SCRIPT
  - Windows systems: REM ITCAM_DC_SCRIPT

  The configuration of the Data Collector is inserted after this anchor when the Configuration Tool runs.
- Add the **ITCAM_JVM_OPTS** anchor as the last JVM option in the customized script. Find where the JVM options is and insert *${ITCAM_JVM_OPTS}* (on operating systems such as AIX or Linux) or *%ITCAM_JVM_OPTS%* (on Windows). Specify the *ITCAM_JVM_OPTS* anchor as the last JVM option, before the main class *%MAINCLASS%* in the J2SE JVM startup options.

  **Note:** Any existing Garbage Collection (GC) logging argument or Java security policy will be overwritten after the configuration process.

  Examples:

```
%_EXECJAVA% %JAVA_OPTS% %CATALINA_OPTS% %DEBUG_OPTS%
-Djava.endorsed.dirs="%JAVA_ENDORSED_DIRS%" -classpath "%CLASSPATH%"
-Dcatalina.base="%CATALINA_BASE%" -Dcatalina.home="%CATALINA_HOME%"
-Djava.io.tmpdir="%CATALINA_TMPDIR%" %ITCAM_JVM_OPTS% %MAINCLASS%\
    %CMD_LINE_ARGS% %ACTION%
```

## Common steps for configuration

The following steps are identical for each of the supported platforms. When you have completed the steps, see "Application-server-specific steps for configuration" on page 98 for your platform to complete the configuration process.

**Note:** For WebLogic users, run installService.cmd or startWebLogic.cmd in domain directory to start WebLogic server before you start the Configuration Tool.

**Note:** For Oracle users, Oracle process manager must be stopped for oracle 9i/10g while configuring the oracle server instances, enter the following command line: `$OracleHome/opmn/bin/opmnctl -stopall` to stop the Oracle process manager.

**Note:** For NetWeaver users configuring *Distributed dialog instance*, complete the following steps. Before configuring the ITCAM for J2EE Data Collector, mount *Central instance home* on the central instance computer to a local folder (for example, /mnt/sap/J2E/JC00). Make sure your user ID has the writing rights.

### Step 0: Launch the Configuration Tool

The InstallShield Wizard prompts you to either launch the Configuration Tool or to defer the configuration until a later time. Click **Launch the Configuration Tool**. A separate Wizard opens that guides you through the configuration process.

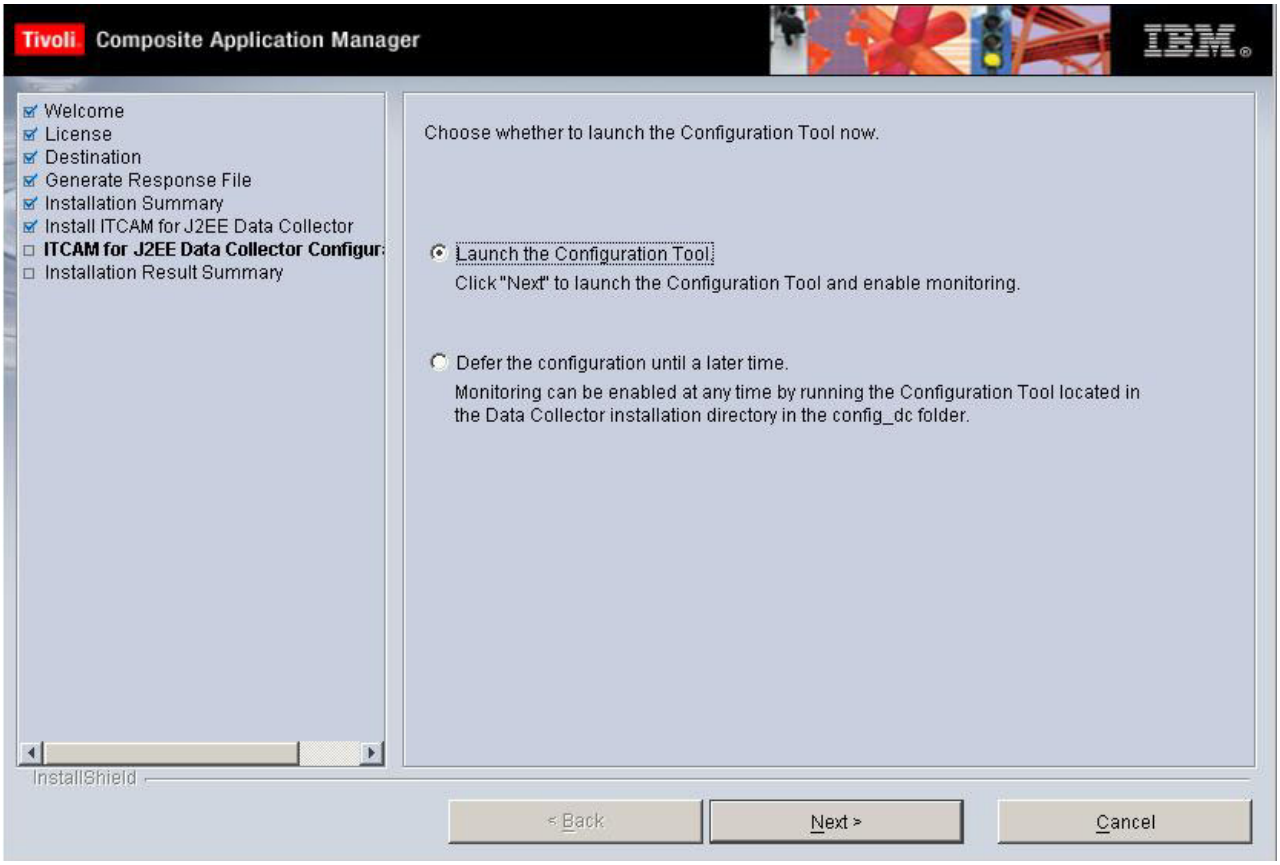



*Figure 17. Launch prompt from the InstallShield Wizard*

Click **Next** to proceed with the configuration.

If you select to **Defer the configuration until a later time** during the DC installation, you might start the Configuration Tool by locating and running the configuration startup script. Complete one of the following steps:

- For Windows, locate the file in which you installed the Data Collector, click **installer > config_dc > config_dc.bat**.
- For UNIX/Linux users, click: **installer > config_dc > config_dc.sh** and run the script with the following command: `$ ./config_dc.sh`

## Step 1: Proceed from the Welcome window

The ITCAM for J2EE Data Collector Configuration Tool is displayed in a window separate from the InstallShield Wizard.

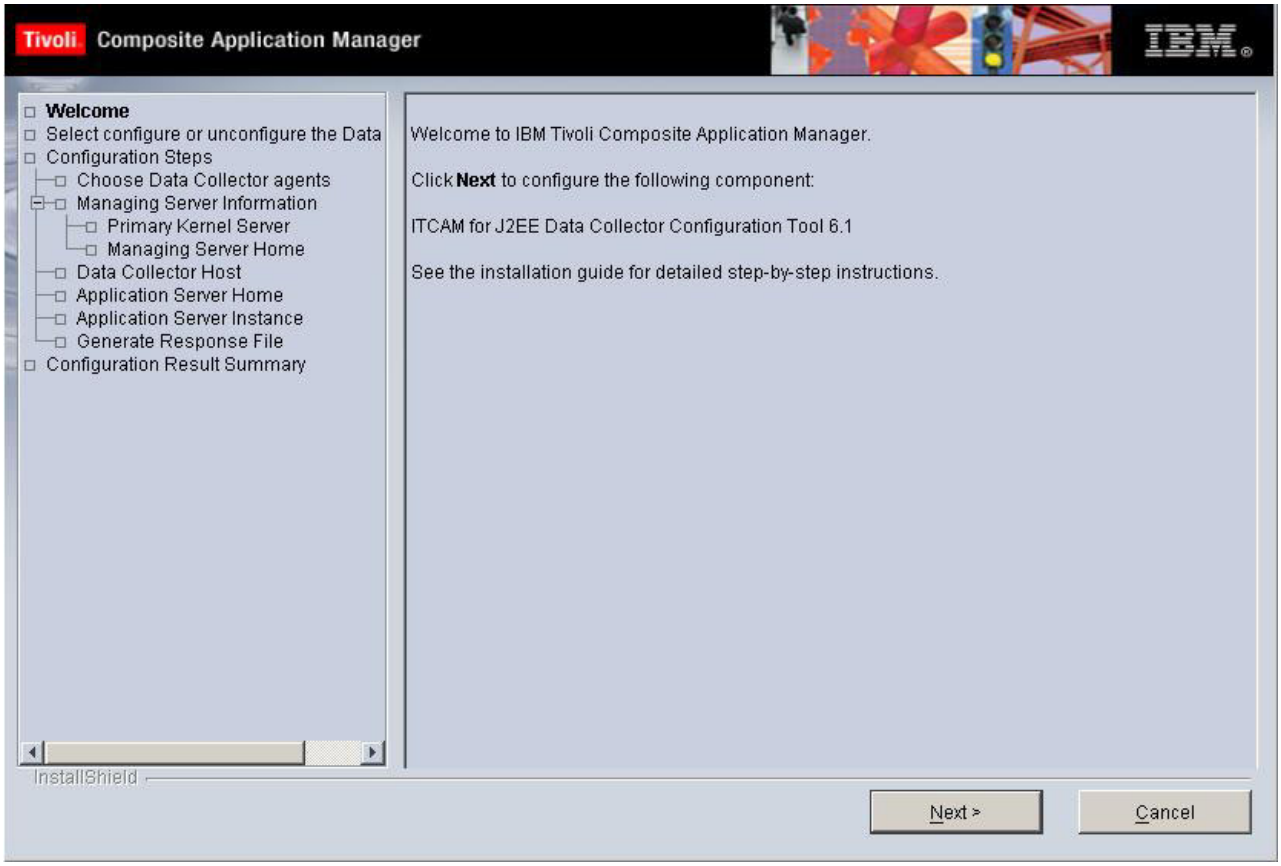



*Figure 18. Configuration Tool welcome window*

Click **Next** to configure the servers. You can click **Cancel** at any time to exit the Configuration Tool and return to the DC's InstallShield Wizard.

## Step 2: Configure servers for data collection

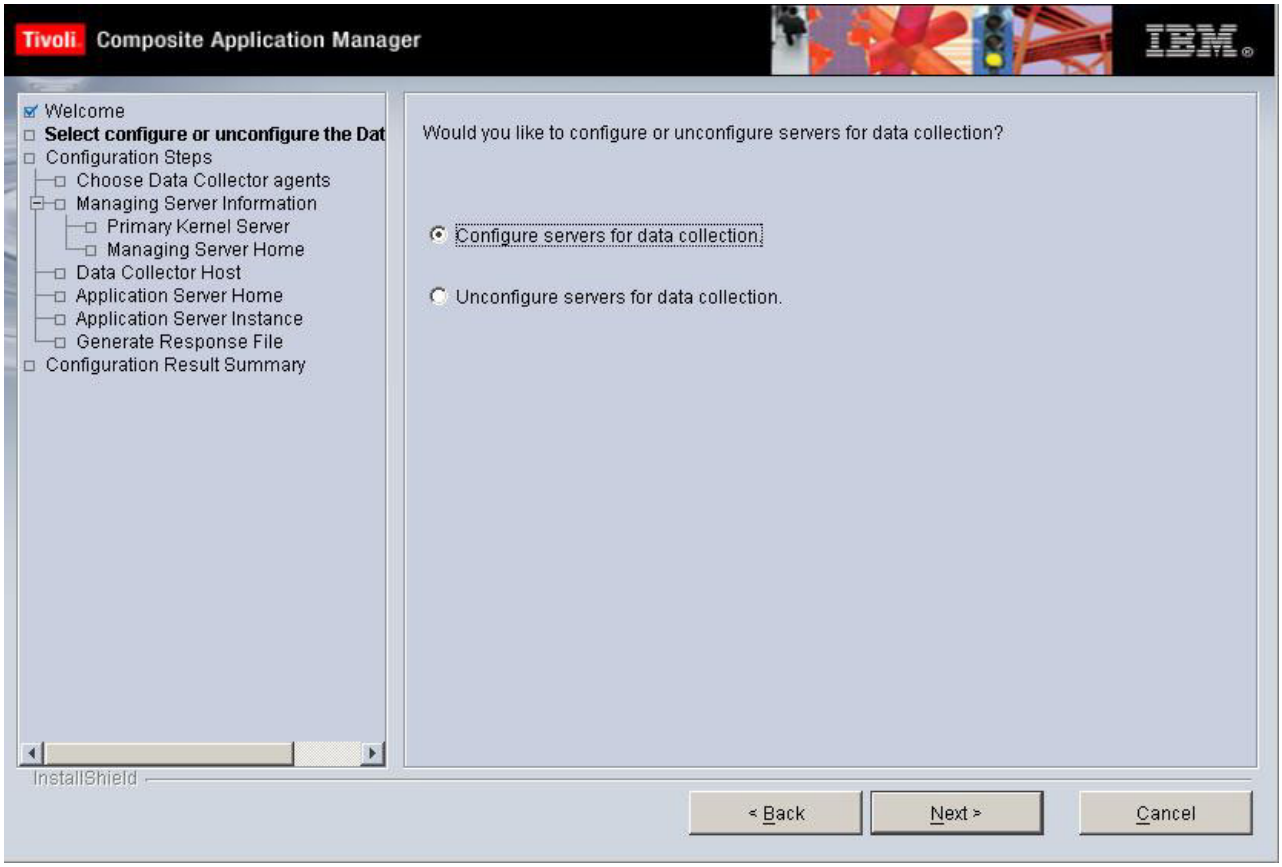



*Figure 19. Configure or unconfigure servers for data collection*

Click **Configure servers for data collection**. Click **Next** to continue.

If you need to return to the previous windows, click **Back**. Clicking **Unconfigure servers for data collection** unconfigures the Managing Server instance from the DC.

## Step 3: Choose the data collection agent to configure

Choose one or more data collection agents to configure the ITCAM for J2EE Data Collector to. You can select either **Data Collection for ITCAM for J2EE's Application Monitor user interface**, or **Data Collection for ITCAM for J2EE's Tivoli Enterprise Portal user interface**. The Application Monitor user interface requires a separate installation of ITCAM for J2EE's Managing Server. The Tivoli Enterprise Portal user interface requires a separate installation of the ITCAM for J2EE's Tivoli Enterprise Monitoring Agent.

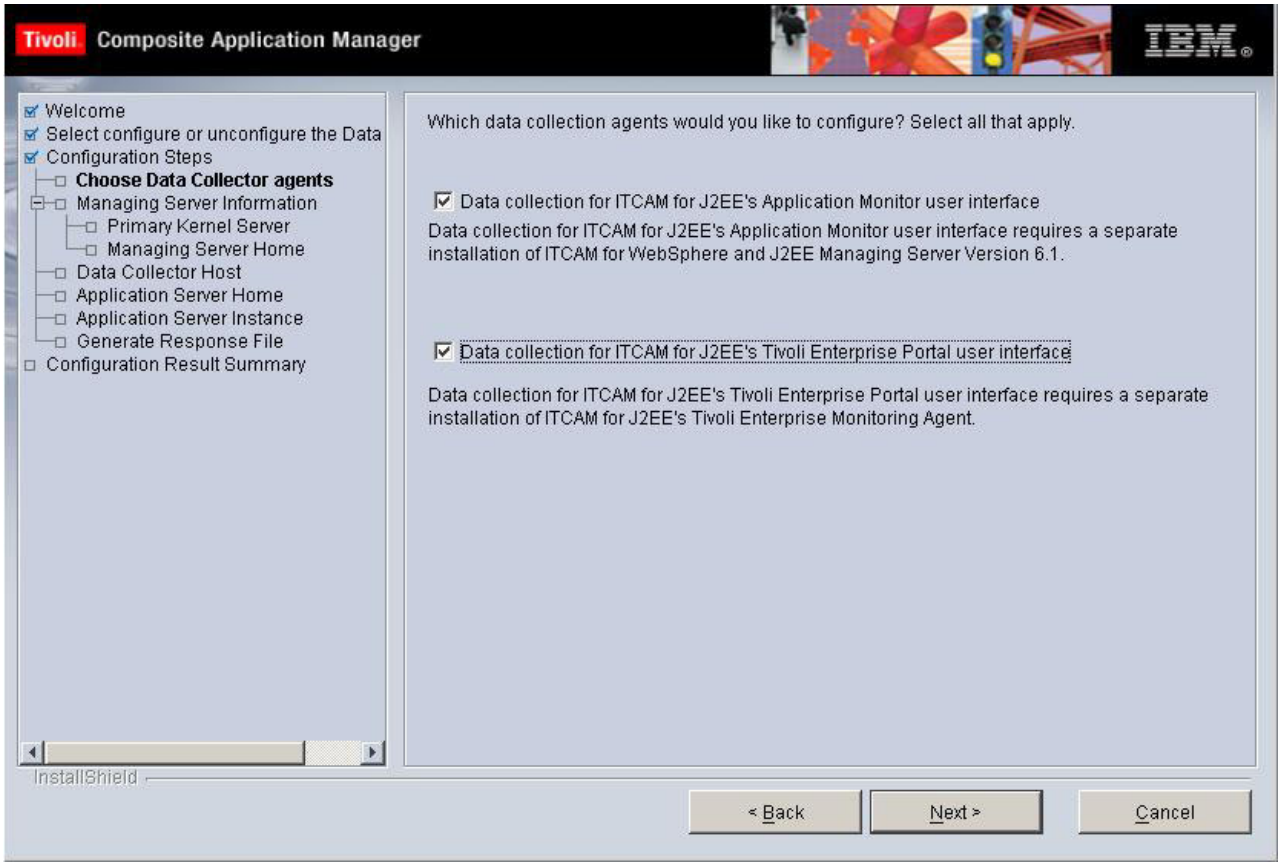



*Figure 20. Data collection agent selection*

By default, only the **Data Collection for ITCAM for J2EE's Application Monitor Interface** is selected. Select to configure the Data Collector to the portal if you have the monitoring agent already installed.

Click **Next**.

## Step 4: Enter the Managing Server host name and codebase Port

You are prompted for information concerning communication with the Managing Server.

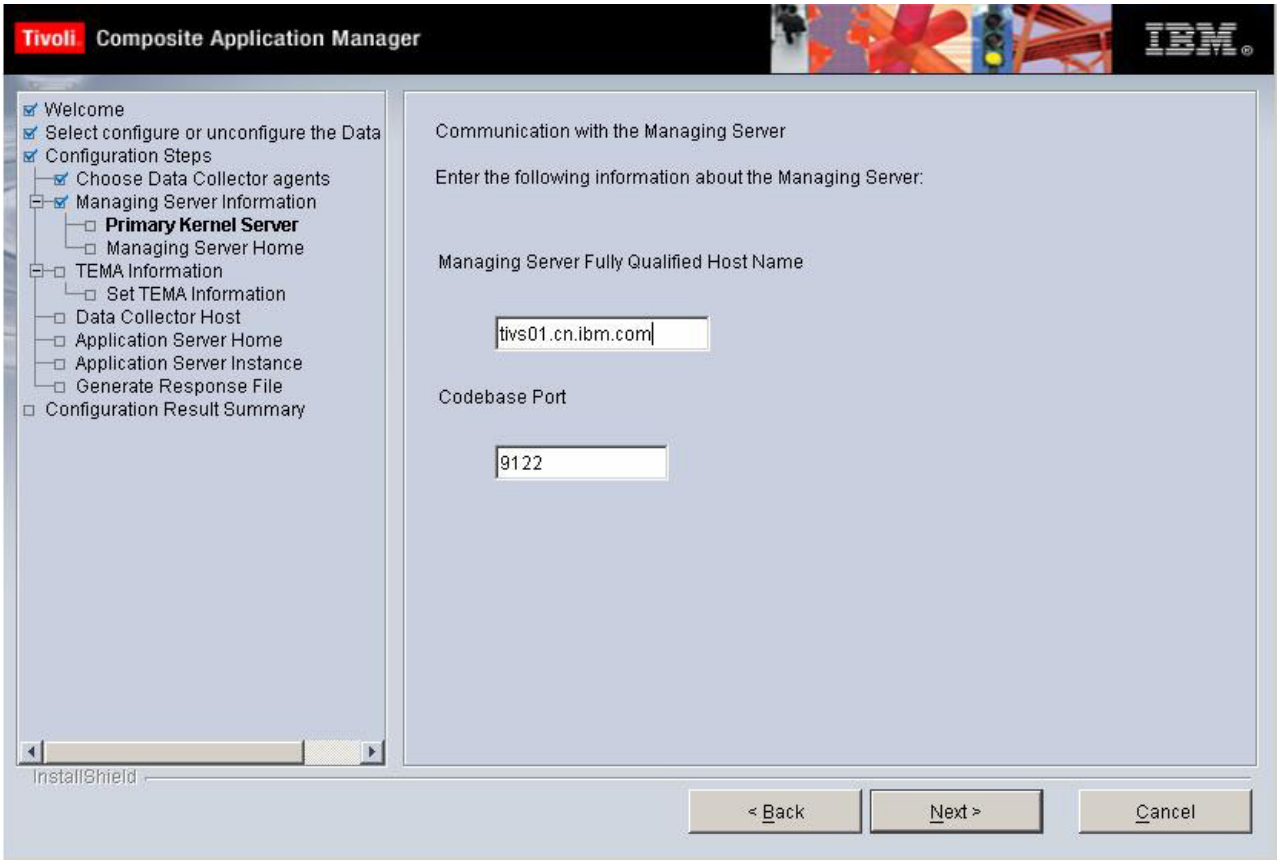



*Figure 21. Managing Server information*

Enter a fully qualified Managing Server host name and the codebase port number.

Click **Next** to continue.

## Step 5: Enter the Managing Server home directory

The installation program detects the MS_HOME on MS server and display the directory in the text field of **Managing Server Home Directory** automatically.

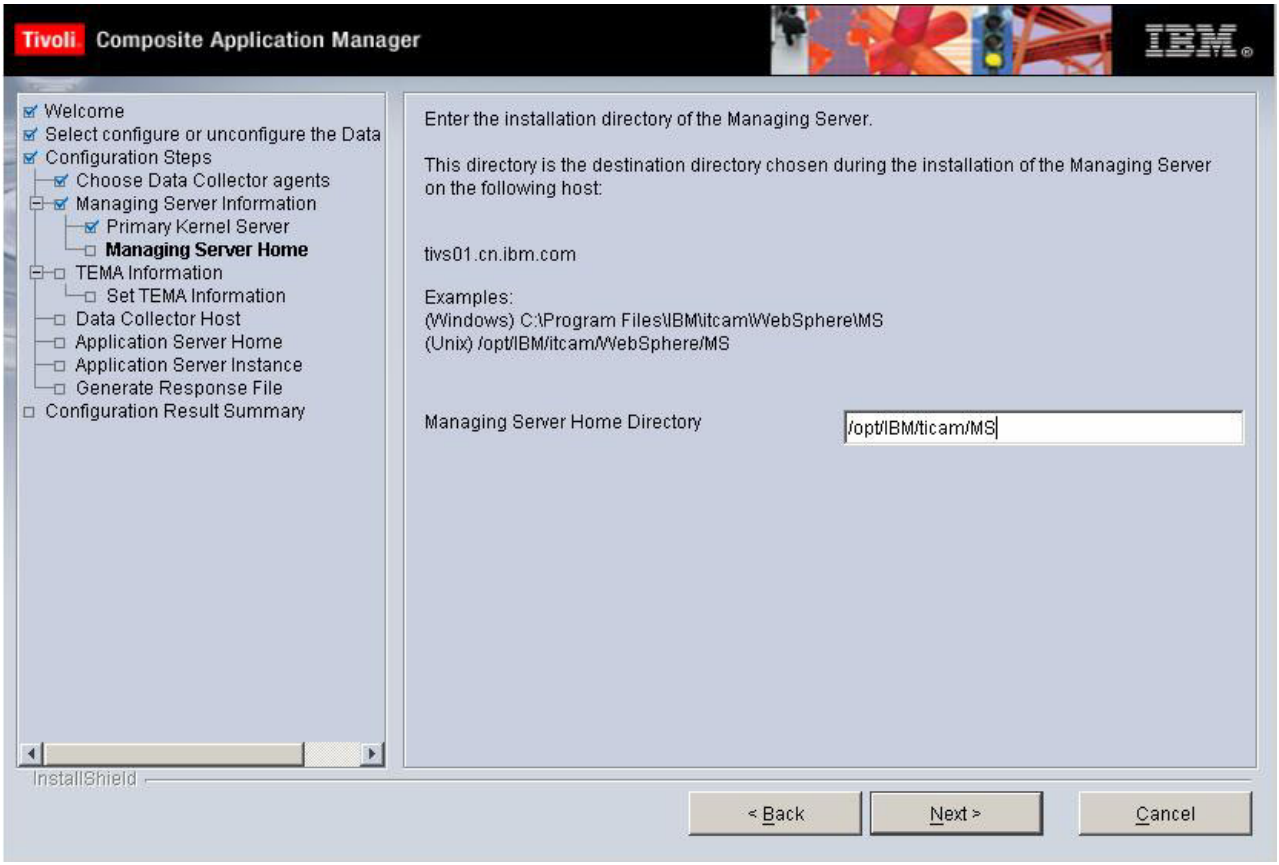



*Figure 22. Managing Server home directory*

Click **Next**.

## Step 6: Enter the monitoring agent information

If you selected **Data Collection for ITCAM for J2EE's Tivoli Enterprise Portal user interface** in "Step 3: Choose the data collection agent to configure" on page 93, the following window opens; otherwise, skip to Step 7.

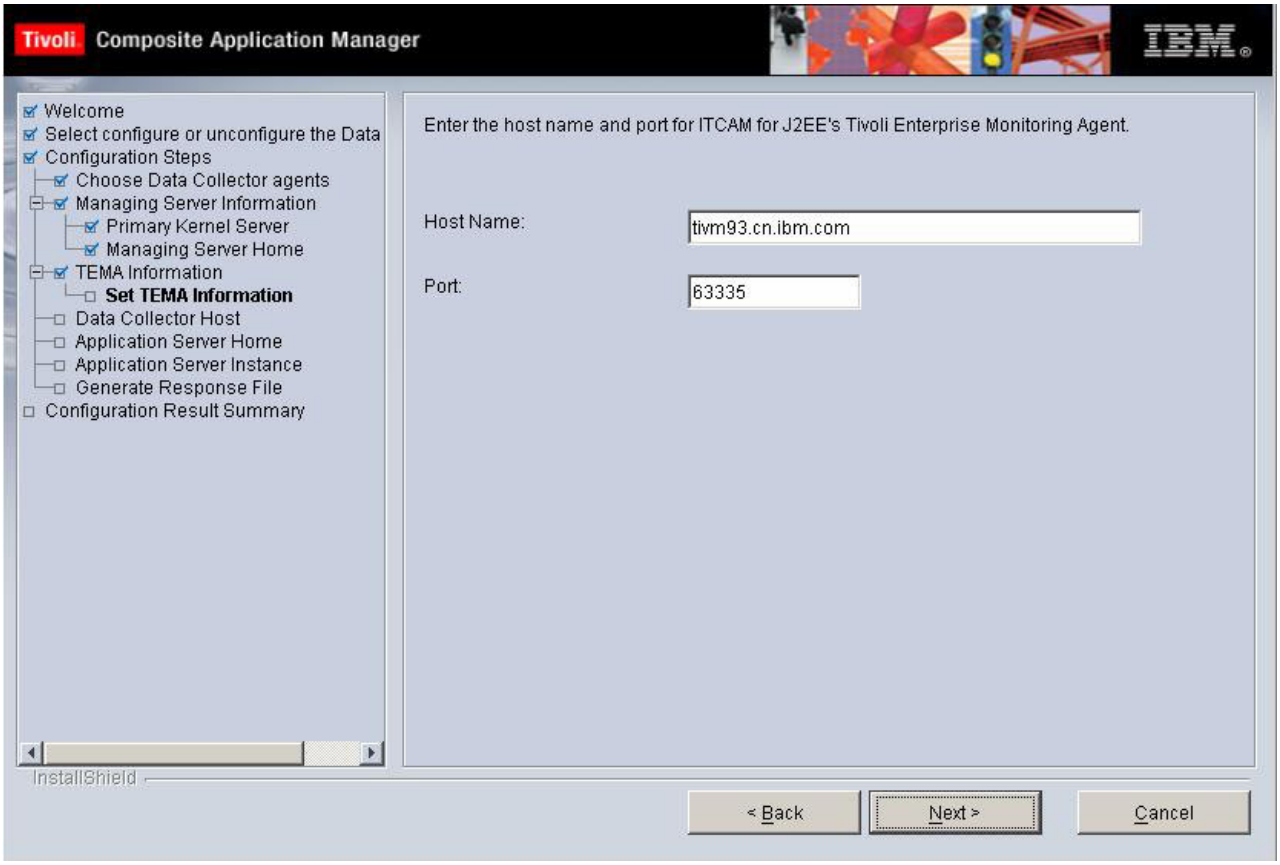



*Figure 23. Secondary kernel server information*

Enter the host name and port for ITCAM for J2EE's Tivoli Enterprise Monitoring Agent.

Click **Next**.

### Step 7: Enter the Data Collector host name

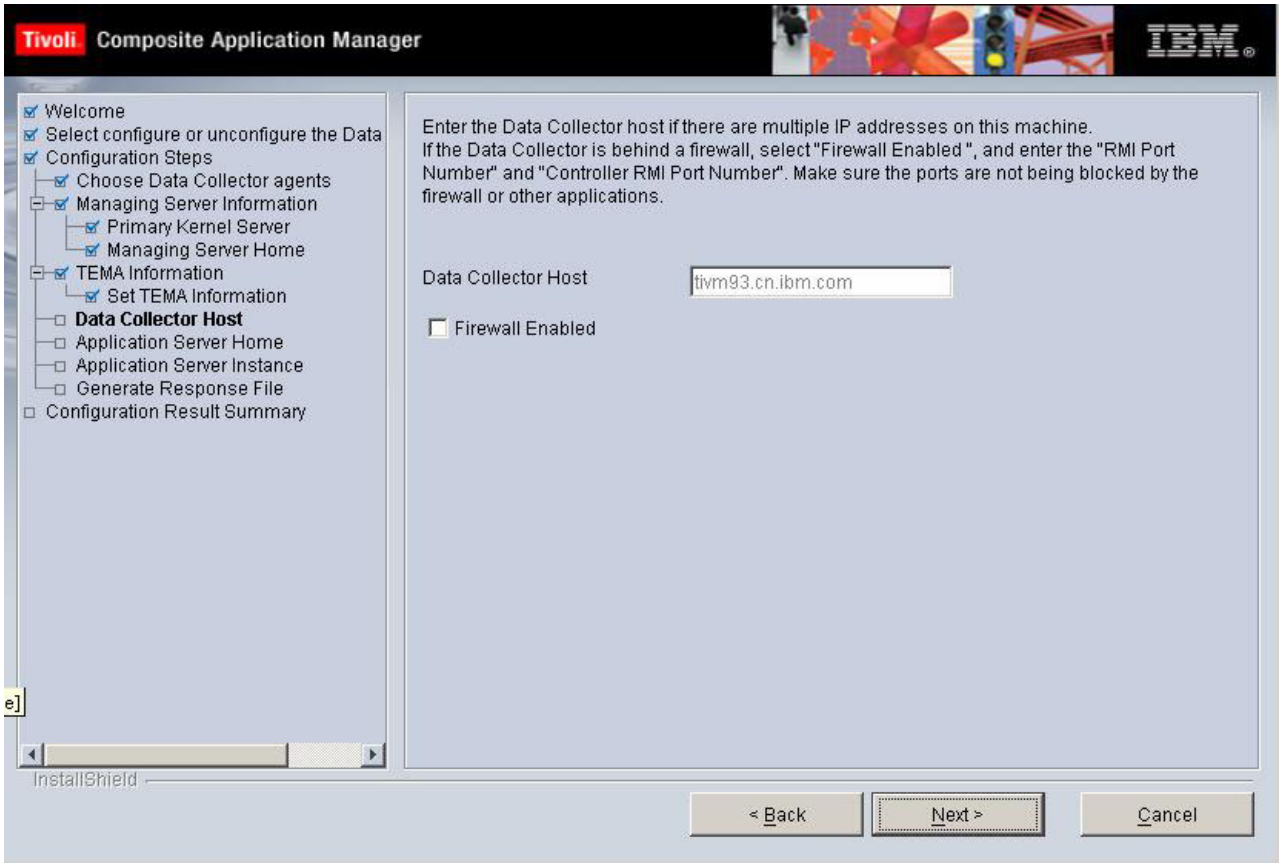



*Figure 24. Secondary kernel server information*

Enter the Data Collector host name if there are multiple IP addresses on the server. Select **Firewall Enabled** if the Data Collector is behind a firewall, and enter the Remote Method Invocation (RMI) port number and controller RMI port number. Make sure the ports are not being blocked by the firewall or other applications.

Click **Next** to continue.

## Application-server-specific steps for configuration

The following sections describe application-server-specific configuration procedures. See the section for the application server environment you are running to proceed.

- “Configuring the J2EE Data Collector for WebLogic/WebLogic Portal Server” on page 99
- “Configuring the J2EE Data Collector for NetWeaver” on page 109
- “Configuring the J2EE Data Collector for JBoss” on page 117
- “Configuring the J2EE Data Collector for Tomcat” on page 122
- “Configuring the J2EE Data Collector for Oracle” on page 127
- “Configuring the J2EE Data Collector for J2SE” on page 132
- “Configuring the J2EE Data Collector for JSAS” on page 137

# Configuring the J2EE Data Collector for WebLogic/WebLogic Portal Server

## Step 8: Select the WebLogic Server home, Server version, and Java home

After entering the Managing Server directory location, you are prompted to enter information regarding the specific WebLogic environment that you have installed on your computer.

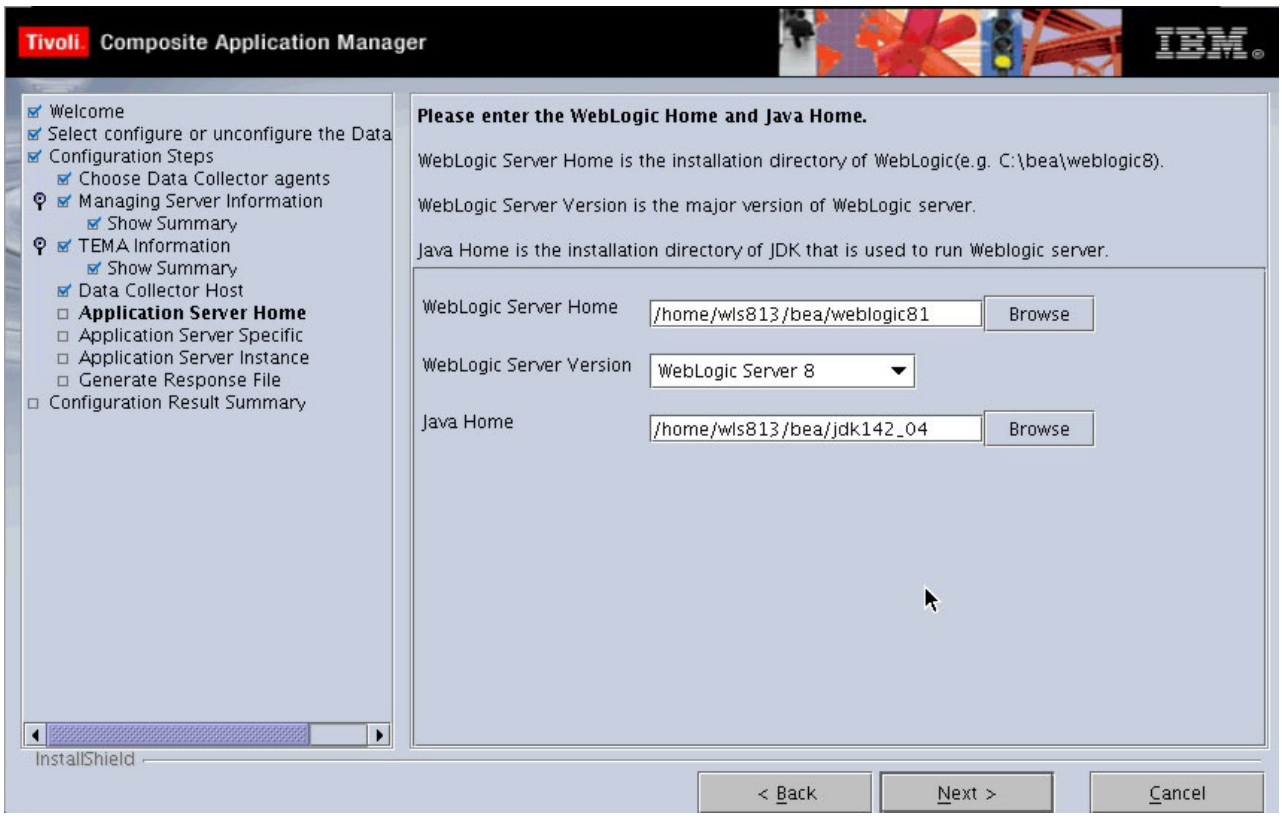



*Figure 25. WebLogic general information*

In the **WebLogic Server Home** field, click **Browse** and select the folder in which WebLogic has been installed. In the **WebLogic Server Version** field, select the version number of WebLogic that you are running. In the **Java Home** field click **Browse** and select the JDK that was installed with WebLogic.

If you are running the Configuration Tool on HP-UX or Solaris OS. A 64-bit check box will appear. Select **Use JDK as 64 bit** if you are using JDK as 64 bit.

Click **Next** to continue.

## Step 9: Enter the WebLogic Server specifics

In the next window, you are prompted for additional information specific to WebLogic.

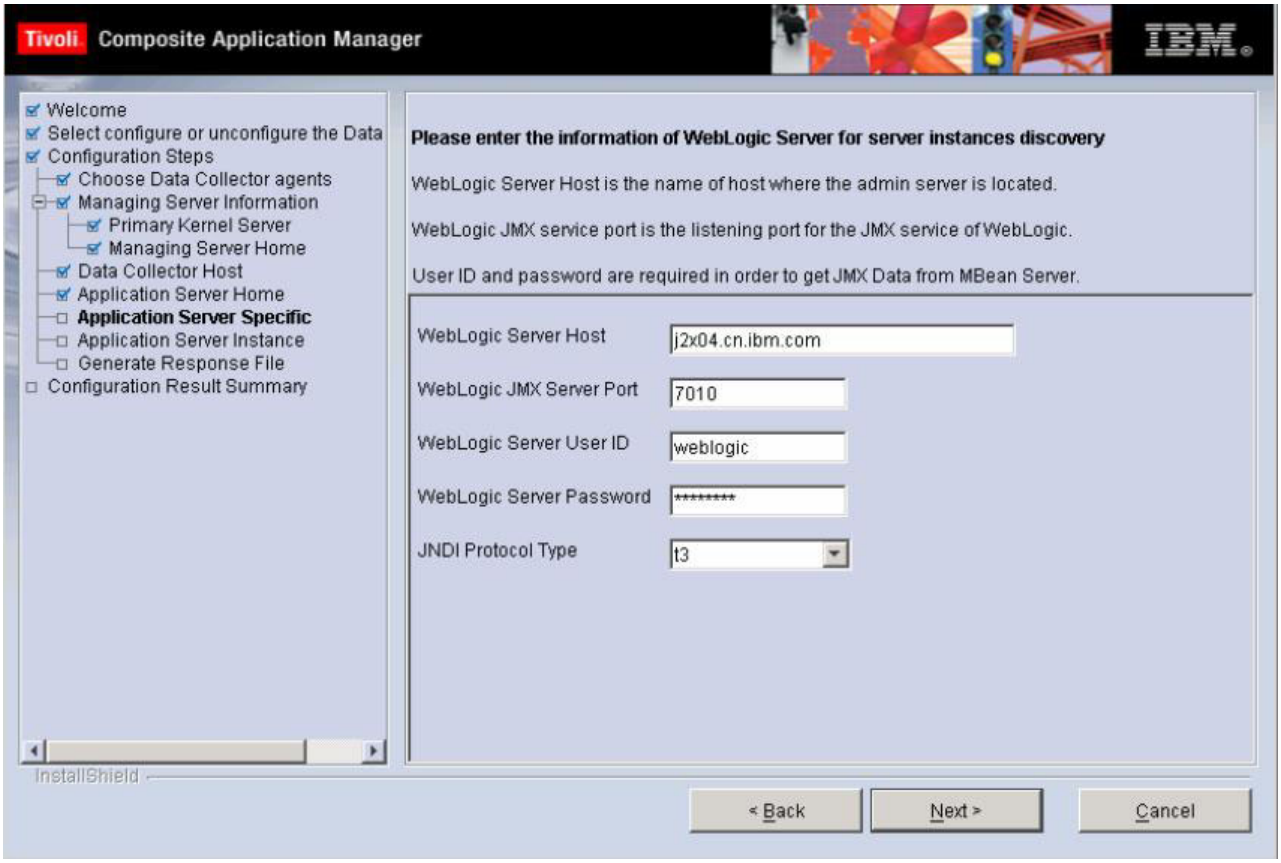



*Figure 26. WebLogic specific data*

In the data entry box labeled **WebLogic Server Host** enter the host name or IP address that WebLogic has been installed on. The field **WebLogic JMX Server Port** already contains a default value. Both the **WebLogic Server User ID** and **WebLogic Server Password** field values are entered by default as *weblogic*. Also, select a protocol type for **JNDI Protocol Type**.

**Note:** The default values of Java Management Extensions (JMX) Server Port, User ID and Password are pre-populated. You need to overwrite them with the values used in your environment.

If you select **t3s(one way SSL)** for **JNDI Protocol Type**, click **Browse** to locate the directory of the SSL trust CA key store file in the **SSL trust CA key store file** field, and follow instructions in "Step 10.a (SSL one way mode): Select the server instance to configure" on page 103 to continue the configuration.

**Note:** If you have chosen SSL one way mode, to ensure WebLogic 9 application server runs normally, you need to change the SSL configuration attribute Two Way Client Cert Behavior. First change it to Client Certs Request But Not Enforced and save the change; then change the its value again to Client Certs Not Requested and save the change. By doing this, WebLogic 9 application server will not verify client certificates under SSL one way mode.

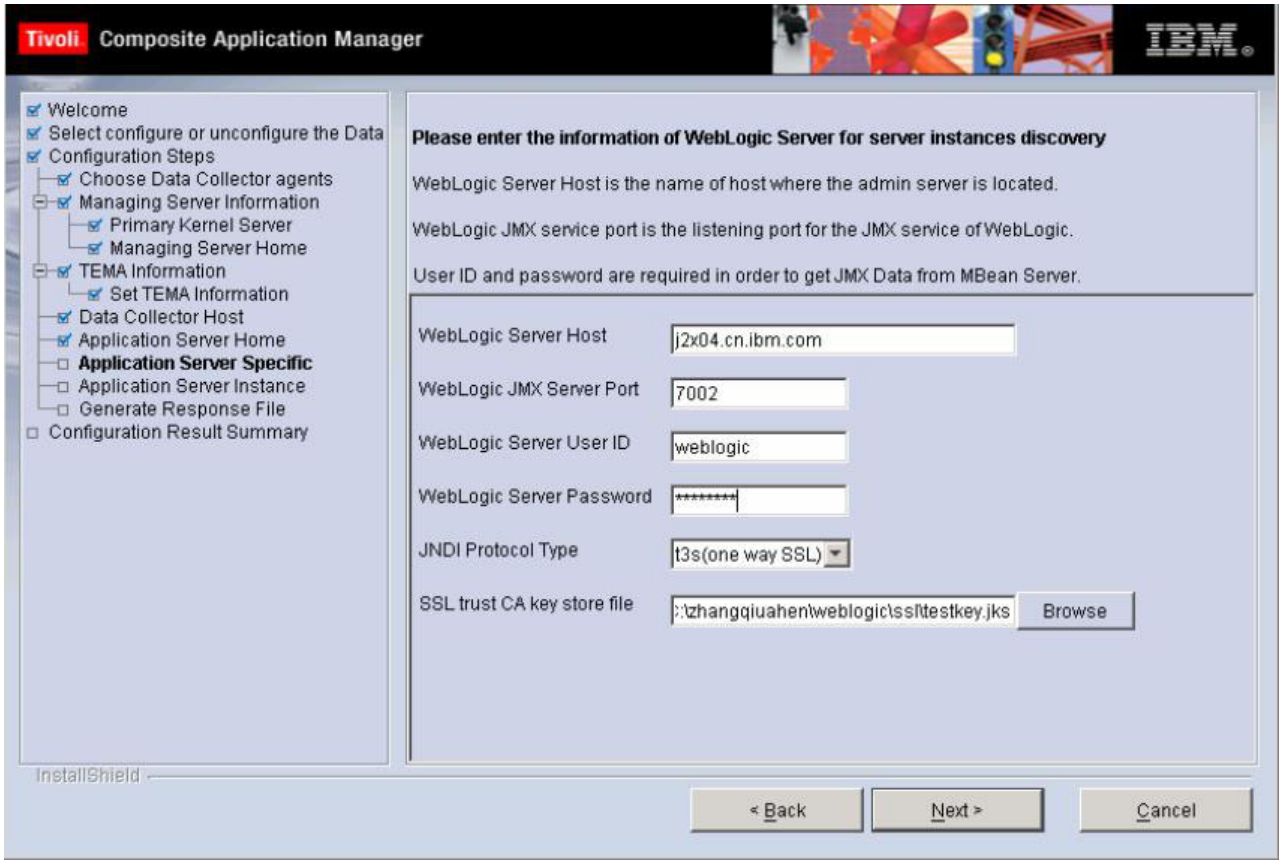



*Figure 27. JNDI Protocol Type as one way SSL*

Click **Next**.

### Step 10: Select the server instance to configure

The instance on the Managing Server is shown in this window. Select it to configure.

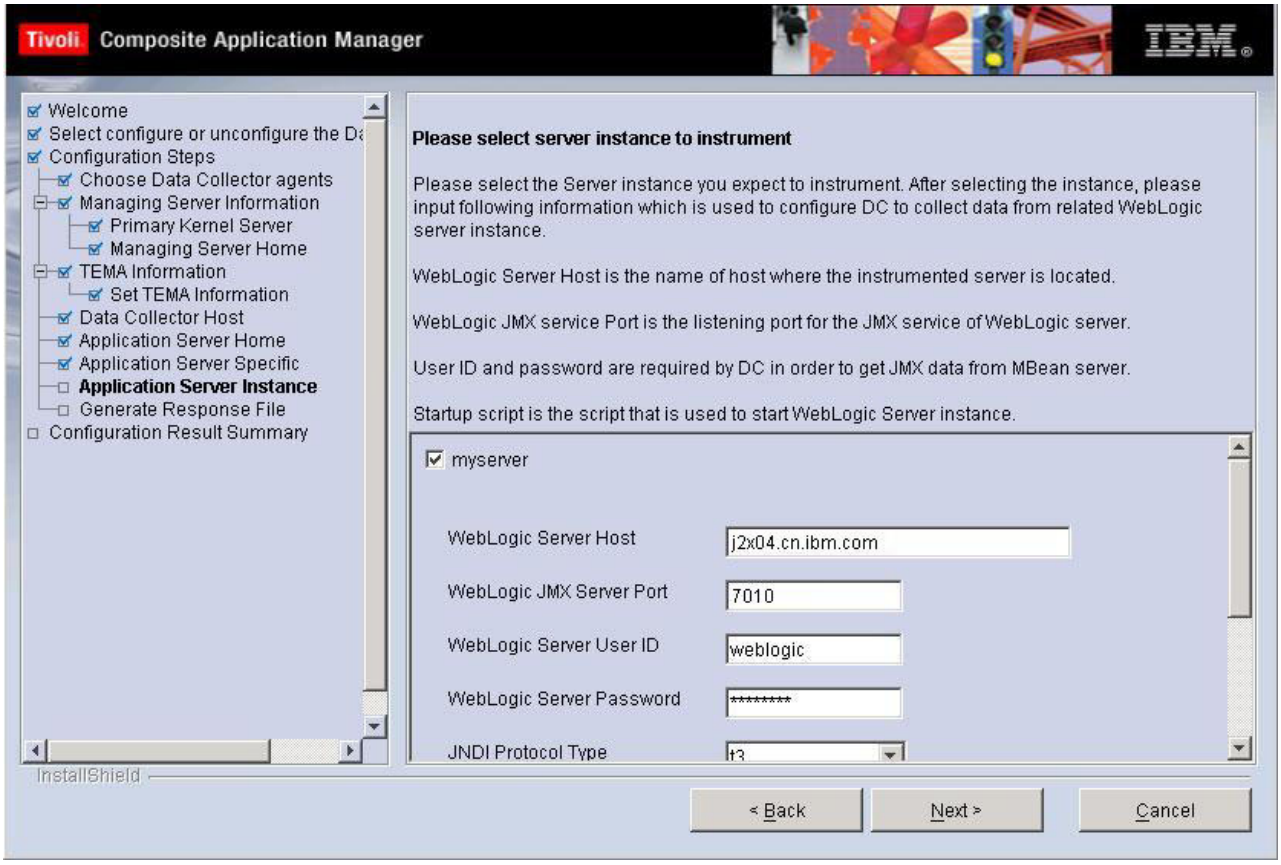



*Figure 28. Server instance selection*

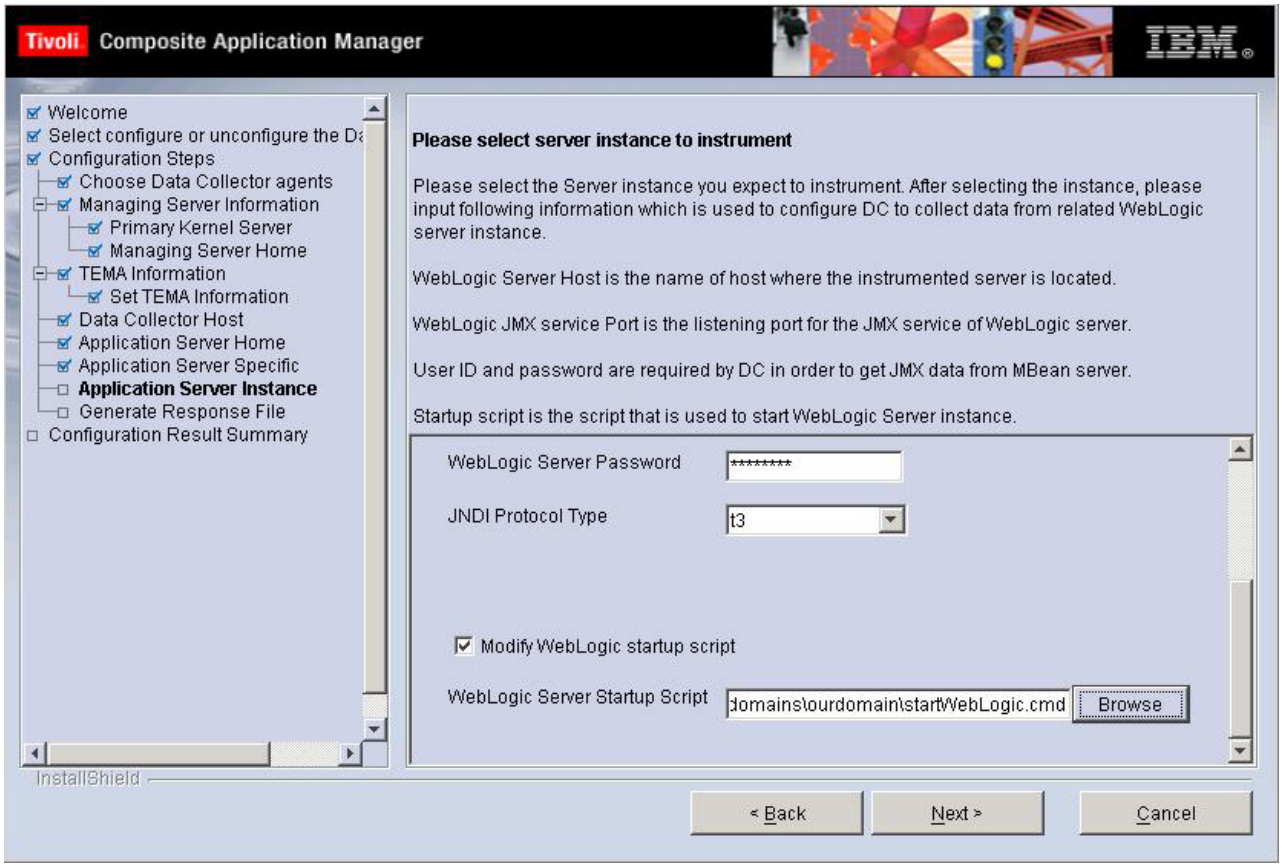



*Figure 29. Server instance selection (continued)*

The data of the instance is displayed as what is entered from the previous screen except the Password input, which is pre-populated with the default value *weblogic*. Please overwrite the Password data with the one used in your environment.

If you use startup script to start the WebLogic server, you must choose to modify WebLogic startup script by select **Modify WebLogic startup script**. The WebLogic server startup script is a command file that contains the prompts that launch the WebLogic application server instance. To find where your WebLogic startup script is located, check the"Table for WebLogic/WebLogic Portal server startup script locations" on page 108.

**Note:** If the server instance to be configured is a managed server started by Node Manager, do not check box **Modify WebLogic startup** script.

Click **Next** to configure the Data Collector.

## Step 10.a (SSL one way mode): Select the server instance to configure

The instances in the domain are shown in the window below, select one or more to configure.

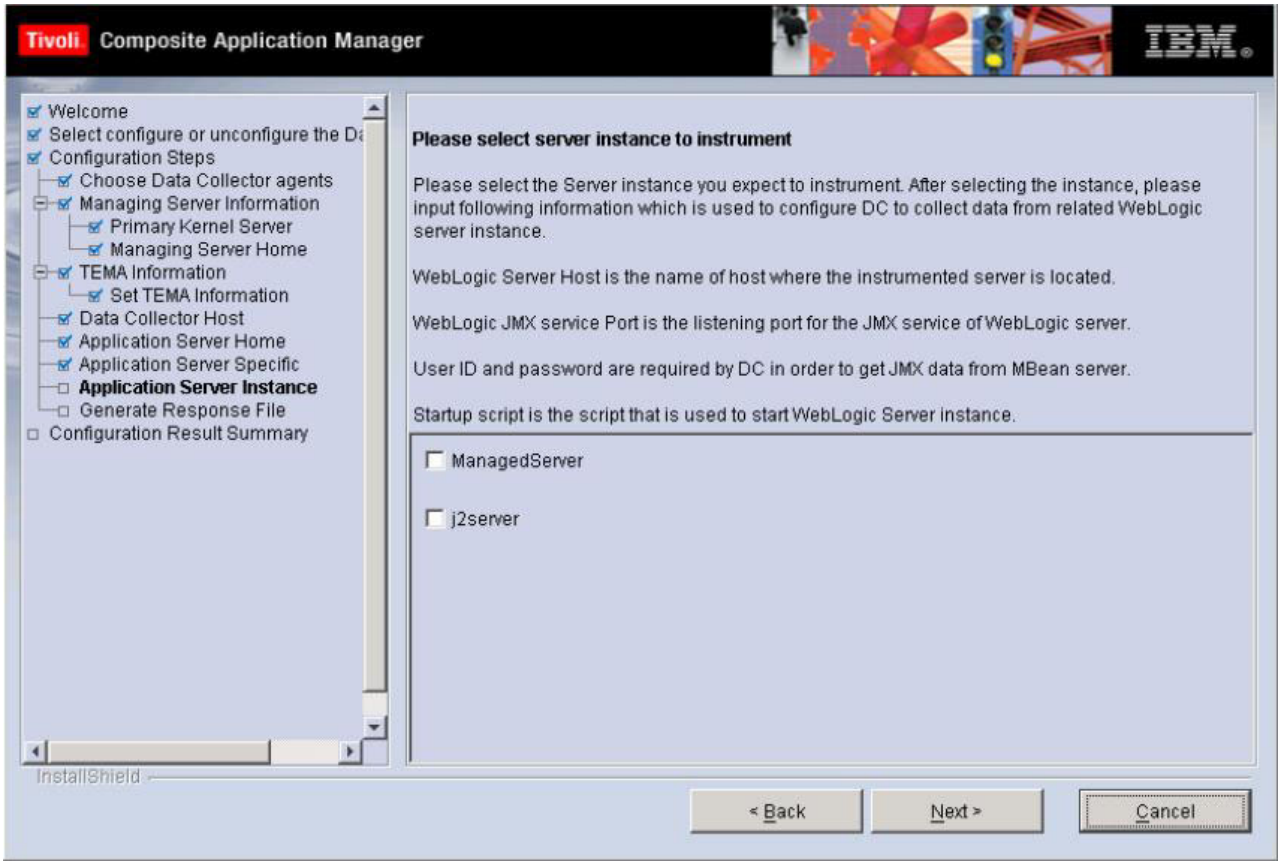



*Figure 30. Server instance selection (SSL one way mode)*

Select an instance to configure, and follow the instructions in "Step 10.b (SSL one way mode): Select the server instance to configure" on page 105.

### Step 10.b (SSL one way mode): Select the server instance to configure

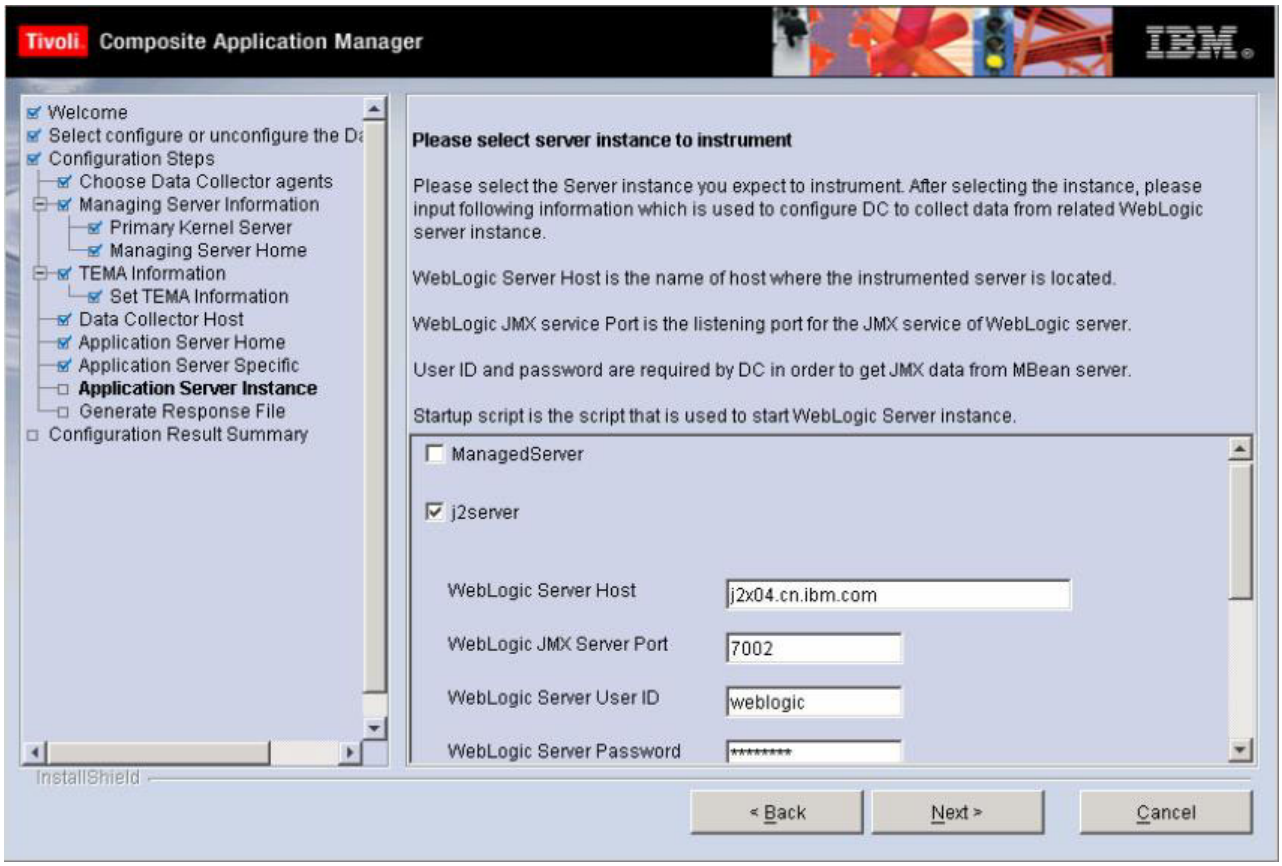



*Figure 31. Server instance selection (SSL one way mode, continued)*

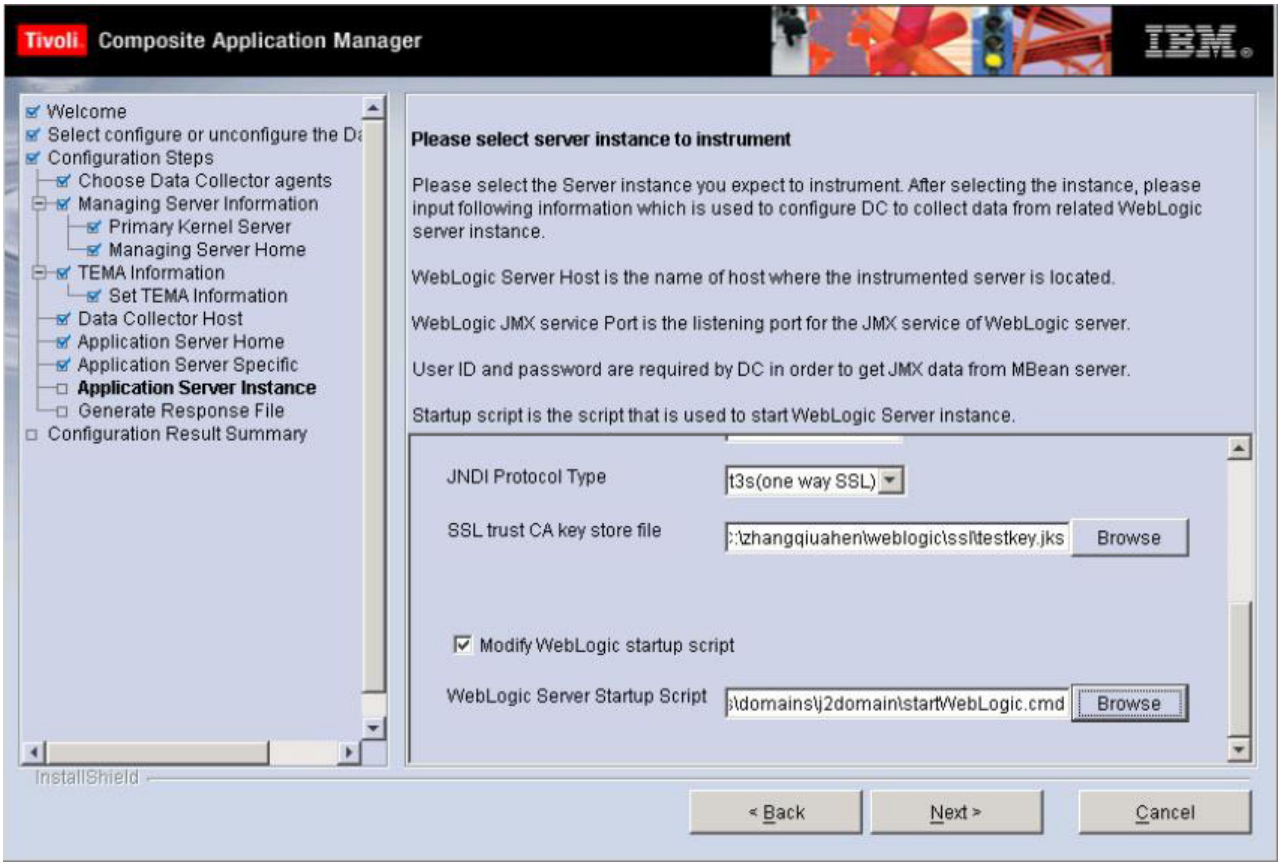



*Figure 32. Server instance selection (SSL one way mode, continued)*

The instance on the Managing Server is shown in this window. Select it to configure. The server instance data displayed in this window is the same as what is entered from the previous screen in Step 9. Correct the data if it is incorrect.

You can choose to modify WebLogic startup script by select **Modify WebLogic startup script**. The WebLogic server startup script is a command file that contains the prompts that launch the WebLogic application server instance. If the WebLogic instance is started by the Node Manager, clear check box near **Modify WebLogic startup script**. To find where your WebLogic startup script is located, check the"Table for WebLogic/WebLogic Portal server startup script locations" on page 108.

Click **Next** to configure the Data Collector.

## Step 11: Generate a response file

You can choose to generate a response file to save all your settings. If you use a response file, you can have the same installation settings when you want to configure the Data Collector later again on this computer or on another computer using a silent installation.

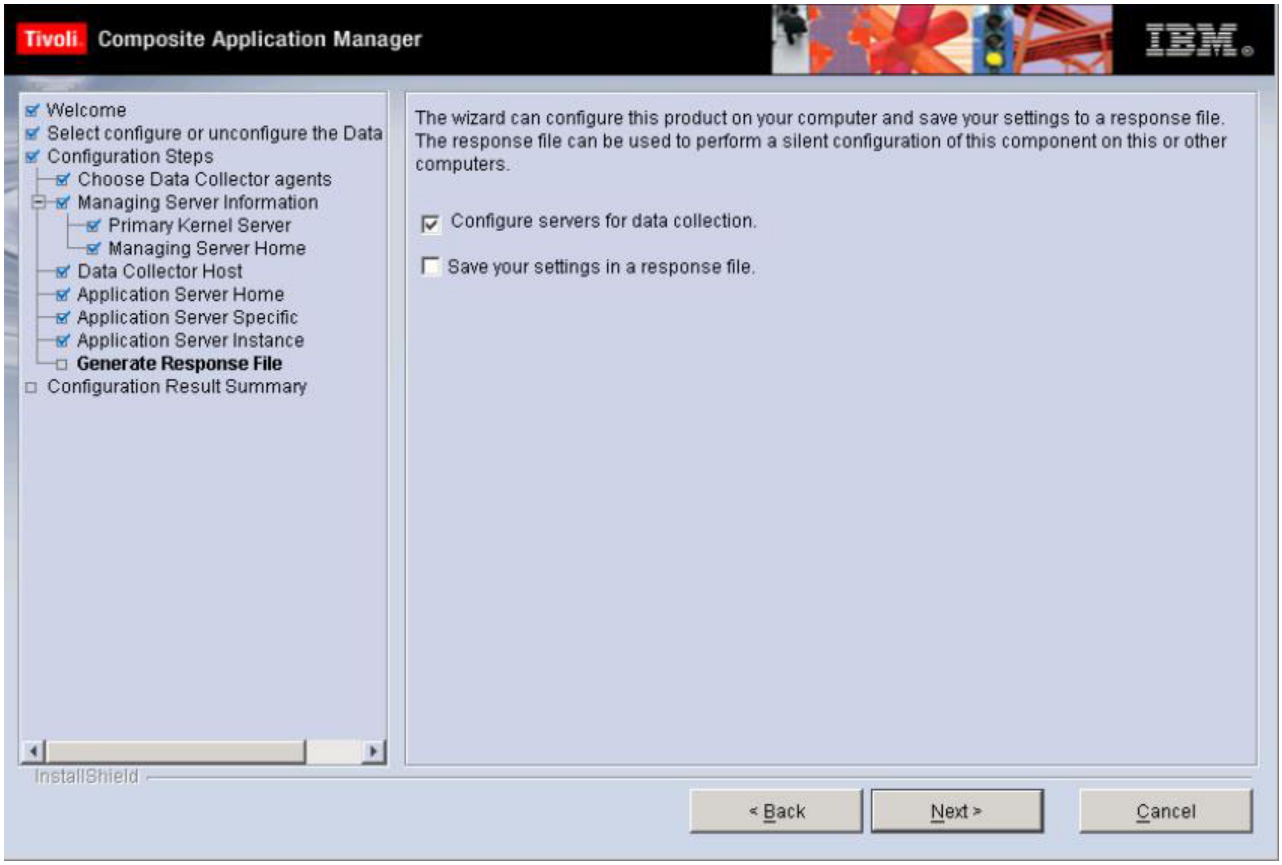



*Figure 33. Choose to save your settings in a response file*

**Configure servers for data collection** is selected by default. If you want to create a response file with all the settings in this configuration, select **Save your settings in a response file**, and choose a location where the response will be generated.

Click **Next** to proceed.

## Step 12: Finalize the configuration

After the Data Collector is configured, the following window opens:

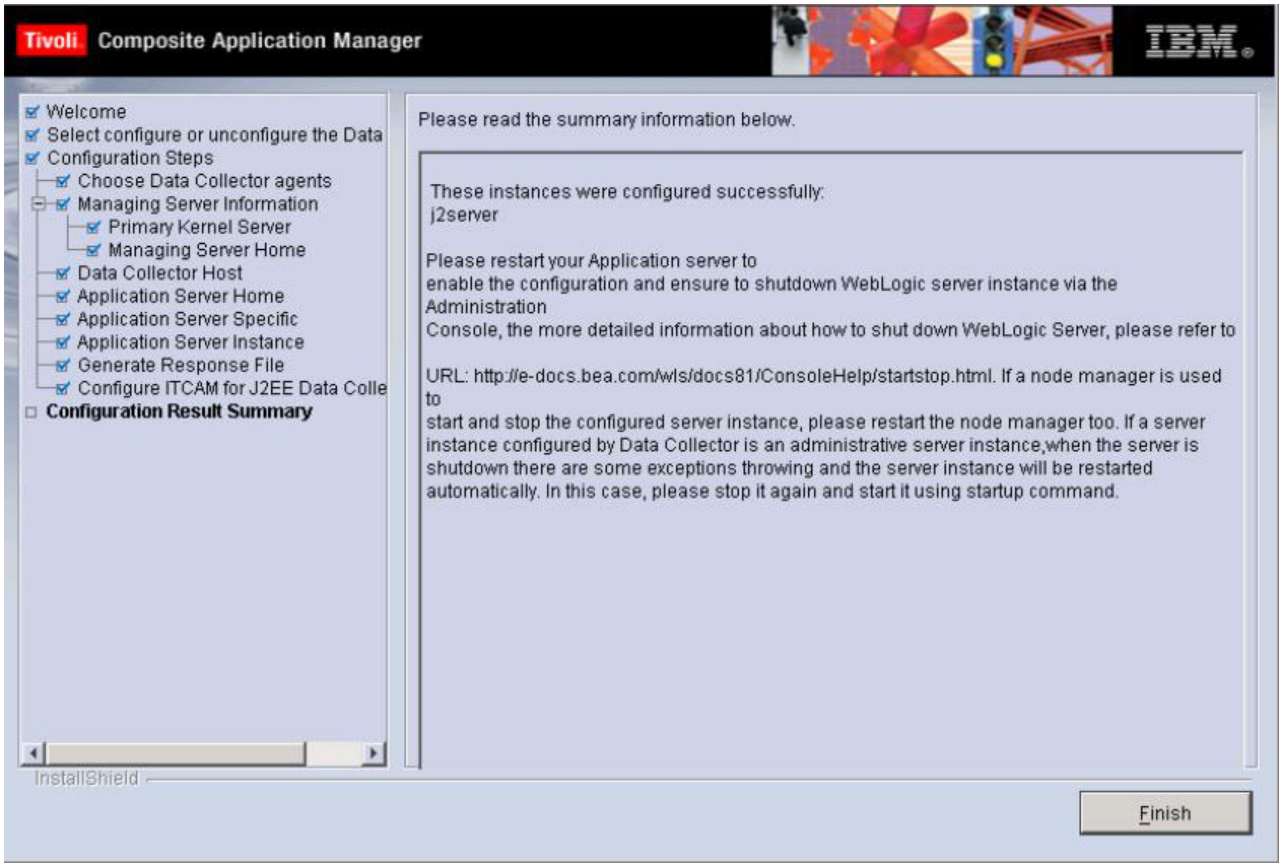



*Figure 34. Configuration results summary*

Read the summary information. The configuration status of the server instance that you selected is shown. Click **Finish** to finalize the configuration and close the Configuration Tool. If you are currently installing the DC, you will go back to the InstallShield Wizard. There you will be prompted to finalize the installation.

## Table for WebLogic/WebLogic Portal server startup script locations

*Table 30. WebLogic/WebLogic Portal Server startup scripts locations*

| Server Type \ Startup Method | | start from command line | start as a Windows service |
|---|---|---|---|
| Standalone / Admin WebLogic Server | WebLogic 8 | <*wl_domain*>/startWebLogic.cmd(sh) | <*wl_domain*> /installService.cmd |
| | WebLogic Portal Server 8 | | |
| | WebLogic 9 | <*wl_domain*>/bin/startWebLogic.cmd(sh) | Not Applicable |
| Managed WebLogic Server | WebLogic 8 | <*wl_domain*>/ startManagedWebLogic.cmd(sh) | <*wl_domain*>/ installService.cmd |
| | WebLogic Portal Server 8 | | |
| | WebLogic 9 | <*wl_domain*>/bin/startWebLogic.cmd(sh) | Not Applicable |

For Managed WebLogic/WebLogic Portal Server started from the Node Manager, those files were changed after configuration. To update the *PATH/LD_LIBRARY_PATH/LIBPATH/SHLIB_PATH* environment variable, use one of the following commands:

```
<WL_HOME>/server/bin/startNodeManager.cmd(sh)
<WL_HOME>/server/bin/installNodeMgrSvc.cmd(sh)
<WL_HOME>/common/bin/commEnv.cmd(sh)
```

The server specific startup arguments and the classpath are saved in the config.xml file on the domain admin server.

For users that start Node Manager from command line, restart the Node Manager before start the managed server.

For users that start Node Manager as windows service, reinstall the Node Manager Windows service by running uninstallNodeMgrSvc.cmd and installNodeMgrSvc.cmd.

For WebLogic 9 users that start Node Manager from WebLogic Script Tool, first stop Node Manager and exit the WebLogic Script Tool, then re-run setWLSEnv.cmd(sh) for the changed environment to work. Then, start Node Manager from the WebLogic Script Tool again.

**Note:** *<wl_domain>* is the directory where you have the domain admin server of WebLogic/WebLogic Portal Server installed.

**Note:** For users who start the WebLogic/WebLogic Portal Server as a Windows service, remember to re-install Windows service.

## Configuring the J2EE Data Collector for NetWeaver

### Step 8 : Enter the NetWeaver server information

After entering the Managing Server directory location, you are prompted to enter information regarding the specific NetWeaver environment that you have installed on your computer.

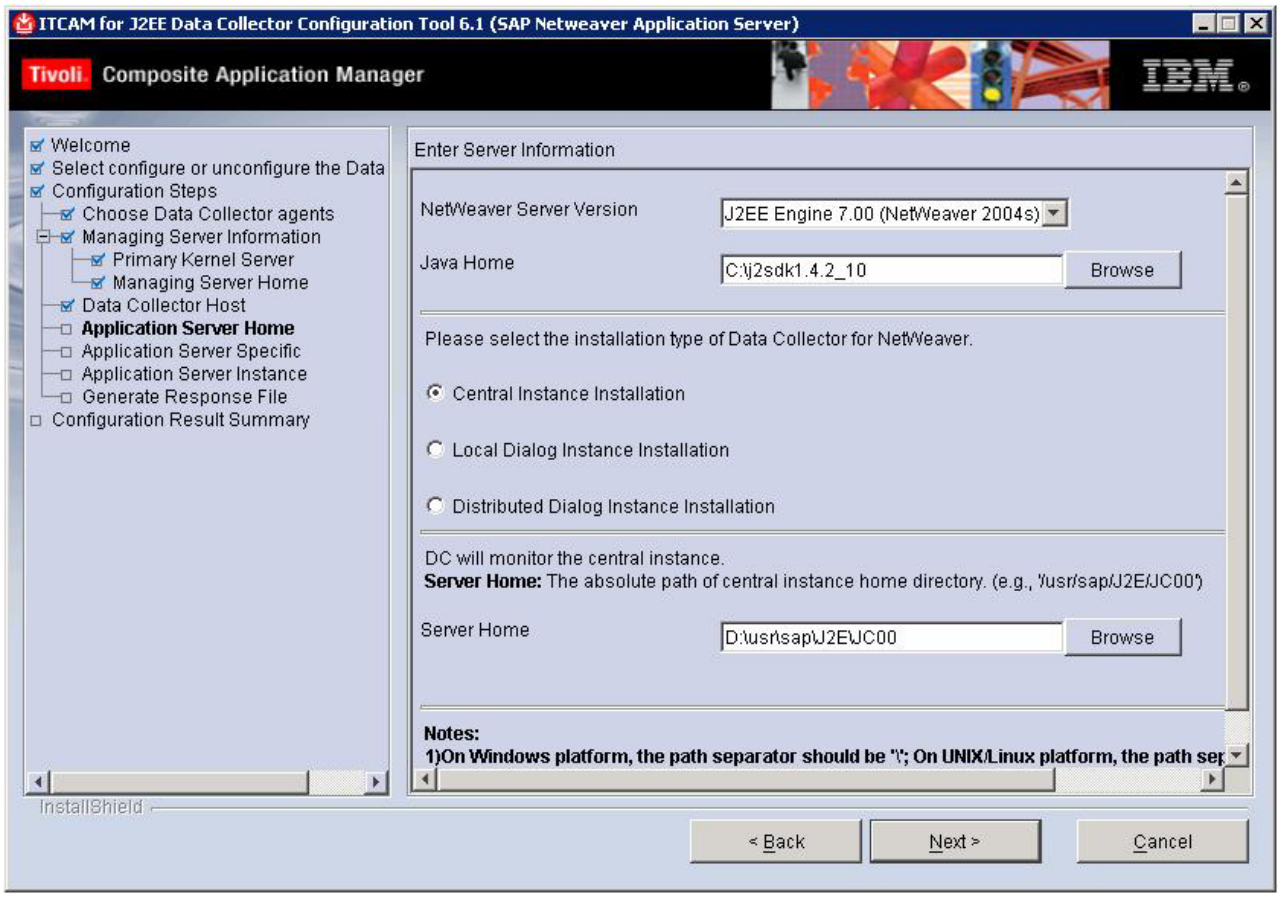



*Figure 35. NetWeaver server information*

Select the server version number of NetWeaver you are running in the **NetWeaver Server Version** field. Click **Browse** in the **Java Home** field and locate the JDK supporting the application server.

You should decide which installation type you want to use. For the explanation of the three installation types, refer to "Three installation types of ITCAM for J2EE Data Collector for NetWeaver" on page 4. Depending on your requirements, complete the steps in one of the following sections:

1. "Central instance installation"
2. "Local dialog instance installation" on page 111
3. "Distributed dialog instance installation" on page 112

**Central instance installation:** Select **Central instance installation** if you are installing the Data Collector to monitor the server on the central instance.

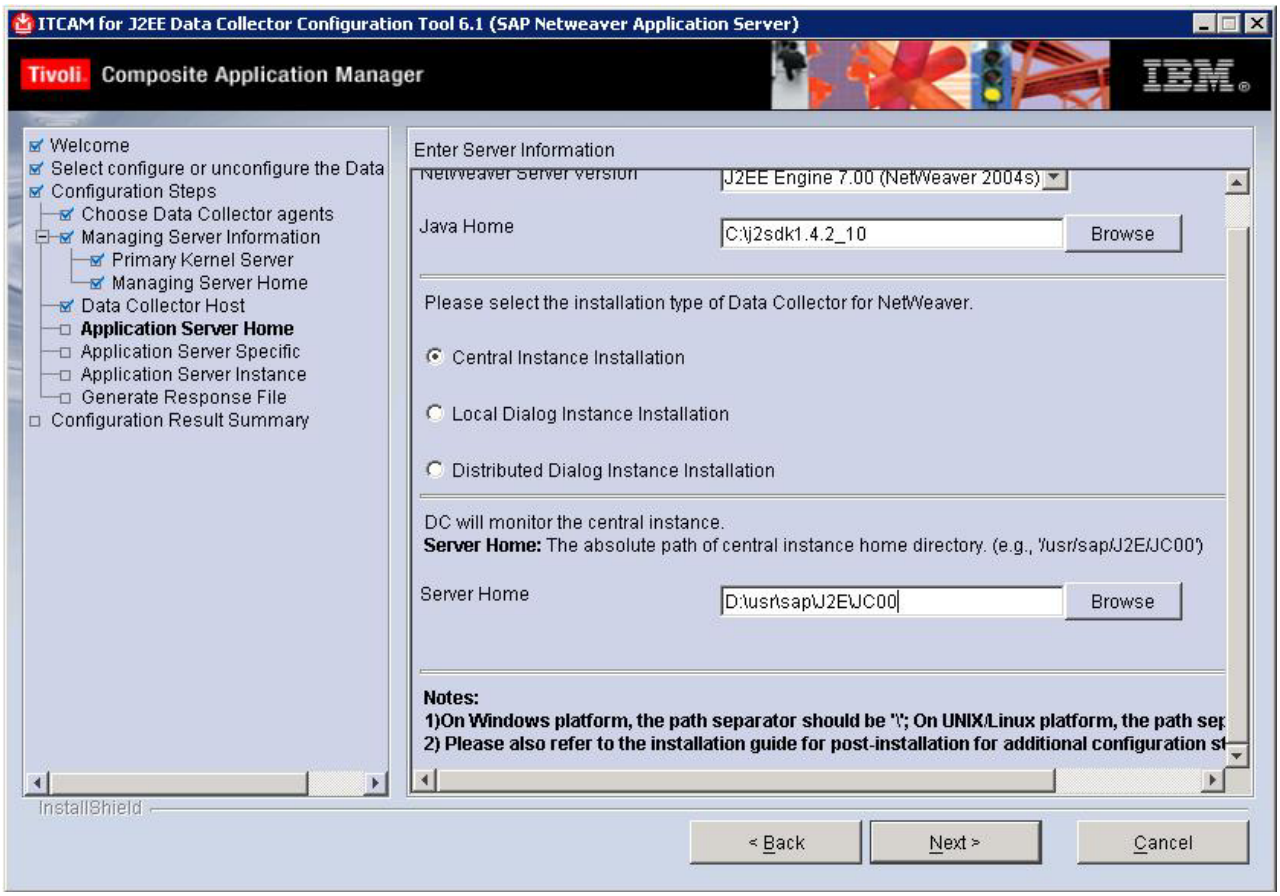



*Figure 36. Central Instance Installation for NetWeaver*

In the **Server Home Directory** field, click **Browse** and locate the directory in which NetWeaver is installed. The **Server Home** is the absolute path of central instance home directory (for example, C:\usr\sap\J2E\JC00).

**Local dialog instance installation:** If the dialog and central instance are on the same computer and you want to install DC to monitor the server on the dialog instance, select **Local Dialog Instance Installation**. Enter the **Server Home** and the **Central Instance Home** information. Where the **Server Home** is the absolute path of local dialog instance home directory (for example, C:\usr\sap\J2E\J01). The **Central Instance Home** is the absolute path of central instance home directory (for example, C:\usr\sap\J2E\JC00).

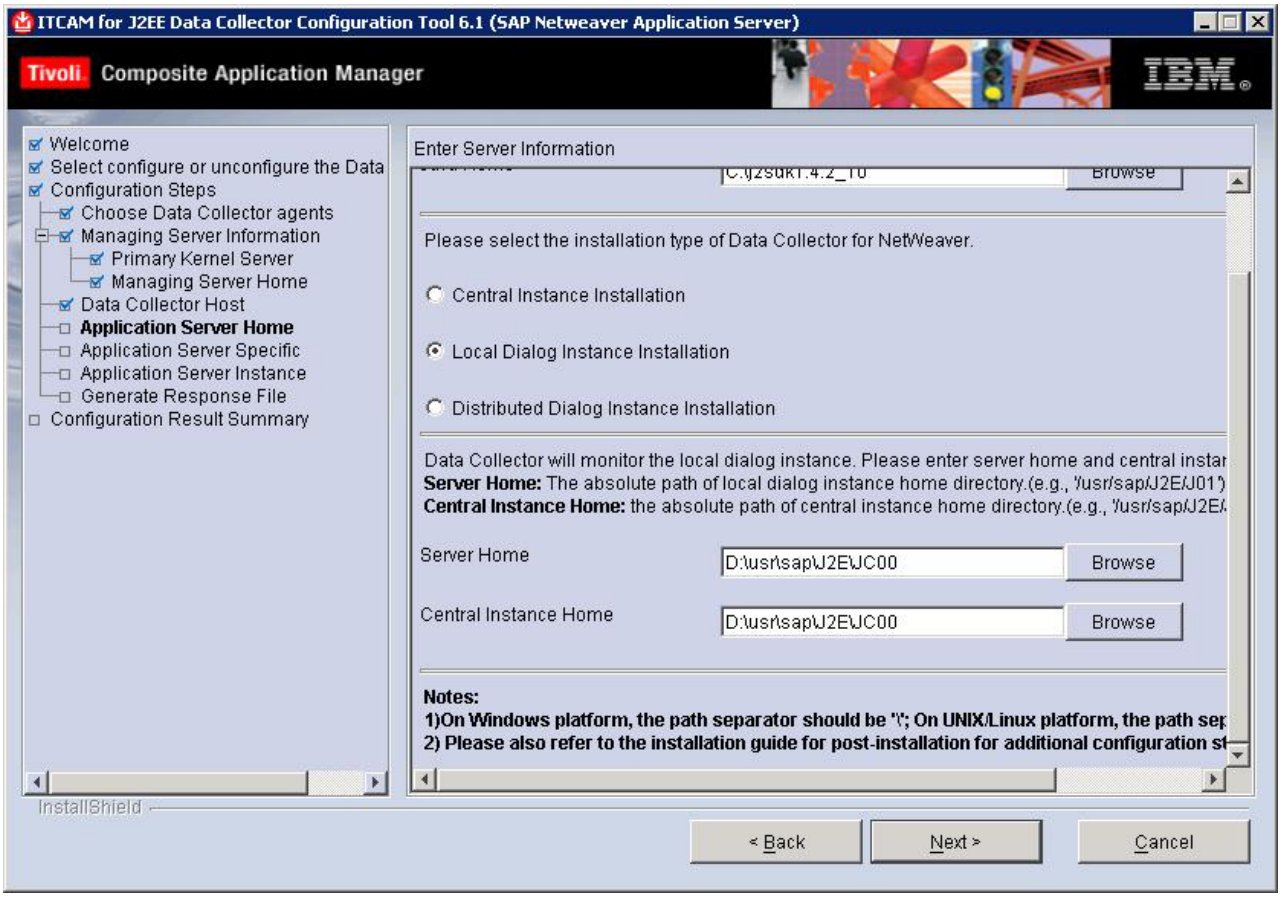



*Figure 37. Local Dialog Instance Installation for NetWeaver*

**Distributed dialog instance installation:** If the dialog and central instance are not on the same computer and you want to install DC to monitor the server on the dialog instance, select **Distributed Dialog Instance Installation**. Enter the **Server Home**, the **Central Instance Home** and the **Central Instance Network Home** filed information.

The **Server Home** is the absolute path of distributed dialog instance home directory (for example, C:\usr\sap\J2E\J01). The **Central Instance Home** is the absolute path of central instance home directory (for example, C:\usr\sap\J2E\JC00). The **Central Instance Network Home** is a local path mounted from the central instance home directory (for example, Y:\usr\sap\J2E\JC00).

For the **Central Instance Network Home** field information, you can use the remote path of the **Central instance home** on Windows platforms, as shown in figure 36.

Be sure to verify whether you are authorized to access the remote path of the **Central instance home**. Click **Start > Run** and enter the remote path of the **Central instance home**, and press Enter. The system prompts for your user ID and password. Enter correct user ID and password to navigate to the remote directory.

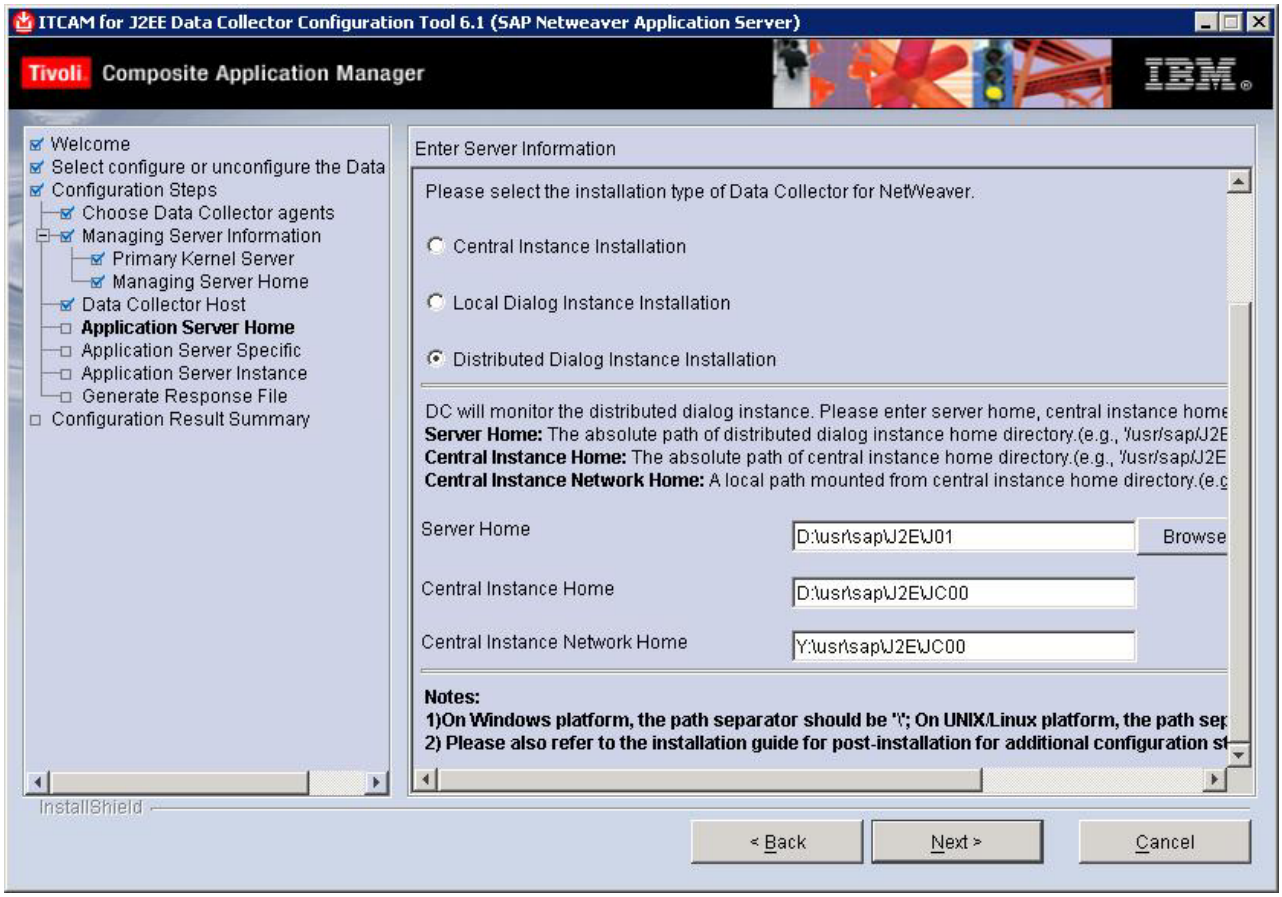



*Figure 38. Distributed Dialog Instance Installation for NetWeaver*

**Note:** On both Windows and Unix/Linux platforms, mount *Central instance home* on central instance computer to a local folder (for example, /mnt/sap/J2E/JC00) before clicking **Next**. And make sure that you have writing rights.

Click **Next** to proceed.

## Step 9: Enter NetWeaver server specifics

In this window, enter information about NetWeaver server specifics for server instance discovery.

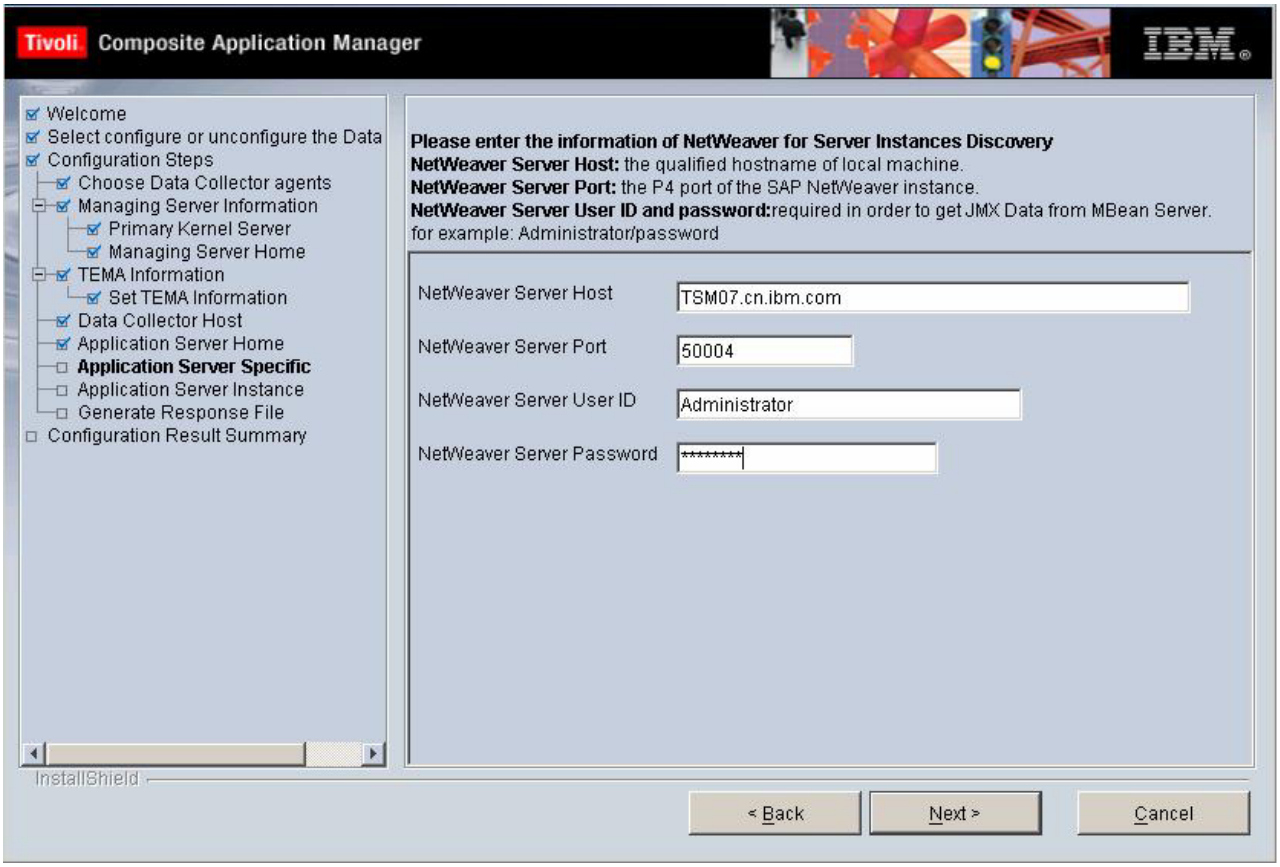



*Figure 39. NetWeaver server specific data*

Enter the IP address or the qualified host name of the local computer in the **NetWeaver Server Host** field. You must enter a port number in the **NetWeaver Server Port** field, which should be a P4 port number of this server. This field is not completed with a default value.

In the fields **NetWeaver Server User ID** and **NetWeaver Server Password** enter the user ID and password created during your installation of NetWeaver. Usually, the **NetWeaver Server User ID** and **NetWeaver Server Password** are the user ID and password you use to log on the Visual Administrator tool.

Click **Next** to continue.

### Step 10: Select the server instance for data collection

In this window, select the server instance that you want to configure.

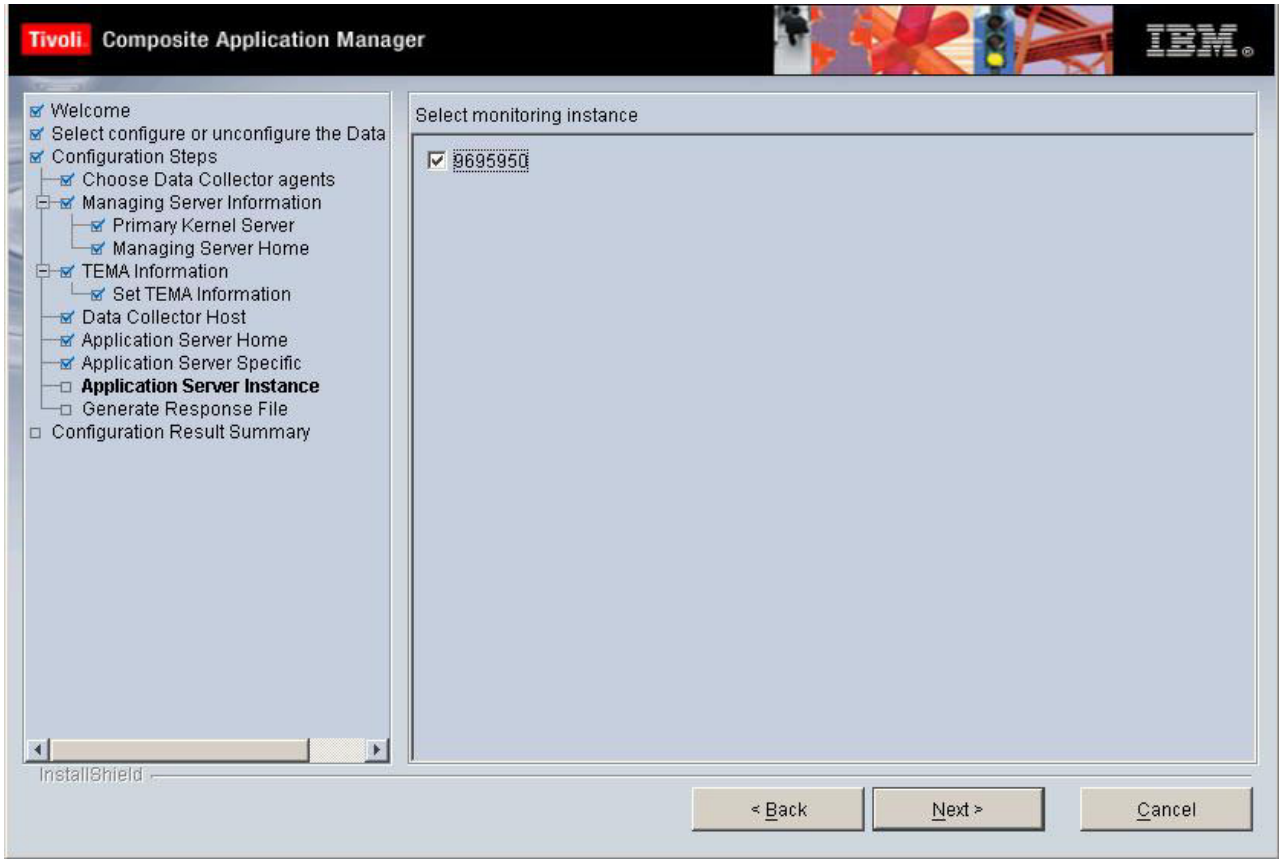



*Figure 40. Server instance selection*

Click **Next** to configure the Data Collector.

## Step 11: Generate a response file

You can choose to generate a response file to save all your settings. If you use a response file, you can have the same installation settings when you want to configure the Data Collector later again on this computer or on another computer using a silent installation.

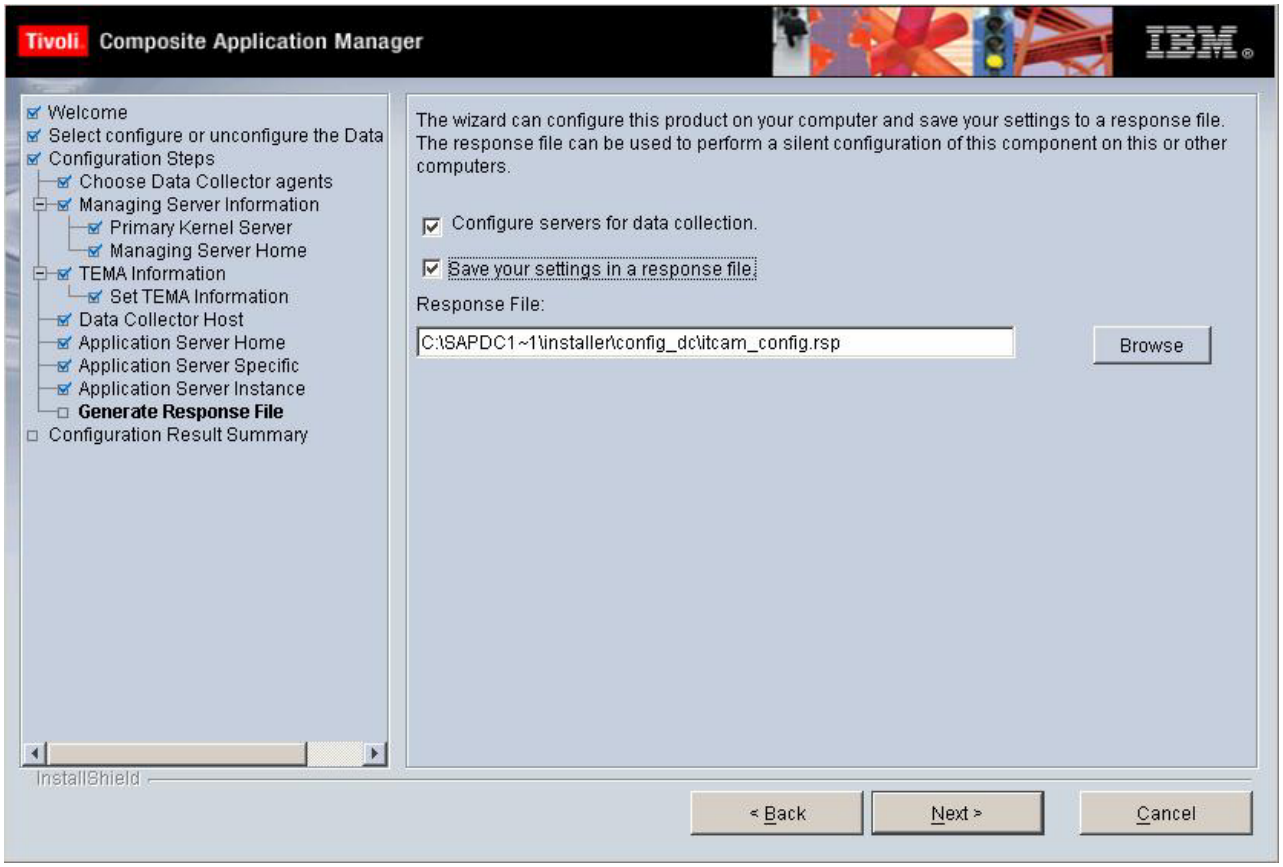



*Figure 41. Choose to save your settings in a response file*

**Configure servers for data collection** is selected by default. If you want to create a response file with all the settings in this configuration, select **Save your settings in a response file**, and choose a location where the response file will be generated.

Click **Next** to proceed.

## Step 12: Finalize the configuration

After the Data Collector is configured, the following window opens:

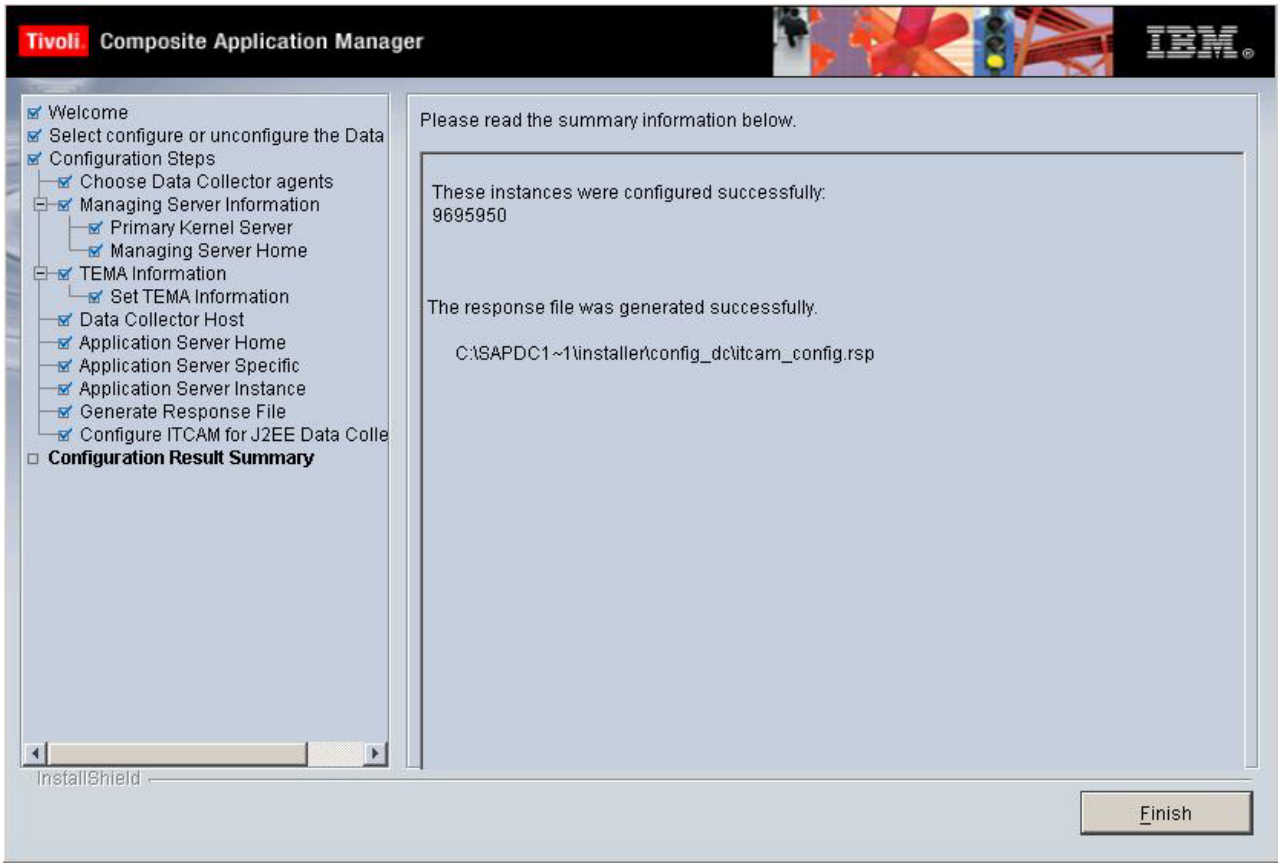



*Figure 42. Configuration results summary*

Read the summary information. The configuration status of the server instance that you selected is shown. Click **Finish** to finalize the configuration and close the Configuration Tool. If you are currently installing the DC, you will go back to the InstallShield Wizard. There you will be prompted to finalize the installation.

After the installation is completed, follow the instructions ("Post-configuration steps for NetWeaver" on page 151) to post-configure your Data Collector.

## Configuring the J2EE Data Collector for JBoss

### Step 8: Enter the JBoss Server information and Java home

In this window, you are prompted to enter information regarding the specific JBoss environment that you have installed.

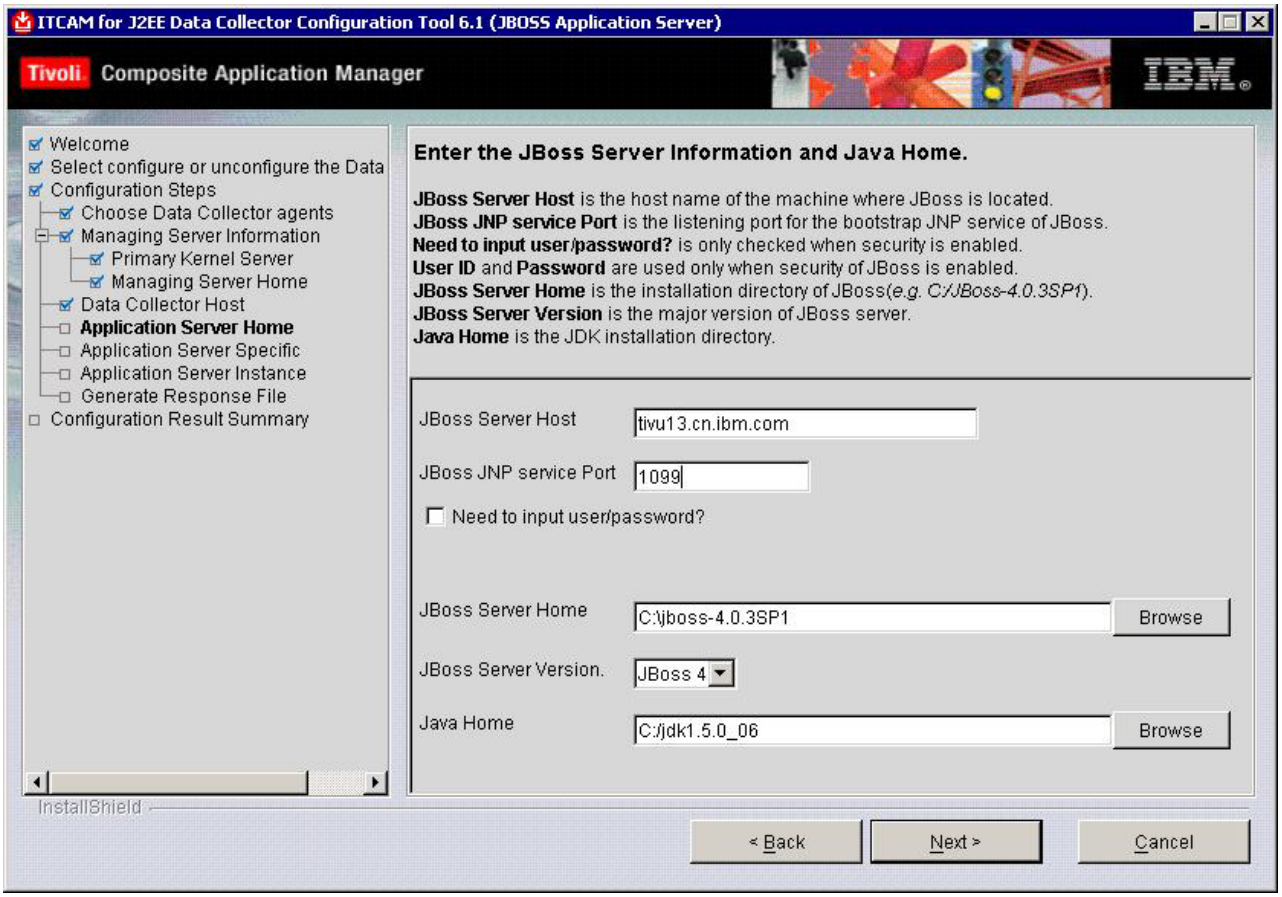



*Figure 43. JBoss general information*

Enter information for in the **JBoss Server Host** and **JBoss JNP Service Port** field. If you need to specify a user ID or password, select the check box and enter the user ID and password.

Click **Browse** and select the folder in which JBoss has been installed in the **JBoss Server Home** field. In the **JBoss Server Version** field select the version number of JBoss that you are running from the drop-down menu. In the **Java Home** field, click **Browse** and select the JDK that was installed in conjunction with JBoss.

If you are running the Configuration Tool on HP-UX or Solaris OS. A 64-bit check box will appear. Select **Use JDK as 64 bit** if you are using JDK as 64 bit.

Click **Next** to continue.

### Step 9: Enter the startup script of JBoss Server

In this window, you are prompted to locate the JBoss server startup script.

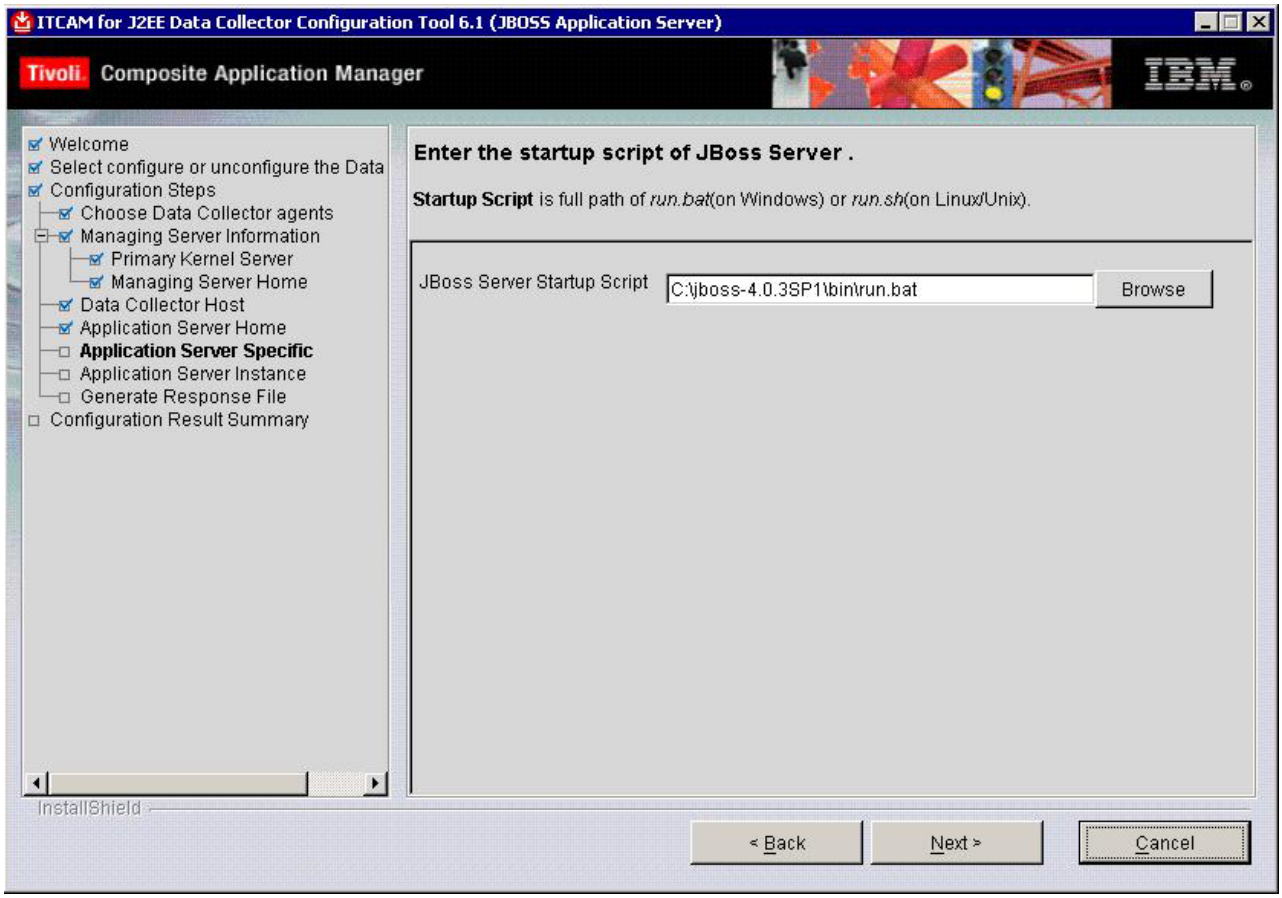



*Figure 44. JBoss server discovery and configuration*

Browse to locate the JBoss server startup script and click **Next** to proceed.

### Step 10: Select the server instance to configure

In this window, select the server instance that you want to configure.

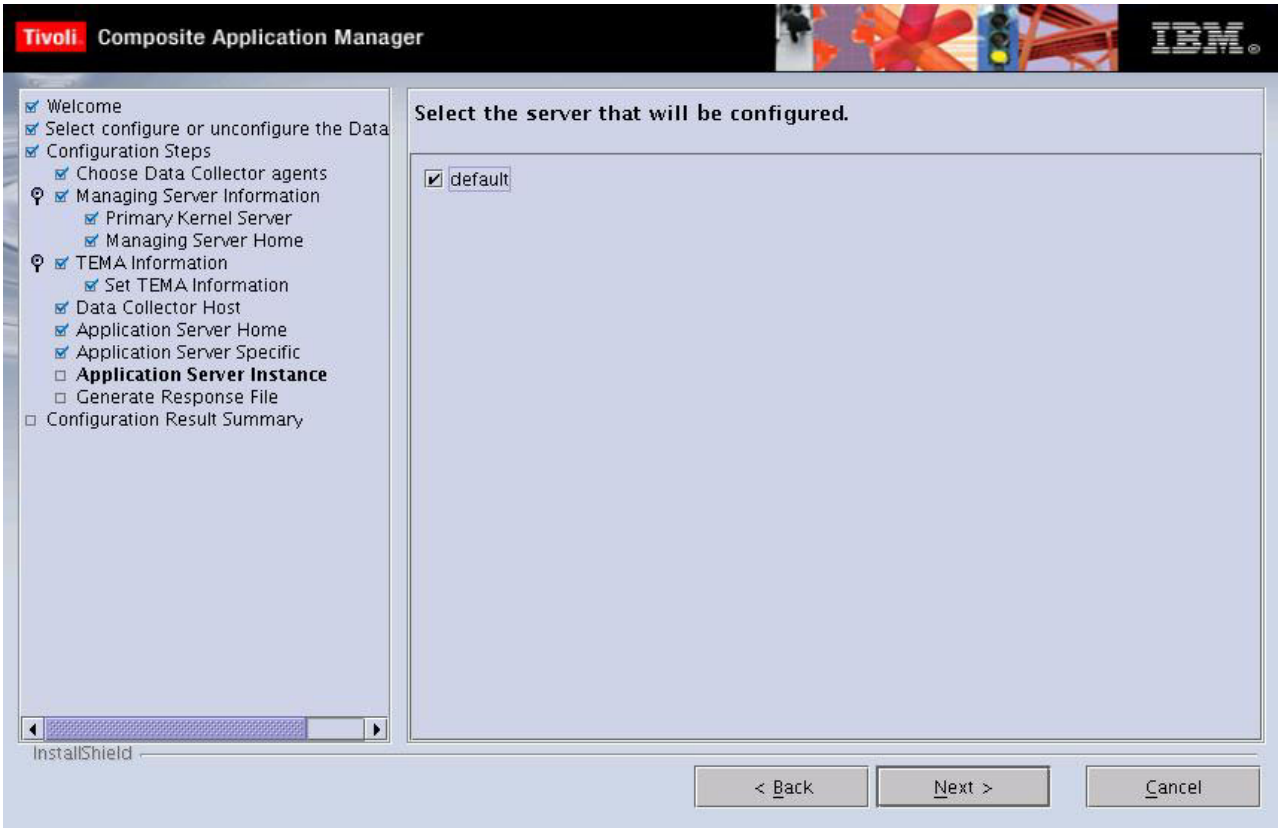



*Figure 45. Server instance selection*

Click **Next** to configure the DC.

### Step 11: Generate a response file

You can choose to generate a response file to save all your settings. If you use a response file, you can have the same installation settings when you want to configure the Data Collector later again on this computer or on another computer by silent installation.

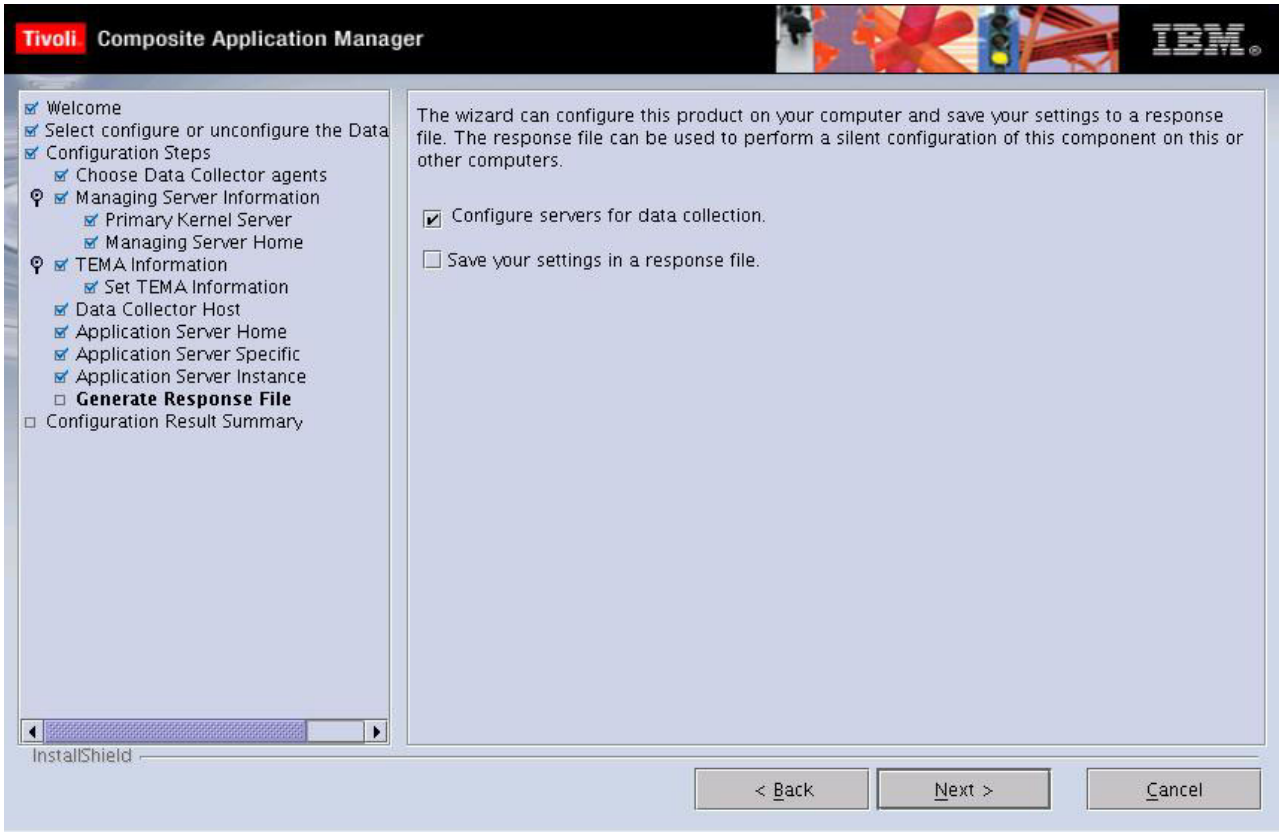



*Figure 46. Choose to save your settings in a response file*

**Configure servers for data collection** is selected by default. If you want to create a response file with all the settings in this configuration, select **Save your settings in a response file**, and choose a location where the response file can be generated.

Click **Next** to proceed.

## Step 12: Finalize the configuration

After the Data Collector is configured, the following window opens:

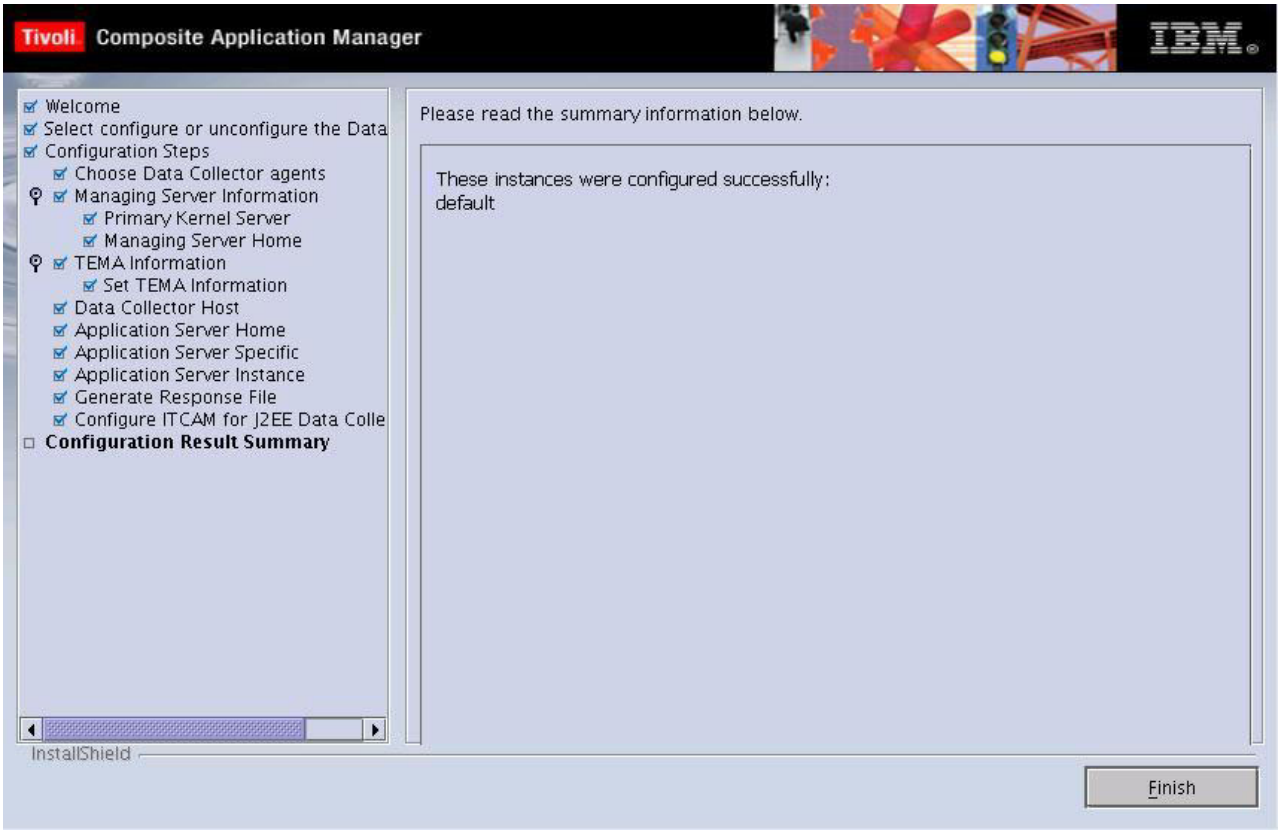



*Figure 47. Configuration results summary*

Read the summary information. The configuration status of the server instance that you selected is shown. Click **Finish** to finalize the configuration and close the Configuration Tool. If you are currently installing the DC, you will go back to the InstallShield Wizard. There you will be prompted to finalize the installation.

## Configuring the J2EE Data Collector for Tomcat

### Step 8: Enter Tomcat server information and Java Home

In this window, you are prompted to enter information regarding the specific Tomcat environment that is installed on your computer.

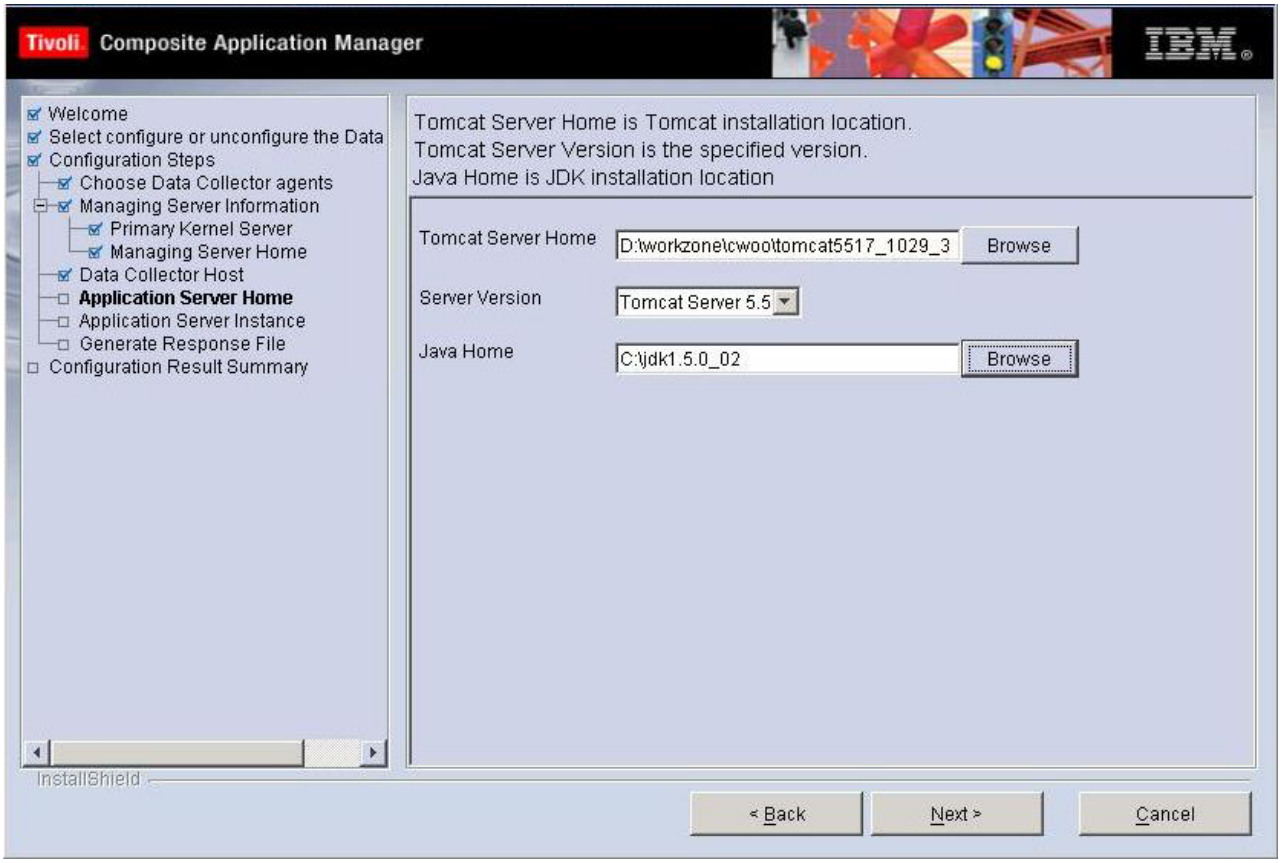



*Figure 48. Tomcat general information*

Click **Browse** to enter a value in the **Tomcat Server Home** field, which specifies the directory in which Tomcat is located.

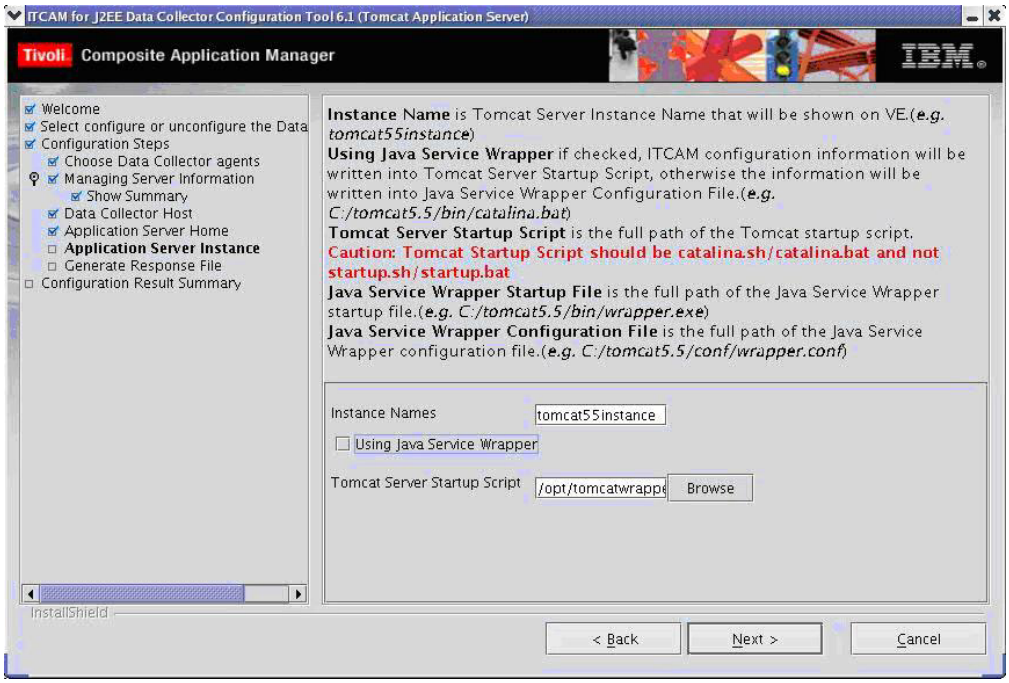
In the **Server Version** field, select the version of Tomcat that you are currently running. Click **Browse** to enter a value in the **Java Home** field, which specifies the directory of the JDK that is supporting the application server.

If you are running the Configuration Tool on HP-UX or Solaris OS. A 64-bit check box will appear. Select **Use JDK as 64 bit** if you are using JDK as 64 bit.

After you have entered the required information, click **Next** to proceed.

## Step 9: Enter Tomcat application instance information

You are prompted for information regarding the Tomcat Server instance to be configured for data collection.



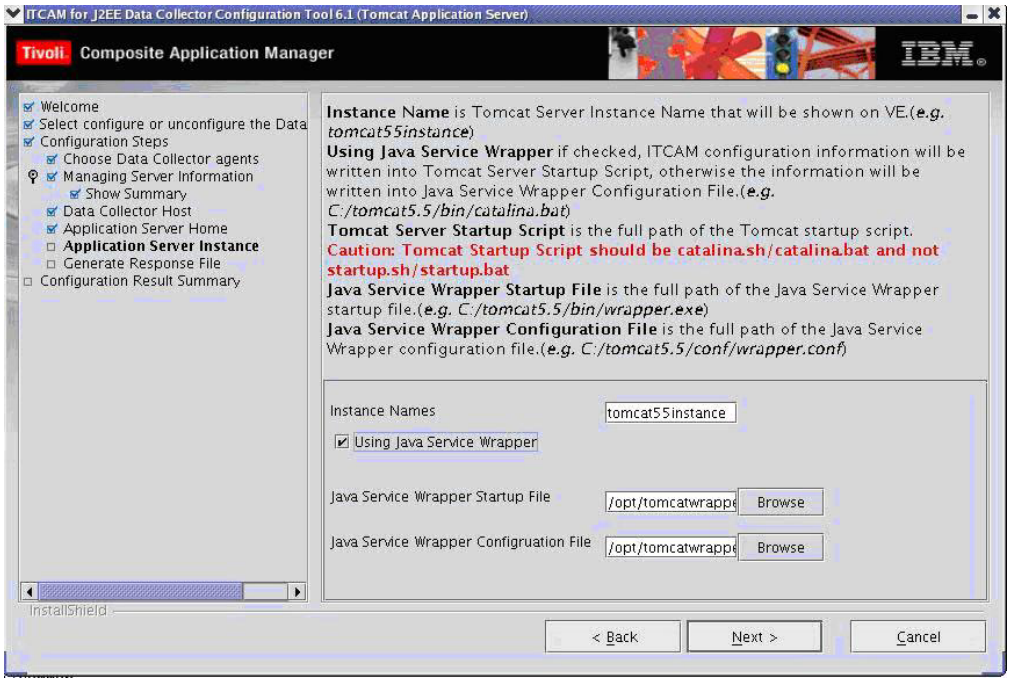

In the **Instance Names** field, enter the name of the Tomcat Server instance that you wish to configure for data collection.

**Note:** Use only English characters and Arabic numbers for instance names.

**Note:** If you are configuring a new Tomcat server instance or editing an existing instance, ensure that each instance name is unique. The instance name information can be found in the directory, <*DC_HOME*>/runtime/. If there is an existing Tomcat Server instance name, you can find a child directory under this directory. The child directory takes the form as <Server Name>.<Node Name>.<Instance Name>. For example, tomcat_55_1029_1 is the instance name in the <*DC_HOME*>/runtime/tomcat55.tiv147.cn.ibm.com.tomcat_55_1029_1 directory.

In the **Tomcat Server Startup Script** field, browse to select the folder in which Tomcat is installed. In Windows, select **bin > catalina.bat** or in Unix, select **bin > catalina.sh**. The startup script contains the command lines to launch the application server.

If you wish to use a java service wrapper, select **Using Java Service Wrapper**. The **Tomcat Server Startup Script** field is replaced with two new fields, -**Java Service Wrapper Startup File** and **Java Service Wrapper Configuration File**.




In the **Java Service Wrapper Startup File** field, enter the full path of the java service wrapper startup file, e.g. c:/tomcat5.5/bin/wrapper.exe.

To support cascading configuration files in the java service wrapper framework, the base directory of the java service wrapper needs to be specified. This enables a user to define a relative path for an included configuration file. By default, the base-directory is the location of the wrapper.exe in Windows, or the script used to launch the wrapper in Unix. If the `wrapper.working.dir` property is defined in the java service wrapper configuration file, ITCAM will use the value of the property as the base directory.

In the **Java Service Wrapper Configuration File** field, enter the full path of the java service wrapper configuration file, e.g. c:/tomcat5.5/conf/wrapper.conf.

The java service wrapper configuration file is similar to the java properties file. It contains the information necessary to launch a JVM instance with the correct command line required by an application. The default file is wrapper.conf. When you configure Tomcat to use the java service wrapper, ITCAM creates a new file called itcam_wrapper.conf in the same directory as wrapper.conf. This file includes all ITCAM configuration items. The wrapper.conf file references the itcam_wrapper.conf file using an include statement.

Click **Next** to proceed.

## Step 10: Generate a response file

You can choose to generate a response file to save all your settings. If you use a response file, you can have the same installation settings when you want to configure the Data Collector later again on this computer or on another computer using a silent installation.

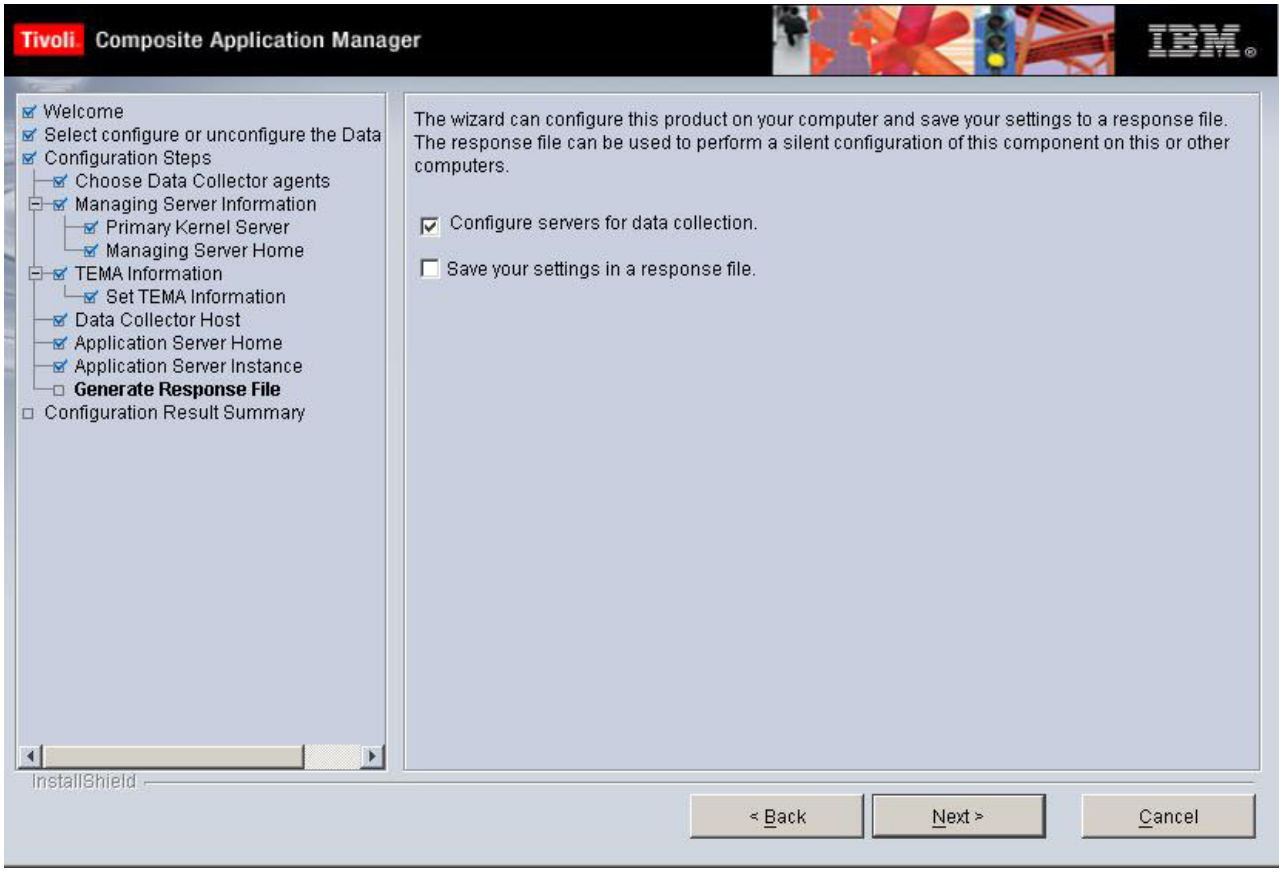



*Figure 49. Choose to save your settings in a response file*

**Configure servers for data collection** is selected by default. If you want to create a response file with all the settings in this configuration, select **Save your settings in a response file**, and choose a location where the response file can be generated.

Click **Next** to proceed.

## Step 11: Finalize the configuration

After the Data Collector is configured, the following window opens:

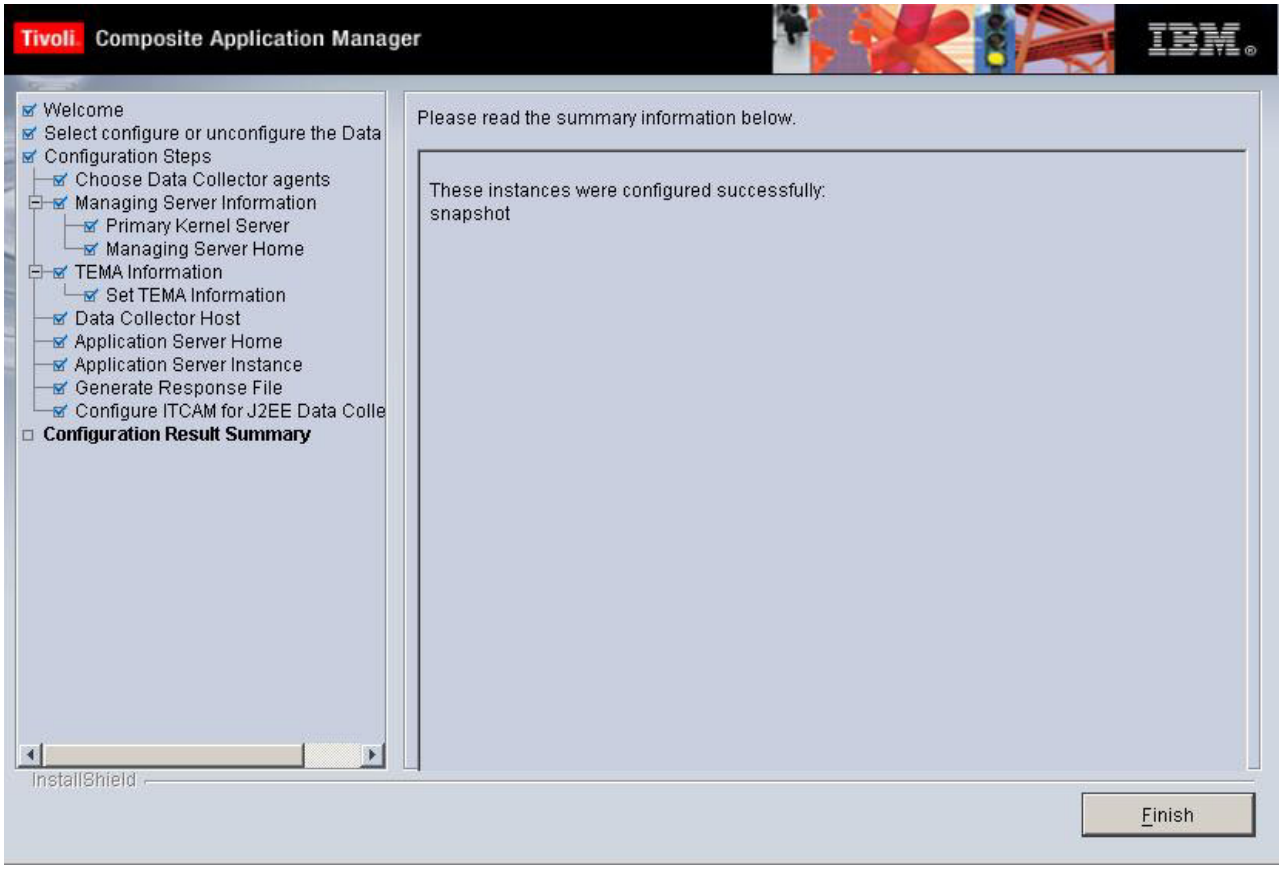



*Figure 50. Configuration results summary*

Read the summary information. The configuration status of the server instance that you selected is shown. Click **Finish** to finalize the configuration and close the Configuration Tool. If you are currently installing the DC, you will go back to the InstallShield Wizard. There you will be prompted to finalize the installation.

## Configuring the J2EE Data Collector for Oracle

### Step 8: Enter Oracle Server Information and Java Home

In this window, you are prompted to enter information regarding the specific Oracle environment that is installed on your computer.

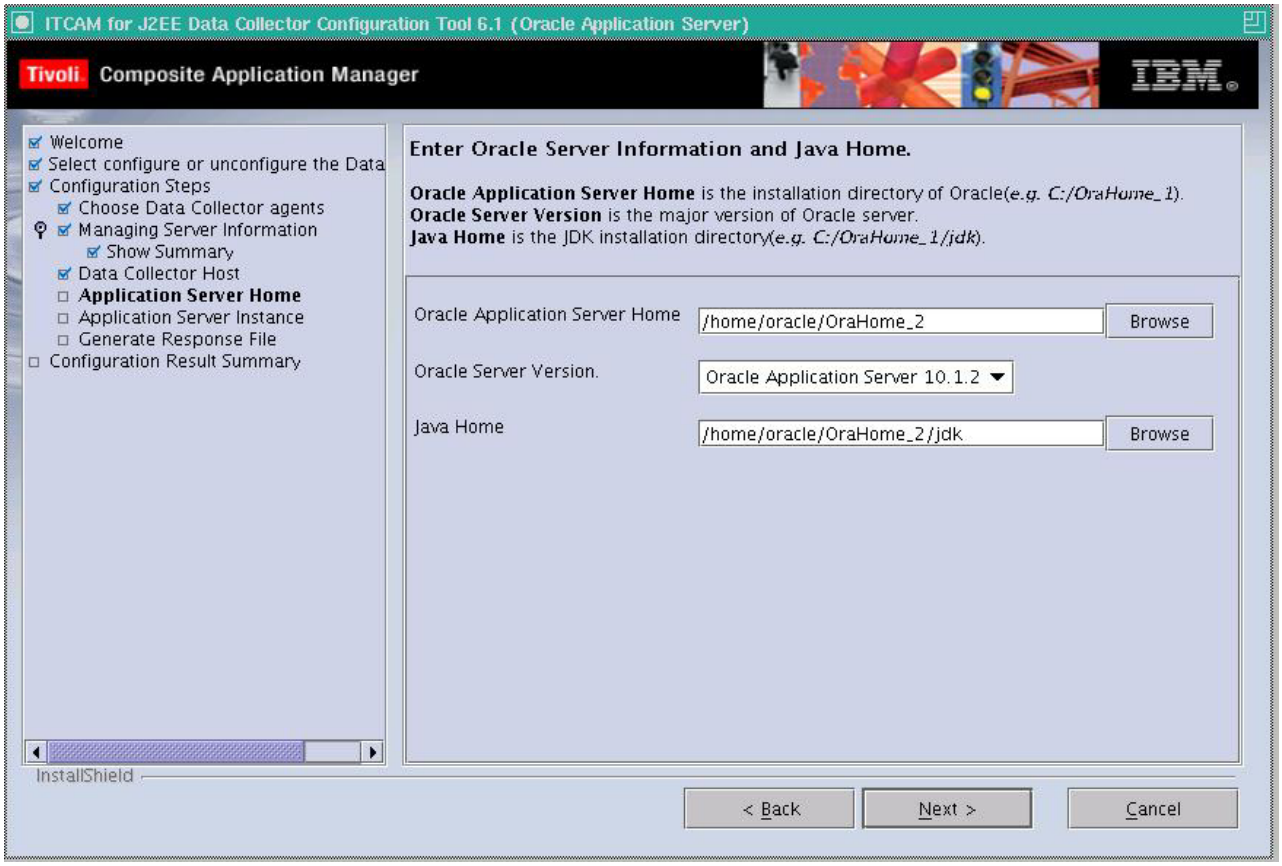



*Figure 51. Oracle general information*

Click **Browse** to complete the **Oracle Application Server Home** field, which is the directory in which the Oracle application server is located. Select the correct Oracle server version in the **Oracle Server Version** field. Click **Browse** to enter a value in the **Java Home** field, which specifies the directory of the JDK supporting Oracle.

If you are running the Configuration Tool on HP-UX or Solaris OS. A 64-bit check box will appear. Select **Use JDK as 64 bit** if you are using JDK as 64 bit.

After you have entered the required information, click **Next** to proceed.

## Step 9: Select the server instance to configure

Select the server instance that you want to configure for data collection.

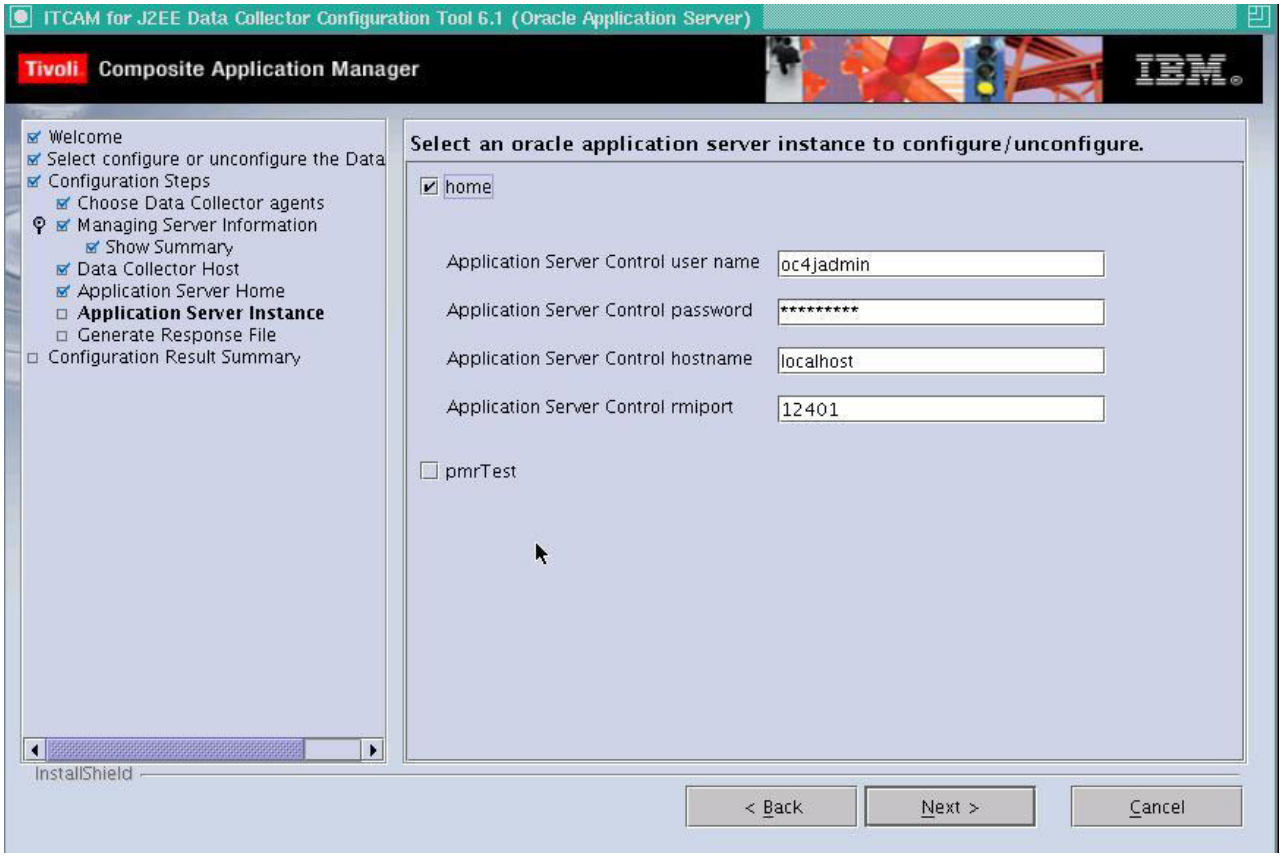



*Figure 52. Server instance selection*

A panel is displayed requesting four parameters for the Oracle Application Server. It is a requirement in Oracle Application Server version 10.1.3, that the application server is running, this is not required in previous Oracle Application Server versions.

1. In the **Application Server Control user name** field and the **Application Server Control password** field, enter the user name and password you use to login into the web console. Usually the URL for the web console is similar to the following URL: http://host:7777/em.
2. If the Oracle Application Server is installed on the same server as the data collector, leave the **Application Server Control hostname** as localhost, otherwise enter the address of the server where the Oracle Application Server is installed.
3. The **Application Server Control rmiport** field value is dynamic, to find this port number, ensure the server is running, then execute the following command:

   ```
   ./opmnctl status -l
   ```

   The option 1 for list. The opmnctl command is the start script for the Oracle Application Server, it is available here: <ORACLE_HOME>/opmn/bin

Click **Next** to configure the DC.

## Step 10: Generate a response file

You can choose to generate a response file to save all your settings. If you use a response file, you can have the same installation settings when you want to

configure the Data Collector later again on this computer or on another computer by silent installation.

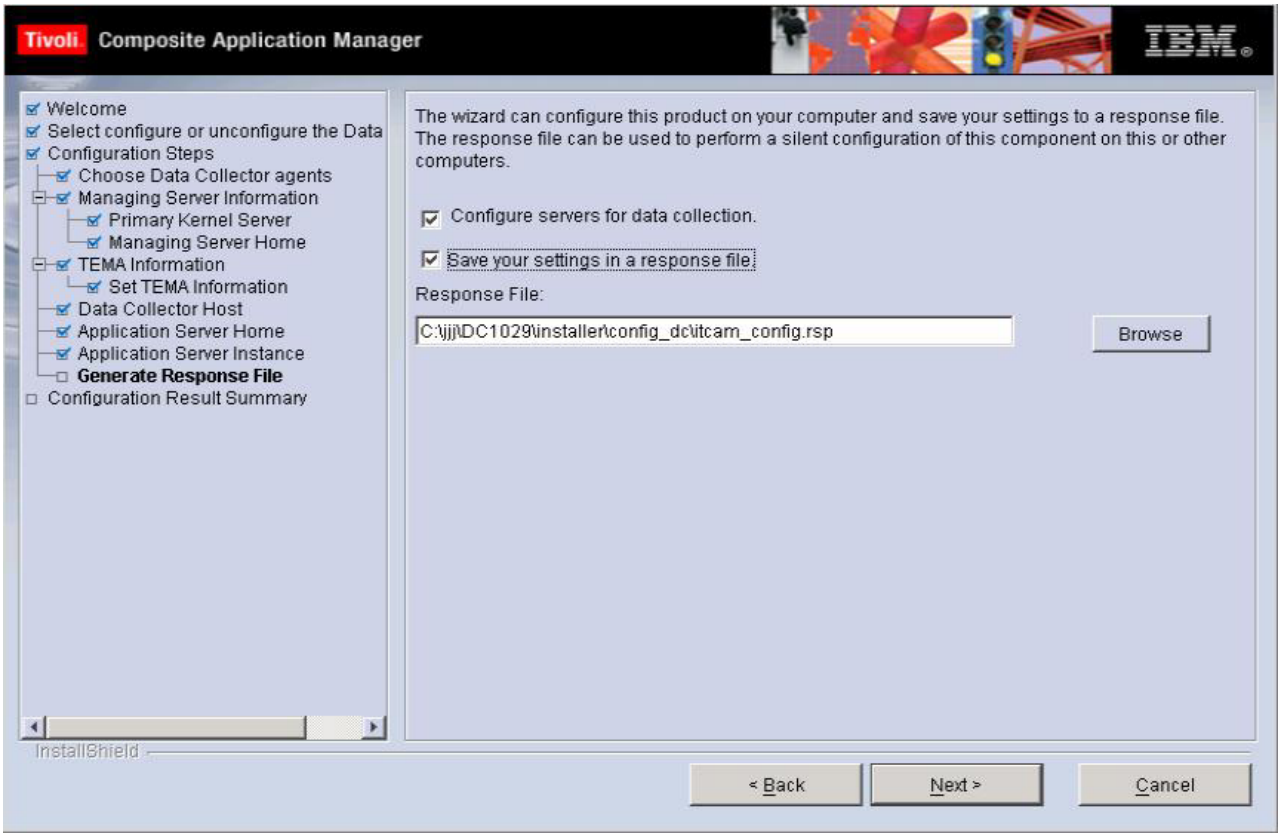



*Figure 53. Choose to save your settings in a response file*

**Configure servers for data collection** is selected by default. If you want to create a response file with all the settings in this configuration, select **Save your settings in a response file**, and choose a location where the response file can be generated.

Click **Next** to proceed.

## Step 11: Finalize the configuration

After the Data Collector is configured, the following window opens:

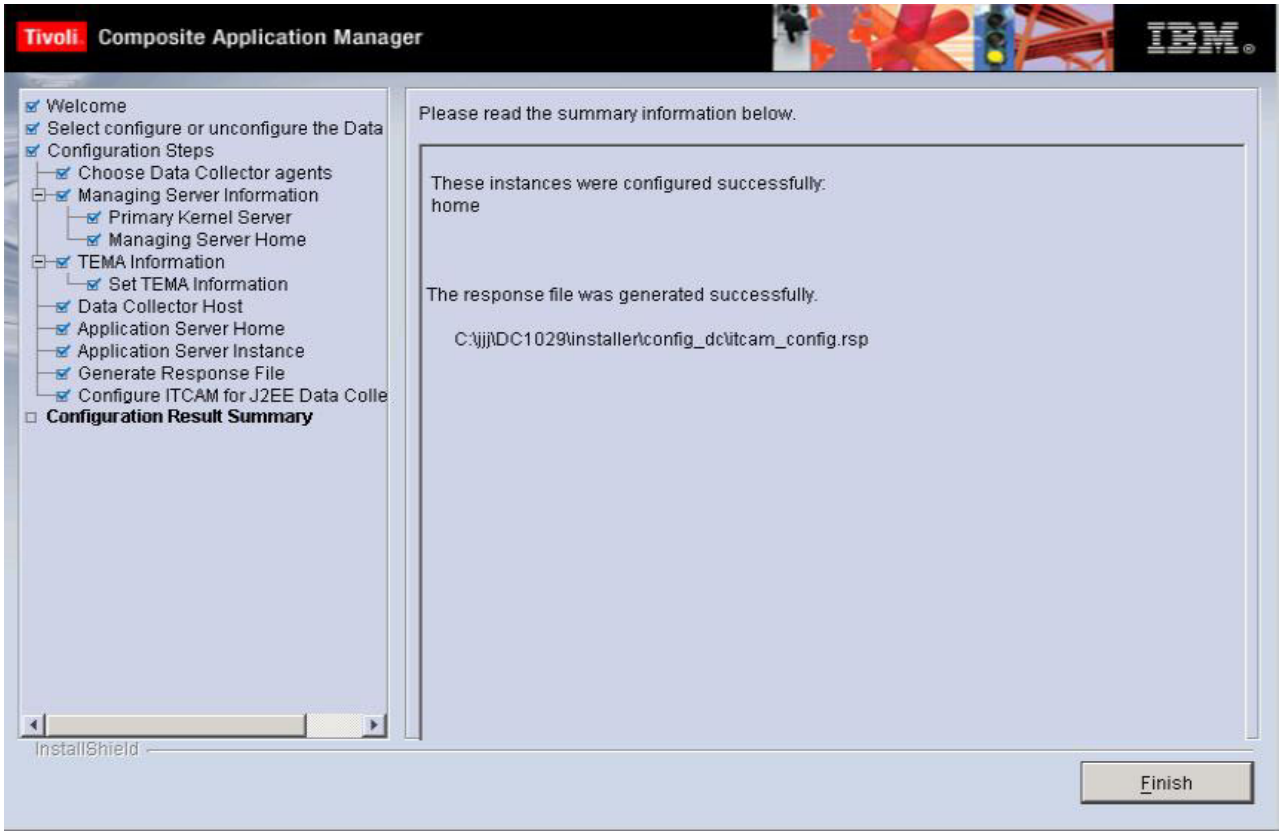


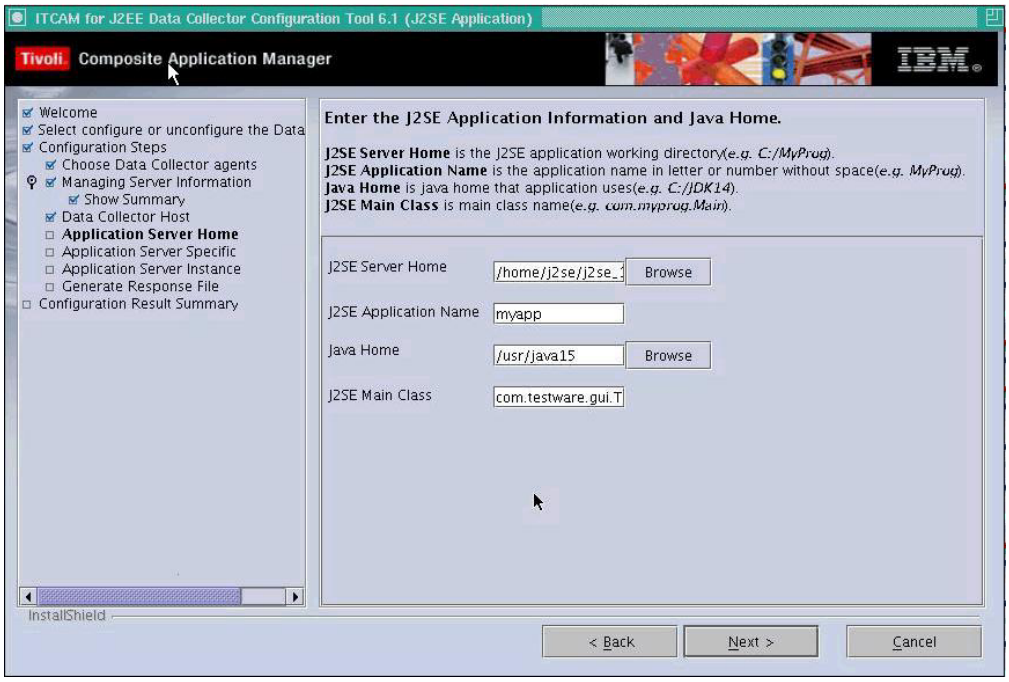

*Figure 54. Configuration results summary*

Read the summary information about this screen. The configuration status of the server instance that you selected is shown. Click **Finish** to finalize the configuration and close the Configuration Tool. If you are currently installing the DC, you will go back to the InstallShield Wizard. From there you will be prompted to finalize the installation.

# Configuring the J2EE Data Collector for J2SE

## Step 8: Enter J2SE specific information

In this window, you enter information that is specific to your J2SE environment.




In the **J2SE Server Home** field, click **Browse** to locate the directory in which J2SE has been installed. Ensure the J2SE server home value you enter is correct as there is no validation performed on this field. The value will be displayed in Tivoli Enterprise Portal after the installation. Enter the application name under which J2SE runs in the **J2SE Application Name** field. For the **Java Home** field, click **Browse** to locate the JDK that is supporting the application. In the field **J2SE Main Class** locate the .bat file under the J2SE server home directory and copy the CLASSPATH. For example, in *$JAVA_OPTS $ITCAM_JVM_OPTS -classpath $CLASSPATH com.testware.standalone.Main [LOG]*, the CLASSPATH should be *com.testware.standalone.Main*.

If you are running the Configuration Tool on HP-UX or Solaris OS. A 64-bit check box will appear. Select **Use JDK as 64 bit** if you are using JDK as 64 bit.

Click **Next**.

## Step 9: Enter JMX variables

In the following window, enter the Java Management Extensions (JMX) variables.

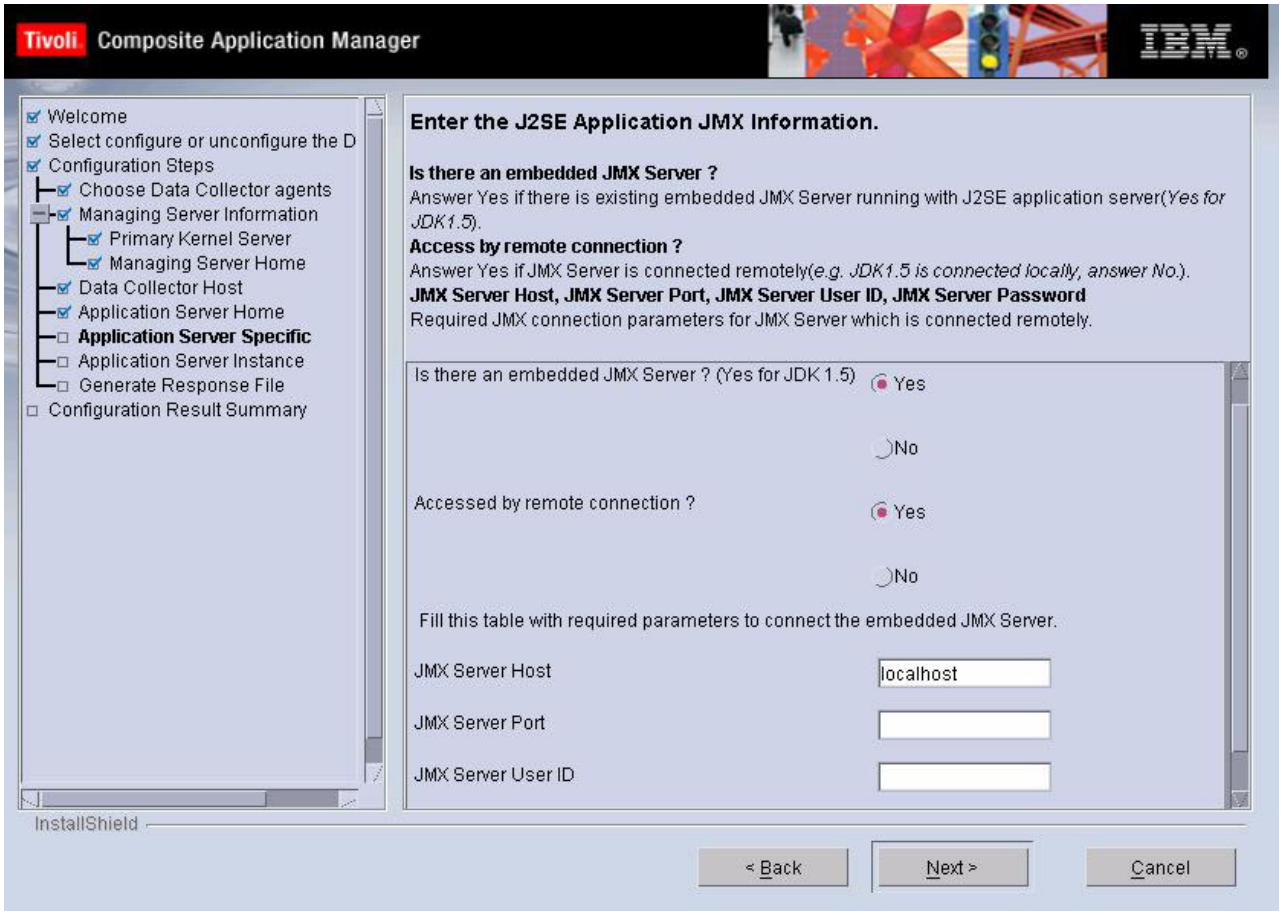



*Figure 55. JMX Variables*

Select the appropriate answers for the first two questions. Enter the host name of the J2SE host computer in the **JMX Server Host** field. Enter the computer's port number in the **JMX Server Port** filed.

Enter the user ID in the **JMX Server User ID** field and the password in the **JMX Server Password** field.

Click **Next** to proceed.

### Step 10: Enter J2SE application instance information

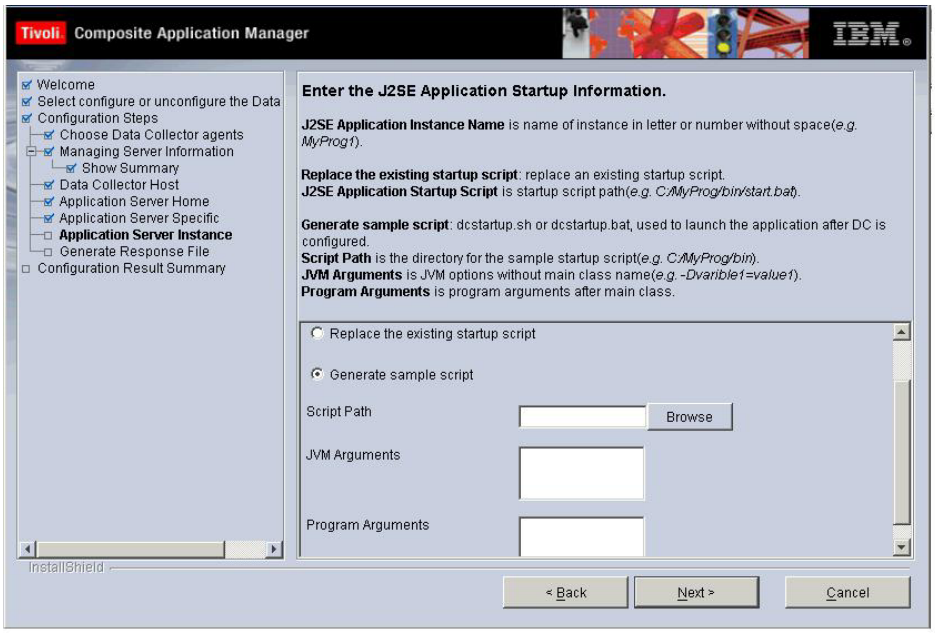
In this window, enter the information required to configure the J2SE instance.


*Figure 56. J2SE Managing Server instance information*

1. In the **J2SE Application Instance Name** field, enter the name of the Managing Sever instance to be configured for the data collection.

   **Note:** Use only English characters and Arabic numbers for the instance name.
2. Select either **Replace existing startup script**. or **Generate sample script**
3. If you select **Replace existing startup script**, click **Browse** in the **J2SE Application Startup Script** field to locate a startup script that will launch the application server.

   **Note:** When you are reconfiguring the application server, if you use a different application name or different instance name, the startup script will be modified incorrectly, to avoid this, use a different start up script without any existing data collector configuration information.
4. If you select **Generate sample script**, the following fields are displayed:




5. In the **Script Path** field, enter the directory for the sample startup script.
6. In the **JVM Arguments** field, enter the JVM options without the main class name, for example: -Dvarible1=value1
7. In the **Program Arguments** field, enter the program arguments after the main class.
8. After entering the required information, click **Next** to configure the DC.

## Step 11: Generate a response file

You can choose to generate a response file to save all your settings. If you use a response file, you can have the same installation settings when you want to configure the Data Collector later again on this computer or on another computer using a silent installation.

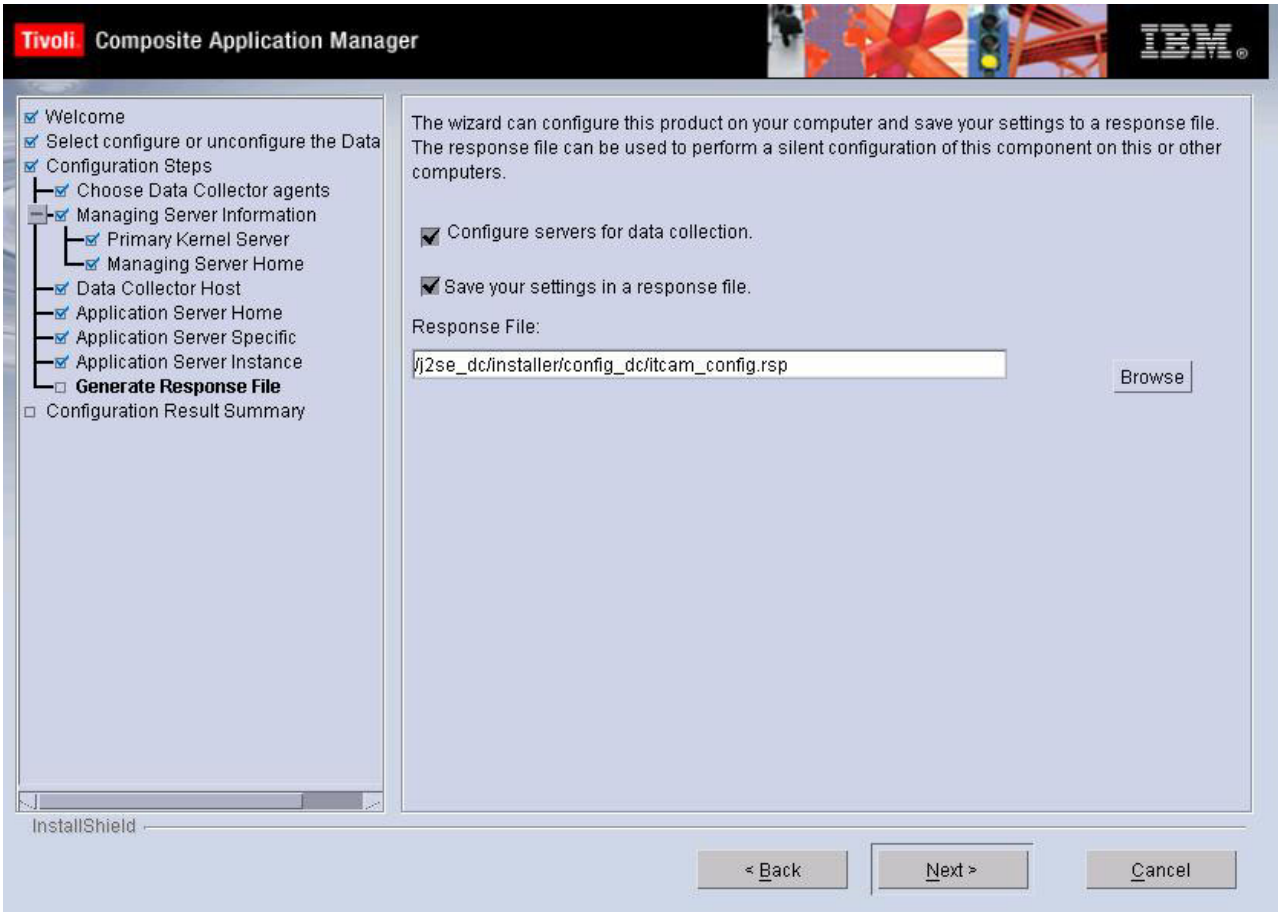



*Figure 57. Choose to save your settings in a response file*

**Configure servers for data collection** is selected by default. If you wish to create a response file with all the settings in this configuration, select **Save your settings in a response file**, and choose a location where the response file will be generated.

Click **Next** to proceed.

## Step 12: Finalize the configuration

After the Data Collector is configured, the following window opens:

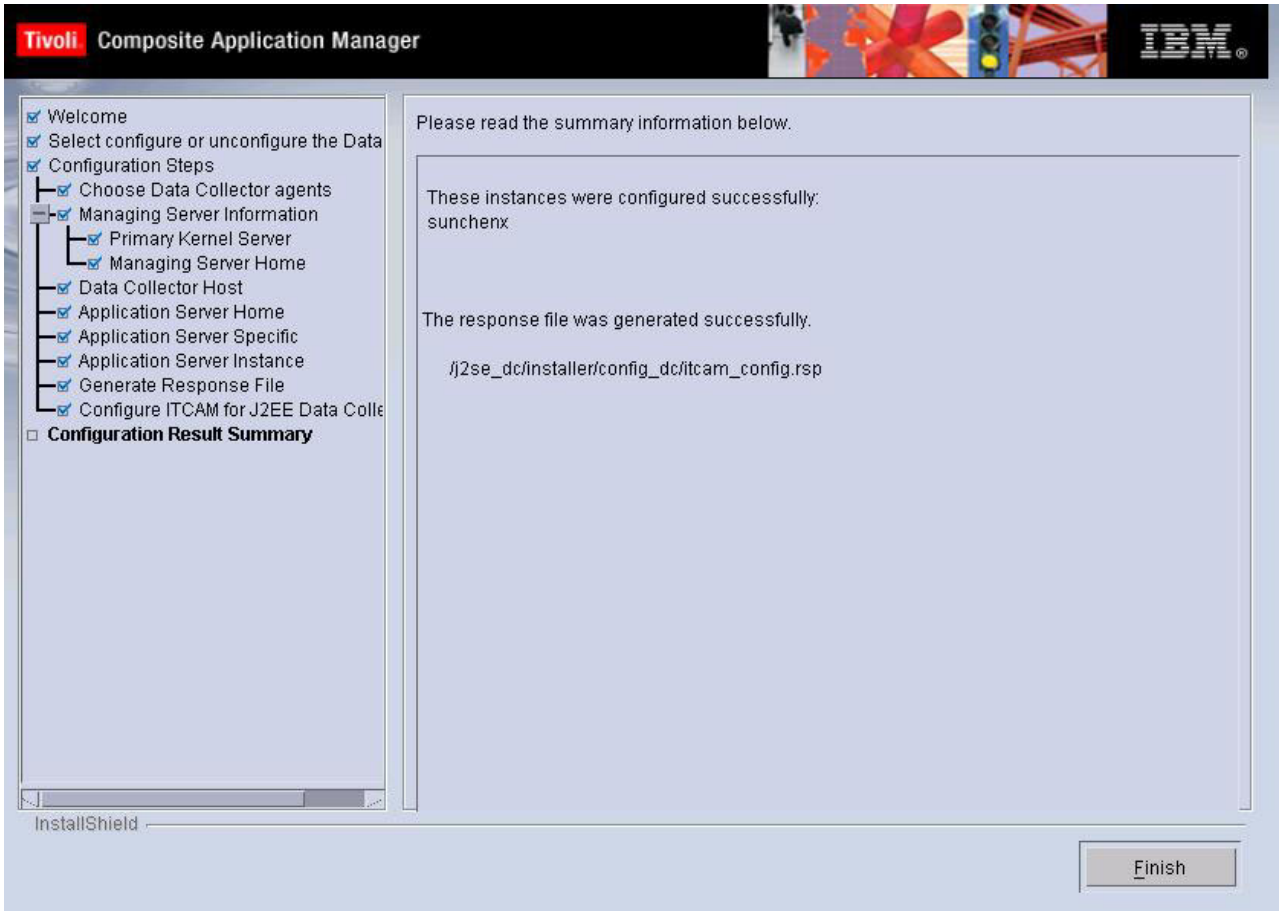



*Figure 58. Configuration results summary*

Read the summary information. The configuration status of the server instance that you selected is shown. Click **Finish** to finalize the configuration and close the Configuration Tool. If you are currently installing the DC, you return to the InstallShield Wizard. There you are prompted to finalize the installation.

## Configuring the J2EE Data Collector for JSAS

The configuration steps for iPlanet Application Server (IAS) 6.5 differs from Sun Java System Application Server (JSAS) 7 and 8. Complete the steps in one of the following sections:

- Configuring the J2EE Data Collector for IAS 6.5
- Configuring the J2EE Data Collector for JSAS 7 and 8

### Configuring the J2EE Data Collector for IAS 6.5

**Note:** Before you configuring the J2EE Data Collector for IAS 6.5, stop any running server instance.

**Step 8: Specify IAS-specific information:** Specify the JSAS-specific information in the following window.

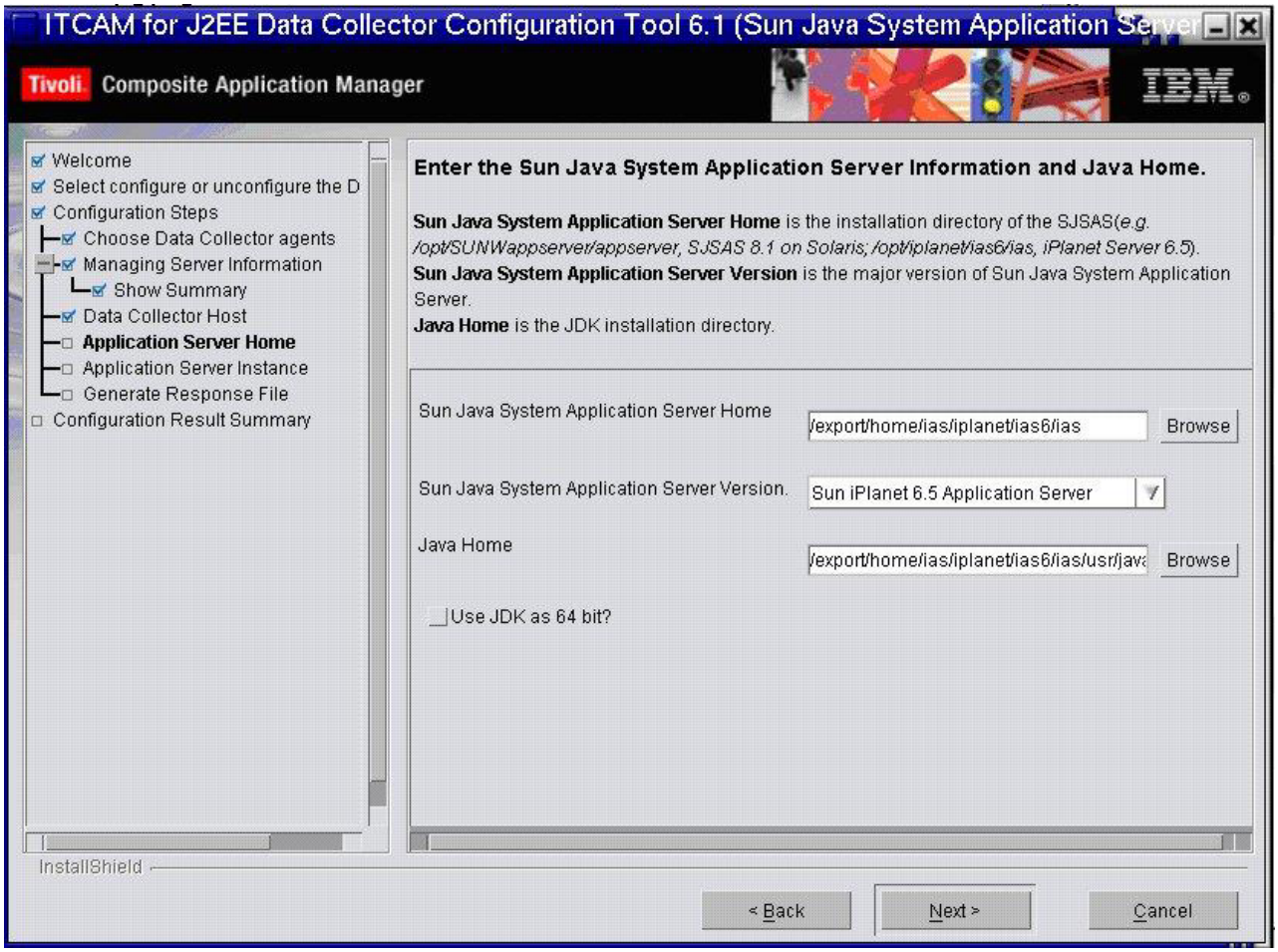



*Figure 59. IAS-specific information*

In the **Sun Java System Application Server Home** field, click **Browse** to locate the directory in which IAS has been installed. Select the IAS version in the **Sun Java System Application Server Version** field. For the **Java Home** field, click **Browse** to locate the JDK that is supporting the application.

Select or clear the checkbox near **Use JDK as 64 bit** as appropriate.

Click **Next**.

**Step 9: Specify the instance name of IAS:** In the following window, specify the instance name of the IAS.

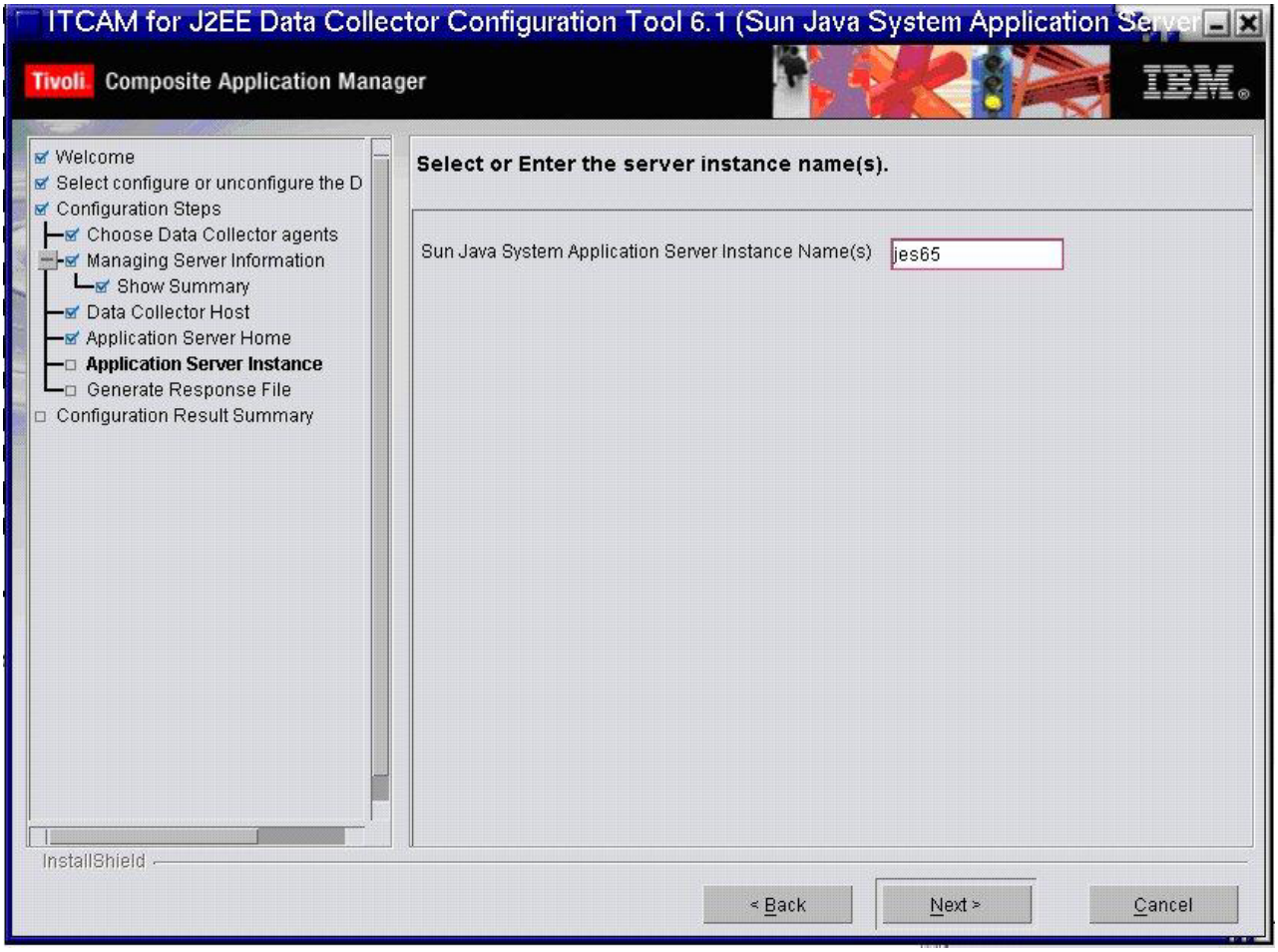



*Figure 60. IAS instance name*

Specify the instance name in the **Sun Java System Application Server Instance Name** field.

Click **Next** to proceed.

**Step 10: Generate a response file:** You can choose to generate a response file to save all your settings. You can have the same installation settings when you want to configure the Data Collector on any computer by using a silent installation.

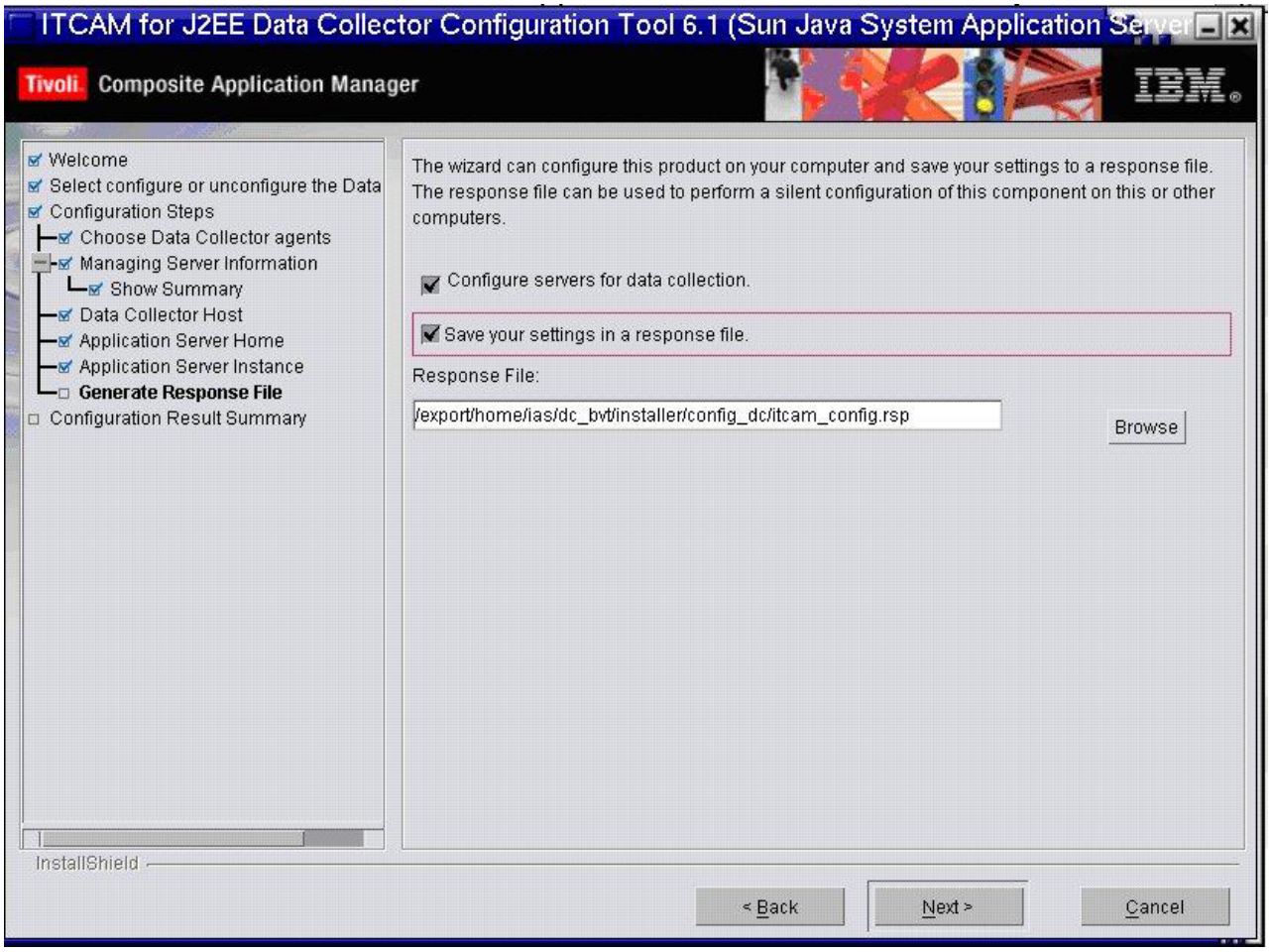



*Figure 61. Choose to save your settings in a response file*

**Configure servers for data collection** is selected by default. If you wish to create a response file with all the settings in this configuration, select **Save your settings in a response file**. Choose a location where the response file is generated.

Click **Next** to proceed.

**Step 11: Finalize the configuration:** After the Data Collector is configured, the following window opens:

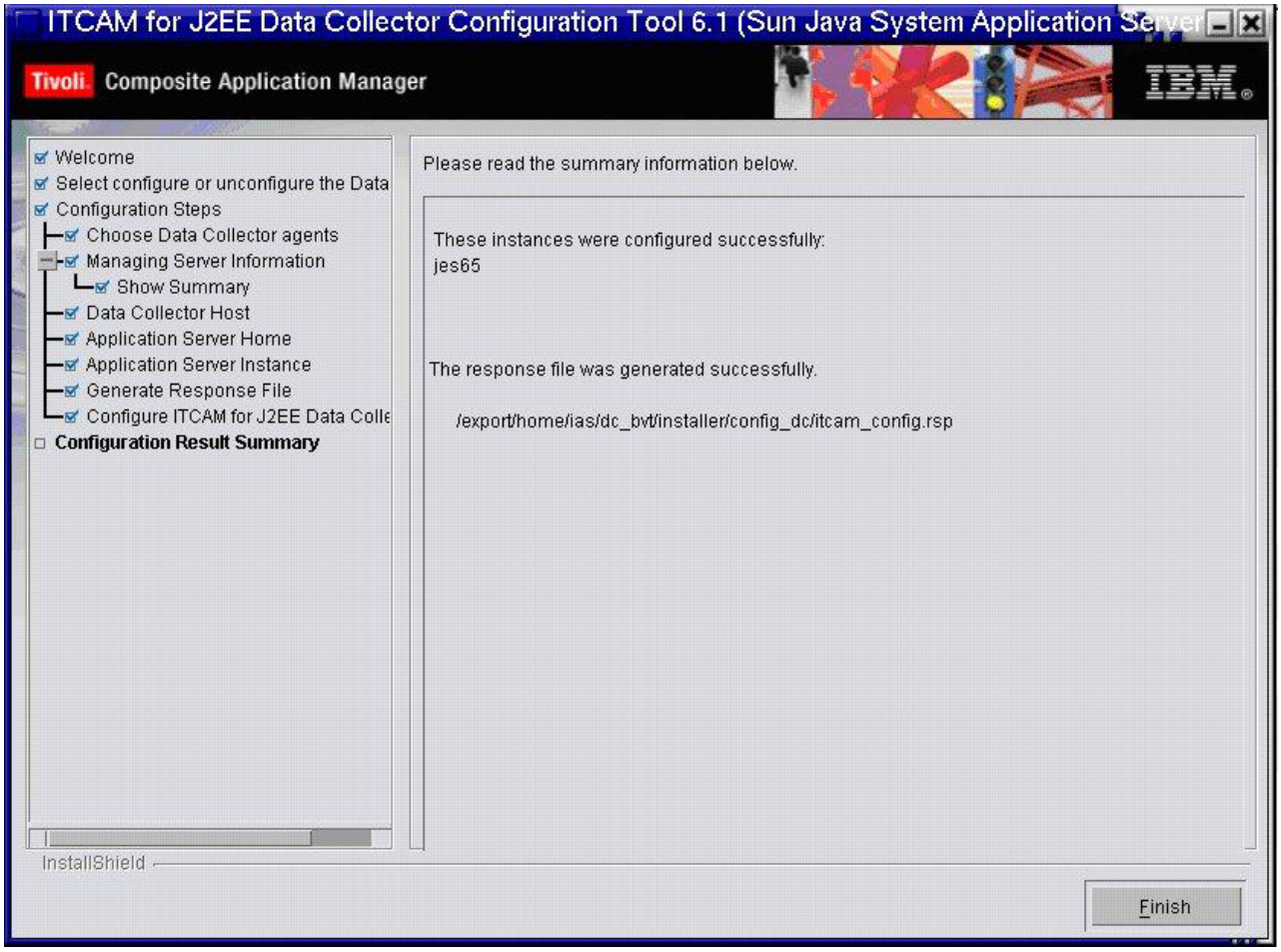



*Figure 62. Configuration results summary*

Read the summary information. The configuration status of the server instance that you selected is shown. Click **Finish** to finalize the configuration and close the Configuration Tool. If you are currently installing the DC, you return to the InstallShield Wizard. There you are prompted to finalize the installation.

## Configuring the Data Collector for JSAS 7 and 8

**Note:** Before you configuring the J2EE Data Collector for JSAS, stop any running server instance.

**Step 8: Specify JSAS-specific information:** Specify the JSAS-specific information in the following window.

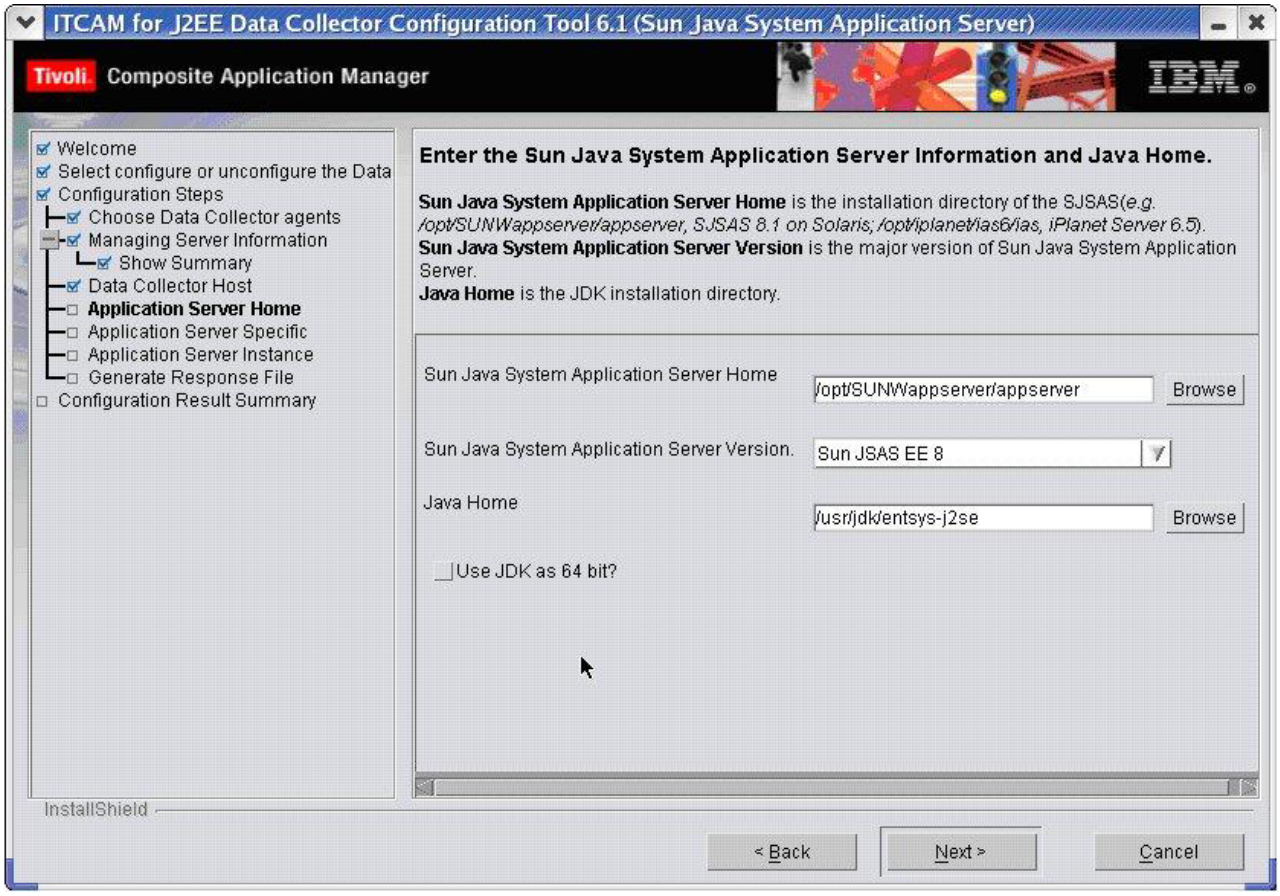



*Figure 63. JSAS-specific information*

In the **Sun Java System Application Server Home** field, click **Browse** to locate the directory in which JSAS has been installed. Select the JSAS version in the **Sun Java System Application Server Version** field. For the **Java Home** field, click **Browse** to locate the JDK that is supporting the application.

Select or clear the checkbox near **Use JDK as 64 bit** as appropriate.

Click **Next**.

**Step 9: Specify parameters for JSAS domain admin server:** This step shows different windows depending on your JSAS version. Select one of the following links as appropriate:

- "Parameters for JSAS 7 domain admin server"
- "Parameters for JSAS 8 domain admin server" on page 143

*Parameters for JSAS 7 domain admin server:* In the following window, specify the parameters for the JSAS 7 domain admin server.

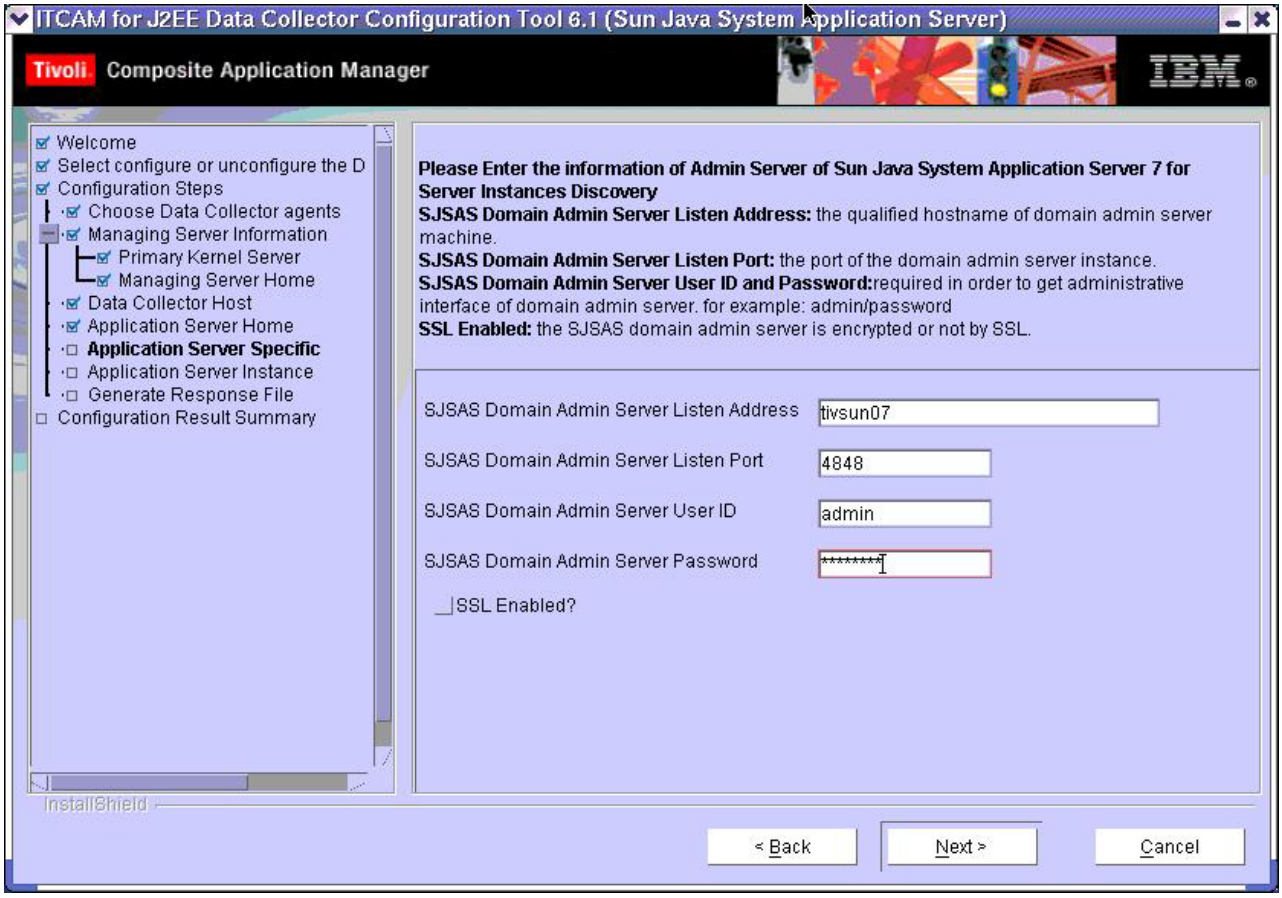



*Figure 64. JSAS 7 domain admin server information*

Specify the the listening IP address or the hostname of the domain admin server in the **SJSAS Domain Admin Server Listen Address** field. Specify the port of the domain admin server instance in the **SJSAS Domain Admin Server Listen Port** field.

Enter the logon user ID and password in the **SJSAS Domain Admin Server User ID** field and **SJSAS Domain Admin Server Password** field.

Select the checkbox near **SSL Enabled** if the SSL for the domain admin server is enabled. Clear it otherwise.

Click **Next** to "Step 10: Select server instances to be configured" on page 144.

*Parameters for JSAS 8 domain admin server:* In the following window, specify the parameters for the JSAS 8 domain admin server.

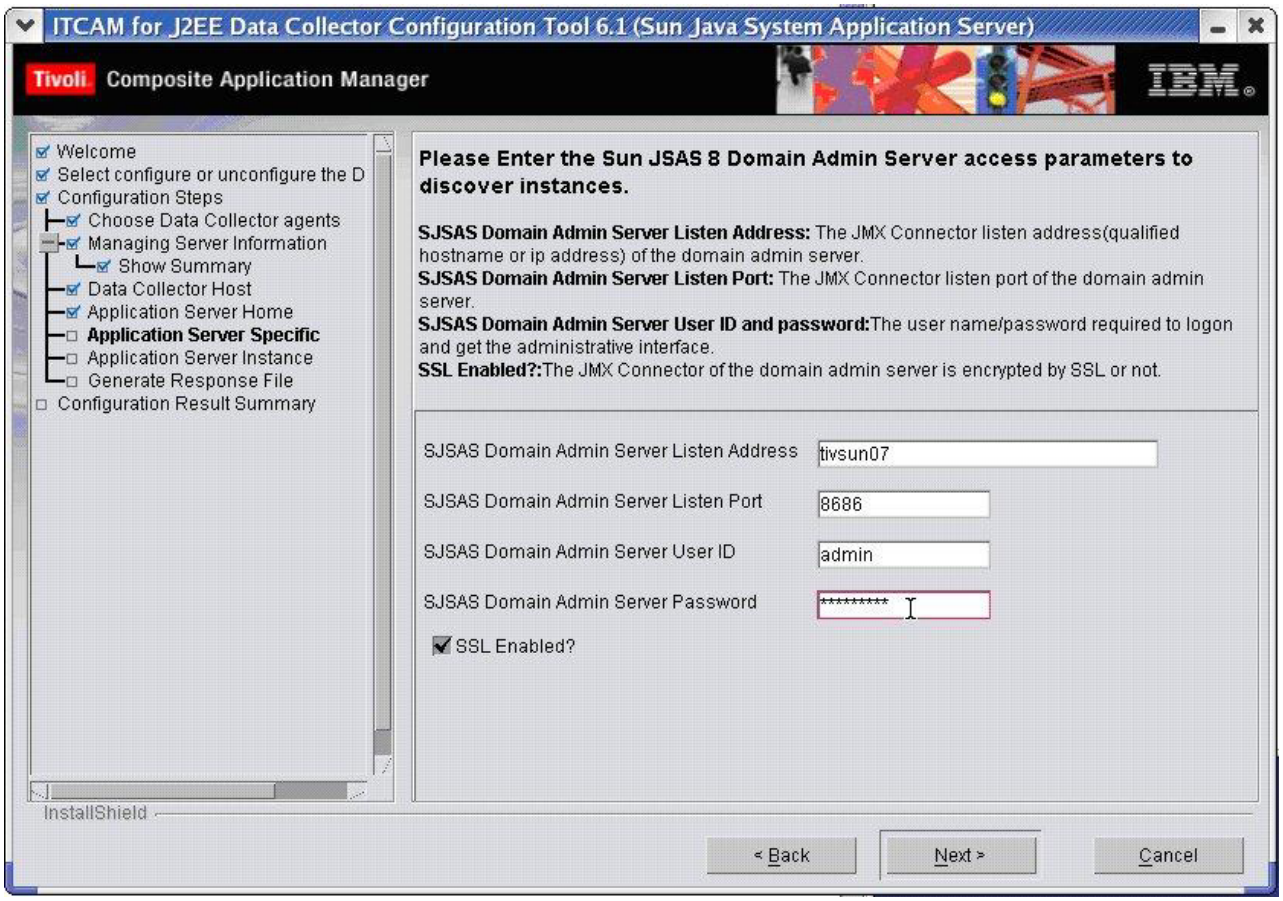



*Figure 65. JSAS 8 domain admin server information*

Specify the Java Management Extensions (JMX) connector listening IP address or the hostname of the domain admin server in the **SJSAS Domain Admin Server Listen Address** field. Specify the JMX connector listening port number of the domain admin server in the **SJSAS Domain Admin Server Listen Port** field.

Enter the logon user ID and password in the **SJSAS Domain Admin Server User ID** field and **SJSAS Domain Admin Server Password** field.

Select the checkbox near **SSL Enabled** if the SSL for the domain admin server is enabled. Clear it otherwise.

Click **Next** to "Step 10: Select server instances to be configured."

**Step 10: Select server instances to be configured:** This window lists all your server instances covered by JSAS. Select the checkboxes near the specific server instances to be configured.

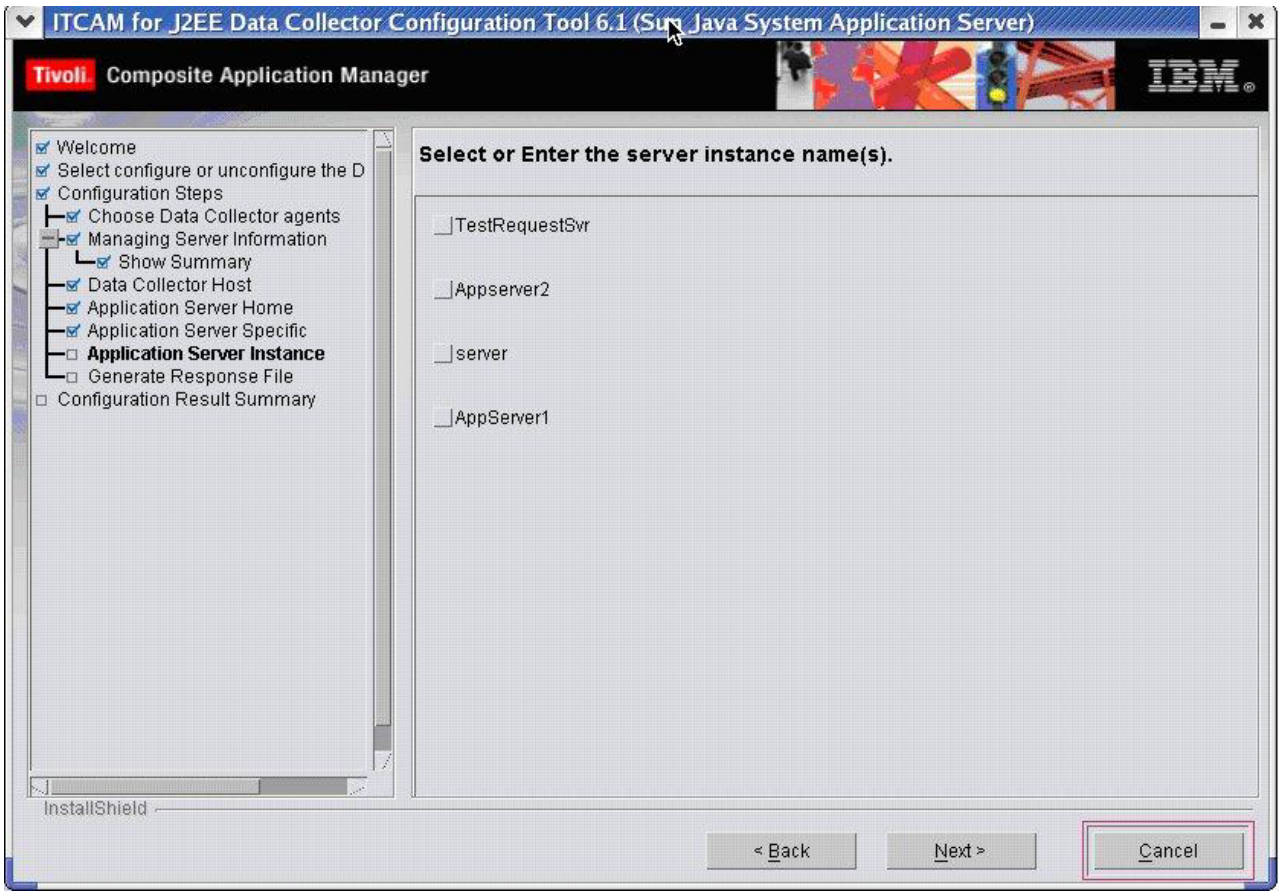



*Figure 66. Server instance information*

After entering the required information, click **Next** to configure the DC.

**Step 11: Generate a response file:** You can choose to generate a response file to save all your settings. You can have the same installation settings when you want to configure the Data Collector on any computer by using a silent installation.

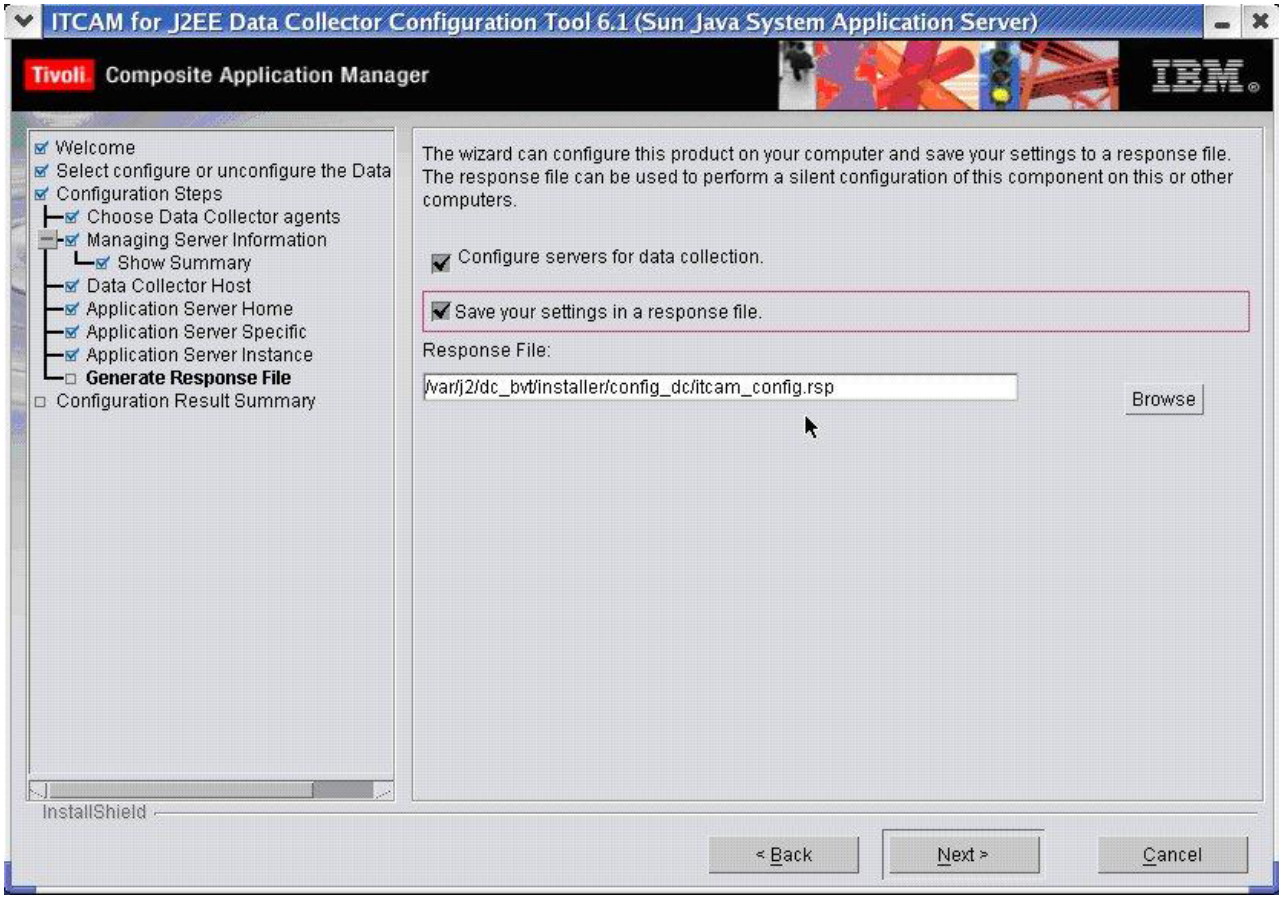



*Figure 67. Choose to save your settings in a response file*

**Configure servers for data collection** is selected by default. If you wish to create a response file with all the settings in this configuration, select **Save your settings in a response file**. Choose a location where the response file is generated.

Click **Next** to proceed.

**Step 12: Finalize the configuration:** After the Data Collector is configured, the following window opens:

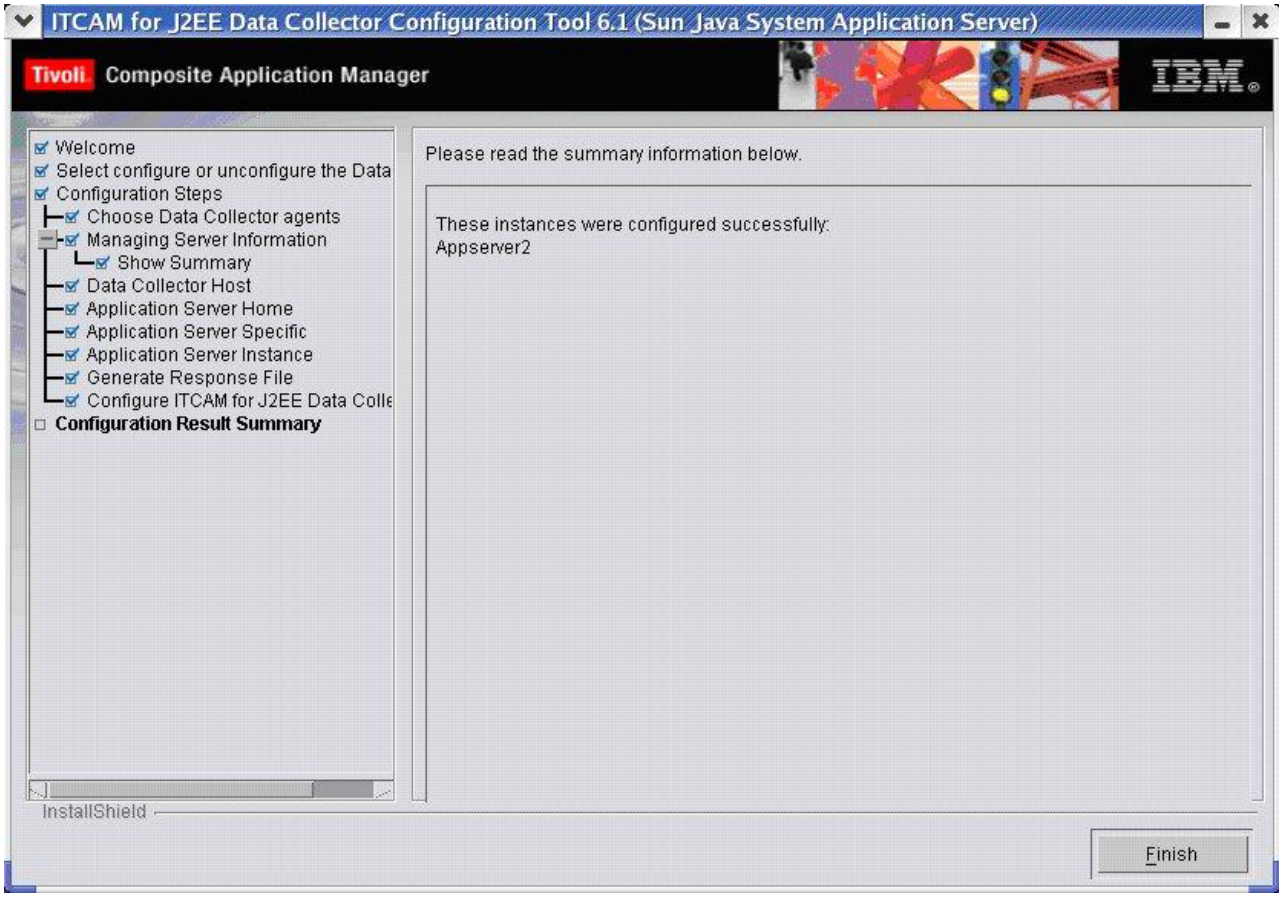



*Figure 68. Configuration results summary*

Read the summary information. The configuration status of the server instance that you selected is shown. Click **Finish** to finalize the configuration and close the Configuration Tool. If you are currently installing the DC, you return to the InstallShield Wizard. There you are prompted to finalize the installation.

## Post-configuration steps for ITCAM for J2EE Data Collector

1. Increase the JVM Maximum Heap Size by at least 128 megabytes.

2. Apply the latest level of maintenance (such as fix packs or interim fixes) from the following Web site:

http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliCompositeApplicationManagerforJ2EE.html

## Post-configuration steps for all application servers using Sun JDK 1.5 or HP JDK 1.5

This applies only if you have installed the Java Virtual Machine Tool Interface (JVMTI) interim fix.

If your application server is using Sun JDK 1.5 (J2EE or Community Edition application servers) or HP JDK 1.5 (J2EE application servers only), you need to set the JVM parameter MaxPermSize to -XX:MaxPermSize=196m or above in order to prevent out-of-memory errors.

## Post-configuration steps for all application servers using Sun JDK

For Sun JDKs, Data Collector configuration enables verbose garbage collection output by -Xloggc JVM argument. By default, the -Xloggc causes JVM to generate class loading and unloading events to native standard output stream, if user chooses to redirect it to log files, it may fill the log files and consume excessive disk space.

To suppress class loading and unloading events, add the *-XX:-TraceClassUnloading -XX:-TraceClassLoading* options to the JVM argument of the application server. Please refer to the administration guide of the application server for instructions on how to add options to JVM arguments.

For more information about the -XX:-TraceClassUnloading -XX:-TraceClassLoading options, refer to:

http://java.sun.com/docs/hotspot/gc1.4.2/faq.html

http://java.sun.com/docs/hotspot/gc5.0/gc_tuning_5.html

## Post-configuration steps for Oracle users

It is necessary to run the "*opmnctl reload*" command after configuring the Data Collector for Oracle application server and before starting the application server instance. Server will fail to start with the following error message if the command is not run after the configuration process.

*java.lang.ClassNotFoundException: com.ibm.tivoli.itcam.oracle.oracle10.sdc.DCStartup*

## Post-configuration steps for Tomcat users

If you want to monitor Java Message Service (JMS), you need to do the following step. Otherwise, skip this post-configuration step.

Put the JMS standard interface library (all the interfaces and classes with package, javax.jms.*) into <*DC_HOME*>/common/lib in UNIX/Linux or <*DC_HOME*>\common\lib in Windows, instead of any other location. In this way, JMS application can be monitored by Tomcat DC.

You need to perform different post-configuration steps for the Tomcat server started by Java Service Wrapper. If you want to reconfigure the DC right after it is unconfigured, continue your reconfiguration and the DC configuration tool will pick up all properties in the itcam_wrapper.conf file and reuse them. If you want to change the wrapper.conf file after the DC is unconfigured, perform this procedure:

1. Manually remove the whole ITCAM Configuration section which begins with the line `###include ITCAM Data Collector Configuration File Begin` and ends with the line `###include ITCAM Data Collector Configuration File End` in the `wrapper.conf` file.

2. If there are missing numbers in JVM arguments after you removed the section above, please follow the Java Service Wrapper guidelines and add the missing properties or change the numbering of other properties to ensure that the `wrapper.conf` file is well formed.
3. Permanently remove the `itcam_wrapper.conf` file from disk.
4. At this time, ITCAM will be completely unconfigured and you can continue your changes on the `wrapper.conf` file.

# Post-configuration steps for WebLogic users

The following post-configuration steps are specific for WebLogic users.

## Restarting and shutting down the application server

Restart your application server to enable the configuration and make sure to shut down the WebLogic application server instance through the Administration Console. For more detailed information about how to shut down the WebLogic application server, refer to the following Web site:

http://docs.oracle.com/cd/E13222_01/wls/docs90/server_start/startquickref.html.

If the configured application server instance is controlled by a Node Manager, restart the Node Manager as well.

If a application server instance in which the Data Collector is configured is an administrative application server instance, some exceptions are produced when the application server is shutting down. Ignore these exceptions.

For users who start the managed server from the Node Manager, the following JVM property must be added:

```
-Dcom.ibm.tivoli.jiti.injector.IProbeInjectorManager=com.ibm.tivoli.itcam.toolkit.
ai.bcm.bootstrap.ProbeInjectorManager
```

## Refreshing the Windows service

On Windows, if WebLogic is installed as a Windows service, you need to refresh the service. The procedure depends on whether WebLogic is started by Node Manager.

If WebLogic is running in Windows service mode, not started by Node Manager:

1. After the Data Collector is configured successfully, if the WebLogic Windows service is running, stop it and run `uninstallService.cmd` .
2. Reinstall the Windows service by using the following command: `InstallService.cmd` *`user_id user_pwd`* .
3. Open the system service window and start the WebLogic server.
4. If any problems occur, find the cache file in directory *domain_dir**instance_dir**.wlnotdelete**extract* and remove the following directories:

   *instance_name*_console_console

   *instance_name*_uddi_uddi

   *instance_name*_uddiexplorer_uddiexplorer

   *instance_name*_wl_management_internal1_wl_management_internal1

   *instance_name*_wl_management_internal2_wl_management_internal2

*domain_dir* refers to the name of the domain, and *instance_name* refers to the server instance name. For example, if you create a basic portal domain named

*portalDomain*, and a server instance named *portalServer*, the cache files would be found in the \portalDomain\portalServer\.wlnotdelete\extract directory.

If WebLogic is running in Node Manager Windows service mode:

1. After the Data Collector is configured successfully, if the Node Manager server service is running, stop it and run `uninstallNodeMgrSvc.cmd` .
2. In the directory *AppServer_home*/server/bin, run `installNodeMgrSvc.cmd` .
3. Open the system service window and start the Node Manager service.

Use Node Manager to start the managed server. You do not have to run `startNodeManager.cmd` .

## Post-configuration steps for JSAS

By default, the CORBA Interceptor for the Data Collector is disabled for Sun JSAS 7 and 8. To enable the CORBA Interceptor for the Data Collector, perform one of the following procedures:

For JSAS 7 and 8.1 EE, manually add the following Java system property to the JVM options for the monitoring server instance:

```
-Dorg.omg.PortableInterceptor.ORBInitializerClass.com.ibm.tivoli.itcam.dc.
  orbinterpretor.Initializer
```

For JSAS 8.2 EE, in the Administration Console, go to the server instance and click **Configuration > ORB > Properties**. Then, manually add the following property and specify the value as `true`:

```
org.omg.PortableInterceptor.ORBInitializerClass.com.ibm.tivoli.itcam.
  dc.orbinterpretor.Initializer
```

## Post-configuration steps for J2SE

### JMX server settings

If there is a custom JMX implementation for the application, write an implementation class to implement JMXEnginePlugin interface. This class must implement the JMXEnginePlugin interface, which is described in Appendix B, "J2SE JMXEnginePlugin interface," on page 203.

In Appendix C, "J2SE JMX plug-in sample," on page 205, there is a sample java file, which shows you how to implement the JMXEnginePlugin interface.

To enable this class, set it in the classpath, and edit *<DC_Home>*/rumtime/*<server_type>*.*<app_name>*.*<host_name>*.*<inst_name>*/dc.properties file, set j2se.jmxe.pluginclass as the custom class name.

If your JDK version is 1.5 and there is no default JMX implementation for the application, append the following information in the startup script of J2SE:

- For users of SUN JRE, append `set ITCAM_JVM_OPTS=%ITCAM_JVM_OPTS% -Dcom.sun.management.jmxremote` to the startup script to enable your remote management.
- For users of IBM JRE, append `set ITCAM_JVM_OPTS=%ITCAM_JVM_OPTS% -Dcom.sun.management.jmxremote.port=0 -Dcom.sun.management.jmxremote.ssl=false -Dcom.sun.management.jmxremote.authenticate=false`.

- For users of BEA JRE, append `set ITCAM_JVM_OPTS=%ITCAM_JVM_OPTS% -Xmanagement`.
-

If you are not using a JDK with version 1.5 or there is a default JMX implementation for the application, ignore this message.

## Edge request setting

There is no default edge request for J2SE DC, configure custom edge request referring to *IBM Tivoli Composite Application Manager User Guide*.

## Enabling special request monitoring

To enable DC to monitor JDO/CTG/MQI/JMX requests, edit the toolkit_custom.properties file in the <*DC_HOME*>\runtime\ appname.instname.hostname.dcname\custom directory.

If you want to monitor CTG requests, set `-Dam.sdc.probe.l1aspectfamily.ctg=CTGASPECTS,both` in your **Java Options**.

If you want to monitor Remote Method Invocation over Internet InterORB Protocol (RMI/IIOP) requests, set

```
-Dorg.omg.PortableInterceptor.ORBInitializerClass.com.ibm.tivoli.itcam.
dc.orbinterpretor.Initializer
```

in your **Java Options**.

# Post-configuration steps for NetWeaver

## Configuring ITCAM for J2EE DC for Netweaver to monitor the system resources

You must make some configuration changes in Netweaver in order to have data reported in System Resources. To enable the system resources monitoring, perform the following steps:

1. Logon the Visual Administrator.
2. Select the target server and then *Services -> Monitoring -> Root*
3. Subnodes are shown after expanding the tree node *Root* and each node attribute represents one type of system resources metric. Please use the following mapping for enabling the metrics displayed in System Resources. After modifying the attribute, go to *Monitoring Configuration* panel, select *Configuration -> Edit -> Save* to save the changes.

*Table 31. Metrics displayed in System Resources*

| **Metric in System Resources** | **Node attribute in Netweaver** |
|---|---|
| Component Performance | Services -> Monitoring -> Root -> Performance -> Application Response Time -> Component Content |
| Request Performance | Services -> Monitoring -> Root -> Performance -> Application Response Time -> Request Content |
| Performance Summary | Services -> Monitoring -> Root -> Performance -> Application Response Time -> Summary Content |

*Table 31. Metrics displayed in System Resources (continued)*

| Metric in System Resources | Node attribute in Netweaver |
|---|---|
| Thread Pool | Services -> Monitoring -> Root -> Kernel -> Application Threads Pool -> *<br><br>Services -> Monitoring -> Root -> Kernel -> System Threads Pool -> * |
| Web Container | Services -> Monitoring -> Root -> Services -> Web Container -> * |
| Entity EJB | Services -> Monitoring -> Root -> Services -> EJB -> Entity Beans -> ** -> *Bean -> * |
| Stateless EJB | Services -> Monitoring -> Root -> Services -> EJB -> Session Stateless Beans -> ** -> *Bean -> * |
| Stateful EJB | Services -> Monitoring -> Root -> Services -> EJB -> Session Stateful Beans -> ** -> *Bean -> * |
| Message EJB | Services -> Monitoring -> Root -> Services -> EJB -> Message Driven Beans -> ** -> *Bean -> * |
| Transaction | Services -> Monitoring -> Root -> Services -> Transactions -> * |
| Memory | Services -> Monitoring -> Root -> Services -> Memory -> * |
| JVM | Services -> Monitoring -> Root -> System -> VM info -> * |
| System | Services -> Monitoring -> Root -> System -> System Properties -> * |
| Web Service Performance | Services -> Web Services -> Performance Data -> ** -> Implementation Time/PostProcessing Time/Preprocessing Time |
| Web Service Request | Services -> Web Services -> Requests Number -> ** -> CurrentClient/FailedRequests/SuccessfulRequests |
| HTTP | Services -> Monitoring -> Root -> Services -> Http Provider -> ** |

## Configuring ITCAM for J2EE DC for NetWeaver to monitor the HTTP session

Configure the HTTP session settings in NetWeaver to obtain live session data in Server Overview and Server Activity Display in the Application Monitor user interface. To configure the HTTP session settings in NetWeaver, perform the following steps:

1. Log in to the Visual Administrator tools.
2. Go to **Server instance > services > monitoring > Services > Web Container > CurrentHttpSessions**.
3. In the **Monitoring Configuration** panel, click **Configuration**.
4. Edit the current HTTP session settings and save the settings.

## Import the JVM parameters of DC for NetWeaver to monitor the server on the distributed dialog instance

This step is only required when you select the installation type as **Distributed dialog instance installation**.

If the ITCAM for J2EE DC is installed on the distributed dialog instance computer, manually configure your DC on central instance computer. Complete this task after the DC configuration steps described in “Configuring the J2EE Data Collector for NetWeaver” on page 109 are finished. Configure the following steps before “Configuring references from J2EE services to Tivoli custom service” on page 153.

1. Log on the central instance computer.
2. Navigate to <*Central instance home*>/j2ee/configtool
3. Edit BatchConfig.bat on Windows platform or BatchConfig.sh on Unix/Linux platforms. Modify the <*Java home*> setting as the <*Java home*> used by the central instance.
4. Navigate to <*Central instance home*>/SDM/program
5. Run config.bat on Windows platforms or config.sh on Unix/Linux platforms. For unconfiguration, run unconfig.bat or unconfig.sh.

**Note:** Before you perform the post configuration steps, it is recommended to save a backup of the database of NetWeaver J2EE Engine.

## Configuring references from J2EE services to Tivoli custom service

You need to set up 6 references of the J2EE services in the NetWeaver server to the Tivoli custom service. The services to be modified are shown in the following table:

*Table 32. Services and related xml files*

| Service name | Related xml file |
|---|---|
| connector | connector-provider.xml |
| naming | naming-provider.xml |
| servlet_jsp | servlet_jsp-provider.xml |
| ejb | ejb-provider.xml |
| jms_provider | jms_provider-provider.xml |
| jmsconnector | jmsconnector-provider.xml |

Apply the following steps to setup the references one by one:

1. Start the J2EE Engine Visual Administrator and connect it to the J2EE Engine.
2. Select **Server** > **Services** > **Configuration Adapter Service**.
3. Select **Runtime** > **Display Configuration**.
4. Select **Edit mode**.
5. Select **cluster_data** > **server/dispatcher** > **cfg** > **services** > <*component_name*>-provider.xml. In the dialog window that is displayed, add the component reference into the configuration of components respectively:

```
<reference type="service" strength="weak">
    tivoli
</reference>
```

.

6. Click **OK** to save your changes.

   **Note:** You need to repeat steps 5 and 6 to set up the references for all the components.
7. Restart the corresponding cluster element.

**CAUTION:**
**The Tivoli service is not undeployed during unconfiguration. You cannot undeploy it because all the Data Collectors share the Tivoli service. If you want to undeploy the Tivoli service, complete the following steps before undeployment.**

- **Unconfigure all Data Collectors from all servers on the corresponding instance.**
- **Remove references from servlet_jsp, naming, ejb, jms_provider, jms_connector, and connector components to Tivoli component. Remove the bidirectional references between the CTG/JDO/IMS/MQI library components and Tivoli service component.**

**Otherwise, the Netweaver server cannot start.**

For more information about how to modify the reference of a component, refer to the *SAP Note (857025)*.

## Configuring ITCAM for J2EE DC for NetWeaver to monitor the CTG/JDO/MQI/IMS

When CICS® Transaction gateway (CTG), Java Data Objects (JDO), Message Queue Interface (MQI), or IMS™ are deployed as libraries, to monitor their request data, perform the following configuration steps.

Make sure that there are bidirectional references between Tivoli service component and CTG/JDO/MQI/IMS library component. For example, if the CTG jars is deployed as the CTGLIB Library, complete the following steps:

1. Start the J2EE Engine Visual Administrator and connect it to the J2EE Engine.
2. Select **Server** > **Services** > **Configuration Adapter Service**.
3. Select **Runtime** > **Display Configuration**.
4. Select **Edit mode**.
5. Select **cluster_data** > **server/dispatcher** > **cfg** > **services** > *<component_name>*-provider.xml. In the dialog window that is displayed, add the component reference before </references>:

   ```
   <reference type="service" strength="weak">
        tivoli
    </reference>
   ```

   .
6. Select **cluster_data** > **server/dispatcher** > **cfg** > **ext** > tivoli-provider.xml. In the dialog window that is displayed, add the component reference before </references>:

   ```
   <reference type="library" strength="weak">
        CTGLIB
    </reference>
   ```

   .
7. Click **OK** to save your changes.

   **Note:** If you want to monitor JDO, MQI, and IMS, repeat steps 5 and 6. Establish bidirectional references between JDO, MQI, or IMS library component and the Tivoli service component.
8. Restart the corresponding cluster element.

**CAUTION:**
**If CTG/JDO/IMS/MQI deployed as libraries in the NetWeaver server and the DC is installed to monitor the server, and you want to undeploy CTG/JDO/IMS/MQI library components, remove the bidirectional references between Tivoli service component and the library components to be undeployed. Otherwise, the Netweaver server cannot start.**

For more information about how to modify the references of a component, refer to the *SAP Note (857025)*.

## Additional post-configuration tasks

Perform the following steps:

1. Restart the instance of the application server that will be monitored by the Data Collector.

   If the application server fails to start up, Data Collector configuration has failed. See 2.
2. You know the Data Collector configuration has failed if any of the following has occurred:
   - After the configuration, the application server fails to restart.
   - During a GUI configuration, the summary panel for the Configuration Tool indicates the configuration has failed.
   - During a silent configuration, the command line indicates a message that the configuration has failed.
   - After the configuration, there are messages in the Tivoli common log file that indicates configuration has failed.
3. Perform the tasks described in each of the following sections, if applicable.
4. If Terminal Services is enabled on **Windows 2000** or **Windows 2003 Server**, run the following from a command prompt:

   ```
   change user /execute
   ```

### Distinguishing log files for multiple Data Collectors installed on the same server

When multiple Data Collectors are installed on the same server, you need to configure them to write to different log files:

1. In *instance_runtime_directory*/cyn-cclog.properties, for each of the Data Collectors, change the file names for handler.file.dc.msg.fileName and handler.file.dc.trace.fileName to be different from the file names for the other Data Collectors.
2. In *instance_runtime_directory*/cynlogging.properties, for each of the Data Collectors, change the file names for CYN.handler.file.trc.fileName and CYN.handler.file.msg.fileName to be different from the file names for the other Data Collectors.

### Enabling instrumentation and monitoring of RMI/IIOP requests between two application servers

If two application servers are using Remote Method Invocation over Internet InterORB Protocol (RMI/IIOP), and you need to enable instrumentation and monitoring of RMI/IIOP requests and view correlation icons in the Application

Monitor user interface, both servers must be instrumented by Data Collectors connected to the same Managing Server. Also, for both application servers, you must set an additional JVM parameter.

On each of the hosts, use your Application Server to add the following parameter for the Java Virtual Machine:

```
-Dorg.omg.PortableInterceptor.ORBInitializerClass.com.ibm.tivoli.itcam.dc.
  orbinterpretor.Initializer
```

## JDK 1.4.2: enabling Java core dumps and heap dumps

If you have JDK 1.4.2 J9, you need to perform the procedure in this section.

J9 is typically used on the following platforms:

- 1.4.2 JDK, 64 bit AMD64 on **Windows** and **Linux**
- 1.4.2 JDK, 32 bit i386. (J9 JVM is used only if the -Xj9 JVM option is specified.)

One way to check whether you have J9 is to check the system out log (typically SystemOut.log) for a line that contains `J2RE 1.4.2 IBM J9`.

Use your Application Server to add the following parameter for the Java Virtual Machine:

```
-Xtrace
```

If you do not have JDK 1.4.2 J9: contact IBM Software Support for additional assistance on creating Java core dumps or heap dumps.

## More than one Data Collector installed on a server with a firewall enabled: setting a range of port numbers

The configuration program requires you to set unique port numbers for probe.rmi.port and probe.controller.rmi.port. Communication problems with the Managing Server arise if ports for separate Data Collectors installed on a server with a firewall are not unique. If you have many Data Collectors, it might be difficult to set unique ports for all the Data Collectors.

Instead of ensuring that individual port numbers assigned for each of the Data Collectors are unique, you can set a range of port numbers in the Data Collectors' properties files. The following procedure resets the individual port numbers entered during the configuration to a range of port numbers:

For each Data Collector, in the *custom_directory*/datacollector_custom.properties file, set the following properties:

```
probe.rmi.port=range_of_port_numbers
probe.controller.rmi.port=range_of_port_numbers
```

For example,

```
probe.rmi.port=8200-8299
probe.controller.rmi.port=8300-8399
```

If you use the same range for both properties, make sure that range is larger than or equal to twice the number of Data Collectors installed on the server.

## Unix/Linux: If you used the root ID for the Data Collector installation and the application server is not owned and operated by the root ID

On Unix/Linux, you may use the root user ID to perform Data Collector installation. The installer will have the authority to use whatever directories and files it requires, and will be able to find most application server installations on the server. But, if the application server is not owned and operated by root ID, you will need to finish the following tasks, in order for the Data Collector to work correctly:

1. Use the chown command to turn over the Data Collector installation from root to the application server owner ID:

   ```
   chown -R serverOwnerId:serverGroupId DC_home
   ```

2. Make sure that the application server owner ID can write to the /var/ibm/tivoli/common/CYN directory:

   ```
   chown -R serverOwnerId:serverGroupId /var/ibm/tivoli/common/CYN
   ```

## What to do next

You have completed configuration of the Data Collector. Complete the following steps:

1. Restart the instance of the application server that is monitored by the Data Collector.
2. If it is not already running, start the Managing Server and the Application Monitor user interface.
3. See "Verifying the installation and configuration."

# Verifying the installation and configuration

This section describes how to verify the installation and configuration of Data Collectors.

**Notes:**

1. You cannot perform these verification steps without having installed a Managing Server. If you have not already done so, install a Managing Server. See the following section:*IBM Tivoli Composite Application Manager: Managing Server Installation and Customization Guide*
2. In the final steps for "Additional post-configuration tasks" on page 155, you should have already completed the following steps:
   a. Restart the instance of the application server that will be monitored by the Data Collector.
   b. If it is not already running, start the Managing Server and the Application Monitor user interface.

## Procedure

Perform the following procedure to verify the installation and configuration:

1. Verify installation of the Data Collector. This procedure shows Data Collector details, including the administrative server name, application server name, and platform:
   a. From the Application Monitor user interface, click **Administration > Server Management > Data Collector Configuration > Unconfigured Data Collectors**.

b. Check to see that the server for the Data Collector is listed.

2. Apply a configuration to the Data Collector in the Application Monitor user interface: see the topic on configuring a Data Collector in the online helps.
3. Verify that the Data Collector components are enabled and running in the Self-Diagnosis page of the Application Monitor user interface. See the topic on viewing the Self-Diagnosis for the Data Collector Controller in the online helps.
4. Verify that the Data Collector is communicating with the Managing Server: see the topic on viewing a stack trace in the online helps.

## What to do next

After you have started monitoring your application servers with this product, ensure that you perform periodic maintenance on the Managing Server. See the chapter on maintaining the monitoring environment in the *IBM Tivoli Composite Application Manager: Managing Server Installation and Customization Guide*. Perform the following optional steps:

1. Customize the Data Collector, see Chapter 5, "Customization and advanced configuration for the Data Collector," on page 159.
2. Install a language pack, see Chapter 7, "Installing and uninstalling a Language Pack," on page 195.

# Chapter 5. Customization and advanced configuration for the Data Collector

This section contains instructions for customizing your configuration of the Data Collector (DC).

## Fine-tuning datacollector.properties

To best suit the needs of your environment, you can fine-tune the settings in the Data Collector properties file. The name of this file depends on the application server:

*Table 33. Locations of the Data Collector properties file*

| | |
|---|---|
| WebLogic | If the monitored server instance is represented by a weblogic machine:<br><br>*DC_home*/runtime/wls*app_server_version.domain_name.machine_name.instance_name*/<br>wls*app_server_version.domain_name.machine_name.instance_name*.datacollector.properties<br><br>else:<br><br>*DC_home*/runtime/wls*app_server_version.domain_name.host_name.instance_name*/<br>wls*app_server_version.domain_name.host_name.instance_name*.datacollector.properties |
| Tomcat | *DC_home*/runtime/tomcat*app_server_version.host_name.instance_name*/*DC_home*/runtime/<br>tomcat*app_server_version.host_name.instance_name*.datacollector.properties |
| Sun Java System Application Server (JSAS) | *DC_home*/runtime/sjsas*app_server_version.domain_name.node_name.instance_name*/<br>sjsas*app_server_version.domain_name.node_name.instance_name*.datacollector.properties |
| JBoss | *DC_home*/runtime/jboss*app_server_version.host_name.instance_name*/<br>jboss*app_server_version.host_name.instance_name*.datacollector.properties |
| NetWeaver | *DC_home*/runtime/netweaver*app_server_version.sap_node_ID_host_name.sap_instance_number*/<br>netweaver*app_server_version.sap_node_ID_host_name.sap_instance_number*.datacollector.properties |
| Oracle | *DC_home*/runtime/oracle*app_server_version.host_name.node_name.instance_name*/<br>oracle*app_server_version.host_name.node_name.instance_name*.datacollector.properties |
| J2SE | *DC_home*/runtime/j2se.*application_name.host_name.instance_name*/*DC_home*/runtime/<br>j2se.*application_name.host_name.instance_name*.datacollector.properties |

However, to facilitate future upgrades, do not change this file. Instead, add the settings you want to modify to the Data Collector custom properties file *custom_directory*/datacollector_custom.properties; this custom properties file overrides the values in the Data Collector properties file.

The following properties are in the Data Collector properties file. Only the properties that are recommended for you to modify are listed.

**kernel.codebase**
The value of this property is filled in during installation time by the installer. It specifies where the Managing Server codebase can be found.

**kernel.rfs.address**
The value of this property is filled in during installation time by the installer. This value is used by the Application Monitor to locate the Managing Server components.

**probe.library.name**

The default value is am. This property specifies the name of the native shared library which the Data Collector needs to run. If the value of the property is am, the Data Collector searches for a shared library. This shared library is named libam.so on UNIX platforms and libam.dll on the Windows platform. In normal cases, this property does not need to be specified or changed from the default. Only when the user needs to run a native shared library with a different name does this property need to change.

Example:

```
probe.library.name=am
```

**internal.probe.event.packet.size**

The default value is 70 or (70 X 1024 kbytes). Changing to below the default is not recommended. Valid values are 1 - 4000000 (or up to available process memory on the server). This property specifies the size of the Data Collector's internal send buffer. The send buffer controls how much data the Data Collector can be sent to the Publish Server at a given time. In normal situations, this property does not have to be changed, as the default send buffer size is more than adequate. However, if the user sees a problem with the amount of data the Data Collector sends to the Publish Server, this property can be set to configure the size of the send buffer.

**internal.memory.limit**

The default value is 100 (MB). This property limits the amount of memory the Data Collector can use.

**internal.memory.accept.threshold**

The default value is 2 (MB). This property specifies the minimum free memory after which the Data Collector starts accepting data once it reaches the upper limit. The upper limit is specified by the internal.memory.limit property.

**internal.url.limit**

The default value is 1000. This property controls the maximum URL length accepted by the Data Collector.

**internal.sql.limit**

The default value is 5000. This property controls the maximum SQL length accepted by the Data Collector.

**internal.probe.event.queue.size.limit**

The default value is 900000. This property controls the maximum size of the queue of events maintained by the Data Collector. When the queue is full, the Data Collector drops events.

**internal.lockanalysis.collect.L*n*.lock.event**

The variable *n* can represent Mod L1, L2, or L3. Possible values are true or false. This parameter controls whether lock acquisition/release events are collected. The recommended setting at all levels is false as there is little benefit in displaying lock acquisition events if they are not experiencing contention.

Example:

```
internal.lockanalysis.collect.L1.lock.event = false
```

**internal.lockanalysis.collect.L*n*.contend.events**

The variable *n* can represent Mod L1, L2, or L3. Possible values are true, false, or justone. This parameter controls whether lock contention events are collected.

True indicates contention records are collected. For each lock acquisition request that results in contention, a pair of contention records is written. These records are written for each thread that acquired the lock ahead of the requesting thread. False indicates contention records are not written. Justone indicates contention records are written. However, a maximum of one pair of contention records are written for each lock acquisition request that encounters contention. This event occurs regardless of how many threads actually acquired the lock prior to the requesting thread.

Setting this parameter to true enables you to determine the problem. You can check if a single thread is holding a lock for an excessive time, or if the problem is due to too many threads all attempting to acquire the same lock simultaneously. The recommended setting at L1 is false. The recommended setting at L2 is justone. This setting enables you to collect just one pair of contention records for each lock acquisition that encountered contention. The recommended setting at L3 is true but for a limited time to reduce performance cost. This setting enables you to identify every thread that acquired the lock ahead of the requesting thread.

Example:

```
internal.lockanalysis.collect.L2.contend.events = justone
```

**internal.lockanalysis.collect.L*n*.contention.inflight.reports**

The variable *n* can represent Mod L1, L2, or L3. Possible values are true or false. This parameter controls whether data is collected for the Lock Contention report. The recommended setting at L1 is false. The recommended setting at L2 and L3 is true.

Example:

```
internal.lockanalysis.collect.L3.contention.inflight.reports = true
```

**deploymentmgr.rmi.port**

It is not necessary to define the property deploymentmgr.rmi.port if you are running a stand-alone application server. This property is needed for version 5 application server clusters or application servers controlled by a Deployment Manager.

Example:

```
deploymentmgr.rmi.port=<Deployment Manager RMI (bootstrap) port>
```

**deploymentmgr.rmi.host**

It is not necessary to define the property deploymentmgr.rmi.host if you are running a standalone application server. This property is needed for version 5 application server clusters or application servers controlled by a deployment manager.

Example:

```
deploymentmgr.rmi.host=<Deployment Manager host>
```

**networkagent.socket.resettime**

The default is no reset. Time interval after which the connection between the Data Collector and the Publish Server is reset.

Example:

```
networkagent.socket.resettime=-1
```

**am.mp.cpuThreshold**
The default is 30 milliseconds. Only the methods which take at least the minimum amount of CPU time specified in this property are captured for method profiling data. This property avoids unnecessary clutter. Generally, methods with greater than the value specified in this property are considered useful. Customers can reduce or increase this value if needed.

**am.mp.clockThreshold**
The default is 30 milliseconds. Only the methods which take at least the minimum amount of wall clock time specified in this property are captured for method profiling data. This property avoids unnecessary clutter. Generally, methods with greater than the value specified in this property are considered useful. Customers can reduce or increase this value if needed.

**am.mp.leagueTableSize**
The default is 1000. This value is the maximum number of methods that are monitored for method profiling data. Customers can reduce or increase this value if needed. Decreasing this value helps in reducing memory requirements.

**am.mp.methodStackSize**
The default is 100. This value is the maximum stack size of any running thread that is recorded in method profiling.

**am.mp.threadSize**
The default is 1000. This value is the maximum running thread size that can be monitored at any instance of time.

**dc.turbomode.enabled**
The default setting is `true`, which enables turbo mode.

By default, the Data Collector limits the amount of native memory it uses to 100 MB, see the description of internal.memory.limit on page "internal.memory.limit" on page 160. The Data Collector enters turbo mode when the Data Collector native memory use exceeds 75% of the native memory limit, by default 75 MB. (You can adjust this percentage with turbo.mem.ulimit to adjust the percentage. However, do not set turbo.mem.ulimit unless directed by IBM Software Support.) The behavior when the memory utilization is below 75 MB is the same whether turbo mode is enabled or disabled.

*Behavior when dc.turbomode.enabled is enabled and the Data Collector is in turbo mode*

When the Data Collector switches to turbo mode, a message `Switching to Turbo Mode` is logged in the trace-dc-native.log file.

In turbo mode, the Data Collector stops monitoring new requests and holds existing requests. It also switches Network Agent and Event Agent threads to the higher priorities specified by the na.turbo.priority and ea.turbo.priority properties respectively. It also lowers the sleep time of the Event Agent and Network Agent threads specified by the ea.turbo.sleep and na.turbo.sleep properties respectively. All these actions are done to drain the native memory quickly by sending accumulated event data to the Publish Server.

In turbo mode, if a new request comes in, the Data Collector simply does not monitor the new request. It continues to monitor the already running requests. The Data Collector notifies the Publish Server that a new request was not monitored when in turbo mode. A notification is sent to the

Managing Server for every new request that is not monitored by sending a dropped record. The Publish Server in turn reflects this status in Publish Server corrupted request counters obtained through `amctl.sh ps1 status`.

When turbo mode is enabled, data in the Application Monitor user interface is always accurate. The accuracy comes at the cost of pausing application threads for a few seconds.

*Behavior when dc.turbomode.enabled is enabled and the Data Collector is in normal mode*

The Data Collector switches back to normal mode, when the Data Collector native memory use falls below 75% of the limit. When the switch to normal mode happens, the Data Collector releases the requests that were placed on hold while switching to turbo mode. The Data Collector resumes monitoring all requests from then on.

When the Data Collector switches to normal mode, a message `Switching to Normal Mode` is logged in the trace-dc-native.log file. It also logs memory utilization and a time stamp.

*Behavior when dc.turbomode.enabled is disabled*

A value of `false` disables turbo mode. When turbo mode is disabled, the Data Collector does not pause the application thread when the native memory use exceeds 75% of the limit. Instead, it drops the accumulated diagnostic data instead of sending it to the Managing Server. Therefore, the data shown in the Application Monitor user interface is incomplete. But the response time of the application threads is not negatively impacted. An appropriate message indicating data is dropped is logged in msg-dc-native.log and trace-dc-native.log. The Managing Server discards all the diagnostic data gathered for the request when the Data Collector drops records related to that request.

*Disabling dc.turbomode.enabled*

The default setting is `true`, which enables turbo mode.

If any of the following conditions apply, disable turbo mode by setting dc.turbomode.enabled to `false`:

- Within the first 10 minutes after starting the Data Collector, it goes into turbo mode (search for the message `Switching to Turbo Mode` in trace-dc-native.log).
- You do not want your applications to be paused temporarily as the Data Collector native memory exceeds 75% of the limit. Disabling turbo mode comes at the cost of losing the monitoring data when this boundary condition is reached.

An alternative is increasing the internal.memory.limit to allow more native memory use. This increase is done at the risk of requesting more native memory from the JVM than what is available. In this event, the JVM issues OutOfMemory errors. See the description of internal.memory.limit on page "internal.memory.limit" on page 160.

## Changing the Managing Server that connects to the Data Collector

If you want to change the Managing Server for your Data Collector, complete the following steps:

1. Log on to the computer where you installed the Data Collector using the user that performed the installation.

2. Start the instance of the application server that is being monitored by the Data Collector.
3. If it is not already running, start the new Managing Server for your Data Collector.
4. Run the Data Collector Configuration Tool. Perform the instructions in Chapter 4, “Configuring the ITCAM for J2EE Data Collector,” on page 83.

   Make sure that you enter information in the windows that applies to the new Managing Server for your Data Collector.
5. Restart the instance of the application server that is being monitored by the Data Collector.

## Configuring the Data Collector after changing the application server version

If you change the version of the application server being monitored by the Data Collector, you must reconfigure the Data Collector to point to the updated instance of the application server.

Complete the following steps:

1. Log on to the computer where you installed the Data Collector using the user that performed the installation.
2. Start the instance of the application server that is being monitored by the Data Collector.
3. If it is not already running, start the Managing Server for your Data Collector.
4. Use the Data Collector Configuration Tool to unconfigure the Data Collector. See “Unconfiguring the server instances” on page 185 for instructions for unconfiguring the Data Collector with the Configuration Tool.
5. Run the Data Collector Configuration Tool to reconfigure the Data Collector. Perform the instructions in Chapter 4, “Configuring the ITCAM for J2EE Data Collector,” on page 83.
6. Restart the instance of the application server that is being monitored by the Data Collector.

## Changing the IP address of the Data Collector host computer

To change the IP address of the Data Collector host computer, perform the following procedure:

1. Use the Data Collector Configuration Tool to unconfigure the Data Collector. See “Unconfiguring the server instances” on page 185 for instructions for unconfiguring the Data Collector with the Configuration Tool.
2. If the instance of the application server that is being monitored by the Data Collector is not stopped, stop it.
3. Perform the IP address change at the operating system and network level.
4. Run the Data Collector Configuration Tool to reconfigure the Data Collector. Perform the instructions in Chapter 4, “Configuring the ITCAM for J2EE Data Collector,” on page 83.
5. If the instance of the application server that is being monitored by the Data Collector is not started, start it.

## Moving the Data Collector to a different host computer

The following prerequisites are required if you want to move the Data Collector to a different host computer while keeping the same Probe ID and Controller ID:

- Host A and host B must have the same configuration at the operating system level.
- You must move the same version of the Data Collector from host A to host B.

To maintain the Probe ID and Controller ID when moving to another physical host, you need to use the ID file:

*Table 34. Locations of the ID file*

| | |
|---|---|
| WebLogic | If the monitored server instance is represented by a weblogic machine:<br><br>*DC_home*/runtime/wls*app_server_version.domain_name.machine_name.instance_name*/wls*app_server_version.domain_name.machine_name.instance_name*.id<br><br>else:<br><br>*DC_home*/runtime/wls*app_server_version.domain_name.host_name.instance_name*/wls*app_server_version.domain_name.host_name.instance_name*.id |
| Tomcat | *DC_home*/runtime/tomcat*app_server_version.host_name.instance_name*/*DC_home*/runtime/tomcat*app_server_version.host_name.instance_name*.id |
| Sun Java System Application Server (JSAS) | *DC_home*/runtime/sjsas*app_server_version.domain_name.node_name.instance_name*/sjsas*app_server_version.domain_name.node_name.instance_name*.id |
| JBoss | *DC_home*/runtime/jboss*app_server_version.host_name.instance_name*/jboss*app_server_version.host_name.instance_name*.id |
| NetWeaver | *DC_home*/runtime/netweaver*app_server_version.sap_node_ID_host_name.sap_instance_number*/netweaver*app_server_version.sap_node_ID_host_name.sap_instance_number*.id |
| Oracle | *DC_home*/runtime/oracle*app_server_version.host_name.node_name.instance_name*/oracle*app_server_version.host_name.node_name.instance_name*.id |
| J2SE | *DC_home*/runtime/j2se.*application_name.host_name.instance_name*/*DC_home*/runtime/j2se.*application_name.host_name.instance_name*.id |

*Table 35. ID file name*

| | |
|---|---|
| WebLogic | If the monitored server instance is represented by a weblogic machine:<br><br>*DC_home*/runtime/wls*app_server_version.domain_name.machine_name.instance_name*.id<br><br>else:<br><br>*DC_home*/runtime/wls*app_server_version.domain_name.host_name.instance_name*.id |
| Tomcat | *DC_home*/runtime/tomcat*app_server_version.host_name.instance_name*.id |
| Sun Java System Application Server (JSAS) | *DC_home*/runtime/sjsas*app_server_version.domain_name.node_name.instance_name*.id |
| JBoss | *DC_home*/runtime/jboss*app_server_version.host_name.instance_name*.id |
| NetWeaver | *DC_home*/runtime/netweaver*app_server_version.sap_node_ID_host_name.sap_instance_number*.id |
| Oracle | *DC_home*/runtime/oracle*app_server_version.host_name.node_name.instance_name*.id |
| J2SE | *DC_home*/runtime/j2se.*application_name.host_name.instance_name*.id |

Perform the following procedure:

1. On host A, stop the instance of the application server that is being monitored by the Data Collector.
2. On host B, install the Data Collector and configure it using the Application Monitor user interface. Configuring the Data Collector generates the ID file and other Data Collector runtime property files.
3. On host B, unconfigure the Data Collector. This step deletes all information about this Data Collector from the ITCAM for J2EE database.
4. On host B, stop the instance of the application server that is being monitored by the Data Collector.
5. Copy the contents in the ID file of host A to the ID file of host B.
6. On host B, save the ID file.
7. On host B, start the instance of the application server that is being monitored by the Data Collector.

The Data Collector on host B assumes the identity of the Data Collector on host A and is configured with the runtime configuration of the Data Collector on host A.

## Controlling Instrumentation of Application Classes for Memory Leak, Lock, and L3 Method Analysis

ITCAM for J2EE uses a technique called Byte Code Instrumentation (BCI). BCI collects Level 3 tracing data, Memory Leak Diagnosis data, and Lock Contention data from your applications. BCI is enabled by adjusting properties in the *custom_directory*/toolkit_custom.properties file.

Making these adjustments activates the use of one or more configuration files in the *DC_home*/itcamdc/etc directory, which contain the default settings to control BCI. The configuration files are described in the following table:

*Table 36. BCI Configuration Files*

| File Name | Purpose | Default Behavior |
|---|---|---|
| method_entry_exit.xml | Defines application method entry and exit BCI | All non-trivial methods for all application classes are Byte-Code-Instrumented for method entry and exit analysis. |
| memory_leak_diagnosis.xml | Defines application Memory Leak Diagnosis BCI | Heap allocations for all classes instantiated by all application classes are Byte-Code-Instrumented. |
| lock_analysis.xml | Defines application lock analysis BCI | Lock acquire and release requests for all application classes are Byte-Code-Instrumented. |

If you want to enable one or more of the BCI features with the default settings, see "Enabling BCI features with default settings" on page 167.

If you want to customize the default settings and choose what classes and methods to modify, see one or more of the following sections:

- "Customizing L3 Method Entry and Exit Analysis" on page 167
- "Customizing Memory Leak Diagnosis" on page 168
- "Customizing Lock Analysis" on page 170

## Enabling BCI features with default settings

Perform the following procedure to enable one or more of the BCI features with the default settings:

1. In the *custom_directory*/toolkit_custom.properties file, uncomment one or more of the following lines by removing the number sign (#) at the beginning of the line:

   ```
   am.camtoolkit.gpe.customxml.L3=DC_home/itcamdc/etc/method_entry_exit.xml
   am.camtoolkit.gpe.customxml.leak=DC_home/itcamdc/etc/memory_leak_diagnosis.xml
   am.camtoolkit.gpe.customxml.lock=DC_home/itcamdc/etc/lock_analysis.xml
   ```

   See Table 36 on page 166 for a description of the default behaviors when each of these configuration files is activated.

2. Set one or more of the following properties to true:

   ```
   com.ibm.tivoli.itcam.toolkit.ai.enablememoryleakdiagnosis=true
   com.ibm.tivoli.itcam.toolkit.ai.methodentryexittrace=true
   com.ibm.tivoli.itcam.toolkit.ai.enablelockanalysis=true
   ```

## Customizing L3 Method Entry and Exit Analysis

Perform the following procedure to enable L3 method entry and exit analysis with customized settings:

1. Make a copy of the *DC_home*/itcamdc/etc/method_entry_exit.xml file, and open it up in a text editor.
2. Modify the parameters in the method_entry_exit.xml file. The following table describes the parameters you can modify:

*Table 37. Parameters for L3 Method Entry and Exit Analysis Configuration File*

| Tag Name | Description |
|---|---|
| methodSelection | Defines the classes and methods to be modified. By default, all classes and methods are selected. By modifying the className and methodName tags within the methodSelection tag, you can implement a more granular selection. Each methodSelection tag must contain exactly one className tag, and one or more methodName tags. Multiple methodSelection tags can be specified. |
| className | Identifies the name of a class or classes to be modified. Each methodSelection tag must contain exactly one className tag. |
| methodName | Identifies a method or method within the class or classes identified by the className tag to be modified for entry/exit tracing. Each methodSelection tag must contain one or more methodName tags. |

Both the className and the methodName tags can include wildcard characters. The following summary describes how the wildcard characters work:

- Asterisk (*) stands for zero or more occurrences of any character when used by itself. When embedded within a sequence of characters (for example, `java.*.String`), it matches zero or more occurrences of any character except the package separator (.).
- Two periods (..) can be used to specify all sub-packages (for example, `java..String` matches `java.lang.String`). It matches any sequence of characters that starts and ends with the package separator (.).
- If the method name begins with an exclamation point (!), any methods that match the method name are specifically excluded from BCI for entry and exit tracing. This is useful for indicating that all methods within a class or group of classes are to be Byte-Code-Instrumented except for those methods that are specifically excluded.

For example, an application with a package name of com.mycompany.myapp has the following requirements:

- Within the Customer class, all methods should be Byte-Code-Instrumented.
- Within the Supplier class, all methods should be Byte-Code-Instrumented except for those methods beginning with the `get` or `set`.

The following example shows the contents of the customized method_entry_exit.xml file that accomplishes this:

```
<aspect>
  <type>application</type>
  <name>com.ibm.tivoli.itcam.toolkit.ai.aspectj.apptrace.EntryExitAspect</name>
  <enabledProperty>
         com.ibm.tivoli.itcam.toolkit.ai.methodentryexittrace</enabledProperty>
   <defaultEnabled>true</defaultEnabled>
   <methodSelection>
        <className>com.mycompany.myapp.Customer</className>
        <methodName>*</methodName>
   </methodSelection>
   <methodSelection>
        <className>com.mycompany.myapp.Supplier</className>
        <methodName>!get*</methodName>
        <methodName>!set*</methodName>
   </methodSelection>
</aspect>
```

3. Complete one of the following steps:
   - Save the file in the *custom_directory*, then complete the following steps:
     a. In the *custom_directory*/toolkit_custom.properties file, uncomment the following line by removing the number sign (#) at the beginning of the line:

        ```
        am.camtoolkit.gpe.customxml.L3=DC_home/itcamdc/etc/method_entry_exit.xml
        ```

     b. Change this line by replacing the path with just the file name of the file you modified in Step 2 on page 167.
     c. Set the following property to true:

        ```
        com.ibm.tivoli.itcam.toolkit.ai.methodentryexittrace=true
        ```

   - Save the file in any directory on your server, then complete the following steps:
     a. In the *custom_directory*/toolkit_custom.properties file, uncomment the following line by removing the number sign (#) at the beginning of the line:

        ```
        am.camtoolkit.gpe.customxml.L3=DC_home/itcamdc/etc/method_entry_exit.xml
        ```

     b. Change this line by specifying the path and name for the file you modified in Step 2 on page 167.
     c. Set the following property to true:

        ```
        com.ibm.tivoli.itcam.toolkit.ai.methodentryexittrace=true
        ```

## Customizing Memory Leak Diagnosis

Perform the following procedure to enable Memory Leak Diagnosis with customized settings:

1. Make a copy of the *DC_home*/itcamdc/etc/memory_leak_diagnosis.xml file, and open it up in a text editor.
2. Modify the parameters in the memory_leak_diagnosis.xml file. The following is a description of the parameters you can modify:

*Table 38. Parameters for Memory Leak Diagnosis Configuration File*

| Tag Name | Description |
|---|---|
| heapAllocationTarget | Defines the allocating and allocated classes for which heap allocations will be Byte-Code-Instrumented. By default, all allocating and allocated classes are selected. By modifying the allocatingClassName and allocatedClassName tags within the heapAllocationTarget tag, you can implement a more granular selection. Each heapAllocationTarget tag must contain exactly one allocatingClassName tag, and one or more allocatedClassName tags. Multiple heapAllocationTarget tags can be specified. |
| allocatingClassName | Identifies the name of a class or classes to be modified. Each heapAllocationTarget tag must contain exactly one allocatingClassName tag. |
| allocatedClassName | Identifies the specific heap allocation requests within the class or classes identified by the allocatingClassName tag that are to be Byte-Code-Instrumented. Each heapAllocationTarget tag must contain one or more allocatedClassName tags. |

Both the allocatingClassName and the allocatedClassName tags can include wildcard characters. The following summary describes how the wildcard characters work:

- Asterisk (*) stands for zero or more occurrences of any character when used by itself. When embedded within a sequence of characters (for example, `java.*.String`), it matches zero or more occurrences of any character except the package separator (.).
- Two periods (..) can be used to specify all sub-packages (for example, `java..String` matches `java.lang.String`). It matches any sequence of characters that starts and ends with the package separator (.).
- If the allocated class name begins with an exclamation point (!), any heap allocations for classes that match the allocated class name are specifically excluded from BCI for Memory Leak Diagnosis. This is useful for indicating that all heap allocations within a class or group of classes are to be Byte-Code-Instrumented except for those allocations that are specifically excluded.

For example, an application with a package name of com.mycompany.myapp has the following requirements:

- Within the Customer class, all heap allocations should be Byte-Code-Instrumented.
- Within the Supplier class, all heap allocations should be Byte-Code-Instrumented except for allocations for classes beginning with `java.lang.String`.

The following example describes the contents of the customized memory_leak_diagnosis.xml file that accomplishes this:

```
<aspect>
    <type>application</type>
    <name>com.ibm.tivoli.itcam.toolkit.ai.aspectj.apptrace.CaptureHeap</name>
    <enabledProperty>
                com.ibm.tivoli.itcam.toolkit.ai.enablememoryleakdiagnosis</enabledProperty>
    <defaultEnabled>true</defaultEnabled>
    <-- Modify the heapAllocationTarget tag to select or deselect the allocating and
          allocated classes for Memory Leak Diagnosis -->
    <heapAllocationTarget>
        <allocatingClassName>
                    com.mycompany.myapp.Customer</allocatingClassName>
        <allocatedClassName>*</allocatedClassName>
    </heapAllocationTarget>
    <heapAllocationTarget>
        <allocatingClassName>
```

```
                com.mycompany.myapp.Supplier</allocatingClassName>
        <allocatedClassName>!java.lang.String*</allocatedClassName>
    </heapAllocationTarget>
</aspect>
```

3. Complete one of the following steps:
   - Save the file in *custom_directory*, then complete the following steps:
     a. In the *custom_directory*/toolkit_custom.properties file, uncomment the following line by removing the number sign (#) at the beginning of the line:

        ```
        am.camtoolkit.gpe.customxml.leak=DC_home/itcamdc/etc/
        memory_leak_diagnosis.xml
        ```

     b. Change this line by replacing the path with just the file name of the file you modified in Step 2 on page 168.
     c. Set the following property to true:

        ```
        com.ibm.tivoli.itcam.toolkit.ai.enablememoryleakdiagnosis=true
        ```

   - Save the file in any directory on your server, then complete the following steps:
     a. In the *custom_directory*/toolkit_custom.properties file, uncomment the following line by removing the number sign (#) at the beginning of the line:

        ```
        am.camtoolkit.gpe.customxml.leak=DC_home/itcamdc/etc/
        memory_leak_diagnosis.xml
        ```

     b. Change this line by specifying the path and name for the file you modified in Step 2 on page 168.
     c. Set the following property to true:

        ```
        com.ibm.tivoli.itcam.toolkit.ai.enablememoryleakdiagnosis=true
        ```

## Customizing Lock Analysis

Perform the following procedure enable lock analysis with customized settings:

1. Make a copy of the *DC_home*/itcamdc/etc/lock_analysis.xml file, and open it up in a text editor.
2. Modify the lockingClasses parameter in the lock_analysis.xml file.

   The parameter defines the classes for which lock requests will be Byte-Code-Instrumented. By default, all lock requests in all application classes are selected. By modifying this tag, you can implement a more granular selection, although within a class all lock requests are Byte-Code-Instrumented. Multiple lockingClasses tags can be specified.

   The lockingClasses tag can include wildcard characters. The following summary describes how the wildcard characters work:

   - Asterisk (*) stands for zero or more occurrences of any character when used by itself. When embedded within a sequence of characters (for example, `java.*.String`), it matches zero or more occurrences of any character except the package separator (.).
   - Two periods (..) can be used to specify all sub-packages (for example, `java..String` matches `java.lang.String`). It matches any sequence of characters that starts and ends with the package separator (.).
   - If the locking class name begins with an exclamation point (!), any classes matching the classes identified in the tag are specifically excluded from BCI for lock analysis. This is useful for indicating that all classes are to be Byte-Code-Instrumented except for those classes that are specifically excluded.

For example, an application with a package name of com.mycompany.myapp has the following requirements:

- Only classes that begin with `Cus` or `Sup` should be Byte-Code-Instrumented for lock analysis.
- The Supplier class should not be Byte-Code-Instrumented for lock analysis.

The following would be the contents of the customized lock_analysis.xml file that accomplishes this:

```
<aspect>
  <type>application</type>
  <name>com.ibm.tivoli.itcam.toolkit.ai.aspectj.apptrace.CaptureLock</name>
  <enabledProperty>
          com.ibm.tivoli.itcam.toolkit.ai.enablelockanalysis</enabledProperty>
  <defaultEnabled>true</defaultEnabled>
  <lockingClass>com.mycompany.myapp.Cus*</lockingClass>
  <lockingClass>com.mycompany.myapp.Sup*</lockingClass>
  <lockingClass>!com.mycompany.myapp.Supplier</lockingClass>
</aspect>
```

3. Complete one of the following steps:
   - Save the file in *custom_directory*/, then complete the following steps:
     a. In the *custom_directory*/toolkit_custom.properties file, uncomment the following line by removing the number sign (#) at the beginning of the line:

        ```
        am.camtoolkit.gpe.customxml.lock=DC_home/itcamdc/etc/lock_analysis.xml
        ```

     b. Change this line by replacing the path with just the file name of the file you modified in Step 2 on page 170.
     c. Set the following property to true:

        ```
        com.ibm.tivoli.itcam.toolkit.ai.enablelockanalysis=true
        ```

   - Save the file in any directory on your server, then complete the following steps:
     a. In the *custom_directory*/toolkit_custom.properties file, uncomment the following line by removing the number sign (#) at the beginning of the line:

        ```
        am.camtoolkit.gpe.customxml.lock=DC_home/itcamdc/etc/lock_analysis.xml
        ```

     b. Change this line by specifying the path and name for the file you modified in Step 2 on page 170.
     c. Set the following property to true:

        ```
        com.ibm.tivoli.itcam.toolkit.ai.enablelockanalysis=true
        ```

**Note:** See the Monitoring on Demand chapter of the *IBM Tivoli Composite Application Manager: User's Guide* for a description of monitoring levels and information about how to manage monitoring levels.

## Setting the Heap Dump scan interval and logging

The Heap Dump Management function of ITCAM for J2EE can create Heap Dumps of the monitored IBM WebSphere Application Server by user request.

Once in a defined time interval, ITCAM for J2EE scans the existing Heap Dumps, to inform the user of their existence. This scan also serves to delete heap dump files that are over 48 hours old.

By default, this interval is every 12 hours. To change the interval, set the following property in the *custom_directory*/toolkit_custom.properties file to the new interval in seconds:

```
am.mddmgr.poll.delay
```

To enable logging of heap Dump scans, set the following property in the cynlogging.properties file. This file is located in the directory that also contains *custom_directory*:

```
CYN.trc.datacollector.level=DEBUG_MIN
```

Once every scan interval (12 hours by default), Heap Dump scan messages are logged in to the trace-dc-ParentLast.log file.

## Defining custom requests

A custom request is an application class and method that you designate as an edge or nested request. When the method runs, a start and end request trace record is written to the Level 1 or Level 2 tracing.

Custom requests are defined in the *DC_home*/itcamdc/etc/custom_requests.xml file. The product-supplied version of this file is only a sample and must be customized by the user. In addition, this feature is enabled by adjusting properties in the *custom_directory*/toolkit_custom.properties file.

Perform the following procedure to enable and define tracing of custom requests:

1. Make a copy of the custom_requests.xml file, and open it up in a text editor.
2. Modify the parameters in the custom_requests.xml file. The following table describes the parameters you can modify:

*Table 39. Parameters for Custom Requests Configuration File*

| Tag Name | Description |
|---|---|
| edgeRequest | Identifies one or more application methods that are to be Byte-Code-Instrumented for custom request processing. By modifying the requestName, Matches, type, and methodName tags within the edgeRequest tag, you can customize the selection. Each edgeRequest tag must contain exactly one methodName tag, and one or more Matches tags. Multiple edgeRequest tags can be specified. |
| requestName | Defines a unique name for this request. The request name is displayed in the L1 or L2 trace entry that is produced when one of the methods identified by this custom request runs. |
| Matches | Identifies a class or classes that contain the methods that are to be Byte-Code-Instrumented for custom request processing. Multiple Matches tags can be present within a single edgeRequest tag. |
| type | Indicates whether a class must be a system or application class to match the edgeRequest tag. |
| methodName | Identifies the names of the methods within one of the classes identified by the Matches tag that are to be Byte-Code-Instrumented for custom request processing. Exactly one methodName tag can be specified in each edgeRequest tag. |

The Matches and the methodName tags can include wildcard characters. The following section describes how the wildcard characters work:

- Asterisk (*) stands for zero or more occurrences of any character when used by itself. When embedded within a sequence of characters (for example, `java.*.String`), it matches zero or more occurrences of any character except the package separator (.).

- Two periods (..) can be used to specify all subpackages (for example, `java..String` matches `java.lang.String`). It matches any sequence of characters that starts and ends with the package separator (.).

For example, an application with a package name of com.mycompany.myapp has the following requirements:

- Within the Customer class, treat the creditCheck() method as a custom request called CreditCheck.
- Within the Supplier class, treat the inventoryCheck() method as a custom request called SupplyCheck.

The following example shows the contents of the customized custom_requests.xml file that accomplishes these requirements:

```
<customEdgeRequests>
      <edgeRequest>
              <requestName>CreditCheck</requestName>
              <Matches>com.mycompany.myapp.Customer</Matches>
              <type>application</type>
              <methodName>creditCheck</methodName>
      </edgeRequest>
      <edgeRequest>
              <requestName>SupplyCheck</requestName>
              <Matches>com.mycompany.myapp.Supplier</Matches>
              <type>application</type>
              <methodName>inventoryCheck</methodName>
      </edgeRequest>
</customEdgeRequests>
```

3. Complete one of the following steps:
   - Save the file as *DC_home*/itcamdc/etc/custom_requests.xml, then complete the following steps:
     a. In the *custom_directory*/toolkit_custom.properties file, uncomment the following line by removing the number sign (#) at the beginning of the line:

        ```
        #am.camtoolkit.gpe.customxml.custom=DC_home/itcamdc/etc/
        custom_requests.xml
        ```

     b. Change this line by replacing the path with just the file name of the file you modified in Step 2 on page 172.
   - Save the file in any directory on your server, then complete the following steps:
     a. In the *custom_directory*/toolkit_custom.properties file, uncomment the following line by removing the number sign (#) at the beginning of the line:

        ```
        #am.camtoolkit.gpe.customxml.custom=DC_home/itcamdc/etc/
        custom_requests.xml
        ```

     b. Change this line by specifying the path and name for the file you modified in Step 2 on page 172.

## Disabling various types of Byte Code Instrumentation for J2EE APIs

The Data Collector uses a technique called Byte Code Instrumentation (BCI) to collect data from various types of J2EE APIs that typically operate as nested requests. BCI is automatically enabled for these types of APIs. It can be disabled by adding lines to the *custom_directory*/toolkit_custom.properties file.

Disable instrumentation of one or more of the following types of APIs by adding the following lines to the toolkit_custom.properties file:

*Table 40. Adding lines to toolkit_custom.properties*

| Type of J2EE API | Line to add to toolkit_custom.properties file |
|---|---|
| Enterprise JavaBeans (EJB) | `com.ibm.tivoli.itcam.toolkit.ai.enableejb=false` |
| Java Connector Architecture (JCA) | `com.ibm.tivoli.itcam.toolkit.ai.enablejca=false` |
| Java Database Connectivity (JDBC) | `com.ibm.tivoli.itcam.toolkit.ai.enablejdbc=false` |
| Java Naming and Directory Interface (JNDI) | `com.ibm.tivoli.itcam.toolkit.ai.enablejndi=false` |
| Java Message Service (JMS) | `com.ibm.tivoli.itcam.toolkit.ai.enablejms=false` |
| Servlets/ JavaServer Pages (JSP) | `com.ibm.tivoli.itcam.toolkit.ai.enableservlet=false` |
| HTTP session count tracking | `com.ibm.tivoli.itcam.toolkit.ai.enablesessioncount=false` |
| CICS Transaction Gateway (CTG) | `com.ibm.tivoli.itcam.dc.ctg.enablectg=false` |
| IMS | `com.ibm.tivoli.itcam.dc.mqi.enableims=false` |
| Java Data Objects (JDO) | `com.ibm.tivoli.itcam.dc.mqi.enablejdo=false` |
| Message Queue Interface (MQI) | `com.ibm.tivoli.itcam.dc.mqi.enablemqi=false` |
| Axis web service (only on JBoss and WebLogic) | `com.ibm.tivoli.itcam.toolkit.ai.axis.enablewebservice=false` |
| Remote Method Invocation (RMI) | `am.ejb.rmilistener.enable=false` |

For performance reasons, you can also disable BCI for several API types only for Level 1 monitoring. In this case, BCI will for the API types be enabled only when the monitoring level is set to 2 or 3.

To do this, add (or uncomment) the following lines in the *custom_directory*/ toolkit_custom.properties file.

*Table 41. Modifying lines in toolkit_custom.properties*

| Type of J2EE API | Line to add to toolkit_custom.properties file |
|---|---|
| JCA | `com.ibm.tivoli.itcam.toolkit.ai.jca.callback.unconditional=false` |
| JDBC | `com.ibm.tivoli.itcam.toolkit.ai.jdbc.callback.unconditional=false` |
| JNDI | `com.ibm.tivoli.itcam.toolkit.ai.jndi.callback.unconditional=false` |
| JMS | `com.ibm.tivoli.itcam.toolkit.ai.jms.callback.unconditional=false` |

## Specifying data collection for custom MBeans

If you have custom MBeans, customize the generic configuration for Java Management Extensions (JMX) data collection.

Perform the following procedure to customize the generic configuration for JMX data collection:

1. The following table describes the parameters you can use:

*Table 42. Parameters for JMX MBean Configuration file*

| Element Name | Sub-element Name | Description |
|---|---|---|
| DomainList | Version | Defines the version of the application server |
| Domain | Name | Defines a domain. If the asterisk (*) is defined, all MBeans that match the query "ObjectName" will be returned. Otherwise, the MBeans that belong only to this domain name will be returned. |
| Domain | Description | Describes the domain. This can be any text string. |
| Domain | MBean | Defines the MBeans to be collected |
| MBean | ObjectName | Defines the MBean object name for collection. If the MBean element is used within an Attr element (which indicates the embedded MBean), then the object name is any symbolic name, such as $ATTRIBUTE_VALUE. This symbolic name will be replaced with the actual object name internally. |
| MBean | Category | Defines a unique key for the MBean. Each MBean must have a unique key, which is used in the JMXAcquireAttribute to get the MBean attributes. |
| MBean | RetrieveAllAttrs | A value of true indicates that all the attributes for the MBean must be collected. There is no need to define the attributes in the Attr element. |
| MBean | Attr | Defines the attributes to be collected |
| Attr | Name | The attribute name |
| Attr | MappedKey | Defines a unique key for the attribute. Each attribute must have a unique key, which is used in the JMXAcquireAttribute to get the specific attribute. |
| Attr | MBean | Defines the embedded MBean within this attribute. This tag is used when an attribute has an embedded MBean, which points to another MBean with the object name. |
| Attr | JavaBean | Defines the embedded MBean within this attribute. This tag is used when an attribute has an embedded MBean, which points to another MBean object. The object is the java object, which has the elements of a JavaBean (setter, getter). |
| Attr | TargetType | Defines the type of the attribute. This is usually specified for the JavaBean type to determine the attribute type. |

2. The following example shows a customized MBean configuration file:

```
<DomainList>
  <Version>1.0.0</Version>
  <Domain>
    <Name>*</Name>
    <Description>Custom MBean Conf</Description>
    <JSR77Compliant>false</JSR77Compliant>
     <MBean>
      <ObjectName>type=OperatingSystem,*</ObjectName>
      <Category>OPERATINGSYSTEM</Category>
      <Attr>
        <Name>Arch</Name>
```

```
        <MappedKey>OPERATE_ARCH</MappedKey>
      <Attr>
      <Attr>
        <Name>AvailableProcessors</Name>
        <MappedKey>OPERATE_AVAILABLE</MappedKey>
      <Attr>
     </MBean>
    <MBean>
     <ObjectName>type=Runtime,*</ObjectName>
     <Category>JVM</Category>
     <Attr>
       <Name>StartTime</Name>
       <MappedKey>JVM_STARTTIME</MappedKey>
     <Attr>
    </MBean>
  </Domain>
</DomainList>
```

3. Complete one of the following steps:
   - Save the file as *DC_home*/itcamdc/etc/custom_mbeanconfig.xml, and complete the following steps:
     a. Open the *custom_directory*/toolkit_custom.properties file.
     b. Uncomment the line beginning with am.camtoolkit.jmxe.custom by removing the number (#) sign.
   - Save the file in any directory on your server, then complete the following steps:
     a. Open the *custom_directory*/toolkit_custom.properties file.
     b. Uncomment the line beginning with am.camtoolkit.jmxe.custom by removing the number (#) sign.
     c. Change this line by specifying the path and name for the file you modified in Step 1 on page 175.

## Specifying data collection for custom MBeans - an alternative approach

The *custom_directory*/toolkit_custom.properties file contains the following properties with their default values:

```
am.getallmbeans=y
am.jmxkeyword=type_identifier
am.jmxusecanonical=y
am.jmxtruncate=n
am.jmxlength=30
```

These properties are in effect, only if the custom MBeans property is commented out in the toolkit_custom.properties file, as shown in the following example:

```
#  Uncomment the line below to enable custom mbeans
#am.camtoolkit.jmxe.custom=[file_path]/custom_mbeanconfig.xml
```

The presence of these properties displays all the existing MBeans in the application server, except for the ones that are already part of the mbeanconfig xml file. This is the list of the properties and their definitions:

**am.getallmbeans**

You can use this property to get all the existing MBeans in the application server except for those that are already defined in the mbeanconfig.xml

file. This property is in effect while the custom MBeans property is not set. If the custom MBeans property is set, the property has no effect on getting all the MBeans. Set its value to “y” to activate it.

By default, the keyword “type” or “Type” is searched within each acquired object name. Having the domain name and the value of the “type/Type” creates the category name. The category name is displayed on the System Resource page on the Visualization Engine. If “type” or “Type” does not exist, the “name” keyword is searched in the object name, and its value is used to create the category name. If the “name” keyword does not exist, the canonical name that contains all the keywords for the object name is used.

**am.jmxkeyword**

If for some reason the ‘type’ or ‘Type’ keyword does not distinguish the MBeans, and you need more granularity, then you have to define more keywords to be included in the category name.

For example, if you specify the keyword “identifier” in addition to the “type/Type” keyword the value of the “identifier” will be included in the category name. The category name includes the “type/Type” value and the “identifier” value separated by an underscore (_) character. More than one keyword can be specified in the property. The keywords must be separated by a comma (,).

**am.jmxusecanonical**

If for some reason, you need to see the entire keywords in the object name (this could be a long string, so you should avoid doing it), then assign the “y” value to this property. This will result in including the entire keywords values for the category name separated by an underscore (_) character.

**am.jmxtruncate**

In some cases, especially in the case of using the canonical keyword, if the length of the category name is too long JMXEngine will automatically truncate its length to 30 characters. This is the default setting. If there is no need to truncate the category name, assign the "n" value to this property to prevent the truncation.

**am.jmxlength**

The default truncation length is 30 characters. If you want to have a different truncation length set it in this property. Values above and below "30" are accepted.

## Customizing CICS transaction correlation

CICS is a transaction framework, primarily used to run mature applications. To communicate with CICS, Java applications can use the CICS Transaction Gateway (CTG).

ITCAM for J2EE can use BCI (Byte Code Instrumentation) to collect data on CTG calls. The BCI engine injects callback code into CTG classes. To enable this feature, set the following property in the *custom_directory*/toolkit_custom.properties file:

```
com.ibm.tivoli.itcam.dc.ctg.enablectg=true
```

By default, when CTG BCI is enabled, the Data Collector callback code adds composite tracking data, called Global Publish Server (GPS) tokens. This data is added into the communications area (COMMAREA) used to carry transaction

request data to CICS. This data can be used by ITCAM for Transactions, which instruments the CICS transaction framework. ITCAM for Transactions correlates every CICS transaction with the corresponding CTG call using the GPS token. The user can then view a detailed breakdown of transaction response time in the ITCAM Visualization Engine.

However, the presence of the GPS token in COMMAREA might not always be desirable. Disable GPS tokens if ITCAM for Transactions is not used for the CICS server. Otherwise, the GPS token reaches the server application, which might (in some cases) not process it correctly.

You can selectively disable GPS tokens for specific transactions. Selections can be based on CTG gateway address or protocol; by CICS system; by CICS program, or by the CICS transaction ID. To selectively disable GPS tokens, edit the file *custom_directory*/ctg.filters . This file can contain any number of lines with the following syntax:

```
Type=E|I[,Gateway=<CTG URL>][,Server=<CICS Server>][,Program=<CICS Program>]
  [,Transid=<Mirror tran ID>]
```

Each line defines a filter, which disables or enables GPS tokens for some transactions.

The `Type` parameter is mandatory for each line. A value of "E" sets up an Exclude filter; transactions matching it do not have a GPS token inserted into the COMMAREA. "I" denotes an Include filter; any transactions matching an include filter have a GPS token, overriding any Exclude filter applying to them.

All other parameters are optional, but at least one of them must be present on every line. To match a filter, a transaction must match all of the parameters set on the line:

- `Gateway` is any part of the CTG URL, including the protocol, host name and/or port
- `Server` is the host name of the CICS server (this name might be different from the CTG host name)
- `Program` is the CICS program name (a field in a CICS transaction request)
- `Transid` is the CICS Mirror Transaction ID. Except Multi Regional Operation (MRO) CICS/CTG environments, this parameter is of little use as all CTG transactions have the same Mirror Transaction ID

For example, to disable addition of GPS tokens to the COMMAREA of all transactions routed through the local protocol, add the following line to *custom_directory*/ctg.filters:

```
Type=E,Gateway=local://*
```

To disable addition of GPS tokens to some transactions while enabling them for other transactions, use lines similar to the following example:

```
Type=E,Program=CYN$*,Server=CICS3101
/*Disables addition of GPS tokens to transactions for programs starting 'CYN$' to be run on the CICS
Type=I,Program=CYN$ECI2,Server=CICS3101
/*Enables addition of GPS tokens for transactions for the CYN$ECI2 program to be run on the CICS3101
```

To disable addition of GPS tokens to all transactions, use the following line:

```
Type=E,Gateway=*
```

## Enabling instrumentation of Web Services as new request types

On the JBoss and Weblogic application servers, Web Services can be instrumented by the Data Collector. By default, this feature is disabled.

To enable instrumentation of Web Services as new request types, set (uncomment) the following property in the *DC_HOME*/runtime/*instance_name*/dc.properties file:

```
ws.instrument=true
```

Only JAX-RPC 1.1 and Axis 1.x Web services will be instrumented.

To enable Web Services correlation in the Visualization Engine and in ITCAM for Transactions, you need to instrument both the Web services client and the Web services server using ITCAM for WebSphere Data Collectors, and these Data Collectors must be connected to the same Managing Server.

## Installing Memory Dump Diagnostic for Java with IBM Support Assistant

Memory Dump Diagnostic for Java (MDD for Java) either analyzes a single heap dump or analyzes and compares two heap dumps and searches for evidence of a memory leak. In order to download MDD for Java, you will need to first install IBM Support Assistant (ISA). ISA provides extra help with diagnosing problems and provides extra tools and components for troubleshooting as well as providing a place to write problems (PMRs).

MDD for Java analyzes manual or scheduled heap dumps performed by ITCAM's Heap Dump Management feature.

You can use ITCAM's Heap Dump Management feature to schedule or immediately initiate the collection of an IBM Heap Dump for a particular application server. Then this dump must be downloaded and post-processed outside ITCAM's user interface (Application Monitor) using MDD for Java. (The other Memory Diagnosis tools provided by ITCAM, such as Memory Analysis, Heap Analysis and Memory Leak Diagnosis, provide analysis via the Application Monitor.)

MDD for Java only analyzes heap dumps from IBM JDKs. For non-IBM JDKs use the ITCAM Memory Leak Diagnosis feature.

Searching capabilities are not supported for ITCAM for J2EE in ISA.

### Where to Install ISA and MDD for Java

The following section describes two common configurations:

- Install ISA & MDD for Java on a standalone server that is not running an application server. After the IBM heap dump has been collected on the application server, it must be transferred to the MDD for Java server for post-processing.

  This configuration is recommended for production environments where you do not want the post-processing of the dump to impact the performance of the application server.
- Install ISA and MDD for Java on each application server host computer, so that you can analyze the heap dump locally without having to transfer it.

This configuration may be suitable for a development or test environment where the overhead of analyzing the heap dump is not a concern.

The decision on where to install may also be influenced by the platforms supported by ISA.

### Downloading, installing, configuring, and launching ISA

See the online helps in the Managing Server's user interface (Application Monitor) for instructions on how to download, install, configure, and launch ISA and to install the ISA plugin. Go to **Help > Welcome > Using IBM Support Assistant to diagnose problems**.

**Note:** ISA can be installed on both the Data Collector and Managing Server servers, but only the ISA installed on the Managing Server server can be invoked from the user interface (Application Monitor).

### Installing MDD for Java

See the online helps in the Managing Server's user interface (Application Monitor) for instructions on how to install MDD for Java. Go to **Help > Welcome > > Memory Diagnosis > Heap Dump Management > Downloading Memory Dump Diagnostic for Java from IBM Support Assistant**.

**Note:** To download MDD for Java from ISA, the server where ISA is running needs to access the IBM Web site.

## Configuring a Data Collector for multiple network cards and NATs

If a Data Collector needs to expose a specific IP to the Managing Server, complete one of the following steps:

- If the Data Collector is not using Port Consolidator, complete the following steps:
  1. Specify a system property java.rmi.server.hostname for the application server and set it to the IP address of the Data Collector.
  2. Make sure that Managing server can access the IP address of the Data Collector (You can verify this by doing a ping).
- If the Data Collector is using Port Consolidator, complete the following steps:
  1. Specify a system property java.rmi.server.hostname for the application server and set it to the IP address of the Data Collector.
  2. Specify a system property java.rmi.server.hostname in the `start` section of the script used to start Port Consolidator and set its value to the IP address of the Data Collector.
  3. Make sure that the Managing server can access the IP address of the Data Collector (You can verify this by doing a ping).

## Parameters specified with multiple network cards

To install multiple network cards: make sure that the IP specified for the Data Collector server are IPs that can be used to communicate with each other (In other words, if there is a network configuration where one of the IPs does not have a path to the other server, do not use that IP).

Complete the following steps:

1. On the Data Collector servers, define an additional Java system property and set it to the IP address of the Data Collector:

   `java.rmi.server.hostname`
2. On the Data Collector server, in the *custom_directory*/datacollector_custom.properties file set kernel.codebase and kernel.rfs.address parameters to point to the Managing Server IP.
3. On the Data Collector host, in the *instance_runtime_directory* open any existing generated Data Collector property files (named `*datacollector.properties`). Delete kernel.codebase and kernel.rfs.address parameters from these files, if they are present.
4. Start the instance of the application server that will be monitored by the Data Collector.

## Enabling the secondary Data Collector (for the monitoring agent) if not done during an initial installation

This instruction applies if you chose not to enable a secondary Data Collector for the IBM Tivoli Enterprise Monitoring Agent during the initial installation of the Data Collector, but you now want to enable it. If you do not want to perform the following manual procedure, you can unconfigure and reconfigure the Data Collector.

You will need to edit the kwjdc properties file:

*Table 43. Locations of the kwjdc properties file*

| | |
|---|---|
| WebLogic | If the monitored server instance is represented by a weblogic machine:<br><br>*DC_home*/runtime/wls*app_server_version.domain_name.machine_name.instance_name*/wls*app_server_version.domain_name.machine_name.instance_name*.kwjdc.properties<br><br>else:<br><br>*DC_home*/runtime/wls*app_server_version.domain_name.host_name.instance_name*/wls*app_server_version.domain_name.host_name.instance_name*.kwjdc.properties |
| Tomcat | *DC_home*/runtime/tomcat*app_server_version.host_name.instance_name*/*DC_home*/runtime/tomcat*app_server_version.host_name.instance_name*.kwjdc.properties |
| Sun Java System Application Server (JSAS) | *DC_home*/runtime/sjsas*app_server_version.domain_name.node_name.instance_name*/sjsas*app_server_version.domain_name.node_name.instance_name*.kwjdc.properties |
| JBoss | *DC_home*/runtime/jboss*app_server_version.host_name.instance_name*/jboss*app_server_version.host_name.instance_name*.kwjdc.properties |
| NetWeaver | *DC_home*/runtime/netweaver*app_server_version.sap_node_ID_host_name.sap_instance_number*/netweaver*app_server_version.sap_node_ID_host_name.sap_instance_number*.kwjdc.properties |
| Oracle | *DC_home*/runtime/oracle*app_server_version.host_name.node_name.instance_name*/oracle*app_server_version.host_name.node_name.instance_name*.kwjdc.properties |
| J2SE | *DC_home*/runtime/j2se.*application_name.host_name.instance_name*/*DC_home*/runtime/j2se.*application_name.host_name.instance_name*.kwjdc.properties |

Perform the following procedure to manually enable the monitoring agent:

1. In the kwjdc properties file, make the following modifications:
   a. Uncomment the following line and enter the port number to be used by the monitoring agent:

      `com.ibm.tivoli.kwj.agentport=`

b. Uncomment the following line and enter the IP address of the monitoring agent:

```
com.ibm.tivoli.kwj.agenthostname=
```

2. Restart the instance of the application server that is being monitored by the Data Collector.

## Suppressing verbose garbage collection output in Data Collectors with a Sun JDK

For Sun JDKs, the Data Collector configuration enables verbose garbage collection output using the -Xloggc generic JVM argument. By default, the -Xloggc causes the JVM to generate class loading and unloading events to the native standard output stream. The process might fill the log files and consume excessive disk space.

To suppress class loading and unloading events, use your application server to add the -XX:-TraceClassUnloading -XX:-TraceClassLoading options to the arguments for the Java Virtual Machine. Then, Restart the instance of the application server that is being monitored by the Data Collector.

## Configuring the Tomcat Data Collector to run as a Windows service

Once you have configured the Data Collector, you can complete the following steps to configure the Tomcat Data Collector to run as a Windows service.

1. Open the <AppServer_home>/bin/catalina.bat file.
2. Right-click the Tomcat Service icon on the Windows taskbar and click Configure.
3. When the Apache Tomcat properties window opens, click the Java tab.
4. From the open catalina.bat file, copy the value for JAVA_OPTS, and paste it into the text box labeled Java Options (in the Apache Tomcat Properties window).
5. Then paste the following text into the text box labeled Java Options:

```
Xbootclasspath/p:
%PRODUCT_HOME%\itcamdc
\lib\ext\tomcat\bcm\tomcat.bcm.jar -Dam.appserver=%APPSERVER% -Dam.nodename
=%NODENAME% -Djava.rmi.server.RMIClassLoaderSpi=com.ibm.tivoli.itcam.tomcat
.sdc.DCRMIClassLoaderSpi -Dappserver.platform=%PLATFORM% -Dam.home
=%PRODUCT_HOME%\itcamdc -Ditcam61.home=%PRODUCT_HOME% -agentlib:
am_sun_15 -DArm40.ArmTransactionFactory=com.ibm.tivoli.itcam.toolkit.arm.j2.
transaction.Arm40TransactionFactory -DITCAMfJ2=true -DArm4EventListener.
0=com.ibm.tivoli.itcam.dc.event.ARM4TransactionDataHandler -Dcom.ibm.tivoli.
transperf.instr.probes.impl.was.Globals.traceLevel=0 -Dorg.omg.
PortableInterceptor.ORBInitializerClass.com.ibm.tivoli.itcam.dc.
orbinterpretor.Initializer -Xloggc:"E:\TOMCA5~1\DC\tomcat123-gc-log.log.
ibmtest" -Djava.security.policy=E:\TOMCA5~1\DC\runtime\tomcat123.tivoli.us.
abc.com.ibmtest\tivu15.cn.ibm.com.ibmtest.datacollector.policy
```

6. In the text box labeled Java Options, replace the variables %PRODUCT_HOME%, %APPSERVER%, %PLATFORM%, and %NODENAME% with the actual values. You can use the sample text from step 4, E:\TOMCA5~1\DC, ibmtest, tomcat123, and tivoli.us.abc.com respectively.
7. Go to the Control Panel, click System, and click the Advanced tab.
8. Click Environment Variables.
9. Under System variables, add <DC_home>\toolkit\lib\w32-ix86 to the Path variable. (Replace <DC_home> with the real path for the Data Collector installation directory.)

10. Add the new variables `QUALDIR`and `CCLOG_COMMON_DIR`. Specify the values that are in catalina.bat file.
11. Restart Windows.

# Chapter 6. Uninstalling and unconfiguring ITCAM for J2EE Data Collector

This chapter gives step-by-step instructions on unconfiguring and uninstalling ITCAM for J2EE Data Collector (DC). If you want to unconfigure server instances only, see "Unconfiguring the server instances." If you want to unconfigure and uninstall ITCAM for J2EE Data Collector, refer to instructions in "Uninstalling the Data Collector" on page 189. Currently, silent unconfiguration and uninstallation is not supported.

**Important:** Launch _uninst/uninstaller.bin or _uninst/uninstaller.exe to uninstall Data Collector, or uninstall DC with software maintenance tool on your system. Do not delete the Data Collector manually. Otherwose, when you want to install the DC again under the same directory, your installation might fail .

On Linux and UNIX systems, in order to unconfigure the data collector the user needs to have full permissions to the server runtime subdirectory under the *DC_home*/runtime directory. In order to uninstall the data collector, the user needs to have full permissions to the *DC_home* directory

For NetWeaver users, perform the following steps, depending on whether you are running on a Windows, UNIX, or Linux system.

- For Windows:
  1. Stop the NetWeaver server by logging in as the NetWeaver Admin user.
  2. Run the uninstallation or unconfiguration program.
  3. Launch the NetWeaver server by logging in as the NetWeaver Admin user.

  For Unix or Linux:
  1. Stop the NetWeaver server by logging in as the NetWeaver Admin user.
  2. Launch the NetWeaver Database by logging in as the NetWeaver Database Admin user.
  3. Run the uninstallation or unconfiguration program.
  4. Launch the NetWeaver by logging in as the NetWeaver Admin user.

## Unconfiguring the server instances

This section provides the necessary instructions for unconfiguring the Data Collector from the managed server instances.

### Step 1: Launch the Configuration Tool

For Windows, locate the directory in which the Data Collector was installed, then select **installer > config_dc** and run the file config_dc.bat.

For UNIX or Linux, select **installer > config_dc** in the directory where you have the Data Collector installed and locate the file config_dc.sh. Invoke the Configuration Tool by entering the following command: `$ ./config_dc.sh`

The Configuration Tool will guide you through the unconfiguration process.

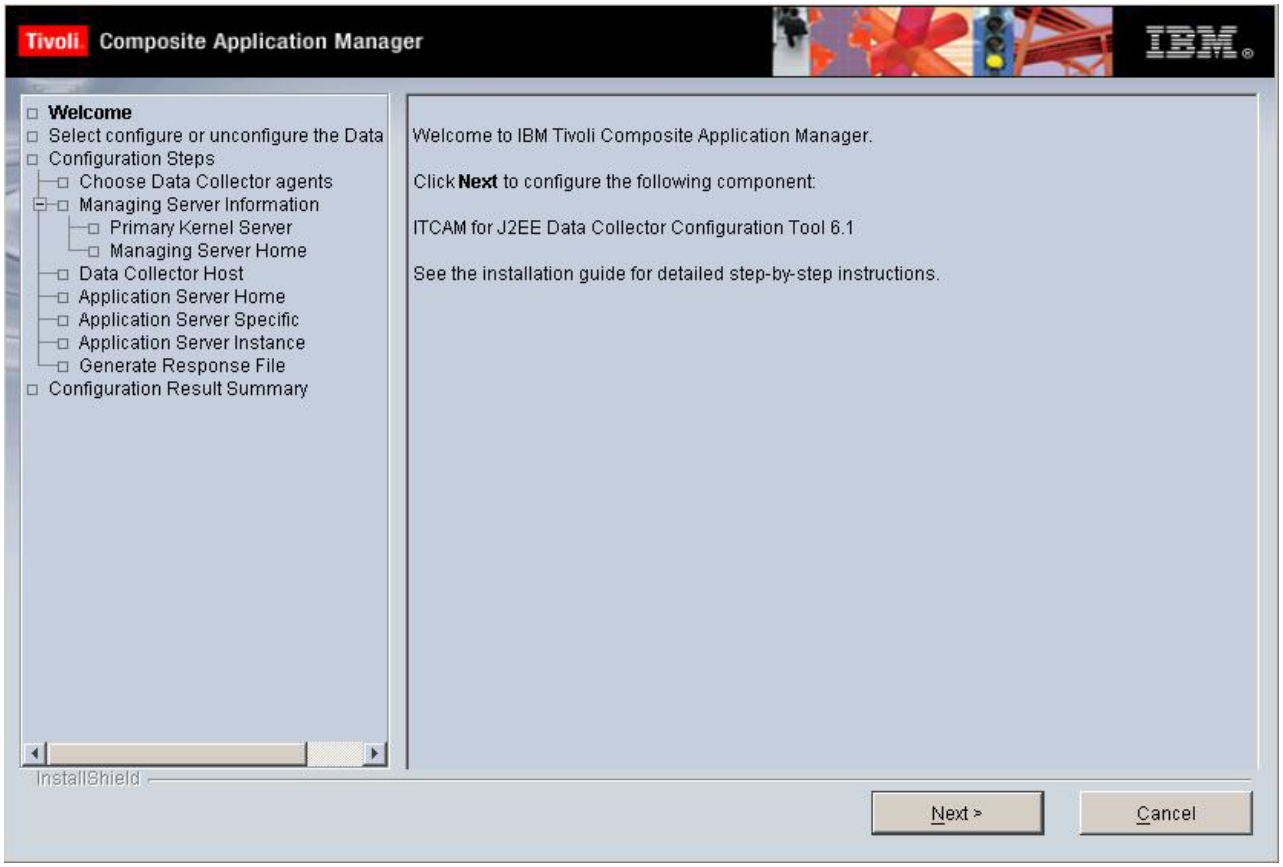



*Figure 69. Configuration Tool welcome screen*

Click **Next** to proceed.

## Step 2: Select unconfigure servers for data collection

In this window, you are prompted to either configure or unconfigure servers for data collection.

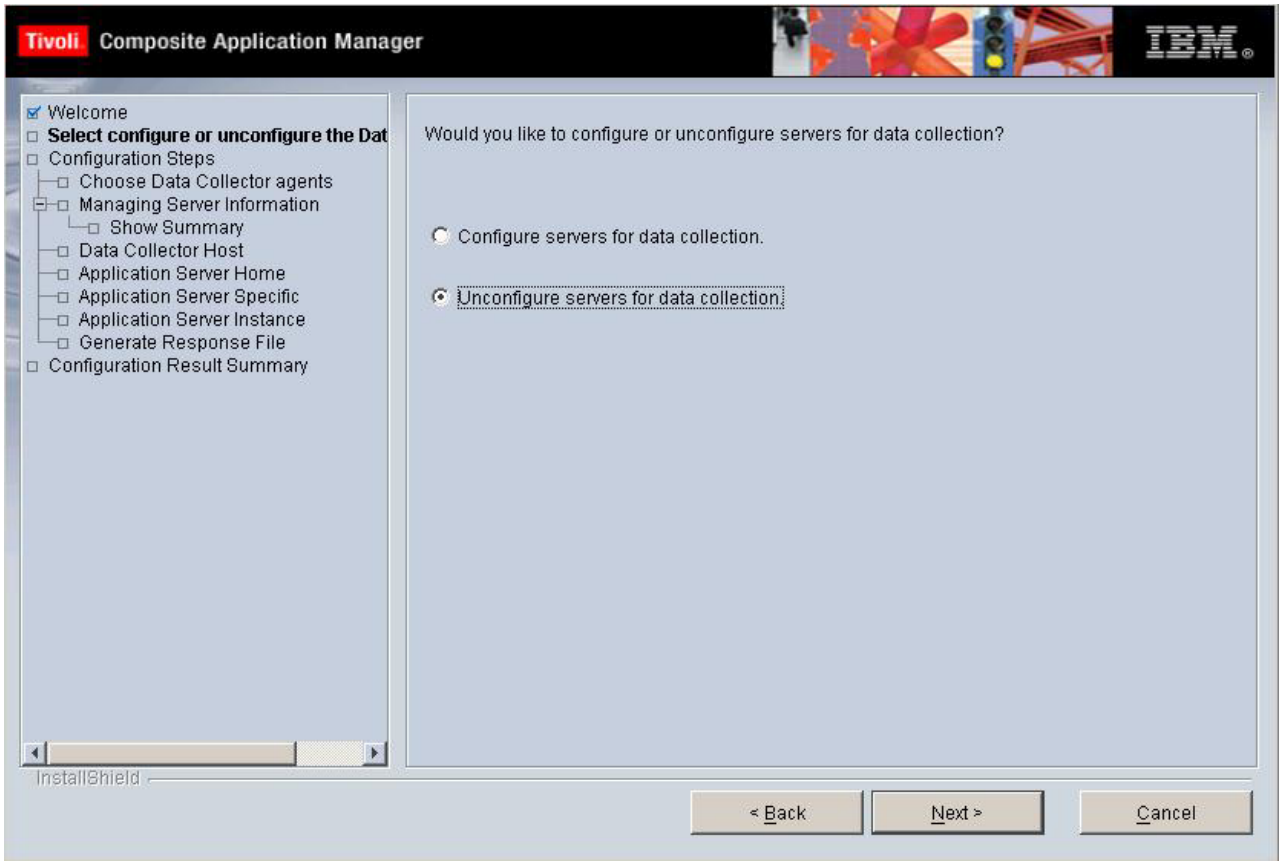



*Figure 70. Configure or unconfigure servers for data collection*

Select **Unconfigure servers for data collection**. Click **Next** to continue.

## Step 3: Select server instances to unconfigure

The Managing Server instance or instances that you have configured for data collection are displayed along with their root directory location.

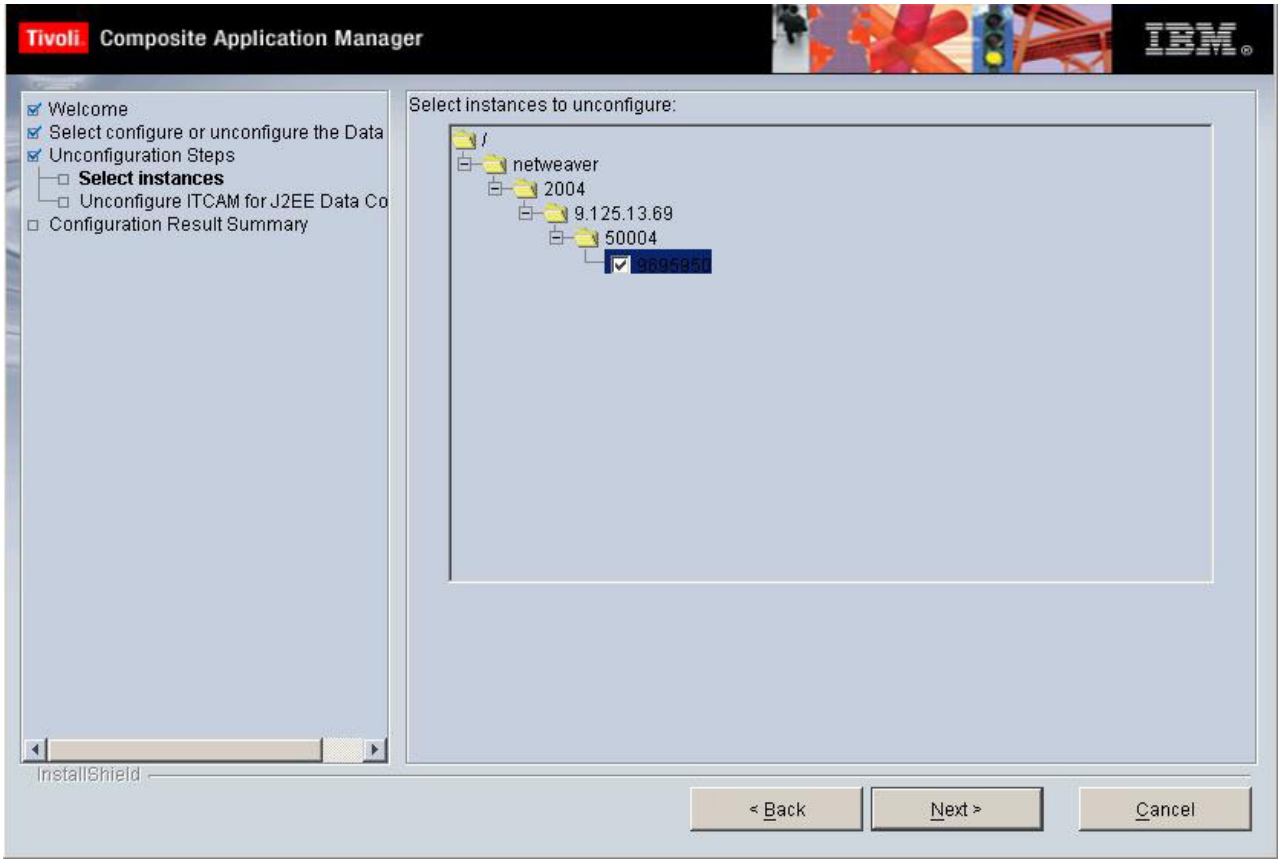



*Figure 71. Select server instances to unconfigure*

Select the check box of the server instance or instances to be unconfigured. Click **Next** to proceed.

## Step 4: Finalize the unconfiguration

A summary is displayed for the unconfiguration process.

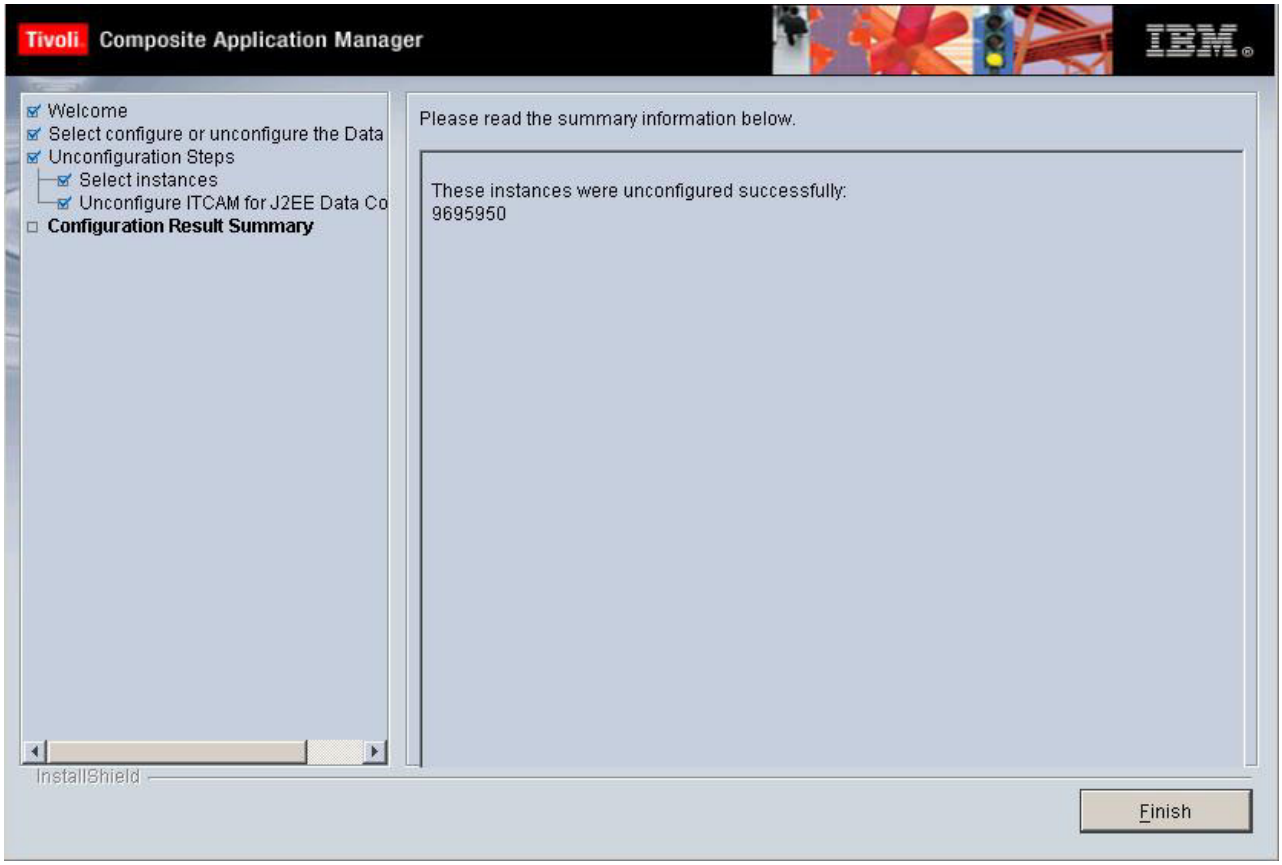



*Figure 72. Unconfiguration summary*

Read the summary review. Click **Finish** to finalize the unconfiguration and exit the Configuration Tool.

**CAUTION:**
**For NetWeaver server, the Tivoli service is not undeployed during unconfiguration. You can not undeploy it because all the Data Collectors share the Tivoli service. If you want to undeploy the Tivoli service, complete the following steps before undeployment.**

- **Unconfigure all Data Collectors from all servers on the corresponding instance.**
- **Remove references from servlet_jsp,naming,ejb,jms_provider,jms_connector,connector components to Tivoli component, and remove the bidirectional references between the CTG/JDO/IMS/MQI library components and Tivoli service component.**

**Otherwise, the NetWeaver server can not start.**

Restart the application server instances so that the unconfiguration can take effect. On Windows, if any monitored J2SE application is started from a command window, close and restart this window.

## Uninstalling the Data Collector

This section provides the necessary instructions for unconfiguring and uninstalling the Data Collector (DC) from the managed server instances.

## Step 1: Launch the InstallShield Wizard

For Windows, complete these steps to launch the InstallShield Wizard to uninstall the data collector:

1. From the desktop, click **Start** > **Settings** > **Control Panel** (for Windows 2000) or **Start** > **Control Panel** (for Windows 2003).
2. Click **Add or Remove Programs**.
3. Select **J2EE Data Collector**.
4. Click **Uninstall**.

For UNIX or Linux, select **installer > _uninst** in the directory where you have the Data Collector installed and locate the file uninstaller.sh. Invoke the InstallShield Wizard by entering the following command: `$ ./uninstaller.sh`

The InstallShield Wizard will guide you through the unconfiguration and uninstallation process.

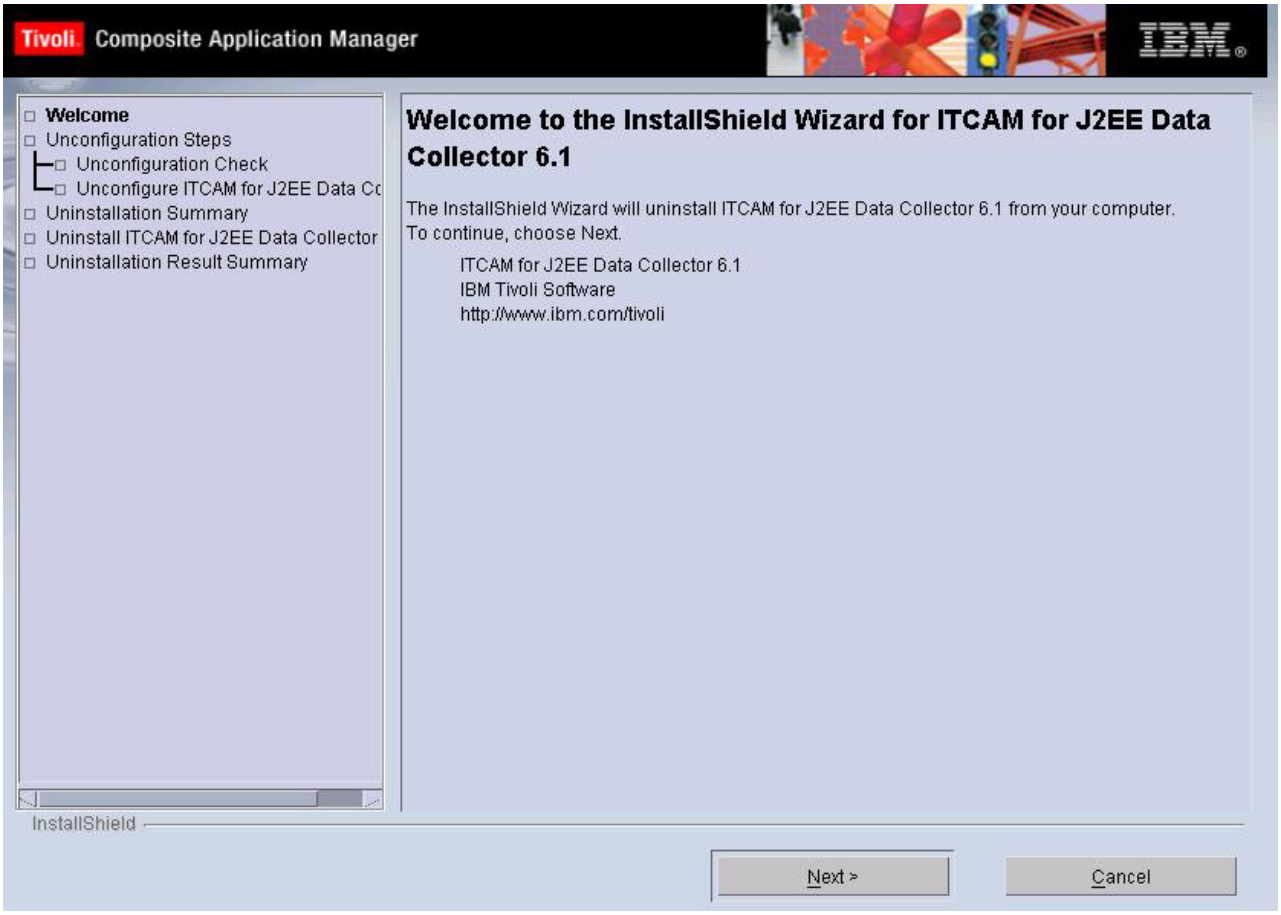



*Figure 73. InstallShield Wizard welcome screen*

Click **Next** to proceed.

## Step 2: Unconfiguration check

The Installshield Wizard determines whether the DC has already been unconfigured.

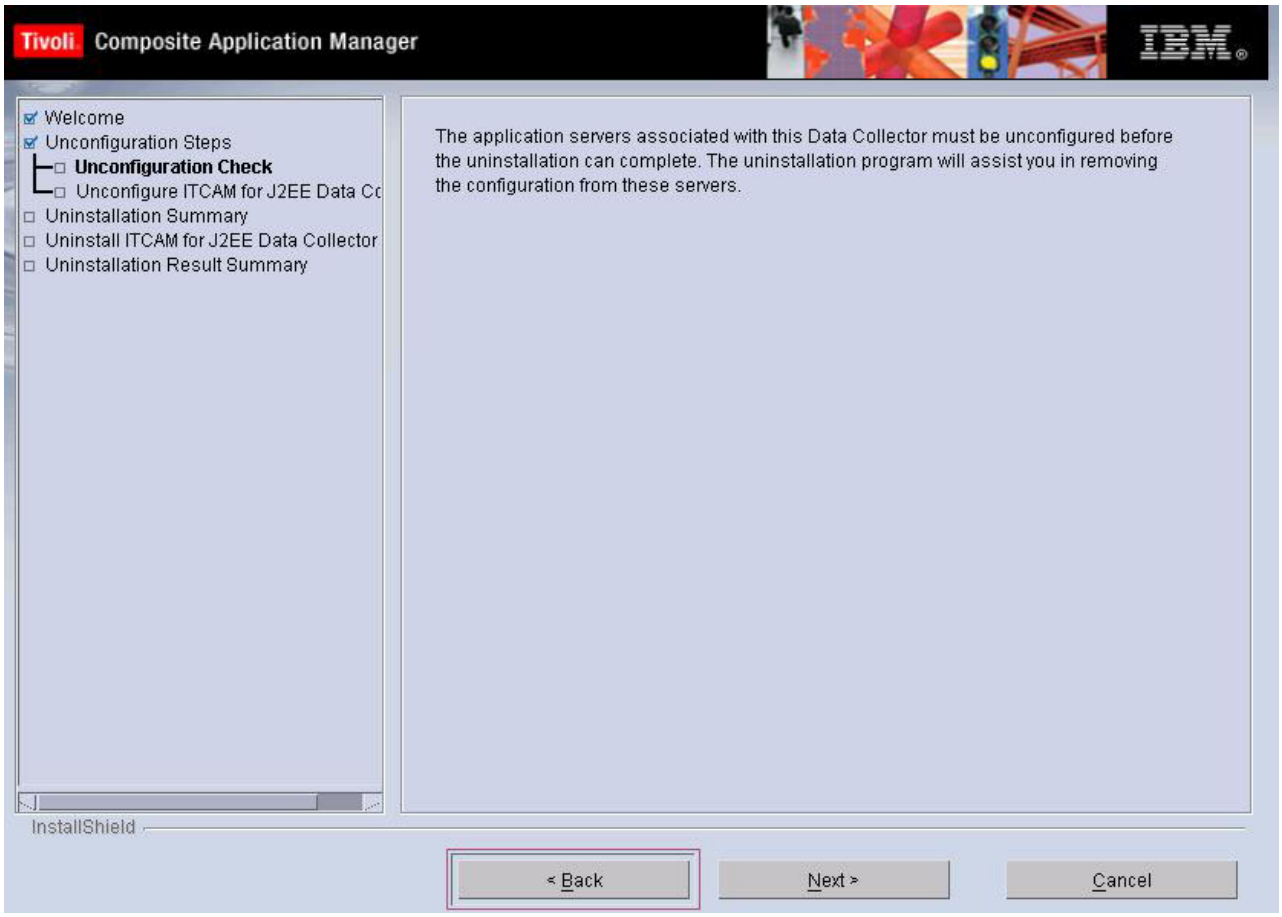



*Figure 74. Unconfiguration check page*

Click **Next** to continue.

## Step 3: Review the uninstallation summary

In this window, an uninstallation summary is displayed.

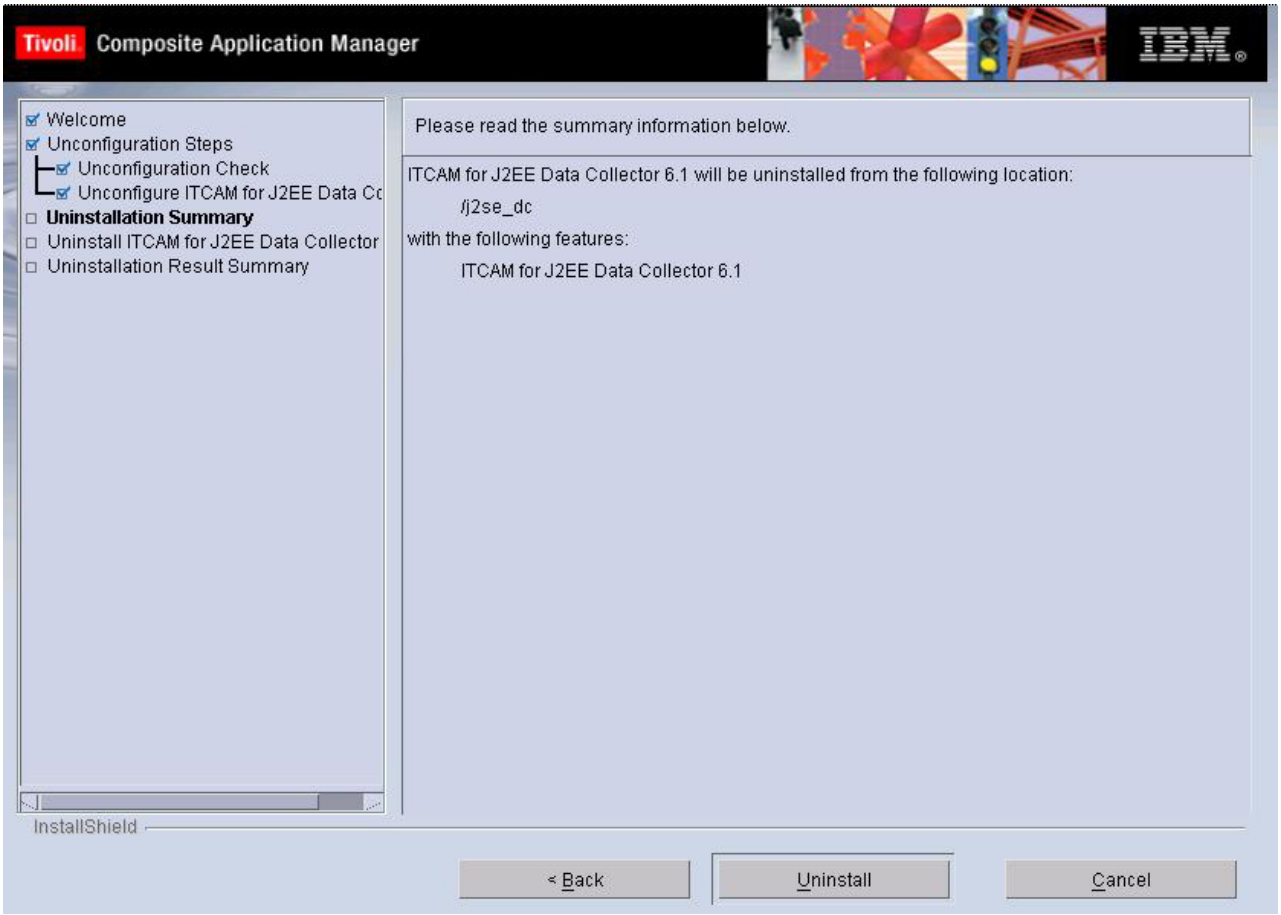



*Figure 75. Uninstallation summary*

Review the summary. Click **Uninstall** to start the uninstallation.

## Step 4: Finalize the uninstallation

A summary is displayed for the uninstallation process.

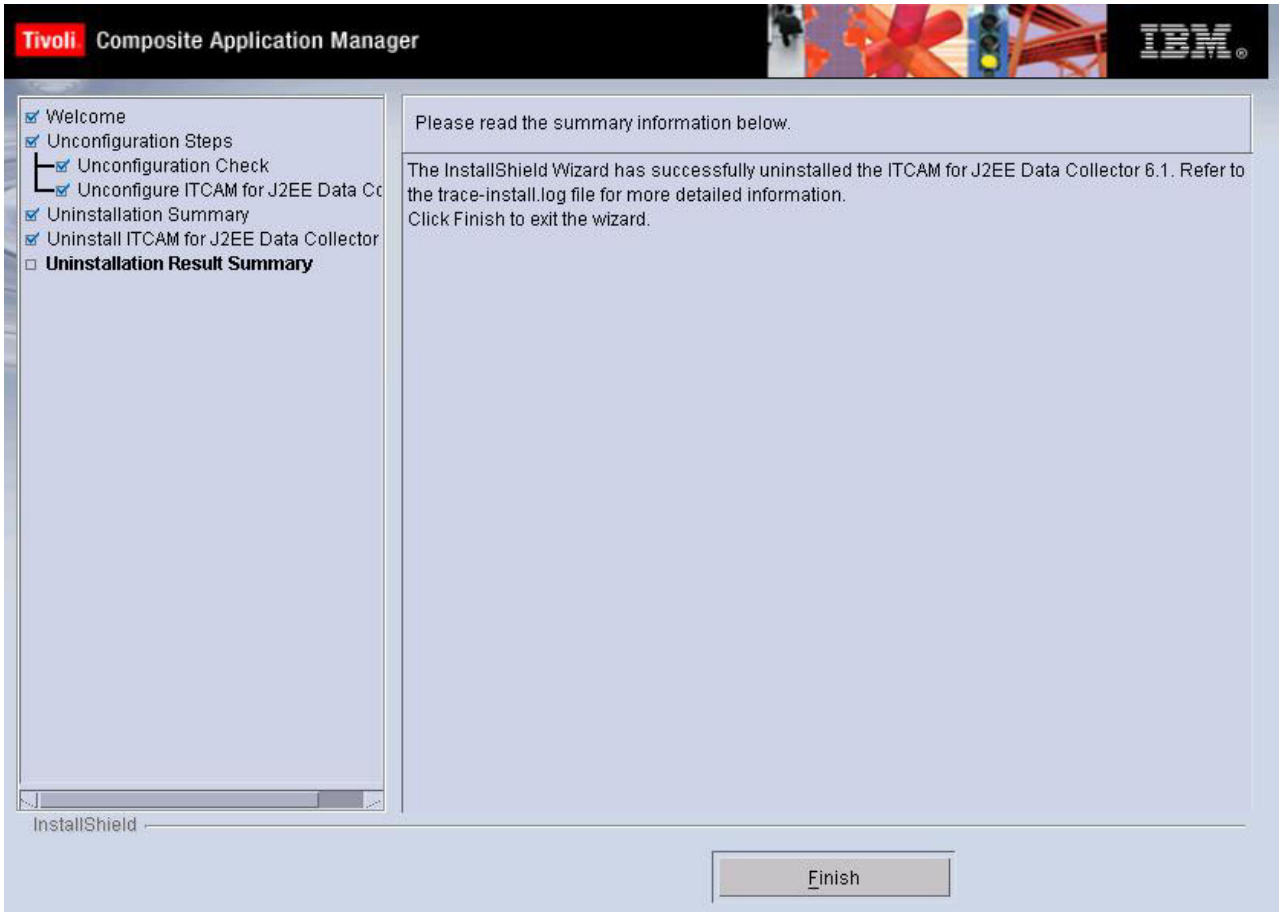



*Figure 76. Uninstallation process summary*

Read the summary review. Click **Finish** to finalize the uninstallation and exit the InstallShield Wizard.

# Chapter 7. Installing and uninstalling a Language Pack

A Language Pack enables user interaction with the Data Collector in a language other than English.

If you no longer want to use a language, uninstall the language pack for it.

## Installing a Language Pack on Windows

To install a Language Pack on Windows you need to use the installer on the Language Pack DVD.

Perform the following procedure:

1. Start `j2dclpinstaller.bat` from the Language Pack DVD.
2. Select the language of the installer and click OK.

   **Note:** In this step, you select the language for the installer user interface, not the language pack that will be installed.
3. Click **Next** on the Introduction window.
4. Select **Add/Update** and click **Next**.
5. Select the folder where the Data Collector is installed and click **Next**.
6. Select **ITCAM Agent for J2EE Data Collector** and click **Next**.
7. Examine the installation summary page and click **Next** to begin installation.
8. Click **Done** to exit the installer.

## Uninstalling a Language Pack on Windows

To uninstall a Language Pack on Windows you need to use the installer on the Language Pack DVD.

Perform the following procedure:

1. Start `j2dclpinstaller.bat` from the Language Pack DVD.
2. Select the language of the installer and click OK.

   **Note:** In this step, you select the language for the installer user interface, not the language pack that will be installed.
3. Click **Next** on the Introduction window.
4. Select **Remove** and click **Next**.
5. Select **ITCAM Agent for J2EE Data Collector** and click **Next**.
6. Examine the installation summary page and click **Next** to begin uninstallation.
7. Click **Done** to exit the installer.

## Installing a Language Pack on Linux and UNIX systems

To install a Language Pack on Linux and UNIX systems you need to use the installer on the Language Pack DVD.

Perform the following procedure:

1. Mount the Language Pack DVD. Make sure that the full path to the mount directory does not include spaces.
2. Use the following commands to start the installer from the Language Pack DVD:

   ```
   cd dir_name
   ./j2dclpinstaller.sh -c ITM_home
   ```

3. Select the language of the installer and click OK.

   **Note:** In this step, you select the language for the installer user interface, not the language pack that is installed.
4. Click **Next** on the Introduction window.
5. Select **Add/Update** and click **Next**.
6. Select the folder where the Data Collector is installed and click **Next**.
7. Select **ITCAM Agent for J2EE Data Collector** and click **Next**.
8. Examine the installation summary page and click **Next** to begin installation.
9. Click **Done** to exit the installer.

## Uninstalling a Language Pack on Linux and UNIX systems

To uninstall a Language Pack on Linux and UNIX systems you need to use the installer on the Language Pack DVD.

Perform the following procedure:

1. Mount the Language Pack DVD. Make sure the full path to the mount directory does not include spaces.
2. Use the following commands to start the installer from the Language Pack DVD:

   ```
   cd dir_name
   ./j2eelpinstaller.sh -c ITM_home
   ```

3. Select the language of the installer and click OK.

   **Note:** In this step, you select the language for the installer user interface, not the language pack that will be installed.
4. Click **Next** on the Introduction window.
5. Select **Remove** and click **Next**.
6. Select **ITCAM Agent for J2EE Data Collector** and click **Next**.
7. Examine the installation summary page and click **Next** to begin uninstallation.
8. Click **Done** to exit the installer.

# Appendix A. Support information

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

## Searching knowledge bases

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

### Finding release notes

You can find Release Note information online by viewing IBM Technotes. Technotes replace the Release Notes® manual for this product. *Technotes* are short documents that cover a single topic. You can search the Technote collection for common problems and solutions, as well as known limitations and workarounds. Technotes are continuously updated to provide current product information.

The following two procedures describe how to find Technotes and subscribe to have future Technotes e-mailed to you. Alternatively, you can watch demonstrations of these procedures at the following Web site: http://www-306.ibm.com/software/support/sitetours.html

#### Finding Technotes

Perform the following actions to access Technotes for this product:

1. Launch the IBM Software Support Web site: http://www.ibm.com/software/support
2. From *Select a brand and/or product* list, select *Tivoli*.
3. From *Select a product* list, select **IBM Tivoli Composite Application Manager for J2EE**.
4. Click the *Go* button.
5. To search the technotes for a particular problem, enter the keyword(s) in the text box under *Enter terms, error code or APAR #*.
6. Check the box *Solve a problem*.
7. Click the *Search* button.
8. Scroll through the search results, or you can optionally type a search term to refine the displayed data.

#### Subscribing to new Technotes

You can subscribe to an RSS feed of the product support page or subscribe to receive e-mail notification about product tips and newly published fixes through My support. To subscribe to an RSS news feed of the product support page, click the orange RSS button under the **Stay up to date** pane.

My support is a personalized portal that enables you to:

- Specify the products for which you want to receive notifications
- Create a personalized page that provides product information for the products you use
- Choose from flashes, downloads, and Technotes

- Receive an e-mail update in your inbox

Perform the following actions to subscribe to My support e-mails:

1. Launch an IBM support Web site such as the following site: http://www.ibm.com/support/us/
2. Click **My support** in the upper-right corner of the page.
3. If you have not yet registered, click **register** in the upper-right corner of the support page to create your user ID and password.
4. Sign in to **My support**.
5. On the My support page, click **Add products**.
6. Make the following selections from the lists to add this product to your personal page:
   a. Software
   b. Systems Management
   c. Application Performance & Availability
7. Click **Add products**.
8. Click **Subscribe to email**.
9. Set your preferences to specify the information you want in your emails.
10. Click **Update**.
11. Click **Submit**.

## Tivoli Support Technical Exchange

You can become a participant in the new Tivoli Support Technical Exchange. You can expand your technical understanding of your current Tivoli products in a convenient format hosted by Tivoli support engineers. This program provides support discussions about product information, troubleshooting tips, common issues, problem solving resources, and other topics. As Exchange leaders, Tivoli engineers provide subject matter expert direction and value. Participating in the Exchange helps you manage your Tivoli products with increased effectiveness.

What do you do to participate? Review the schedule of Exchange sessions. Find a topic of interest and select register. Provide your name, phone number, company name, number of attendees, the Exchange Topic and IBM Customer number. You are invited to attend a one- to two-hour conference call where the information is presented. The new Tivoli Support Technical Exchange can help with the following areas:

- Increased product knowledge
- Ways to avoid common pitfalls
- Support recommendations
- Proactive customer support
- Helpful hints and tips
- Knowledge transfer
- Expansion of your knowledge base

For more information or to suggest a future Exchange session, contact Support Technical Exchange (xchange@us.ibm.com). To learn more, visit the following Web site: http://www-01.ibm.com/software/sysmgmt/products/support/supp_tech_exch.html

### Search the information center on your local system or network

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

### Search the Internet

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

- IBM technotes
- IBM downloads
- IBM Redbooks®
- IBM DeveloperWorks
- Forums and newsgroups
- Google

## Obtaining fixes

A product fix might be available to resolve your problem. To determine what fixes are available for your IBM software product, follow these steps:

1. Go to the IBM Software Support Web site at http://www.ibm.com/software/support.
2. Click **Downloads** in the **Software** section.
3. Under the **Updates, drivers, and fixes** section, select **Fixes, fixpacks and utilities**.
4. Navigate to ITCAM for J2EE to obtain a list of available fixes.

For more information about the types of fixes that are available, see the *IBM Software Support Handbook* at http://techsupport.services.ibm.com/guides/handbook.html.

## Receiving support updates

To receive e-mail notifications about software support news and updates, follow these steps:

1. Go to the IBM Software Support Web site at http://www-01.ibm.com/software/support.
2. On the right hand side, click **My Notifications**.
3. If you have already registered for **My Notifications**, login. If you have not registered, click **register now**. Complete the registration form with your e-mail address as your IBM ID. When you have logged in, the **My notifications for IBM technical support** home page is displayed.
4. Select the **Subscribe** tab.
5. Under the **Software** list, select **Tivoli**.
6. Select **Tivoli Composite Application Manager for J2EE**. Click **Continue**.

7. In the **Options** section, enter a folder name, update notifications are saved in this folder.
8. In the **Notify me by** section, choose if you want to me notified of updates daily or weekly.
9. In the **Notify me by** section, choose if you want to receive notifications in plain text or html.
10. In the **Document Types** section, customize the types of information you want to be updated on, for example, white papers, drivers, and so on. Click **Submit**.

If you experience problems with the **My Notifications** feature, you can obtain help in one of the following ways:

**Online**
Send an e-mail message to erchelp@ca.ibm.com, describing your problem.

**By phone**
Call 1-800-IBM-4You (1-800-426-4968).

## Contacting IBM Software Support

IBM Software Support provides assistance with product defects.

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

- For IBM distributed software products (including, but not limited to, Tivoli, Lotus®, and Rational® products, as well as DB2 and J2EE products that run on Windows or UNIX operating systems), enroll in Passport Advantage® in one of the following ways:
  - **Online**: Go to the Passport Advantage Web page (http://www.lotus.com/services/passport.nsf/WebDocs/ Passport_Advantage_Home) and click **How to Enroll**
  - **By phone**: For the phone number to call in your country, go to the IBM Software Support Web site (http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html) and click **Contacts**.
- For IBM eServer™ software products (including, but not limited to, DB2 and J2EE products that run in zSeries, pSeries, and iSeries® environments), you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for eServer software products, go to the IBM Technical Support Advantage Web page (http://www.ibm.com/servers/eserver/techsupport.html).

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States or, from other countries, go to the contacts page of the IBM Software Support Handbook on the Web (http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html) and click the name of your geographic region for phone numbers of people who provide support for your location.

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

1. Determine the business impact of your problem.
2. Describe your problem and gather background information.

3. Submit your problem to IBM Software Support.

## Determine the business impact of your problem

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

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

## Describe your problem and gather background information

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

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

## Submit your problem to IBM Software Support

You can submit your problems in one of the two ways:

- **Online**: Go to the "Report and track problems" page on the IBM Software Support site (http://www-01.ibm.com/software/support/probsub.html). Enter your information into the appropriate problem submission tool.
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can the problem be re-created? If so, what steps led to the failure?
- Have any changes been made to the system? (For example, hardware, operating system, networking software, and so on.)
- Are you currently using a workaround for this problem? If so, please be prepared to explain it when you report the problem.

If the problem you submit is for a software defect or for missing or inaccurate documentation, IBM Software Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Software Support provides a workaround for you to implement until the

APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM product support Web pages daily. Users who experience the same problem can benefit from the same resolutions.

# Appendix B. J2SE JMXEnginePlugin interface

```
package com.ibm.tivoli.itcam.j2se.jmxe;

/**
 * This is interface of JMX Engine Plugin. If the J2SE application has
 * an embeded JMX server which can not return MBeanServer by MBeanServerFactory.
   findMBeanServer(null),
 * then user needs to implement this interface to return a working MBeanServer
 * instance.
 */
public interface JMXEnginePlugin {
  /**
   * The system passes necessary properties to user's implementation by this
     function,
   * for example, the PORT, USERNAME, PASSWORD to connect to JMX Server remotely.
   *
   * @param prop necessary properties to connect JMX Server
   * @throws Exception user defined initialization error
   */
   public void initialize(Properties prop) throws Exception;

  /**
   * Get MBeanServer for (un)registration of MBean
   * @return a working MBeanServer that DC can (un)register MBean
   */
   public MBeanServer getRegistrationMBeanServer();

  /**
   * This method is user's implementation to query attribute of a MBean
   * from JMX Server. There is a default implementation from JMX engine
   *
   * @param proxy - object reference
   * @param method - method name
   * @param args - method arguments
   */
  public Object invoke(Object proxy, Method method, Object[] args) throws Throwable;

  /**
   * This method is user's implementation to compose ObjectName for those
   * MBeans to be registered into JMX Server. There is a default implementation
   * from MBeanManager. The string returned by user's function will be inserted
   * before the string "Type=xxx, Name=yyy" which is returned from default function
   * in MBeanManager.
   * @param name : name of MBean.
   * @param type : type of MBean.
   * @param extraProp extra properties of MBean.
   * @return The String of ObjectName
   */
  public String buildObjectNameString(String domainName, String type, String name,
  Properties extraPrope;

  public final static String  HOST                    = J2SELocalSettings.HOST;
  public final static String  PORT                    = J2SELocalSettings.PORT;
  public final static String  USERNAME                = J2SELocalSettings.USERNAME;
  public final static String  PASSWORD                = J2SELocalSettings.PASSWORD;
}
```

# Appendix C. J2SE JMX plug-in sample

```
package com.testware.standalone.jmx;

import java.lang.reflect.Method;
import java.util.HashMap;
import java.util.Map;
import java.util.Properties;
import javax.management.AttributeNotFoundException;
import javax.management.MBeanServer;
import javax.management.MBeanServerConnection;
import javax.management.ObjectName;
import javax.management.QueryExp;
import javax.management.remote.JMXConnector;
import javax.management.remote.JMXConnectorFactory;
import javax.management.remote.JMXServiceURL;
import com.ibm.tivoli.itcam.j2se.jmxe.JMXEnginePlugin;

public class CustomJMXEngine implements JMXEnginePlugin {
 private String hostip = "";
 private int port = 0;
 private String username = "";
 private String password = "";
 MBeanServerConnection mbsc = null;
 /**
  * @param prop All variables about jmx will be set into this properties.
     Such as host, port, username and password
  */
 public void initialize(Properties prop) throws Exception {
  this.hostip = prop.getProperty(HOST,"127.0.0.1");
  String port_s = prop.getProperty(PORT);
  try {
   this.port = Integer.parseInt(port_s);
  } catch (NumberFormatException e) {
   this.port = 0;
  }
  this.username = prop.getProperty(USERNAME);
  this.password = prop.getProperty(PASSWORD);

  if(mbsc == null)
  {
   MBeanUtils.getInstance().createMBeanServer();
   mbsc = this.getMBeanServerConnection();
  }
 }
 private MBeanServerConnection getMBeanServerConnection() throws Exception {
  // Get MBeanServerConnection
  MBeanServerConnection connection;
  try {
   // The address of the connector server
   JMXServiceURL url = new JMXServiceURL("rmi", this.hostip, this.port,
"/jndi/jmx");

   // The credentials are passed via the environment Map
   Map environment = new HashMap();
   String[] credentials = new String[]{this.username, this.password};
   environment.put(JMXConnector.CREDENTIALS, credentials);

   // Connect to the server
   JMXConnector cntor = JMXConnectorFactory.connect(url, environment);

   connection = cntor.getMBeanServerConnection();
  } catch (Exception e) {
   e.printStackTrace();
```

```
   throw e;
  }
  return connection;
 }
 /**
  * Framwork use this method to get customer's mbean server and register
some mbeans into it
  */
 public MBeanServer getRegistrationMBeanServer() {
  MBeanServer server = MBeanUtils.getInstance().getMBeanServer();
  return server;
 }
 /**
  * Proxy function to invoke method of MBean Object.
  */
 public Object invoke(Object proxy, Method method, Object[] args) throws
Throwable {
  Object returnValue = null;

  try {
   if (method.getName().equals("getDefaultDomain")) {
    returnValue = mbsc.getDefaultDomain();
   } else if (method.getName().equals("queryNames")) {
    returnValue = mbsc.queryNames((ObjectName) args[0],(QueryExp) args[1]);
   } else if (method.getName().equals("getAttribute")) {
    returnValue = mbsc.getAttribute((ObjectName) args[0],(String) args[1]);
   } else if (method.getName().equals("invoke")) {
    returnValue = mbsc.invoke((ObjectName) args[0],(String) args[1],
(Object[]) args[2],(String[]) args[3]);
   } else if (method.getName().equals("getMBeanInfo")) {
    returnValue = mbsc.getMBeanInfo((ObjectName) args[0]);
   } else if (method.getName().equals("getAttributes")) {
    returnValue = mbsc.getAttributes((ObjectName) args[0],(String[]) args[1]);
   } else {
     throw new Exception(method.getName()
     + " IS NOT IMPLEMENTED OR IS UNKNOWN");
   }
  }catch (AttributeNotFoundException e) { //ignore all attribute not found
excpetion.
  }catch (Exception re) {
   re.printStackTrace();
  }
  return returnValue;
 }
 public String buildObjectNameString(String domainName, String type, String name,
Properties extraProperties) {
  return null;
 }
}
```

# Appendix D. Summary of permissions required for installing and configuring the Data Collector

This appendix summarizes the permissions required for the user that installs and configures the Data Collector for J2EE application servers:

Required permissions common to all J2EE application servers:

- It is recommended that you use the application server user to install and configure the Data Collector. On UNIX platform (AIX/HP-UX/Linux/Solaris), if the user of the application server and the data collector are not the same, the user of the application server should be a member of the user group for the data collector.
- Read permissions to the <AppServer_home> directory and to all subfiles and subdirectories
- Read, Write, and Create New File permissions to the <DC_home> directory
- Read and Execute File permissions for the JDK directory that is used for starting the application server.
- Read, Write, and Create New File permissions to the common log directory (TIVOLI_COMMON_DIR). In Windows, the default is *C:\Program Files\ibm\tivoli\common*. In UNIX, the default is */var/ibm/tivoli/common*.
- Read, Write, and Create New File permissions to the directory specified in *-is:log* or *-V LOG_DIR* parameter.

Permissions for the application server after the Data Collector has been installed and successfully configured:

- Read, Write, and Create New File permissions to the common log directory (TIVOLI_COMMON_DIR). In Windows, the default is *C:\Program Files\ibm\tivoli\common*. In UNIX, the default is */var/ibm/tivoli/common*
- Read and Write permissions to the garbage collection log file.
- Read, Write, and Create New File permissions to the server-instance-specific runtime directory under <DC_home>/runtime

**Note:** The permissions for this directory are changed automatically by the Configuration Tool

*Table 44. Application-server-specific, required permissions for the user that installs and configures the Data Collector*

| Application Server | File or Directory | Permissions Required |
|---|---|---|
| JBoss | The JBoss startup script file specified by the parameter JBOSSSTARTSH | • Read<br>• Write |
| JBoss | The JBoss run.jar file at <AppServer_home>/bin/run.jar | • Read |
| JBoss | The JBoss server instance directory at <AppServer_home>/server/<AppServer_instance> | • Read<br>• Write<br>• Create New File |
| Tomcat | The Tomcat startup script file specified by the parameter STARTUP_FILE | • Read<br>• Write |

*Table 44. Application-server-specific, required permissions for the user that installs and configures the Data Collector (continued)*

| Application Server | File or Directory | Permissions Required |
|---|---|---|
| Tomcat | The Tomcat configuration file at <AppServer_home>/conf/catalina.properties | • Read<br>• Write |
| Tomcat | The Tomcat catalina.jar file at <AppServer_home>/lib/catalina.jar | • Read |
| J2SE | The J2SE application startup script file specified by the parameter J2SESTARTSH | • Read<br>• Write |
| Oracle | The Oracle server configuration xml file at <AppServer_home>/opmn/conf/opmn.xml | • Read<br>• Write |
| Oracle 10.1.2 and 10.1.3 | The Oracle server instance configuration xml file at <AppServer_home/j2ee/<InstanceName>/config/server.xml | • Read<br>• Write |
| SAP Netweaver2004 and 2004S on UNIX | The Netweaver instance startup profile directory.<br>For example:<br>/usr/sap/J2E/SYS/profile/START_JC00_tiv00<br>In this example, START_JC00_tiv00 is the name of the profile<br>**Note:** The NETWEAVER_INSTANCE_STARTUP_PRFILE file is used for setting the library path and some arguments for the AIX platform. | • Read<br>• Write |
| SAP Netweaver2004 and 2004S | The Central Instance Network Home directory at <central_instance_network_home>/SDM/program | • Read<br>• Write<br>• Create New File |
| SAP Netweaver2004 and 2004S | The Central Instance configtool directory at <central_instance_network_home>/j2ee/configtool | • Read<br>• Write<br>• Create New File |
| WebLogic | The WebLogic startup script file specified by the parameter WL_STARTSH<br>**Note:** This is required only if the WebLogic server instance is started from a script file | • Read<br>• Write |
| WebLogic | The WebLogic node manager startup script file at <AppServer_home>/server/bin/startNodeManager.sh(cmd)<br>**Note:** This is required only if the WebLogic server instance is started by the node manager | • Read<br>• Write |
| WebLogic | WebLogic common environment directory <AppServer_home>/common/bin | • Read<br>• Write |
| WebLogic | WebLogic startup script file directory.<br>In WebLogic 8, the path is <Domain_Home>, for example, /bea/user_projects/domains/mydomain/<br>In WebLogic 9, the path is <Domain_Home>/bin, for example, /bea/user_projects/domains/base_domain/bin | • Read<br>• Write |
| WebLogic on Windows | The WebLogic node manager install service file at <AppServer_home>/server/bin/installNodeMgrSvc.cmd<br>**Note:** This is required only if the WebLogic server instance is started by the node manager and the node manager is installed as a Windows service | • Read<br>• Write |

*Table 44. Application-server-specific, required permissions for the user that installs and configures the Data Collector (continued)*

| Application Server | File or Directory | Permissions Required |
|---|---|---|
| WebLogic 9 and 10 | The WebLogic common environment file at <AppServer_home>/common/bin/commEnv.sh(cmd)<br>**Note:** This is required only if the WebLogic instance or node manager are started by the WebLogic Script Tool (WST) | • Read<br>• Write |
| Sun iAS 6.5 MU7 | The iPlanet Application Server (IAS) Java Engine startup script file at <AppServer_home>/bin/kjs | • Read<br>• Write |
| Sun Java System Application Server (JSAS) 8 | The Common Application Server Environment file at <AppServer_home>/config/asenv.conf | • Read<br>• Write |
| Sun JSAS 7 and 8 | The Server Instance security startup script file at <AppServer_instance_home>/bin/startserv<br>**Note:** <AppServer_instance_home> for Sun JSAS 8 is usually /var/opt/SUNWappserver/nodeagents/<agent_name>/<server_instance_name><br>**Note:** <AppServer_instance_home> for Sun JSAS 7 is usually <AppServer_home>/domains/<domain_name>/<server_instance_name> | • Read<br>• Write |
| Sun JSAS 7 and 8 | The Server Instance security policy file at <AppServer_instance_home>/config/server.policy | • Read<br>• Write |

# Appendix E. Configure Tomcat Data Collector with Java Service Wrapper

To support Tomcat Data Collector with Java Service Wrapper, perform the following steps:

1. Follow the installation and customization guide to install and configure the Tomcat Data Collector as usual. The purpose of this step is to obtain the configuration settings defined in the *catalina.sh* by the Data Collector Configuration Tools. In the next step, we will move the configuration settings from *catalina.sh* to the wrapper configuration file *(wrapper.conf)*.
2. Using a text editor, move the configuration settings from *catalina.sh* to *wrapper.conf*. There are three types of settings to be moved:
   a. Environment settings

      In *catalina.sh*, they are defined as follows. Please remove these lines from the file. Note that some of the values should be defined differently, depending on the environment the Data Collector is running on.

      ```
      PRODUCT_HOME=/export/gqwang/tomcatdc
      export PRODUCT_HOME
      MS_HOME=%2Fopt%2FIBM%2Fitcam%2FWebSphere%2FMS
      export MS_HOME
      APPSERVER=wrapper_tomcat_server
      export APPSERVER
      NODENAME=tivsun06.cn.ibm.com
      export NODENAME
      PLATFORM=tomcat55
      export PLATFORM
      QUALDIR=tivsun06.cn.ibm.com.wrapper_tomcat_server
      export QUALDIR
      CCLOG_COMMON_DIR="/var/ibm/tivoli/common"
      export CCLOG_COMMON_DIR
      LD_LIBRARY_PATH=/export/gqwang/tomcatdc/toolkit/lib/solaris2:${LD_LIBRARY_PATH}
      export LD_LIBRARY_PATH
      ```

      When the settings are moved to *wrapper.conf*, they should be defined as follows. Note that some of the values should be defined differently, depending on the environment the Data Collector is running on.

      ```
      set.PRODUCT_HOME=/export/gqwang/tomcatdc
      set.MS_HOME=%2Fopt%2FIBM%2Fitcam%2FWebSphere%2FMS
      set.APPSERVER=wrapper_tomcat_server
      set.NODENAME=tivsun06.cn.ibm.com
      set.PLATFORM=tomcat55
      set.QUALDIR=tivsun06.cn.ibm.com.wrapper_tomcat_server
      set.CCLOG_COMMON_DIR="/var/ibm/tivoli/common"
      set.LD_LIBRARY_PATH=%PRODUCT_HOME%/toolkit/lib/solaris2:%LD_LIBRARY_PATH%
      wrapper.java.library.path.append_system_path=true
      ```

   b. JAVA options

      In *catalina.sh*, they are defined as follows. Please remove these lines from the file. Note that some of the values should be defined differently, depending on the environment the Data Collector is running on.

      ```
      JAVA_OPTS="-Xbootclasspath/p:$PRODUCT_HOME/toolkit/lib/bcm-bootstrap.jar:
        /export/gqwang/tomcatdc/toolkit/lib/jiti.jar:$PRODUCT_HOME/itcamdc/
        lib/ppe.probe-bootstrap.jar
      -Djava.rmi.server.RMIClassLoaderSpi=com.ibm.tivoli.itcam.tomcat.sdc.
        DCRMIClassLoaderSpi
      -Dam.appserver=$APPSERVER
      -Dam.nodename=$NODENAME
      ```

```
-Dappserver.platform=$PLATFORM
-Dam.home=$PRODUCT_HOME/itcamdc
-Ditcam61.home=$PRODUCT_HOME
-Xrunam_sun_15:/export/gqwang/tomcatdc/runtime/tomcat55.tivsun06.cn.
  ibm.com.wrapper_tomcat_server/jiti.properties
-Djlog.propertyFileDir.CYN=$PRODUCT_HOME/toolkit/etc
-Dcom.ibm.tivoli.itcam.toolkit.util.logging.qualDir=$QUALDIR
-Djlog.propertyFile=cynlogging.properties
-Djlog.qualDir=$NODENAME.$APPSERVER
-DArm40.ArmTransactionFactory=com.ibm.tivoli.itcam.toolkit.arm.j2.
  transaction.Arm40TransactionFactory
-DITCAMfJ2=true
-DArm4EventListener.0=com.ibm.tivoli.itcam.dc.event.
  ARM4TransactionDataHandler
-Dcom.ibm.tivoli.transperf.instr.probes.impl.was.Globals.traceLevel=0
-Dcom.ibm.tivoli.jiti.injector.IProbeInjectorManager=com.ibm.tivoli.
  itcam.toolkit.ai.bcm.bootstrap.ProbeInjectorManager
-Dorg.omg.PortableInterceptor.ORBInitializerClass.com.ibm.tivoli.itcam.
  dc.orbinterpretor.Initializer
-Dibm.common.log.dir=/var/ibm/tivoli/common
-Djlog.common.dir=/var/ibm/tivoli/common
-Djlog.qualDir=tivsun06.cn.ibm.com.wrapper_tomcat_server"
```

When the settings are moved to *wrapper.conf*, they should be defined as follows. Note that some of the values should be defined differently, depending on the environment the Data Collector is running on.

```
wrapper.java.additional.1=-Xbootclasspath/p:%PRODUCT_HOME%/toolkit/lib/
  bcm-bootstrap.jar:/export/gqwang/tomcatdc/toolkit/lib/jiti.jar:
  %PRODUCT_HOME%/itcamdc/lib/ppe.probe-bootstrap.jar
wrapper.java.additional.2=-Djava.rmi.server.RMIClassLoaderSpi=com.ibm.
  tivoli.itcam.tomcat.sdc.DCRMIClassLoaderSpi
wrapper.java.additional.3=-Dam.appserver=%APPSERVER%
wrapper.java.additional.4=-Dam.nodename=%NODENAME%
wrapper.java.additional.5=-Dappserver.platform=%PLATFORM%
wrapper.java.additional.6=-Dam.home=%PRODUCT_HOME%/itcamdc
wrapper.java.additional.7=-Ditcam61.home=%PRODUCT_HOME%
wrapper.java.additional.8=-Xrunam_sun_15:/export/gqwang/tomcatdc/runtime/
  tomcat55.tivsun06.cn.ibm.com.wrapper_tomcat_server/jiti.properties
wrapper.java.additional.9=-Djlog.propertyFileDir.CYN=%PRODUCT_HOME%/
  toolkit/etc
wrapper.java.additional.11=-Dcom.ibm.tivoli.itcam.toolkit.util.logging.
  qualDir=%QUALDIR%
wrapper.java.additional.12=-Djlog.propertyFile=cynlogging.properties
wrapper.java.additional.13=-Djlog.qualDir=%NODENAME%.%APPSERVER%
wrapper.java.additional.14=-DArm40.ArmTransactionFactory=com.ibm.tivoli.
  itcam.toolkit.arm.j2.transaction.Arm40TransactionFactory
wrapper.java.additional.15=-DITCAMfJ2=true
wrapper.java.additional.16=-DArm4EventListener.0=com.ibm.tivoli.itcam.
  dc.event.ARM4TransactionDataHandler
wrapper.java.additional.17=-Dcom.ibm.tivoli.transperf.instr.probes.impl.
  was.Globals.traceLevel=0
wrapper.java.additional.18=-Dcom.ibm.tivoli.jiti.injector.
  IProbeInjectorManager=com.ibm.tivoli.itcam.toolkit.ai.bcm.bootstrap.
  ProbeInjectorManager
wrapper.java.additional.19=-Dorg.omg.PortableInterceptor.
  ORBInitializerClass.com.ibm.tivoli.itcam.dc.orbinterpretor.Initializer
wrapper.java.additional.20=-Dibm.common.log.dir=/var/ibm/tivoli/common
wrapper.java.additional.21=-Djlog.common.dir=/var/ibm/tivoli/common
wrapper.java.additional.22=-Djlog.qualDir=tivsun06.cn.ibm.com.
  wrapper_tomcat_server
```

c. JAVA CLASSPATH

In *catalina.sh*, they are defined as follows. Please remove these lines from the file. Note that some of the values should be defined differently, depending on the environment the Data Collector is running on.

```
CLASSPATH=$PRODUCT_HOME/itcamdc/lib/ext/tomcat/loader/ppe.
  probe_tomcat.loader.jar:$CLASSPATH
CLASSPATH=$PRODUCT_HOME/toolkit/lib/ext/tk_jdbc_aspects.jar:
  $PRODUCT_HOME/toolkit/lib/ext/tk_cl_aspects.jar:$CLASSPATH
```

When the settings are moved to *wrapper.conf*, they should be defined as follows. Note that some of the values should be defined differently, depending on the environment the Data Collector is running on.

```
wrapper.java.classpath.6=%PRODUCT_HOME%/toolkit/lib/ext/tk_jdbc_aspects.jar
wrapper.java.classpath.7=%PRODUCT_HOME%/toolkit/lib/ext/tk_cl_aspects.jar
wrapper.java.classpath.10=%PRODUCT_HOME%/itcamdc/lib/ext/tomcat/loader/
  ppe.probe_tomcat.loader.jar
```

3. Restart the Tomcat server after the configuration changes.

**Note:** Avoid making the following mistakes when editing *wrapper.conf*:

- Repetitive sequence number. For example:

```
wrapper.java.additional.36=...
wrapper.java.additional.37=...
wrapper.java.additional.37=...
```

- Missing sequence number. For example:

```
wrapper.java.additional.35=...
wrapper.java.additional.37=...
wrapper.java.additional.38=...
```

- Double quotation marks on the *wrapper.java.additional* settings.

# Appendix F. Setting up security

Setting up optional security for ITCAM for J2EE is described in this chapter.

Because security for ITCAM for J2EE often involves integration of the various components, this chapter contains information pertaining to both Managing Servers and Data Collectors.

Perform the procedures in each of the following sections, if they apply.

## Node Authentication

In Node Authentication related configuration, the Kernel, Data Collectors or Port Consolidator operate in secure mode either individually or in combination. But the configuration changes are common for all the modes except that a particular component can be made to operate in a different mode by changing the property security.enabled on that particular component.

### Script to run if your SSL certificates have expired

All SSL certificates have an expiration time. For some certificates, the expiration time is 4 years, after which the product will not function if you have enabled Node Authentication and SSL. If this is the case, to increase the expiration time, perform the procedure at "Script to run if your SSL certificates have expired" on page 223.

### Node Authentication on the Managing Server

The following procedures are Node Authentication related configuration that occurs on the Managing Server component.

#### Kernel-related changes

All the properties are already documented in the appropriate property file. Uncomment the data and provide the correct value.

In the Kernel properties file (*MS_home*/etc/kl1.properties) complete the following steps:

1. To enable a Kernel to operate in secure mode, set the following property:
   ```
   security.enabled=true
   ```
2. If you have a multiple NIC environment or are upgrading the Managing Server from version 6.0 to version 6.1.0.4, in the Kernel properties file (*MS_home*/etc/kl1.properties), set `codebase.security.enabled=false`.
   If you have more than one instance of the Kernel, set `codebase.security.enabled=false` in kl2.properties as well.
3. Restart the Managing Server:
   a. If it is not already stopped, stop the Managing Server.
   b. Start the Managing Server.

### Data Collector custom properties file changes

The following procedure is Node Authentication related configuration that occurs by modifying the datacollector_custom.properties file.

### Enabling the Data Collector to operate in secure mode

In the Data Collector custom properties file (*custom_directory*/datacollector_custom.properties), set `security.enabled=true`.

Restart the application server.

## Node Authentication related properties in the Port Consolidator

The following procedure is Node Authentication related configuration that occurs by modifying the proxy.properties file.

In the Port Consolidator properties file (*DC_home*/itcamdc/etc/proxy.properties), complete the following steps:

1. To enable the Port Consolidator to operate in secure mode:
   `security.enabled=true`
2. Restart the application server.

See the Port Consolidator reference and configuration appendix in the Data Collector Installation Guide for instructions on configuring the Data Collector to use the Port Consolidator.

## Keystore management and populating certificates

You do not have to do the following unless you want to create unique certificates with a new storepass and keypass. These commands will populate a new store with those certificates.

**For populating all new keystores do the following**: there are 3 stores used by ITCAM for J2EE: IBMMSStore, IBMDCStore, and IBMProxyStore.

**IBMMSStore contains:** mgmttomgmt.cer (cn=cyaneamgmt)dctomgmt.cer (cn=cyaneadc)proxytomgmt.cer (cn=cyaneaproxy)

**IBMDCStore contains:** proxytodc.cer (cn=cyaneaproxy) mgmttodc.cer (cyaneamgmt)

**IBMProxyStore contains:** mgmttoproxy.cer (cn=cyaneamgmt) dctoproxy.cer (cn=cyaneadc)

To run the keytool commands, you must be in the java/bin directory or have keytool in your PATH. This is the script with the necessary parameters:

keytool -genkey -alias *alias_name* -keyalg RSA -keysize 1024 -sigalg MD5withRSA -validity 2000 -keypass *keypass* -keystore *./storename* -storepass *storepass* -dname "cn=cyaneamgmt, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA, C=US"

The following scripts will create all the necessary stores and certificates:

**Note:** Replace "oakland1" with your custom keypass and "oakland2" with your custom storepass. Replace "IBMMSStore", "IBMDCStore", and "IBMProxyStore" with your custom store names.

```
keytool -genkey -alias mgmttomgmt -keyalg RSA -keysize 1024 -sigalg MD5withRSA
  -validity 2000 -keypass oakland1 -keystore ./IBMMSStore -storepass oakland2
  -dname "cn=cyaneamgmt, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA, C=US"
```

```
keytool -genkey -alias dctomgmt -keyalg RSA -keysize 1024 -sigalg MD5withRSA
  -validity 2000 -keypass oakland1 -keystore ./IBMMSStore -storepass oakland2
  -dname "cn=cyaneadc, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA, C=US"

keytool -genkey -alias proxytomgmt -keyalg RSA -keysize 1024 -sigalg MD5withRSA
  -validity 2000 -keypass oakland1 -keystore ./IBMMSStore -storepass oakland2
  -dname "cn=cyaneaproxy, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA, C=US"

keytool -genkey -alias proxytodc -keyalg RSA -keysize 1024 -sigalg MD5withRSA
  -validity 2000 -keypass oakland1 -keystore ./IBMDCStore -storepass oakland2
  -dname "cn=cyaneaproxy, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA, C=US"

keytool -genkey -alias mgmttodc -keyalg RSA -keysize 1024 -sigalg MD5withRSA
  -validity 2000 -keypass oakland1 -keystore ./IBMDCStore -storepass oakland2
  -dname "cn=cyaneamgmt, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA, C=US"

keytool -genkey -alias mgmttoproxy -keyalg RSA -keysize 1024 -sigalg MD5withRSA
  -validity 2000 -keypass oakland1 -keystore ./IBMProxyStore -storepass oakland2
  -dname "cn=cyaneamgmt, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA, C=US"

keytool -genkey -alias dctoproxy -keyalg RSA -keysize 1024 -sigalg MD5withRSA
  -validity 2000 -keypass oakland1 -keystore ./IBMProxyStore -storepass oakland2
  -dname "cn=cyaneadc, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA, C=US"
```

**Extracting Certificates:**

After creating the 3 Stores, extract the certificates by completing the following steps:

1. Extract all certificates from IBMMSStore by running the following commands:

   ```
   keytool -export -alias mgmttomgmt -keypass oakland1 -keystore ./IBMMSStore
     -storepass oakland2 -file mgmttomgmt.cer

   keytool -export -alias dctomgmt -keypass oakland1 -keystore ./IBMMSStore
     -storepass oakland2 -file dctomgmt.cer

   keytool -export -alias proxytomgmt -keypass oakland1 -keystore ./IBMMSStore
     -storepass oakland2 -file proxytomgmt.cer
   ```

2. Extract all certificates from IBMDCStore by running the following commands:

   ```
   keytool -export -alias proxytodc -keypass oakland1 -keystore ./IBMDCStore
     -storepass oakland2 -file proxytodc.cer

   keytool -export -alias mgmttodc -keypass oakland1 -keystore ./IBMDCStore
     -storepass oakland2 -file mgmttodc.cer
   ```

3. Extract all certificates from IBMProxyStore by running the following commands:

   ```
   keytool -export -alias mgmttoproxy -keypass oakland1 -keystore ./IBMProxyStore
     -storepass oakland2 -file mgmttoproxy.cer

   keytool -export -alias dctoproxy -keypass oakland1 -keystore ./IBMProxyStore
    -storepass oakland2 -file dctoproxy.cer
   ```

After you have extracted your files, copy the following certificates and Stores to the following locations:

*MS_home*/etc:IBMMSStore mgmttoproxy.cer mgmttomgmt.cer mgmttodc.cer

*DC_home*/itcamdc/etc:IBMDCStore IBMProxyStore
proxytomgmt.cerproxytodc.cerdctoproxy.cer dctomgmt.cer

## Configuring components to use new keystores and certificates

Configure components to use new keystores and certificates:

1. Modify *MS_home*/bin/setenv.sh. At the end of the script you will need to modify the following lines with the new keystore name, storepass, and keypass:

```
KEYSTR_LOC=MS_home/etc/IBMMSStore
KEYSTR_PASS=oakland2
KEYSTR_KEYPASS=oakland1
```

2. Modify the Application Monitor user interface with the new keystore name, storepass and keypass. Perform the following procedure:
   a. Start the Managing Server and the Application Monitor user interface.
   b. On the Managing Server host, log into the IBM WebSphere Application Server administrative console.
   c. Depending on your application server version, complete one of the following steps:

*Table 45. Navigation to JVM custom properties in the IBM WebSphere Application Server administrative console*

| | |
|---|---|
| **IBM WebSphere Application Server 6** | 1. Click **Server > Application Servers** and select the *server_name*.<br>2. In the **Configuration** tab, navigate to **Server Infrastructure: Java and Process Management > Process Definition > Additional Properties: Java Virtual Machine > Additional Properties: Custom Properties**. |
| **IBM WebSphere Application Server 5** | 1. Click **Server > Application Servers** and select the *server_name*.<br>2. Navigate to **Additional Properties: Process Definition > Additional Properties: Java Virtual Machine > Additional Properties: Custom Properties**. |

   d. Use your application server to set the following Java Virtual Machine custom properties:
      1) Set the path of the certificate to use when security is enabled for the Application Monitor user interface:
         ```
         certificate.path=MS_home/etc/mgmttomgmt.cer
         ```
      2) Set the keystore location of the Managing Server:
         ```
         keystore.location=MS_home/etc/IBMMSStore
         ```
      3) Set the keystore password of Managing Server:
         ```
         keystore.storepass=oakland2
         ```
      4) Set the keystore key password of Managing Server:
         ```
         keystore.keypass=oakland1
         ```
      5) Set the user ID passed to the other end for authentication:
         ```
         nodeauth.userid=cyaneamgmt
         ```
   e. Restart the application server.
3. Modify *custom_directory*/datacollector_custom.properties file with the new storename, storepass and keypass as specified in the section "Enabling the Data Collector to operate in secure mode" on page 216.
4. Restart the Managing Server:
   a. If it is not already stopped, stop the Managing Server.
   b. Start the Managing Server.

## Secure Socket Layer communications

On distributed platforms, ITCAM for J2EE uses the SSL security protocol for integrity and confidentiality. You have the option of configuring all monitoring components to utilize SSL for communications. The following section describes a sample HTTP-based SSL transaction using server-side certificates:

1. The client requests a secure session with the server.
2. The server provides a certificate, its public key, and a list of its ciphers to the client.
3. The client uses the certificate to authenticate the server (verify that the server is who it claims to be).
4. The client picks the strongest common cipher and uses the server's public key to encrypt a newly-generated session key.
5. The server decrypts the session key with its private key.
6. From this point forward, the client and server use the session key to encrypt all messages.

The monitoring software uses the Java Secure Sockets Extensions (JSSE) API to create SSL sockets in Java applications.

This section describes how to customize the default settings for SSL authentication in ITCAM for J2EE.

## Password encryption and Kernel property file encryption

The amcrypto.sh script comes with the Managing Server and is present in *MS_home*/bin to encrypt the passwords related to Node Authentication and SSL.

### Password encryption

To encrypt a password, complete the following steps:

1. Enter:

   ```
   amcrypto.sh -encrypt password
   ```

   The password is written to stdout and also to a file.
2. Copy this encrypted password and place it in the appropriate config files.

   Currently password encryption is supported only for the following property values on both the Managing Server and Data Collectors:

   - KEYSTR_PASS and KEYSTR_KEYPASS in *MS_home*/bin/setenv.sh
   - JDBC_PASSWORD in *MS_home*/bin/setenv.sh.
   - keystore.storepass, keystore.keypass in the same window mentioned in the Step 2 on page 218.
   - keystore.storepass and keystore.keypass in *custom_directory*/datacollector_custom.properties file.
3. Restart the Managing Server:
   a. If it is not already stopped, stop the Managing Server.
   b. Start the Managing Server.
4. Restart the application server.

### Properties file encryption

Complete the following steps:

1. To encrypt a properties file, use:

   ```
   amcrypto.sh -encyptPropertyFile file
   ```

The *file* is kl1.properties or kl2.properties in *MS_home*/etc. This command encrypts the given input file and stores it in a file with different name. The user can back up the existing properties file and have it replaced by the encrypted file for more security.

2. To decrypt a properties file, use:

   ```
   amcrypto.sh -decryptPropertyFile file
   ```

   The *file* is kl1.properties or kl2.properties in *MS_home*/etc. This command decrypts the given file and writes the decrypted file to another file with a different name.

3. Restart the Managing Server:
   a. If it is not already stopped, stop the Managing Server.
   b. Start the Managing Server.

## Enabling Secure Socket Layer at the Data Collector level

To enable SSL, enable Node Authentication first (See "Node Authentication" on page 215). SSL works only with Node Authentication enabled.

Configuration with default options involves setting one property to `true` to operate the Data Collector in SSL mode:

1. In the *custom_directory*/datacollector_custom.properties file, set the following property to `true` by removing the comment symbol (#) in front of the property definition. (By default, this property is commented out.):

   ```
   comm.use.ssl.dc=true
   ```

2. Restart the application server.

## Verifying secure communications

To verify SSL is properly configured, look for the message labeled CYND4051I in one of the following files:

*Table 46. Location of the CYND4051I message*

| | |
|---|---|
| **Windows** | C:\Program Files\IBM\tivoli\common\CYN\logs*node_name.server_name**java_msg_log_file*. For example:<br><br>C:\Program Files\IBM\tivoli\common\CYN\logs\IBMNode01.server1\msg-dc-Ext.log |
| **UNIX** and **Linux** | /var/ibm/tivoli/common/CYN/logs/*node_name.server_name*/*java_msg_log_file*. For example:<br><br>/var/ibm/tivoli/common/CYN/logs/IBMNode01.server1/msg-dc-Ext.log |

That message includes the text `Join Proxy Server and Kernel successfully`.

Only the CommandAgent port uses SSL. Other ports opened by the Data Collector (the ProbeController port and the Data Collector - Publish Server port do not use SSL. Therefore, when SSL is enabled, only the data on the channels connected to the CommandAgent port is encrypted.

All the data processed on the CommandAgent channel is encrypted when SSL is enabled. The data can be classified as follows:

*Table 47. Classification of the data processed on the CommandAgent channel*

| Classification | Data |
|---|---|
| Command and control data | Configuring and unconfiguring the Data Collector |
| User actions related to threads | • Starting and stopping JVM threads<br>• Changing thread priorities<br>• Getting thread priorities and thread status<br>• Requesting drill down information to see cookies, etc ...<br>• Generating thread dumps<br>• Getting thread stack traces |
| System information | • information<br>• Operating system platform information<br>• JVM information |
| Application information | • All the applications installed on the monitored<br>• Application binaries and location information<br>• Thread pool information related to JMS, JCA, JTA, Servlet, EJB, etc ...<br>• Data source information |
| Performance data | All Performance Monitoring Infrastructure data |
| Transport data | • ORB data<br>• SOAP ports |
| Memory Information | • Obtaining JVM Heap Snapshot data<br>• Performing memory leak analysis<br>• Performing heap dump |

# Privacy filtering

The following procedures describe how to enable and verify privacy filtering.

## Enabling privacy filtering

This is used to filter out SQL, cookie, and HTTP Request query strings. When this property is set to `true`, this data is not collected by the Data Collector.

1. Stop the instance of application server that is being monitored by the Data Collector.
2. Go to *custom_directory*/datacollector_custom.properties .
3. Set the following property definition:

   ```
   secure.filter.on=true
   ```

4. Start the instance of application server that is being monitored by the Data Collector.

### Verifying privacy filtering

The following statement is printed out to the Data Collector log when privacy filtering is properly configured:

```
Privacy Filter is On. Http Request Query String, SQL String and Http Cookie data is
not trasmitted.
```

# Java 2 security in the application server

This section describes how to enable Java 2 security to work with ITCAM for J2EE.

**Note:** During installation of the Managing Server, Java 2 security is automatically enabled. So, for most users, the following steps are not needed.

## Enabling Java security

### About this task

Do the following to enable Java security:

### Procedure

1. Access the java.policy file: *WAS_BASEDIR*/java/jre/lib/security.
2. Edit the file with the following information:

```
grant codeBase "file:/MS_INSTALL_DIR/lib/-" {
  permission java.security.AllPermission;
};


grant codeBase "file:${was.install.root}/lib/-" {
   permission com.tivoli.jmx.MBeanServerPermission "MBeanServer.*";
   permission com.tivoli.jmx.MBeanServerPermission "MBeanServerFactory.*";
   permission com.tivoli.jmx.AllMBeanPermission "*";
};

grant codeBase "file:${java.home}/lib/ext/*" {
    permission java.security.AllPermission;
        permission com.tivoli.jmx.MBeanServerPermission "MBeanServerFactory.*";
        permission com.tivoli.jmx.MBeanServerPermission "MBeanServer.*";
        permission com.tivoli.jmx.AllMBeanPermission "*";
};
```

3.
4. Restart the application server.

## Supporting Java 2 security

The following procedures describe the changes to the server.policy file that you should make when Java 2 security is enabled and when it is disabled.

### Adding properties if Java 2 security is enabled

If Java 2 security is enabled, the following properties are required by the Data Collector to be added to *AppServer_home*/AppServer/properties/server.policy.

```
// Added the following for the Data Collector
grant codeBase "file:/usr/lpp/itcam/wsam/-" {permission
java.security.AllPermission;
};grant codeBase "file:/db2_install_path/db2710/classes/
-" {permission java.security.AllPermission;};
```

For example, add the following for the Data Collector:

```
grant codeBase "file:/usr/lpp/itcam/wsam/-" {permission java.security.AllPermission; };
grant codeBase "file:/usr/lpp/db2/db2710/classes/-" {permission java.security.AllPermission;};
```

### Removing properties if Java 2 security is disabled

If Java 2 security is disabled, the following properties, if they exist, can be removed from the *AppServer_home*/AppServer/properties/server.policy.

```
grant codeBase "file:/usr/lpp/itcam/wsam/-" {
 permission java.security.AllPermission;
};
grant codeBase "file:/db2_install_path/db2710/classes/-" {
permission java.security.AllPermission;
};
```

## Script to run if your SSL certificates have expired

All SSL certificates have an expiration time. For some certificates, the expiration time is 4 years, after which the product will not function if you have enabled Node Authentication and SSL. If this is the case, to increase the expiration time, perform the following procedure:

1. Open the script located at *MS_home*/bin/security_cert.sh with a text editor. The following is the content of the script:

```
#!/bin/sh

# (C) Copyright IBM Corp. 2005  All Rights Reserved.
#
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
#

# Note: This script requires $JDK_HOME to be defined and it requires
# JDK_HOME/bin/keytool to be present. This keytool is available in FULL JDK
# versions and may not be available in JRE versions of the install

# PLEASE DEFINE JDK HOME

JDK_HOME=/opt/IBM/WebSphere/AppServer6/java

PATH=${JDK_HOME}/bin:$PATH

# This script generates ALL the certificates and certificate stores required for
# ITCAMfWAS Product (DC/MS/Port Consolidator). Currently it populates
# certificates with validity of 7000 days. If you feel its too high replace
# validity period to a lower number according to your needs. Please Note: once
# limit is reached, Product will stop working when NodeAuthentication/SSL is ON
# Its your responsibility to re-generate the certificates and stores.
# Please replace ALL the certificates at DC, MS and PortCosolidator level.
# Partial replacement will NOT work


keytool -genkey -alias mgmttomgmt -keyalg RSA -keysize 1024 -sigalg MD5withRSA
  -validity 7000 -keypass cyanea94612 -keystore ./CyaneaMgmtStore -storepass
  cyanea94612 -dname "cn=cyaneamgmt, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA,
  C=US"

keytool -genkey -alias dctomgmt -keyalg RSA -keysize 1024 -sigalg MD5withRSA
  -validity 7000 -keypass cyanea94612 -keystore ./CyaneaMgmtStore -storepass
  cyanea94612 -dname "cn=cyaneadc, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA,
  C=US"

keytool -genkey -alias proxytomgmt -keyalg RSA -keysize 1024 -sigalg MD5withRSA
  -validity 7000 -keypass cyanea94612 -keystore ./CyaneaMgmtStore -storepass
  cyanea94612 -dname "cn=cyaneaproxy, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA,
  C=US"

keytool -genkey -alias proxytodc -keyalg RSA -keysize 1024 -sigalg MD5withRSA
  -validity 7000 -keypass oakland94612 -keystore ./CyaneaDCStore -storepass
  oakland94612 -dname "cn=cyaneaproxy, OU=CyaneaComp, O=Cyanea, L=Oakland,
  ST=CA, C=US"

keytool -genkey -alias mgmttodc -keyalg RSA -keysize 1024 -sigalg MD5withRSA
  -validity 7000 -keypass oakland94612 -keystore ./CyaneaDCStore -storepass
  oakland94612 -dname "cn=cyaneamgmt, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA,
  C=US"

keytool -genkey -alias mgmttoproxy -keyalg RSA -keysize 1024 -sigalg MD5withRSA
  -validity 7000 -keypass oakland94612 -keystore ./CyaneaProxyStore -storepass
  oakland94612 -dname "cn=cyaneamgmt, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA,
  C=US"
```

```
keytool -genkey -alias dctoproxy -keyalg RSA -keysize 1024 -sigalg MD5withRSA
  -validity 7000 -keypass oakland94612 -keystore ./CyaneaProxyStore -storepass
  oakland94612 -dname "cn=cyaneadc, OU=CyaneaComp, O=Cyanea, L=Oakland, ST=CA,
  C=US"

keytool -export -alias mgmttomgmt -keypass cyanea94612 -keystore
  ./CyaneaMgmtStore -storepass cyanea94612 -file mgmttomgmt.cer

keytool -export -alias dctomgmt -keypass cyanea94612 -keystore
  ./CyaneaMgmtStore -storepass cyanea94612 -file dctomgmt.cer

keytool -export -alias proxytomgmt -keypass cyanea94612 -keystore
  ./CyaneaMgmtStore -storepass cyanea94612 -file proxytomgmt.cer

keytool -export -alias proxytodc -keypass oakland94612 -keystore
  ./CyaneaDCStore -storepass oakland94612 -file proxytodc.cer

keytool -export -alias mgmttodc -keypass oakland94612 -keystore
  ./CyaneaDCStore -storepass oakland94612 -file mgmttodc.cer

keytool -export -alias mgmttoproxy -keypass oakland94612 -keystore
  ./CyaneaProxyStore -storepass oakland94612 -file mgmttoproxy.cer

keytool -export -alias dctoproxy -keypass oakland94612 -keystore
  ./CyaneaProxyStore -storepass oakland94612 -file dctoproxy.cer

cp ./CyaneaMgmtStore ./CyaneaMgmtStore_Comm
cp ./CyaneaDCStore ./CyaneaDCStore_Comm
cp ./CyaneaProxyStore ./CyaneaProxyStore_Comm

keytool -keystore ./CyaneaMgmtStore_Comm -storepass cyanea94612 -import
  -alias mgmttodc -file ./mgmttodc.cer

keytool -keystore ./CyaneaMgmtStore_Comm -storepass cyanea94612 -import
  -alias mgmttoproxy -file ./mgmttoproxy.cer

keytool -keystore ./CyaneaDCStore_Comm -storepass oakland94612 -import
  -alias dctomgmt -file ./dctomgmt.cer

keytool -keystore ./CyaneaDCStore_Comm -storepass oakland94612 -import
  -alias dctoproxy  -file ./dctoproxy.cer

keytool -keystore ./CyaneaProxyStore_Comm -storepass oakland94612 -import
  -alias  proxytodc -file ./proxytodc.cer

keytool -keystore ./CyaneaProxyStore_Comm -storepass oakland94612 -import
  -alias proxytomgmt  -file ./proxytomgmt.cer
```

**Note:** Alternatively, if you have not installed the interim fix that contains this script, you can copy and paste the contents into a text file and save it as *MS_home*/bin/security_cert.sh.

2. Specify the path for the location of the Java home directory for the JDK_HOME parameter. For example,

   ```
   JDK_HOME=D:\IBM\AppServer\java
   ```

3. If the increase in expiration time to 20 years (7000 days) is too much, modify the script. Change the value of `-validity 7000` to a lower number of days, in all instances it occurs in the script. For example, change all instances of `-validity 7000` to `-validity 3500`.
4. Save the changes and run the script.

# Appendix G. Port Consolidator reference and configuration

The Port Consolidator is used to reduce network resources. It is used on the Data Collector to limit the number of ports used by the Data Collector when communicating with the Managing Server. The Port Consolidator only consolidates the traffic in one direction: from the Managing Server to the Data Collector. All traffic from the Managing Server to the Data Collector will be routed through the Port Consolidator. However, the traffic from the Data Collector to the Managing Server is direct.

Typically, it is used in a firewall environment. The following sections shows one deployment scenario:

**Note:** All Data Collectors and Port Consolidators are installed on the same physical server.

## Jar files and scripts for manual installations

Typically, the Port Consolidator is installed at the same physical server as the Data Collector.

*DC_home*/itcamdc/lib contains the required jar files.

**Application Server:**

*DC_home*/itcamdc/lib/ext contains the following files:

- ppe.proxy-intf.jar
- ppe.probe.jar
- ppe.probe-intf.jar
- kernel.common.jar
- model.jar
- common.jar
- ppe.proxy.jar

*DC_home*/itcamdc/lib/ext/was contains ppe.was_*version*.jar.

**Note:** Replace *version* with the version of the application server you are running, either 5 or 6.

**UNIX** or **Linux**:

*DC_home*/itcamdc/bin contains the following script to start and stop the Port Consolidator: proxyserverctrl_ws.sh.

**Windows**:

*DC_home*/itcamdc/bin contains the following script to start and stop the Port Consolidator: proxyserverctrl_ws.bat.

### Scripts for starting and stopping the Port Consolidator

The following example shows the script to start and stop the Port Consolidator:

```
./proxyserverctrl_ws.sh
 ( start | stop | forcestop | killall | ping | list | delete | msg | trace )
```

The following table describes the options:

*Table 48. Options for the script to start and stop the Port Consolidator*

| Option | Description |
|---|---|
| start | Starts the Port Consolidator |
| stop | Stops the Port Consolidator |
| killall | Kills all Port Consolidator processes |
| ping | Pings the Port Consolidator |
| list | Lists all registered Data Collectors |
| delete | Deletes all registered Data Collectors |
| msg *logLevel* | Changes the log level for the message logger |
| trace *logLevel* | Change the log level for the trace logger |

The *logLevel* is one of the following values:

- error
- warn
- info
- debug_min
- debug_mid
- debug_max

## Configuring a Data Collector to use the Port Consolidator

If you have a firewall, you can avoid allocation of an excessive number of ports in the firewall for multiple Data Collectors by configuring and using the Port Consolidator.

Perform the following procedure to configure a Data Collector to use the Port Consolidator:

1. Edit the*custom_directory*/datacollector_custom.properties file. Add the following lines to the end of the file:

   ```
   proxy.host=IP_address
   ```

   This is usually the same IP address as the Data Collector server, but it could be different in a multiple IP or virtual host scenario. In any case, specify the same IP address as the one specified in the am.socket.bindip property in *DC_home*/itcamdc/etc/proxy.properties.

   ```
   proxy.port=port
   ```

   This is usually 8800. In any case, specify the same port specified in the PROXY_PORT property in *DC_home*/itcamdc/bin/proxyserverctrl_*.

   **Note:**

   a. Do not use the loopback address for the IP address. Use a valid IP address for the local system.

   b. proxy.port must match the port number for PROXY_PORT that is specified in the startup script you run in Step 4 on page 227.

2. Restart the instance of the application server that is being monitored by the Data Collector.
3. From a command prompt, move to the directory *DC_home*/itcamdc/bin.
4. Start the Port Consolidator using one of the following commands:

*Table 49. Command for starting the Port Consolidator*

| | |
|---|---|
| **Windows** | `proxyserverctrl_j2ee.bat start` |
| **UNIX** and **Linux** | `./proxyserverctrl_j2ee.sh start` |

Do not close the command prompt window.

**Note:** The value for PROXY_PORT that is specified in the script must match the value that you specified for proxy.port in Step 1 on page 226.

5. Open the Self-Diagnosis page of the Application Monitor user interface, and check to see that the following components are listed:
   - `COMMANDAGENTPROXY`
   - `KERNELPROXY`
   - `PROBECONTROLLERPROXY`
6. Verify that the Data Collector is using the Port Consolidator:
   a. Look for the message labeled CYND4051I in one of the following files:

*Table 50. Location of the CYND4051I message*

| | |
|---|---|
| **Windows** | C:\Program Files\IBM\tivoli\common\CYN\logs*node_name.server_name**java_msg_log_file*. For example:<br><br>C:\Program Files\IBM\tivoli\common\CYN\logs\IBMNode01.server1\msg-dc-Ext.log |
| **UNIX** and **Linux** | /var/ibm/tivoli/common/CYN/logs/*node_name.server_name*/*java_msg_log_file*. For example:<br><br>/var/ibm/tivoli/common/CYN/logs/IBMNode01.server1/msg-dc-Ext.log |

That message includes the text `Join Proxy Server and Kernel successfully`.

   b. From a new command prompt, move to the directory *DC_home*/itcamdc/bin, and enter one of the following commands:

*Table 51. Entering the proxyserverctrl_j2ee command*

| | |
|---|---|
| **Windows** | `proxyserverctrl_j2ee.bat list` |
| **UNIX** and **Linux** | `./proxyserverctrl_j2ee.sh list` |

You should see the Data Collector listed as one Service type, `PPECONTROLLER`. Keep this command prompt window open for future use.

7. Verify the Data Collector's connection to the Port Consolidator (again) by entering one of the following commands:

*Table 52. Entering the proxyserverctrl_j2ee command*

| | |
|---|---|
| **Windows** | `proxyserverctrl_j2ee.bat list` |
| **UNIX** and **Linux** | `./proxyserverctrl_j2ee.sh list` |

You should now see the Data Collector listed as two Service types, PPECONTROLLER and PPEPROBE.

The Data Collector is configured to use the Port Consolidator.

## Reconfiguring the Data Collector to bypass the Port Consolidator

If after configuring the Data Collector to use the Port Consolidator, you want the Data Collector to bypass the Port Consolidator, perform the following procedure:

1. Unconfigure the Data Collector in the Application Monitor user interface:
   a. Start the Managing Server and the Application Monitor user interface.
   b. From the top navigation, click **Administration > Server Management > Data Collector Configuration**.

      The Data Collector Management page opens.
   c. Go to the Configured Data Collectors at the top of the page.
   d. To unconfigure the Data Collector, select the check box that is next to the Data Collector, and click **Apply**.

   The unconfigured Data Collector is added to the Unconfigured Data Collectors page.

   **Notes:**
   a. If the data collection has reports associated with it, you are prompted to delete those reports before unconfiguring the Data Collector.
   b. For further information about unconfiguring a Data Collector , see the section on unconfiguring a Data Collector in the *IBM Tivoli Composite Application Manager: User's Guide*.
2. Stop the Port Consolidator. From a command prompt, enter one of the following commands:

*Table 53. Entering the proxyserverctrl_ws command*

| | |
|---|---|
| **Windows** | `proxyserverctrl_ws.bat stop` |
| **UNIX** and **Linux** | `./proxyserverctrl_ws.sh stop` |

3. Verify that the Port Cons olidator is stopped by entering one of the following commands:

*Table 54. Entering the proxyserverctrl_ws command*

| | |
|---|---|
| **Windows** | `proxyserverctrl_ws.bat list` |
| **UNIX** and **Linux** | `./proxyserverctrl_ws.sh list` |

   You should now see the message `KERNELPROXY is down`.
4. Reconfigure the Data Collector to bypass the Port Consolidator:
   a. Stop the application server.
   b. Edit the *custom_directory*/datacollector_custom.properties file. Remove the following lines from the end of the file:

      `proxy.host=`*`IP address of Data Collector`*

      `proxy.port=`*`port`*
   c. Check for the same lines in the Data Collector properties file; if they are present, remove them.

      The name of the Data Collector properties file depends on the application server type:

*Table 55. Locations of the Data Collector properties file*

| | |
|---|---|
| WebLogic | If the monitored server instance is represented by a weblogic machine:<br><br>*DC_home*/runtime/wls*app_server_version.domain_name.machine_name.instance_name*/wls*app_server_version.domain_name.machine_name.instance_name*.datacollector.properties<br><br>else:<br><br>*DC_home*/runtime/wls*app_server_version.domain_name.host_name.instance_name*/wls*app_server_version.domain_name.host_name.instance_name*.datacollector.properties |
| Tomcat | *DC_home*/runtime/tomcat*app_server_version.host_name.instance_name*/*DC_home*/runtime/tomcat*app_server_version.host_name.instance_name*.datacollector.properties |
| Sun Java System Application Server (JSAS) | *DC_home*/runtime/sjsas*app_server_version.domain_name.node_name.instance_name*/sjsas*app_server_version.domain_name.node_name.instance_name*.datacollector.properties |
| JBoss | *DC_home*/runtime/jboss*app_server_version.host_name.instance_name*/jboss*app_server_version.host_name.instance_name*.datacollector.properties |
| NetWeaver | *DC_home*/runtime/netweaver*app_server_version.sap_node_ID_host_name.sap_instance_number*/netweaver*app_server_version.sap_node_ID_host_name.sap_instance_number*.datacollector.properties |
| Oracle | *DC_home*/runtime/oracle*app_server_version.host_name.node_name.instance_name*/oracle*app_server_version.host_name.node_name.instance_name*.datacollector.properties |
| J2SE | *DC_home*/runtime/j2se.*application_name.host_name.instance_name*/*DC_home*/runtime/j2se.*application_name.host_name.instance_name*.datacollector.properties |

d. Restart the instance of the application server that is being monitored by the Data Collector.

5. In the Self-Diagnosis page of the Application Monitor user interface, check to see that the Data Collector is listed. The Data Collector should appear as unconfigured.
6. Check the configuration of your Data Collector. In the Application Monitor user interface, click **Administration > Server Management > Data Collector Configuration**.

   The Data Collector should be listed. However, it should be showing as unavailable.
7. View **Unconfigured Data Collectors**.

   Your Data Collector should be listed.

# Appendix H. 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.

## Regular expression 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. The next section provides the most frequently used expressions for this product. However, you can refer to the following Web page for a full description of the ICU regular expression library and an explanation of how to use the characters and operators for complex expressions: 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, you must 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 addresses: `http://www.ibm.com/marketing/` or `http://www.ibm.com/sales/`, you would do a grouping with a pipe sign (`|`) (represents *or*):

**`http://www.ibm.com/(?:marketing)|(?:sales)/`**

* Matches the preceding element zero or more times. You must 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)

**Note:** This section applies to the entry of URI and client IP filters for 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 values 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 I. Glossary

**application server**
Software in used in an Internet environment that hosts a variety of language systems used to program database queries and general business processing.

**Command line**
Unix or Linux prompt line entered to carry out a certain function.

**command file**
File containing command prompts to launch an application. Usually terminates with the extension .cmd or .bat.

**command syntax**
The pattern in which command line should be written.

**Configuration Tool**
Component of the ITCAM for J2EE Data Collector, the tool guides users through the process of configuring and also unconfiguring the Data Collector.

**Data Collector**
ITCAM for J2EE product that collects data from the Managing Server for analysis and configuration.

**DOS command prompt**
Program in Windows by which users may enter command lines.

**host** Computer with a specific application or software environment installed.

**J2EE** Java 2 Platform, Enterprise Edition. An environment for developing and deploying multi-tier enterprise applications. J2EE simplifies development of enterprise applications by basing them on standard, modular components; it comprises a set of services, application programming interfaces (APIs), and protocols that provide the necessary functions for developing multi-tiered, Web-based applications.

**Java virtual machine**
Java virtual machine, or JVM, converts the Java intermediate language into machine language and then executes it.

**Managing Server**
The server that manages information collected on different Data Collectors.

**Managing Server instance**
An instance of the Managing Server.

**monitored data**
Data on the Managing Server that is configured for data collection. You may see this data through your DC interface agent.

**product license**
Terms and conditions of the product's usage.

**response file**
Text file containing variables and parameters required for an installation of the ITCAM for J2EE Data Collector.

**setup file**
File containing the installation commands for the Data Collector.

**silent installation**
Installation process that does not show messages or windows during the process. Parameter definitions are specified in a text file that the installation runs from.

**startup script**
Command lines necessary to launch the application server.

**text editor**
Notepad or WordPad, an editor in which to alter or write rich text documents.

**unconfiguration**
Process of deselecting Managing Server instances for data collection.

# Appendix J. Accessibility

Accessibility features help users with physical disabilities, such as restricted mobility or limited vision, to use software products successfully.

The accessibility features in the product enable users to:

- Use assistive technologies, such as screen reader software and digital speech synthesizers, to hear what is displayed on the screen. Consult the product documentation of the assistive technology for details on using the technology with this product.
- Perform tasks with the software using only the keyboard.

## General Navigation

Each page has four main sections:

- Headerbar
- Toolbar
- Main tabs
- Content

Each page has navigation points for screen readers. The following navigation points are all H1:

- Title bar
- Main tabs
- Main form
- Section labels
- Table labels

## Menu Navigation

You use the Go To menu at the top of the screen to navigate to any of the applications that you have access to. The Go To menu is a cascading menu that is three levels deep at its deepest point. The following instructions describe how to get started with JAWS:

1. To get to the Go To menu press Alt+G.
2. When you open the menu, JAWS reads the first application in the menu. If JAWS does not begin to read the entry, restart the screen reader.
3. Navigate the list of applications in the menus by using the arrow keys.
4. JAWS indicates if a menu item has submenus. To get to a submenu, press the right arrow or enter.
5. Press the left arrow to move up a level in the hierarchy. If you press the left arrow at the highest level of the Go To menu, you leave the menu completely.
6. Press the Enter key to enter an application.

## Accessibility help

The Accessibility Help panels provide details on general navigation, menu navigation, and hot keys. Click **Accessibility Help** from the toolbar of the product to access the help panels.

## Screen reader setting

The product contains a screen reader flag. When you turn on the screen reader flag, the user interface is optimized to work with JAWS for Windows®. You use the **User** tab in the Users application to turn on the screen reader flag.

## Keyboard shortcuts

You can navigate within the applications by using a combination of keys.

## Accessible reports

To use the accessibility tools to read reports, you must access the reports in Microsoft Excel. In the reports applications, select the **Run Reports** option in the **Select Action** menu. With this option, you can email an .xls file version of a report to yourself at a scheduled time.

## IBM and accessibility

For more information about the commitment that IBM has to accessibility, see the IBM Human Ability and Accessibility Center. The IBM Human Ability and Accessibility Center is at the following web address: http://www.ibm.com/able

# Index

## N



## O



## P



## Q



## R



## S



## T



## U

# V



# W

# 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 http://www.ibm.com/legal/us/en/copytrade.shtml.

Adobe is either a registered trademark or a trademark of Adobe Systems Incorporated in the United States, other countries, or both.

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

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

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

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

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

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).



**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law**:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

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

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

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

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

COPYRIGHT LICENSE:

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

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

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2006, 2009. All rights reserved.

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

## Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's user name for purposes of session management, authentication, and single sign-on configuration. These cookies cannot be disabled.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Printed in USA

SC27-2823-02