IBM Tivoli Composite Application Manager
Version 7.2

Agent for WebSphere Applications Installation and Configuration Guide

SC27-2818-02

IBM Tivoli Composite Application Manager
Version 7.2

Agent for WebSphere Applications Installation and Configuration Guide

SC27-2818-02

Note

Before you use this information and the product that it supports, read the information in "Notices" on page 355.

Contents

Figures

Tables

About this publication

This publication provides information about installing, customizing, starting, and maintaining IBM® Tivoli® Composite Application Manager Agent for WebSphere® Applications on Windows, Linux, and UNIX systems.

Intended audience

This publication is for administrators or advanced users wanting to install or modify the configuration of ITCAM Agent for WebSphere Applications. 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
- Web application servers, such as IBM WebSphere
- 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 Applications library for Agents for WebSphere Applications, J2EE, and HTTP Servers

The following publications are included in the ITCAM for Applications library, available in the: ITCAM for Applications Information Center

- *IBM Tivoli Composite Application Manager: Agents for WebSphere Applications, J2EE, and HTTP Servers User's Guide*

  Provides the user overview, user scenarios, and Helps for agents for WebSphere Applications, J2EE, and HTTP Servers.
- *IBM Tivoli Composite Application Manager: Agents for WebSphere Applications, J2EE, and HTTP Servers Planning an Installation*

  Provides the user with a first reference point for installation or upgrade of agents for WebSphere Applications, J2EE, and HTTP Servers.
- *IBM Tivoli Composite Application Manager: Agent for WebSphere Applications Installation and Configuration Guide*

  Provides installation instructions for setting up and configuring ITCAM Agent for WebSphere Applications on distributed 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*

Provides 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: Agents for WebSphere Applications, J2EE, and HTTP Servers Troubleshooting Guide*

  Provides instructions on problem determination and troubleshooting for agents for WebSphere Applications, J2EE, and HTTP Servers.
- *IBM Tivoli Composite Application Manager: Agents for WebSphere Applications, J2EE, and HTTP Servers: Messaging Guide*

  Provides information about system messages received when installing and using agents for WebSphere Applications, J2EE, and HTTP Servers.
- *IBM Tivoli Composite Application Manager: Agent for WebSphere Applications Reporting Guide*

  Provides information about installing Agent for WebSphere Applications Reports and creating pre-defined and ad-hoc reports.

Related publications

The following documentation also provides useful information:

- IBM Tivoli Documentation Central:

  Information about IBM Tivoli Documentation is provided on the following website:

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

  Information about IBM WebSphere Application Server is provided on the following website:

  http://www.ibm.com/software/webservers/appserv/was/library
- ITCAM for Application Diagnostics library:

  Information about ITCAM for Application Diagnostics Managing Server is provided on the following website:

  http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/index.jsp?topic=%2Fcom.ibm.itcamfad.doc_7101%2Fic-homepage.html
- IBM DB2®:

  Information about IBM DB2 is provided on the following website:

  http://www.ibm.com/software/data/sw-library/
- Tivoli Data Warehouse

  Information about Tivoli Data Warehouse is provided on the following website:

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

  Information about IBM Tivoli Monitoring is provided on the following website:

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

  Information about IBM Tivoli products is provided on the following website:

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

- IBM Tivoli Composite Application Manager for WebSphere Application Server 7.2 support for WebSphere Application Server 8.5: Installation and User Guide:

  The guide is available in the Integrated Service Management (ISM) library on the following website:

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

  The guide is available from the ITCAM for Applications Diagnostics beta. For more information about how to access the beta site, see the following website:

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

Accessing terminology online

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

Accessing publications online

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

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

Ordering publications

You can order many Tivoli publications online at: http://www.ibm.com/e-business/weblink/publications/servlet/pbi.wss.

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 http://www.ibm.com/e-business/weblink/publications/servlet/pbi.wss
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 347.

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 website:

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

Tivoli user groups

Tivoli user groups are independent, user-run membership organizations that provide Tivoli users with information to assist them in the implementation of Tivoli Software solutions. Through these groups, members can share information and learn from the knowledge and experience of other Tivoli users. For more information about Tivoli Users Group, see www.tivoli-ug.org.

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

Access the IBM Software Support site at http://www.ibm.com/software/support/probsub.html .

Troubleshooting Guide

For more information about resolving problems, see the *IBM Tivoli Composite Application Manager: Agents for WebSphere Applications, J2EE, and HTTP Servers 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 guide refers to the following variables:

- *ITM_home*: the top-level directory for installation of IBM Tivoli Monitoring components, including ITCAM Agent for WebSphere Applications. The default location is `C:\IBM\ITM` on Windows systems and `/opt/IBM/ITM` on Linux and UNIX systems:
- *DC_home*: the directory where the data collector files are installed. The default location is *`ITM_home`*`\dchome\`*`DC_version`* on Windows systems, *`ITM_home`*`/dchome/`*`DC_version`* on Linux and UNIX systems.
- *AppServer_home*: the directory where the application server core product files are installed.

  Examples:

  – on Windows, `C:\Program Files\IBM\WebSphere\AppServer`

  – on Linux and UNIX systems, `/opt/IBM/WebSphere/AppServer`

Part 1. Introduction to ITCAM Agent for WebSphere Applications

Chapter 1. IBM Tivoli Composite Application Manager Agent for WebSphere Applications

The ITCAM Agent for WebSphere Applications can help you to monitor, administer, and diagnose your systems that run IBM WebSphere Application Server.

Overview of the monitoring and diagnostic capabilities

ITCAM Agent for WebSphere Applications 7.2 is a component of ITCAM for Applications version 7.2.

ITCAM Agent for WebSphere Applications can function within two different infrastructures: IBM Tivoli Monitoring and ITCAM for Application Diagnostics Managing Server.

The IBM Tivoli Monitoring environment places this agent into the context of the IBM Tivoli Monitoring family, a suite of products used to monitor a mixed-systems environment. With IBM Tivoli Monitoring, you can do the following tasks:

- Monitor for alerts on the managed systems
- Trace the causes leading up to an alert
- Monitor processing time for various requests within WebSphere applications
- Establish your own performance thresholds
- Create custom situations, which are conditions that are automatically monitored by IBM Tivoli Monitoring
- Create and send commands to control system monitoring using the Take Action feature
- Create comprehensive reports about system conditions
- Define your own queries, using the attributes that are provided with ITCAM Agent for WebSphere Applications, to monitor conditions of particular interest to you

The Tivoli Enterprise Portal is the user interface for the IBM Tivoli Monitoring environment. It provides an overall view of the enterprise network; from this view, you can *drill down* to examine components of the environment more closely. The portal includes information from different agents that monitor various parts of the environment; ITCAM Agent for WebSphere Applications is one of them.

For details on the capabilities of IBM Tivoli Monitoring, and information about deploying the IBM Tivoli Monitoring infrastructure, see *IBM Tivoli Monitoring: Installation and Setup Guide*.

Figure 1 on page 4 shows how ITCAM Agent for WebSphere Applications interacts with other IBM Tivoli Monitoring components.

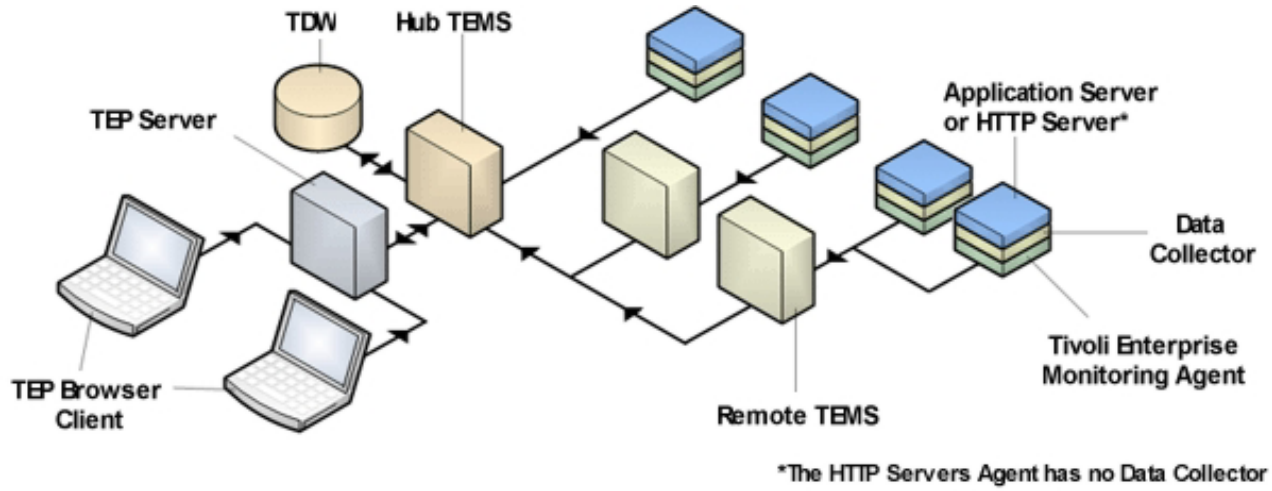

Figure 1. Agent interaction with IBM Tivoli Monitoring

The Managing Server is a component of ITCAM for Application Diagnostics. Its visualization engine provides a user interface for *deep-dive* diagnostics information. The user can *click through* or *launch in context* to the visualization engine from the Tivoli Enterprise Portal when detailed information is required. The visualization engine can also be used as a stand-alone user interface; this user interface is a good solution for software developers and performance analysts.

Important: The managing server deep-dive functionality is not available in ITCAM for Applications version 7.2. You can ignore all references to the ITCAM for Application Diagnostics Managing Server, unless you have an ITCAM for Application Diagnostics Managing Server installed in your environment as part of an ITCAM for Application Diagnostics 7.1.0.3 installation.

Most information that is provided by ITCAM Agent for WebSphere Applications and available through the Tivoli Enterprise Portal can be viewed through the visualization engine. The visualization engine also provides additional diagnostic information, including the following types:

- Method entry/exit and stack tracing
- Lock analysis
- Heap object analysis for memory leak diagnosis
- Thread information
- *In-flight* request analysis to detect malfunctioning applications

For details about the capabilities of ITCAM for Application Diagnostics Managing Server, and information about deploying it, see *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

Figure 2 on page 5 shows how ITCAM Agent for WebSphere Applications interacts with the components of the managing server. (The data collector is a component of the agent).

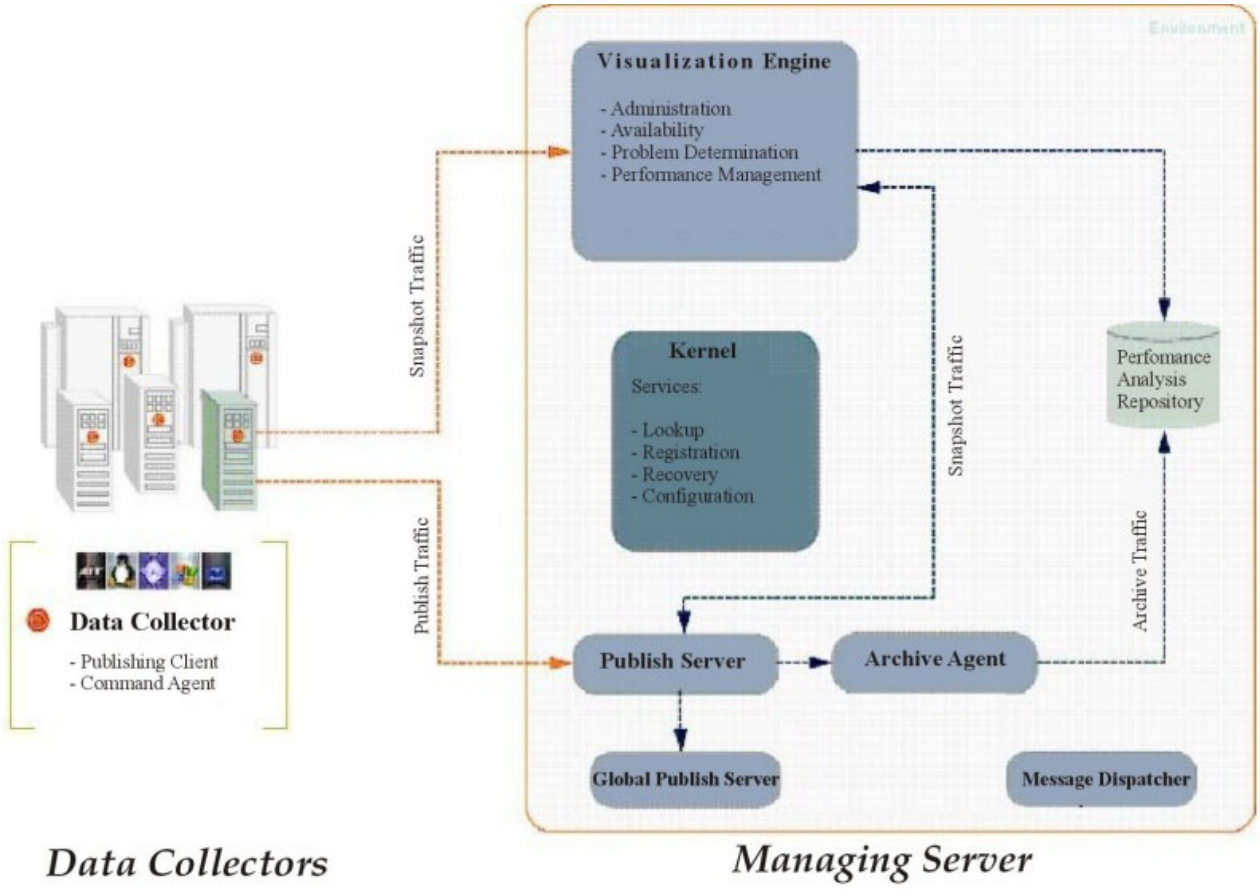

Figure 2. Agent interaction with ITCAM for Application Diagnostics Managing Server

Components of the agent

ITCAM Agent for WebSphere Applications has two components: the *data collector* and the *monitoring agent*. These components are deployed on every monitored host (except the deployment manager in WebSphere Network Deployment, Virtual Enterprise, Compute Grid, and WebSphere eXtreme Scale environments) by a single installation package.

When installing ITCAM Agent for WebSphere Applications interactively, the installation of the monitoring agent automatically triggers the installation of the data collector to a directory you specify. For interaction with IBM Tivoli Monitoring, the agent provides *application support files* that are to be installed on servers and clients in the IBM Tivoli Monitoring infrastructure.

Data collector

The data collector runs on every monitored host (except the Deployment Manager in WebSphere Network Deployment). The data collector is configured for each instance of the application server.

Beginning with ITCAM Agent for WebSphere Applications version 7.2, a new data collector, ITCAM Data Collector for WebSphere, is introduced to collect monitoring

and diagnostic information from application servers. The data collector collects monitoring and diagnostics information from the application server using the following methods:

Byte Code Instrumentation (BCI)
The data collector injects monitoring calls into the code that processes application requests. Data is collected on request processing time and on the different types of JEE API calls within each request.

BCI monitoring requirements can differ. On a production system, request level monitoring might be sufficient. However, on a test or development system, or when a problem is being investigated, BCI can be used to instrument application method entry and exit, synchronized methods, and object allocation.

BCI uses a certain amount of system resources, depending on the amount of injected calls. The level of detail, and thus the use of resources, is determined by the *monitoring level*, which can be set for every monitored application server. With the Tivoli Monitoring infrastructure, levels L1 and L2 are supported; with the ITCAM for Application Diagnostics Managing Server, the additional level L3 is available. The monitoring level can be set for each application server instance, independently of the Tivoli Monitoring components and the managing server.

Performance Monitoring Interface (PMI)
An API provided by WebSphere Application Server, supplying a number of performance metrics.

Garbage Collection logs
The logs are written by WebSphere Application Server and contain detailed information about the garbage collection process. This information is useful for application monitoring and enhancement.

The data collector is shared with the following products:

- ITCAM for SOA version 7.2 and later
- ITCAM for WebSphere Application Server version 7.2 support for WebSphere Application Server version 8.5 and later
- ITCAM Diagnostics Tool that is previewed in the ITCAM for Application Diagnostics beta

Important: If a WebSphere Application Server installation has multiple profiles, all application servers in a single profile must run the same version of ITCAM Data Collector for WebSphere.

In ITCAM Agent for WebSphere Applications version 7.2, after you install the monitoring agent, you are prompted to install the data collector in a location that you specify. Using the ITCAM Data Collector for WebSphere Configuration utility, you can integrate the data collector with the following components:

- ITCAM Agent for WebSphere Applications monitoring agent
- ITCAM for Application Diagnostics Managing Server
- ITCAM for SOA monitoring agent
- Tivoli Performance Viewer, available from the WebSphere administrative console
- ITCAM Diagnostics Tool that is previewed in the ITCAM for Application Diagnostics beta
- ITCAM for Transactions

Integrating with ITCAM Agent for WebSphere Applications monitoring agent

The ITCAM Agent for WebSphere Applications monitoring agent collects information from the data collector, and processes and aggregates it for presentation to the user. The monitoring agent sends monitoring information to the Tivoli Enterprise Monitoring Server.

If you are enabling data collection for ITCAM Agent for WebSphere Applications, you can integrate the data collector with ITCAM Agent for WebSphere Applications monitoring agent, or with ITCAM for Application Diagnostics Managing Server, or with both.

You must configure the ITCAM Agent for WebSphere Applications monitoring agent and install its application support files to complete configuration of ITCAM Agent for WebSphere Applications.

For more information about installing and configuring ITCAM Agent for WebSphere Applications, see *IBM Tivoli Composite Application Manager Agent for WebSphere Applications Installation and Configuration Guide*.

Integrating with ITCAM for Application Diagnostics Managing Server

The managing server is an optional component of ITCAM for Application Diagnostics. The managing server collects information from, and provides services to, the data collector. Through its visualization engine user interface, the managing server provides detailed diagnostics information.

If you have ITCAM for Application Diagnostics version 7.1.0.3 or later installed in your environment, you can integrate ITCAM Data Collector for WebSphere with the managing server. For information about installing and configuring the managing server, see the *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation and Customization Guide*.

Integrating the data collector with ITCAM for SOA

ITCAM for SOA provides real-time monitoring of the SOA lifecycle to ensure high availability and performance. You can integrate the data collector with the ITCAM for SOA monitoring agent.

You might have a version of ITCAM for SOA installed and configured for applications servers in the same WebSphere profile in which you plan to configure data collection for ITCAM Agent for WebSphere Applications. Depending on whether ITCAM for SOA is configured, complete these steps:

- If ITCAM for SOA version 7.2 is configured for the same WebSphere profile, and the data collector is at the same maintenance level, reuse the data collector installation.
- If ITCAM for SOA version 7.2 is configured for the same WebSphere profile, and the data collector is at an lower maintenance level, migrate the data collector to the latest maintenance level. Reconfigure the data collector to integrate it with the ITCAM Agent for WebSphere Applications monitoring agent or the managing server, or both.
- If ITCAM for SOA version 7.2 is not installed, you can integrate the data collector with the ITCAM for SOA monitoring agent when you configure data collection for ITCAM Agent for WebSphere Applications. For information about the additional procedures you must complete to configure ITCAM for SOA, see the *IBM Tivoli Composite Application Manager for SOA Installation Guide*.

- If the ITCAM for SOA version 7.1.1 WebSphere Application Server data collector is configured for the same WebSphere profile in which you plan to install and configure data collection for ITCAM Agent for WebSphere Applications, migrate the ITCAM for SOA data collector before configuring data collection for ITCAM Agent for WebSphere Applications. After migration, the data collector communicates with the ITCAM for SOA version 7.1.1 monitoring agent.
- If the ITCAM for SOA version 7.1.1 WebSphere Application Server data collector is configured for the same WebSphere profile in which you plan to upgrade and configure data collection for ITCAM Agent for WebSphere Applications, migrate the ITCAM Agent for WebSphere Applications data collector to ITCAM Data Collector for WebSphere. Reconfigure the data collector to communicate with the ITCAM for SOA version 7.1.1 monitoring agent. You must not use the migration utility to migrate the ITCAM for SOA WebSphere Application Server data collector.

Integrating with Tivoli Performance Viewer

ITCAM for WebSphere Application Server monitors the performance of the WebSphere Application Server. PMI metrics are gathered with the data collector.

The data that ITCAM for WebSphere Application Server provides augments the data provided by the application server through the existing PMI statistics. The metrics collected by ITCAM for WebSphere Application Server can be viewed in the Tivoli Performance Viewer (TPV). You can access the TPV from the WebSphere Application Server administrative console.

The latest version of ITCAM for WebSphere Application Server is ITCAM for WebSphere Application Server version 7.2 support for WebSphere Application Server 8.5. This version includes ITCAM Data Collector for WebSphere.

You might have a version of ITCAM for WebSphere Application Server installed and configured for applications servers in the same WebSphere profile in which you plan to configure data collection for ITCAM Agent for WebSphere Applications. Depending on whether ITCAM for WebSphere Application Server is configured, complete these steps:

- If ITCAM for WebSphere Application Server version 7.2 support for WebSphere Application Server 8.5 is configured for the same WebSphere profile, and the data collector is at the same maintenance level, reuse the data collector installation.
- If ITCAM for WebSphere Application Server version 7.2 support for WebSphere Application Server 8.5 is configured for the same WebSphere profile, and the data collector is at an earlier maintenance level, migrate the data collector to the latest maintenance level. Reconfigure the data collector to integrate it with the ITCAM Agent for WebSphere Applications monitoring agent or the managing server, or both.
- If WebSphere Application Server version 7.2 support for WebSphere Application Server 8.5 is not installed, you can integrate the data collector with the TPV when configuring data collection for ITCAM Agent for WebSphere Applications. For information about using ITCAM for WebSphere Application Server version 7.2 support for WebSphere Application Server 8.5, see the *IBM Tivoli Composite Application Manager for WebSphere Application Server 72 support for WebSphere Application Server 8.5: Installation and User Guide*.
- If ITCAM for WebSphere Application Server version 7.2 is configured for the same WebSphere profile, you must migrate the ITCAM for WebSphere Application Server data collector before configuring data collection for ITCAM

Agent for WebSphere Applications. ITCAM for WebSphere Application Server version 7.2 is used to monitor WebSphere Application Server version 8.

Important: Server monitoring provided by ITCAM for WebSphere Application Server in the WebSphere Administrative Console continues after the migration.

Integrating with ITCAM Diagnostics Tool

ITCAM Diagnostics Tool is used for diagnostic investigation of applications that run on a WebSphere Application Server. The tool is based on Eclipse. You can analyze data in real time or you can save diagnostic information to a file for later analysis. The tool is previewed in the ITCAM for Application Diagnostics beta.

You might have a version of ITCAM Diagnostics Tool installed and configured for applications servers in the same WebSphere profile in which you plan to configure data collection for ITCAM Agent for WebSphere Applications. Depending on whether ITCAM Diagnostics Tool is configured, complete these steps:

- If ITCAM Diagnostics Tool is configured for the same WebSphere profile, and the data collector is at the same maintenance level, reuse the data collector installation.
- If ITCAM Diagnostics Tool is configured for the same WebSphere profile, and the data collector is at an earlier maintenance level, migrate the data collector to the latest maintenance level. Reconfigure the data collector to integrate it with the ITCAM Agent for WebSphere Applications monitoring agent or the managing server, or both.
- If ITCAM Diagnostics Tool is not installed, you can integrate the data collector with the ITCAM Diagnostics Tool when configuring data collection for ITCAM Agent for WebSphere Applications. For information about using the ITCAM Diagnostics Tool, see the *ITCAM Diagnostics Tool Installation Guide*.

Integrating with ITCAM for Transactions

ITCAM for Transactions tracks transactions within and among applications. The product determines the time spent by the transaction in each application and, where possible, the time spent communicating between applications.

The data collector can be configured to construct and send tracking events through the Transaction Tracking Application Programming Interface (TTAPI) to the ITCAM for Transactions Transaction Collector. ITCAM for Transactions displays the aggregated transaction information and topology in workspaces.

To integrate the data collector with ITCAM for Transactions, you must install ITCAM for Transactions version 7.3 or later within an IBM Tivoli Monitoring environment.

For details of further configuration options and how to view the aggregated transaction information, see *IBM Tivoli Composite Application Agent for WebSphere Applications Configuring and Using TTAPI*.

Monitoring agent

The monitoring agent collects information from the data collector, and processes and aggregates it for presentation. It also parses application server logs.

When cell monitoring is configured in a WebSphere Virtual Enterprise or a Websphere Compute Grid deployment, the monitoring agent communicates with the Deployment Manager over the network to retrieve configuration and performance information for the cell.

Important: Starting in WebSphere Application Server version 8.5, WebSphere Virtual Enterprise and WebSphere Compute Grid are integrated into WebSphere Application Server Network Deployment version 8.5. WebSphere Virtual Enterprise functions in Network Deployment version 8.5 are characterized as intelligent management capabilities. WebSphere Compute Grid functions in Network Deployment version 8.5 are characterized as WebSphere batch capabilities.

The monitoring agent sends monitoring information to the Tivoli Enterprise Monitoring Server. It also receives Take Action commands from the Tivoli Enterprise Monitoring Server. When these commands involve server management actions (starting, stopping, or restarting the application server), the monitoring agent takes these actions.

Application support files

To enable ITCAM Agent for WebSphere Applications interaction with IBM Tivoli Monitoring, the application support files shipped with the agent must be installed on all hub and remote Tivoli Enterprise Monitoring Servers, all Tivoli Enterprise Portal Servers, and Tivoli Enterprise Portal clients except browser-based clients.

On the Tivoli Enterprise Monitoring Server, support files provide the ITCAM Agent for WebSphere Applications data tables and situations.

On the Tivoli Enterprise Portal Server, support files provide the ITCAM Agent for WebSphere Applications workspaces that display the monitoring information and include code that processes situation information for the Summary workspaces.

On the Tivoli Enterprise Portal client, support files provide the ITCAM Agent for WebSphere Applications Helps and Language Packs.

When self-description is enabled on ITCAM Agent for WebSphere Applications and on the monitoring server, application support files are automatically installed on the monitoring servers and the portal server, without the need to recycle the monitoring servers or the portal server. The conditions that must be met for self-description to operate are specified in “Enabling application support through self-description” on page 62 for Windows systems and “Enabling application support through self-description” on page 145 for Linux and UNIX systems.

Prerequisites to installation

The instructions in the subsequent chapters assume the following:

- If ITCAM Agent for WebSphere Applications communicates with the IBM Tivoli Monitoring infrastructure, you are familiar with basic usage of the Tivoli Enterprise Portal and have installed the base components of this infrastructure, including:
  - A Tivoli Enterprise Monitoring Server (monitoring server)
  - A Tivoli Enterprise Portal (portal) server
  - Tivoli Enterprise Portal clients
- If ITCAM Agent for WebSphere Applications communicates with ITCAM for Application Diagnostics Managing Server, you are familiar with basic usage of the visualization engine.
- Java™ Development Kit (JDK) 1.5 or later is already installed on the computer system where ITCAM Agent for WebSphere Applications will be installed.

To obtain the most recent installation updates, review the Technotes for this product. To access the Technotes, see the *IBM Tivoli Composite Application Manager: Agents for WebSphere Applications, J2EE, and HTTP Servers Troubleshooting Guide*.

System and software prerequisites

See the Software product compatibility reports website to generate a variety of reports related to product and component requirements.

Tip: ITCAM Agent for WebSphere Applications version 7.2 is a component of ITCAM for Applications version 7.2. To run a report specific to ITCAM for Applications version 7.2, specify Tivoli Composite Application Manager for Applications as the product name and 7.2 as the version.

To view the system requirements for ITCAM Agent for WebSphere Applications version 7.2, see the Detailed system requirements report.

Where to begin

Begin at the roadmap for your ITCAM Agent for WebSphere Applications installation.

Table 1. Roadmap for the ITCAM Agent for WebSphere Applications

What to do	Where to find more information
Obtain the installation.	You can get the installation files either by downloading from the web or using a product CD.
Verify that your computer meets the system and software prerequisites.	"System and software prerequisites"
Install the ITCAM Agent for WebSphere Applications monitoring agent and the ITCAM Data Collector for WebSphere.	"Installing the agent on Windows systems" on page 19 "Installing the agent on Linux and UNIX systems" on page 104
Configure the ITCAM Agent for WebSphere Applications monitoring agent and the ITCAM Data Collector for WebSphere.	"Configuring the monitoring agent on Windows systems" on page 32 "Configuring the monitoring agent on Linux and UNIX systems" on page 111
Install application support files.	"Enabling application support on Windows systems" on page 61 "Enabling application support on Linux and UNIX systems" on page 145
(Optional) Install and uninstall a language pack.	"Installing and uninstalling a language pack on Windows systems" on page 92 "Installing and uninstalling a language pack on Linux and UNIX systems" on page 176
(Optional) Install the ITCAM Agent for WebSphere Applications monitoring agent and the ITCAM Data Collector for WebSphere in silent mode.	"Performing a silent installation or uninstallation of the monitoring agent on Windows systems" on page 71 "Performing a silent installation or uninstallation of the monitoring agent on Linux or UNIX" on page 155

Table 1. Roadmap for the ITCAM Agent for WebSphere Applications (continued)

What to do	Where to find more information
Uninstall the ITCAM Agent for WebSphere Applications monitoring agent and the ITCAM Data Collector for WebSphere.	"Uninstalling ITCAM Agent for WebSphere Applications on Windows systems" on page 91 "Uninstalling ITCAM Agent for WebSphere Applications on Linux and UNIX systems" on page 176

Part 2. Installing and Configuring ITCAM Agent for WebSphere Applications on Windows

Chapter 2. Prerequisites and pre-installation tasks for ITCAM Agent for WebSphere Applications on Windows systems

You must complete a number of tasks before you install the ITCAM Agent for WebSphere Applications on a Windows system.

System and software prerequisites

See the Software product compatibility reports website to generate a variety of reports related to product and component requirements.

Tip: ITCAM Agent for WebSphere Applications version 7.2 is a component of ITCAM for Applications version 7.2.1. To run a report specific to ITCAM for Applications version 7.2.1, specify Tivoli Composite Application Manager for Applications as the product name and 7.2.1 as the version.

To view the system requirements for ITCAM Agent for WebSphere Applications version 7.2, see the Detailed system requirements report.

Required tasks before installation

Complete the tasks in each of the following sections before you start installing ITCAM Agent for WebSphere Applications.

Permissions

The user who installs ITCAM Agent for WebSphere Applications on a Windows system must have administrator privileges.

For information about the permissions required to run the data collector configuration, reconfiguration, migration, and unconfiguration utilities in interactive mode and silent mode, see “Permissions required for configuration tasks” on page 37.

Adjusting for ports that are blocked by your firewall or that are used by other applications

During the installation, you must specify or accept the defaults for port numbers that are used by ITCAM Agent for WebSphere Applications.

By default, ITCAM Agent for WebSphere Applications communicates in the following ways:

- If the IBM Tivoli Monitoring infrastructure is used, the agent makes outbound connections to the Tivoli Enterprise Monitoring Server host.
- If a managing server is used, and the data collector is configured for one or more application server instances, it opens ports in the 8200 - 8399 range for inbound communication.
- With WebSphere Network Deployment, WebSphere Virtual Enterprise, or WebSphere Compute Grid environments, the agent makes outbound connections to the deployment manager host. The port number is available in the deployment manager administrative console.

Remember: WebSphere Virtual Enterprise functions in Network Deployment version 8.5 are characterized as intelligent management capabilities. WebSphere Compute Grid functions in Network Deployment version 8.5 are characterized as WebSphere batch capabilities.

You must ensure that these connections are not blocked by a firewall. If they are blocked, you must either modify the communication settings during installation and configuration of the data collector, or change the settings of the firewall. To determine the connections that your firewall might block, see the documentation that is supplied with the firewall.

If you use the managing server, you must also make sure that ports that are used for inbound communication are not used by other applications. If they are used by other applications, you must change the ports for data collector inbound communication when configuring the data collector. For more information, see "Configuring ITCAM Data Collector for WebSphere" on page 39. To list the ports that are used by other applications, run the `netstat -a` command; In its output, look for lines that include `LISTENING`.

Increasing the heap size

To increase the heap size configuration to 128 MB greater than the current configuration, complete the following steps from the WebSphere administrative console for each server that you want to configure for data collection:

1. Log in to the IBM WebSphere Application Server administrative console.
2. Click **Server** > **Server Types** > **WebSphere Application Servers** and select the *server_name*.
3. In the **Configuration** tab, go to **Server Infrastructure** > **Java and Process Management** > **Process Definition** > **Additional Properties: Java Virtual Machine**.
4. Edit the **Maximum Heap Size** field. If the default is not specified, then it assumes `256`.

WebSphere Global Security: setting the user name and password in client properties files

The data collector must communicate with WebSphere Administrative Services using the Remote Method Invocation (RMI) or the Simple Object Access Protocol (SOAP) protocol. If WebSphere Global Security is enabled, this communication requires a user name and password. You can set them when configuring the data collector to monitor an application server instance. For security reasons, you might prefer to encrypt the user name and password and store them in client properties files before configuring the data collector.

Use the `sas.client.props` file for an RMI connection, or the `soap.client.props` file for a SOAP connection.

Important: If you complete this operation, you must do it separately for each monitored application server profile.

Enabling user ID and password input from the sas.client.props file for RMI connector types

When you use an RMI connection to WebSphere Application Server and global security is enabled, you can use the ITCAM Data Collector for WebSphere configuration utilities to retrieve the user ID and password from a `sas.client.props` file.

To retrieve the user ID and password from the sas.client.props file, complete the following steps:

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

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

2. Run the following command to encrypt the password:

   ```
   PropFilePasswordEncoder.bat path_to_props_file\sas.client.props
   com.ibm.CORBA.loginPassword
   ```

   Run it from the *AppServer_home*\profiles*profile_name*\bin directory.

Enabling user ID and password input from the soap.client.props file for SOAP connector types

When you use a SOAP connection to WebSphere Application Server and global security is enabled, you can use the ITCAM Data Collector for WebSphere configuration utilities to retrieve the user ID and password from a soap.client.props file.

To retrieve the user ID and password from the soap.client.props file, complete these steps:

1. Set the following properties in the *AppServer_home*\profiles*profile_name*\properties\soap.client.props file on Linux or UNIX systems:

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

2. Run the following command on Windows systems to encrypt the password:

   ```
   PropFilePasswordEncoder.bat
     AppServer_home\profiles\profile_name\properties\soap.client.props
     com.ibm.SOAP.loginPassword
   ```

   Run it from the *AppServer_home*\profiles*profile_name*\bin directory.

Verifying that prerequisite packages have been installed correctly.

Optionally, verify that the prerequisite packages for ITCAM Agent for WebSphere Applications are installed correctly before launching the installer.
The Environment Checking Utility (ECU) generates a report of the operating-system packages and libraries installed. From the report, you can determine if the system prerequisites have been met. For more information about generating an ECU report, see the *IBM Tivoli Composite Application Manager Agents for WebSphere Applications, J2EE, and HTTP Servers Troubleshooting Guide*.

User Account Control settings on Windows 7 platform

On Windows 7 platforms, the User Account Control (UAC) setting is set to level 3, Notify me only when programs try to make changes to my computer, by default. Level 3 is the recommended setting for installing ITCAM Agent for WebSphere Applications in interactive and silent mode on a local system. All other settings are restrictive.

To verify that the value of the UAC setting is set to level 3, go to **Start** -> **Control Panel** -> **Action Center** -> **Change User Account Control Settings**.

The ITCAM Agent for WebSphere Applications installer must be run as the administrator to ensure that sufficient permissions are granted before the installation or upgrade begins. To run the installer as the administrator, right-click the `setup.exe` file in the file explorer and choose **Run as Administrator**.

Important: Remote deployment of ITCAM Agent for WebSphere Applications on a remote Windows 7 platform is not supported.

What to do next

1. Close all other applications.
2. For more information, see "Installing the agent on Windows systems" on page 19.

Chapter 3. Installing and configuring ITCAM Agent for WebSphere Applications on Windows systems

Use the installation utility to install ITCAM Agent for WebSphere Applications on a Windows system.

In older versions of ITCAM Agent for WebSphere Applications, you install the data collector when installing the monitoring agent. Beginning with version 7.2, you install the monitoring agent first. After you install the monitoring agent, you install ITCAM Data Collector for WebSphere in a location that you specify. A configuration tool, ITCAM Data Collector for WebSphere Configuration utility (`config.bat`), is used to configure the data collector.

With the configuration utility, you can integrate the data collector with the following components:

- ITCAM for SOA monitoring agent
- ITCAM Agent for WebSphere Applications monitoring agent
- ITCAM for Application Diagnostics Managing Server
- Tivoli Performance Viewer, available from the WebSphere administrative console
- ITCAM Diagnostics Tool that is previewed in the ITCAM for Application Diagnostics beta

If you integrate the data collector with the managing server only, you must configure the monitoring agent so that it does *not* communicate with a Tivoli Enterprise Monitoring Server, and ensure that the monitoring agent is not started automatically.

New utilities are also provided for configuring the data collector. The utilities that you use and the configuration options that you choose in each utility depend on whether you are installing or upgrading the data collector and whether the same version or an older version of the data collector is configured for the same WebSphere profile in which you plan to enable data collection.

If you are performing an installation of ITCAM Agent for WebSphere Applications, review the installation scenarios. See the "Installing ITCAM Agent for WebSphere Applications version 7.2 and configuring ITCAM Data Collector for WebSphere" section in *IBM Tivoli Composite Application Manager Agents for WebSphere Applications, J2EE, and HTTP Servers: Planning an Installation* guide.

If you are performing an upgrade of ITCAM Agent for WebSphere Applications, review the upgrade scenarios. See the "Upgrading to ITCAM Agent for WebSphere Applications version 7.2 and configuring ITCAM Data Collector for WebSphere" section in *IBM Tivoli Composite Application Manager Agents for WebSphere Applications, J2EE, and HTTP Servers: Planning an Installation* guide.

Installing the agent on Windows systems

If ITCAM Agent for WebSphere Applications version 7.2 is already installed on the host, you can use this process to reinstall it. You are not prompted to specify the installation directory, the encryption key, and the program folder; the reinstallation uses the same settings as the existing installation.

Use the same process to upgrade the monitoring agent, if a monitoring agent is already installed on the host by any of the following products:

- ITCAM for WebSphere version 6.1.0.4 or later
- WebSphere Tivoli Enterprise Monitoring Agent version 6.2.0.4 or later included in ITCAM for Web Resources version 6.2.0.4 or later
- ITCAM Agent for WebSphere Applications version 7.1 included in ITCAM for Applications Diagnostics version 7.1

To upgrade to the data collector component of ITCAM Agent for WebSphere Applications version 7.2, you must upgrade monitoring of application server instances to use ITCAM Data Collector for WebSphere using the migration command-line utility. For more information about migrating the data collector, see "Migrating data collectors to ITCAM Data Collector for WebSphere" on page 54.

Before starting the process, make sure the Manage Tivoli Enterprise Monitoring Services (MTMS) utility is not running. If it is running, stop it. If the utility is running, the upgrade or installation might fail.

Before installing the agent, you must know the host name and IP address for the Tivoli Enterprise Monitoring Server that is to be used.

Step 1: Start setup.exe

When you load the ITCAM Agent for WebSphere Applications installation media, locate and double-click the `setup.exe` file within the WINDOWS directory.

Important: On Windows 7 platforms, the ITCAM Agent for WebSphere Applications installer must be run as the administrator to ensure that sufficient permissions are granted before the installation or upgrade begins. Right-click the `setup.exe` file in the file explorer and choose **Run as Administrator**.

The initial InstallShield window opens.

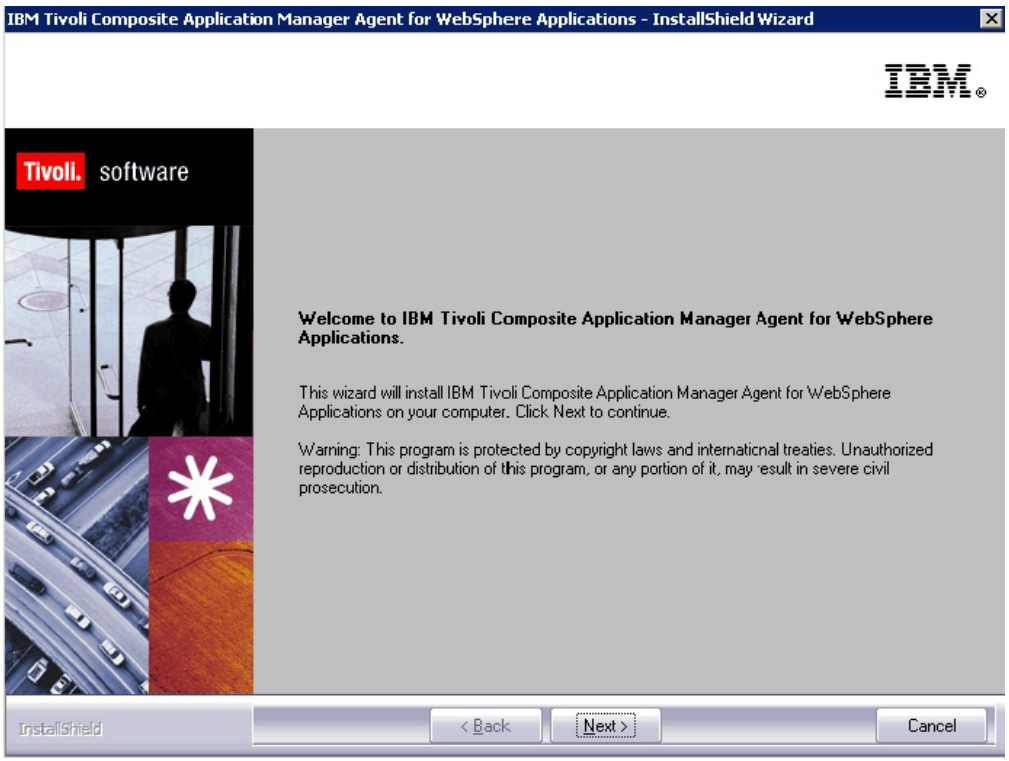

Figure 3. Installation Welcome window

Click **Next**. The product prerequisites window opens.

Figure 4. Prerequisites window

If the environment meets the prerequisites, click **Next**.

Step 2: Accept the product license

The Software License Agreement window is displayed.

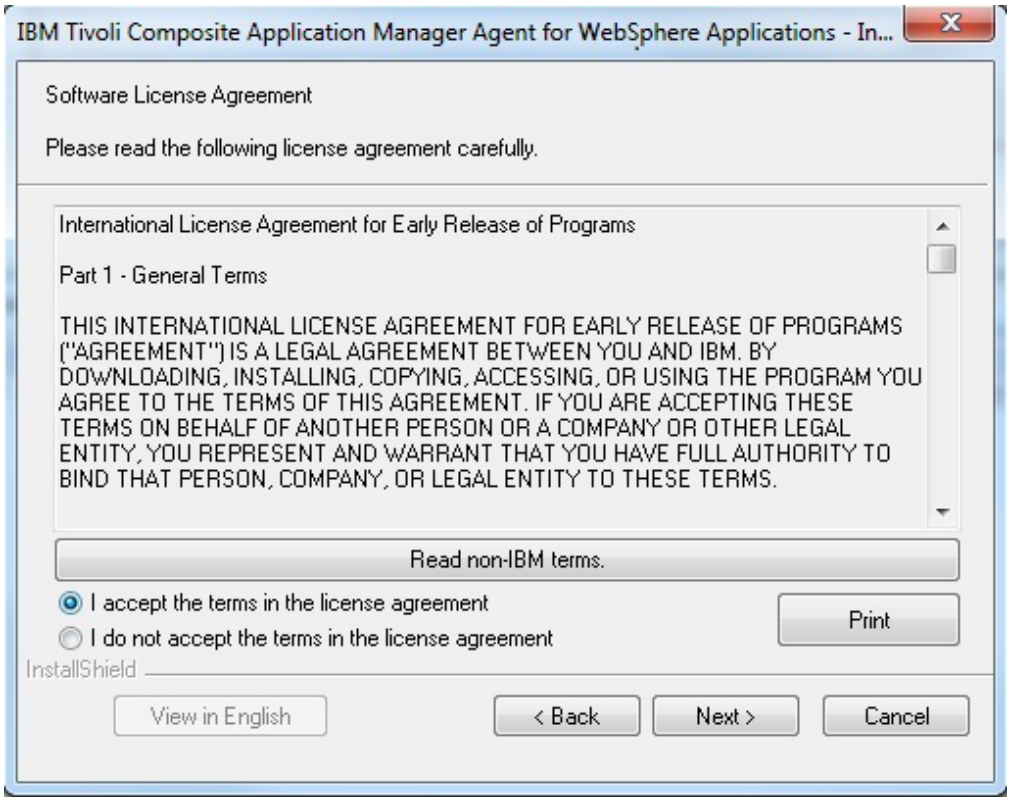

Figure 5. Software License Agreement window

If you accept the terms of the license agreement, select **I accept the terms in the license agreement** and click **Next**.

Step 3: Choose the destination folder for the installation files

If the current version of the agent is already installed on the host, the destination directory is determined automatically and this step is skipped. On a new installation, upgrade, or update, the **Choose destination location** window opens.

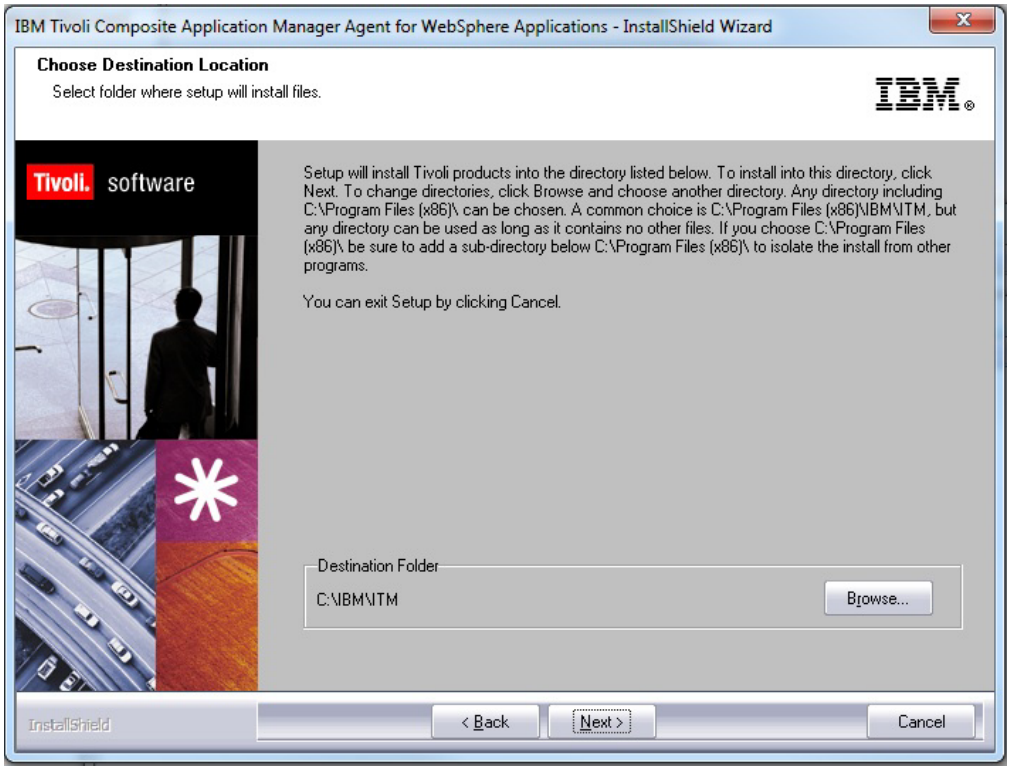

Figure 6. Choose Destination Location window

This window shows the folder (*ITM_home*) where the agent is to be installed. The destination folder can be shared with other IBM Tivoli Monitoring products. To use a location other than the default (`C:\IBM\ITM`), click **Browse**, and select the folder that you want to use.

After the correct folder is specified, click **Next**.

Step 4: Enter the IBM Tivoli Monitoring encryption key

In an upgrade installation or a reinstallation, or when some IBM Tivoli Monitoring components are already installed, the data encryption key is already set, and this step is skipped. On a new installation, the **User Data Encryption Key** window opens. It prompts you for the 32-character encryption key used to secure password transmission and other sensitive data across your IBM Tivoli Monitoring environment.

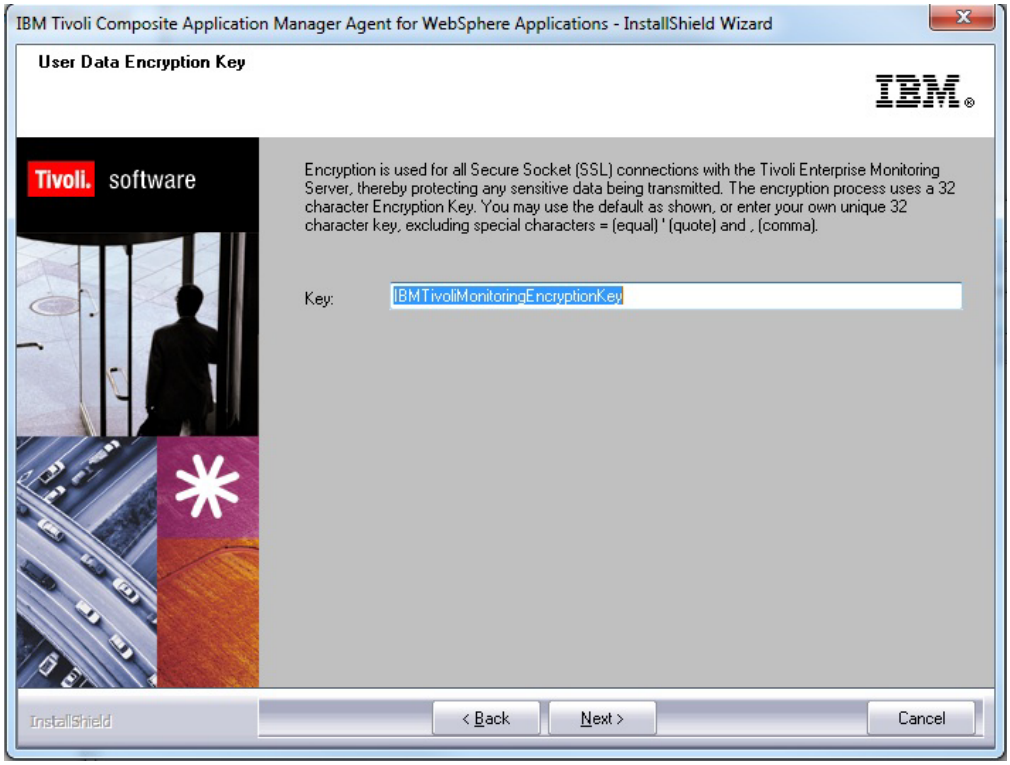

Figure 7. User Data Encryption Key window

For details about the encryption key, see *IBM Tivoli Monitoring: Installation and Setup Guide*. When you specify the key, click **Next**.

A confirmation window opens.

Figure 8. Encryption Key confirmation window

To confirm the encryption key, click **OK**.

Step 5: Select the product components you want to install

The **Select Features** window is displayed.

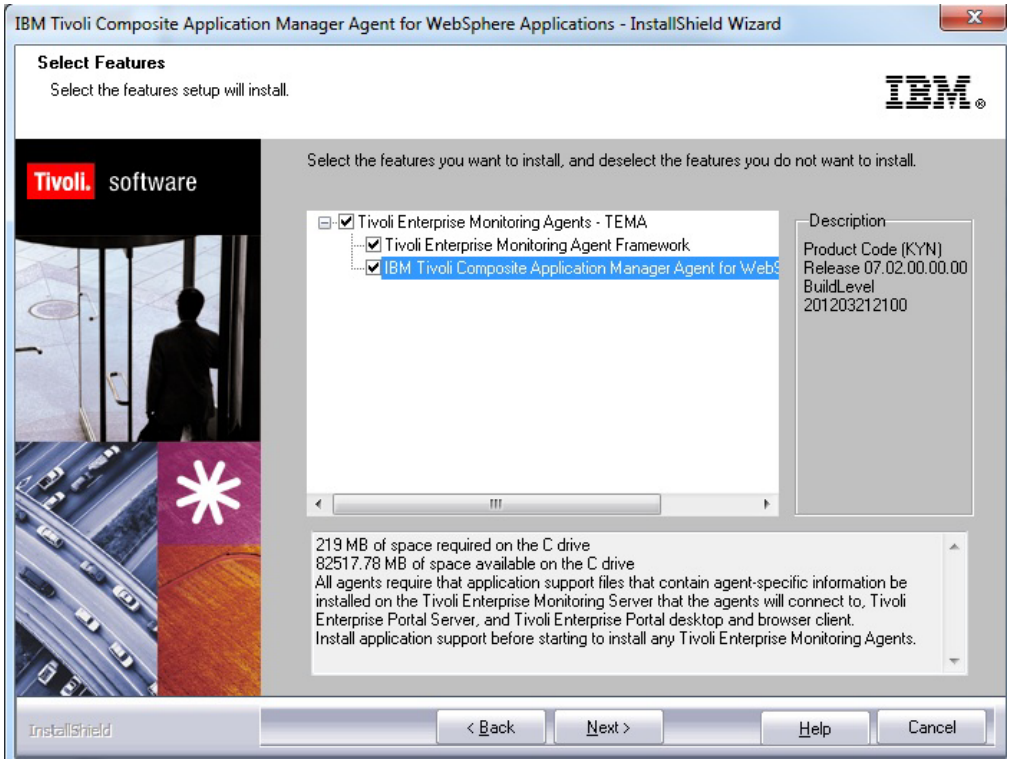

Figure 9. Select Features window

Select **Tivoli Enterprise Monitoring Agents - TEMA**. This window might vary if the IBM Tivoli Monitoring framework is already installed on this host.

Important: If any IBM Tivoli Monitoring Agent is already installed on this host, make sure to expand the tree in this window and explicitly check **IBM Tivoli Composite Application Manager Agent for WebSphere Applications**. By default, if an IBM Tivoli monitoring agent is found, it is not checked even if you check the top-level box.

Click **Next**.

Step 6: Select Windows program folder

If the current version of ITCAM Agent for WebSphere Applications is already installed on the host, the reinstallation uses the same program folder as the existing installation and this step is skipped. On a new or upgrade installation, the **Select Program Folder** window opens. It displays the Windows program folder for IBM Tivoli Monitoring programs.

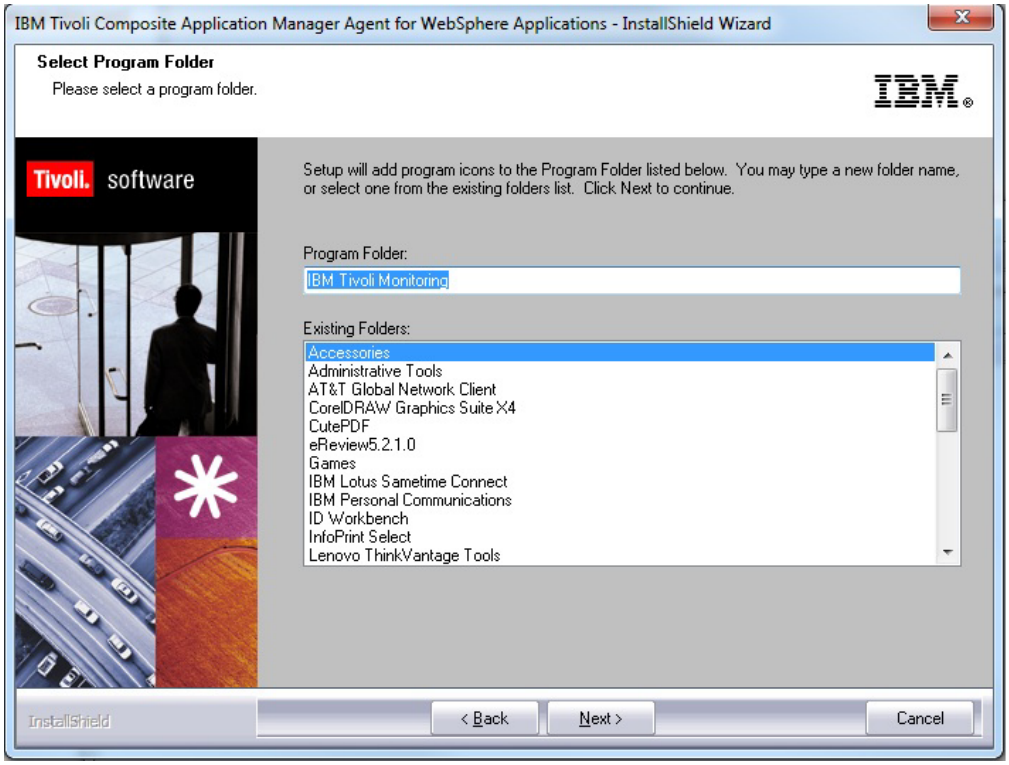

Figure 10. Select Program Folder window

You can modify the name of the folder (under the **Programs** menu) where IBM Tivoli Monitoring programs are listed.

Click **Next**.

Step 7: Verify selected features

The **Start Copying Files** window opens, showing the features that you selected, the disk space requirements for the installation, and the available disk space.

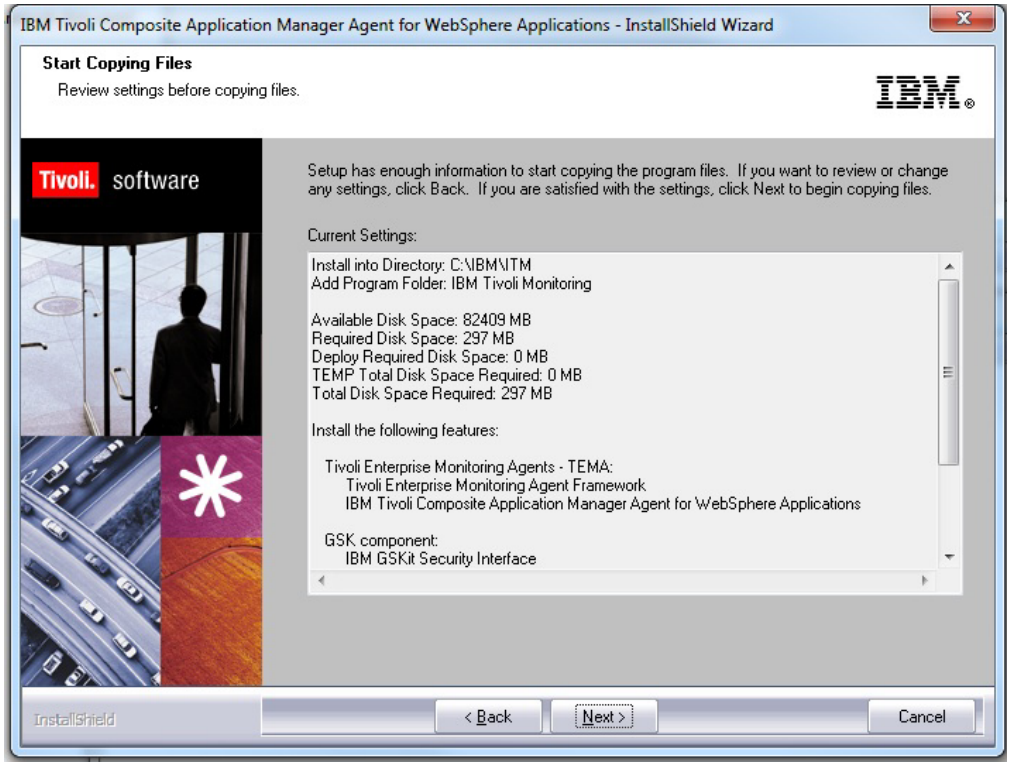

Figure 11. Selected features verification window

Verify that the features that you want to install, including **Monitoring Agent for WebSphere**, are in the list. If you want to make changes, click **Back**.

If the list is correct, click **Next**.

The system displays a warning that you cannot cancel the installation after this point. Click **Yes** to start the installation.

The installer copies the required files to the destination directory.

Step 8: Select the items to configure

When the copying of files is complete, you can select whether to configure the monitoring agent in the **Setup Type** window.

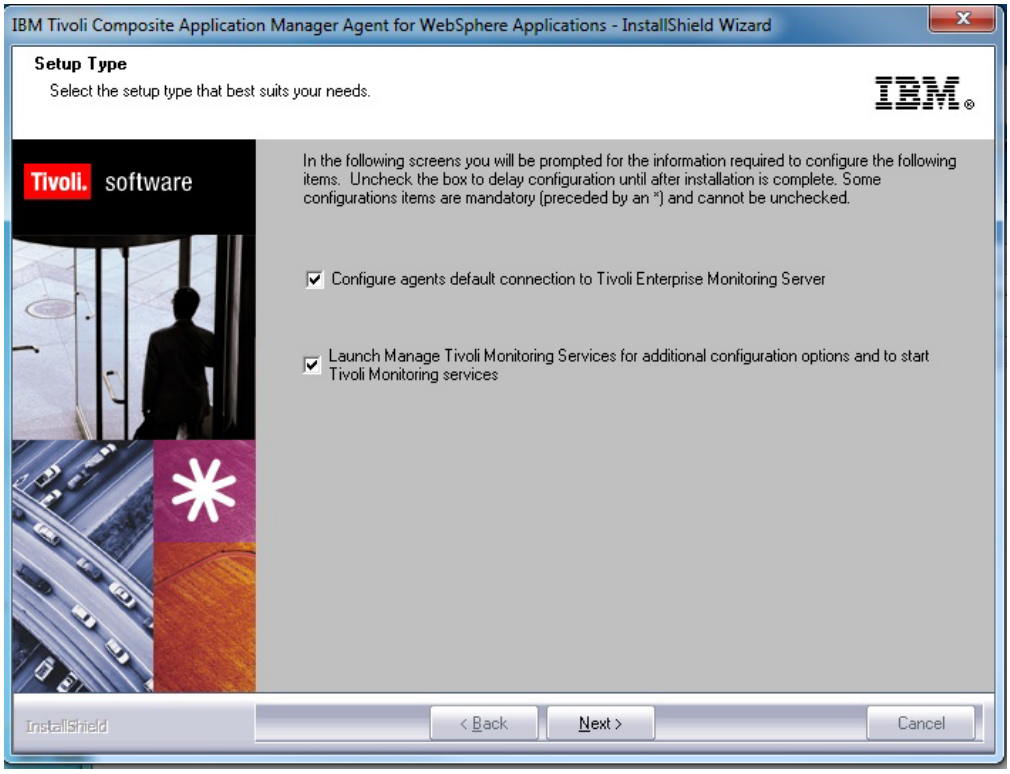

Figure 12. Setup Type window

By default, all of the check boxes are selected. This means that you are prompted to configure the monitoring agent.

If you are *not* using the IBM Tivoli Monitoring infrastructure (in a deep-dive diagnostics-only installation), clear both check boxes. You are still presented with the command-line prompts for installing the data collector so that you can install and configure the data collector to monitor application server instances.

Remember: The managing server deep-dive functionality is not available in ITCAM for Applications 7.2. If you do not have ITCAM for Application Diagnostics version 7.1 installed in your environment, ignore all references to the managing server functionality in this document.

If you use IBM Tivoli Monitoring infrastructure, keep the first check box checked, because you must configure the monitoring agent before the data collector. If you keep the second check box checked, the Managing Tivoli Monitoring Services utility starts after the configuration. Use it to configure automatic starting of the monitoring agent and any other IBM Tivoli Monitoring settings.

When the selections are correct, to finish the installation, click **Next**. If one or both of the configuration options are selected, configuration windows are displayed next. For more information, see "Configuring the monitoring agent on Windows systems" on page 32.

Step 9: Configure the default agent connection the monitoring server

If you did not select **Configure agents default connection to Tivoli Enterprise Monitoring Server** in the "Step 8: Select the items to configure" on page 27, this

step is skipped. Otherwise, for information about configuring the default agent connection to the monitoring server, see “Configuring ITCAM Data Collector for WebSphere” on page 39.

Step 10: Enter the Agent Configuration window

The Agent Configuration window is displayed. If IBM Tivoli Monitoring infrastructure is not used (in a deep-dive diagnostics-only installation with a Managing Server), ignore this window and click **Cancel** to skip to step “Step 12: Installing the data collector.”

For information about configuring the monitoring agent, see “Configuring monitoring agent settings” on page 34.

Step 11: Finalize the installation of the monitoring agent

After you complete all monitoring agent installation and configuration tasks, the Installation Wizard Complete page is displayed. If you choose not to read the product readme file for the last-minute product information, clear the check box.

Click **Finish** to close the installer.

In the next steps, ITCAM Data Collector for WebSphere is installed.

Step 12: Installing the data collector

In an installation or an upgrade, when you complete the configuration of the monitoring agent, the data collector is installed in the location you specify and the data collector configuration utility is launched.

A window is displayed to indicate that the installer has identified additional procedures that need to be performed to complete the installation of the ITCAM Agent for WebSphere Applications.

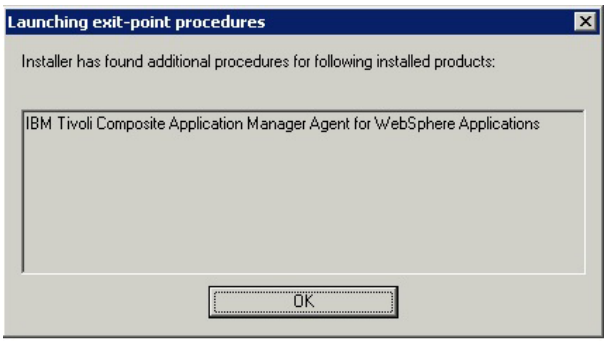

Figure 13. Message indicating that additional procedures have been identified

Click **OK** to close the window.

ITCAM Data Collector for WebSphere in ITCAM Agent for WebSphere Applications version 7.2 is a component that is shared with the following products:

- ITCAM for SOA version 7.2
- ITCAM for WebSphere Application Server version 7.2 support for WebSphere Application Server version 8.5
- ITCAM Diagnostics Tool that is previewed in the ITCAM for Application Diagnostics beta

If ITCAM for SOA version 7.2 is already installed under the *ITM_home* directory or if you are performing a reinstallation, the same version, release, and maintenance level of ITCAM Data Collector for WebSphere might be installed under *ITM_home*. If the installer detects that ITCAM Data Collector for WebSphere is already installed under *ITM_home*, the installation of the data collector is skipped and the data collector configuration utility is displayed. Skip to step "Step 13: Configuring the data collector."

Remember: The same version, release, and maintenance level of ITCAM Data Collector for WebSphere might be installed and configured for the same WebSphere profile, but the data collector installation might not be under the *ITM_home* directory:

- If the data collector is installed by ITCAM for WebSphere Application Server version 7.2 support for WebSphere Application Server version 8.5 or the ITCAM Diagnostics Tool, the data collector installation is outside of the *ITM_home* directory. The installer does not detect that the data collector already exists. When prompted, you must specify the location of the data collector installation.
- If the data collector is installed by ITCAM for SOA version 7.2 outside of *ITM_home*, the installer does not detect that the data collector exists. When prompted, you must specify the location of the data collector installation.

When the same version, release, and maintenance level of the data collector is not already installed under the *ITM_home* directory, the installer opens a command prompt window.

The installer prompts you to specify whether you want to:

- Install the data collector in the *DC_home* directory (default install)
- Reuse an existing data collector home directory (custom install)
- Create a new data collector home directory (custom install)

```
Choose the type of install to perform.
      1. default install
      2. custom install
[default is: 1]:
```

Enter 1 to install the data collector in the *DC_home* directory.

Otherwise, enter 2 and specify the location of the data collector home directory. If the installer finds that the data collector home directory does not exist, it asks you whether you want to create the directory.

```
Directory C:\IBM\ITM\dchome\7.2.0.0.1 does not exist.  Is it ok to create?
[1 - YES, 2 - NO]
```

Enter 1 to create the directory. If you enter 2, you can enter a different data collector home directory or exit the command prompt.

If the data collector installation does not already exist, the installer starts the installation of the data collector.

Step 13: Configuring the data collector

The ITCAM Data Collector for WebSphere Configuration utility is launched for configuring the data collector.

Before you configure the data collector, ensure that you have sufficient permissions to run the data collector configuration utilities (see "Permissions required for configuration tasks" on page 37).

For information about using the utility, see “Configuring ITCAM Data Collector for WebSphere” on page 39.

If you are installing ITCAM Agent for WebSphere Applications and you want to postpone the configuration of ITCAM Data Collector for WebSphere until later, exit the utility. At a later time, use the ITCAM Data Collector for WebSphere Configuration utility to configure the data collector.

You must migrate the data collector components of following products to the ITCAM Data Collector for WebSphere before you enable data collection for ITCAM Agent for WebSphere Applications version 7.2 within the same profile:

- ITCAM for SOA version 7.1.1
- ITCAM for WebSphere Application Server version 7.2

If an older version of the ITCAM Agent for WebSphere Applications is configured for the same profile, exit the utility and migrate the data collector.

For more information about migrating the data collector, see “Migrating data collectors to ITCAM Data Collector for WebSphere” on page 54.

Step 14: Verify completion of installation procedure

In a pristine installation or an upgrade, when you complete the configuration of the monitoring agent, exit the ITCAM Data Collector for WebSphere Configuration utility, and close the command prompt, a confirmation message is presented to indicate that the installation and configuration tasks have completed successfully.

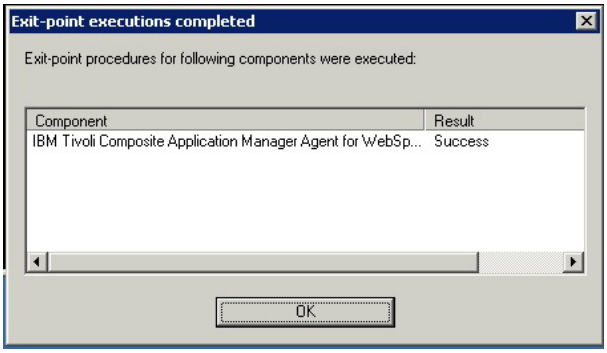

Figure 14. Confirmation that installer has successfully completed the installation task

Click **OK** to close the dialog.

Important: If you cancel the configuration of the data collector after the data collector is installed but before it is configured, the message displays the value *Error* in the result column. This message indicates that the data collector is installed but has yet to be configured.

Important: If you are planning to use ITCAM Agent for WebSphere Applications to monitor WebSphere Extrene Scale (WXS) in a WebSphere Application Server environment with enabled security, you must complete additional configuration steps. See Appendix B, “Configuring the agent for to monitor WebSphere Extreme Scale in security-enabled WebSphere environments,” on page 285.

Configuring the monitoring agent on Windows systems

This section provides instructions for configuring the ITCAM Agent for WebSphere Applications monitoring agent.

Entering the Agent Configuration window

If you choose the option to configure the monitoring agent connection to the monitoring server as part of the installation, the installer automatically launches the Agent Configuration window. You can skip the following instructions for manually opening the window.

To complete most of the configuration procedures described in this section, you must start from the Agent Configuration window. To enter this window, enter the Windows Start Menu and click **Programs** > **IBM Tivoli** > **Monitoring** > **Manage Tivoli Monitoring Services**. The **Manage Tivoli Monitoring Services** window is displayed. For details about the Manage Tivoli Monitoring Services application, see *IBM Tivoli Monitoring: Installation and Setup Guide*.

Right-click **ITCAM Agent for WebSphere Applications** and select **Reconfigure...**.

A window for configuring the Tivoli Enterprise Monitoring Server connection is displayed.

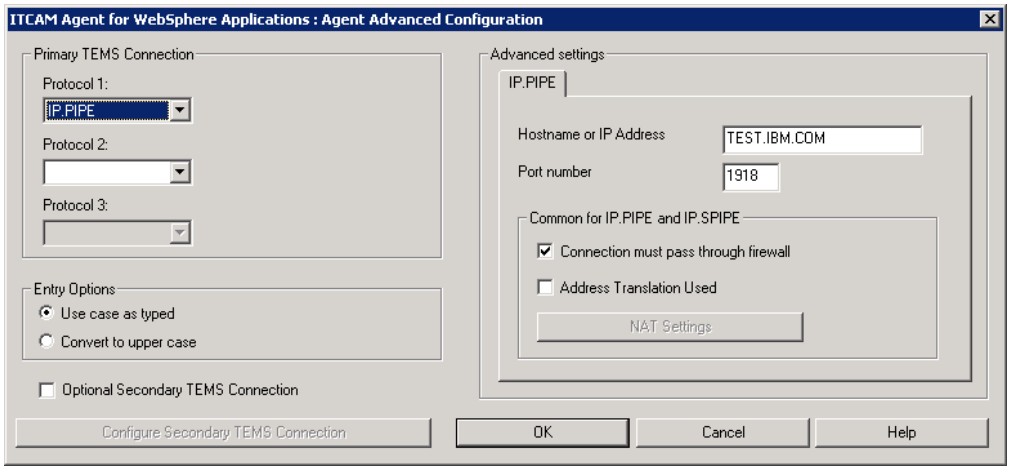

Figure 15. Tivoli Enterprise Monitoring Server connection configuration window

If IBM Tivoli Monitoring infrastructure is not used (in a deep-dive diagnostics-only installation with a Managing Server), ignore this window and click **OK**. If the Tivoli Enterprise Monitoring Server connection is already configured, you do not have to make any changes; click **OK**. Otherwise, for more information, see "Configuring the monitoring agent connection to the monitoring server."

Configuring the monitoring agent connection to the monitoring server

Specify these parameters in the Advanced Agent Configuration window as explained in *IBM Tivoli Monitoring: Installation and Setup Guide*.

- If the monitoring agent must access the monitoring server across a firewall, select **Connection must pass through firewall**.

- Identify the protocol that the monitoring agent uses to communicate with the hub monitoring server. You have five choices:
  - IP.UDP
  - IP.PIPE
  - IP.SPIPE
  - SNA
  - No Tivoli Enterprise Monitoring Server

  The value that you specify here must match the value that is specified when installing the monitoring server. You can also set a secondary protocol if required.
- If your site has set up failover support for its Tivoli monitoring agents, select **Optional Secondary TEMS Connection**, and specify the same communication protocols you chose when installing this monitoring server.

For the protocol or protocols that you selected in the previous window, specify these fields as explained in Table 2.

Table 2. Communications protocol settings

Field	Description
IP.UDP Settings	
Host name or IP address	The host name or IP address for the hub monitoring server.
Port #, or Port Pools, or both	The listening port for the hub monitoring server.
IP.PIPE Settings	
Host name or IP address	The host name or IP address for the hub monitoring server.
Port Number	The listening port for the monitoring server. The default value is 1918.
IP.SPIPE Settings	
Host name or IP address	The host name or IP address for the hub monitoring server.
Port number	The listening port for the hub monitoring server. The default value is 3660.
SNA Settings	
Network Name	The SNA network identifier for your location.
LU Name	The LU name for the monitoring server. This LU name corresponds to the Local LU Alias in your SNA communications software.
LU 6.2 LOGMODE	The name of the LU6.2 LOGMODE. The default value is CANCTDCS.
TP Name	The transaction program name for the monitoring server.
Local LU Alias	The LU alias.

Click **OK**.

After this window, the Agent Configuration window is displayed.

Configuring monitoring agent settings

If the IBM Tivoli Monitoring infrastructure is used, you must configure monitoring agent settings before configuring the data collector to monitor any application server instances. Do not perform this configuration in a deep-dive diagnostics-only installation, where IBM Tivoli Monitoring is not used.

You may change the port that is used for communication between the data collector and the monitoring agent (this communication is on the local host); the default port is 63335. You may also set an alternate node name that determines how the agent is displayed in the Tivoli Enterprise Portal navigation tree. While you can change these at a later time, it is normally most convenient to set them when initially configuring the communication.

To configure monitoring agent settings, perform the following procedure:

1. Enter the Agent Configuration window.

   After you install the agent, this window opens automatically. Otherwise, see "Entering the Agent Configuration window" on page 32.

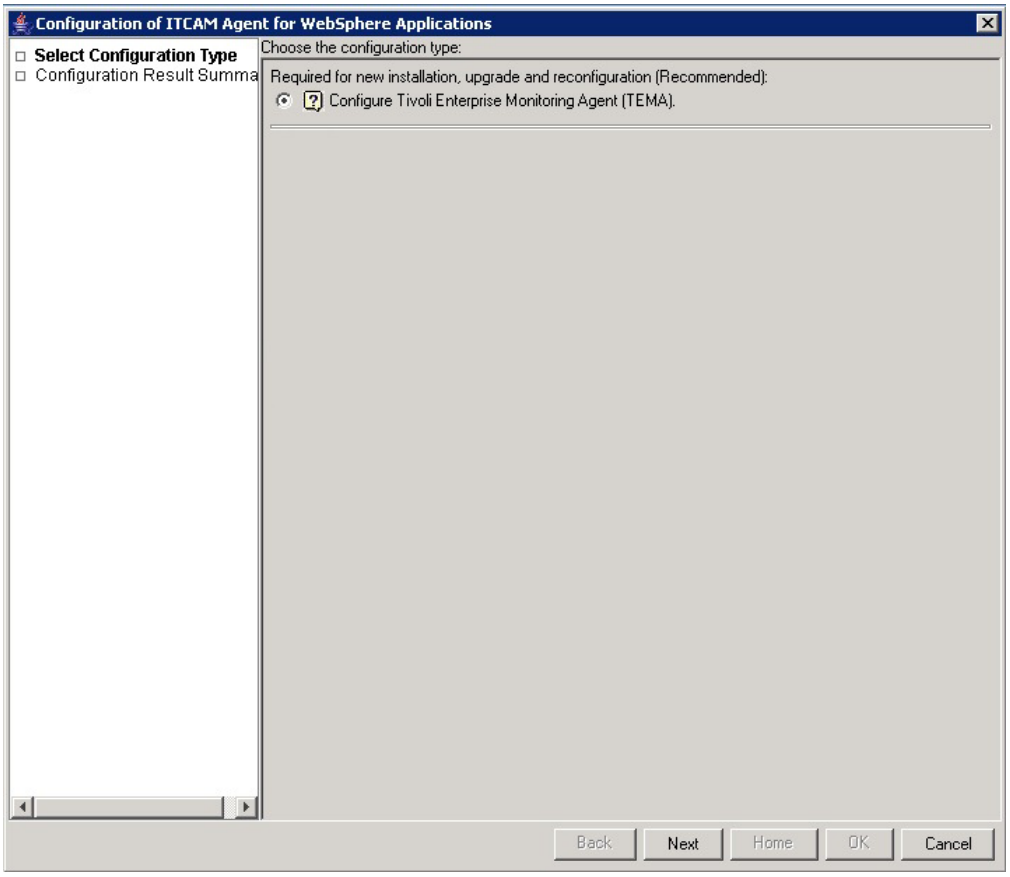

Figure 16. Configuring Communication to the monitoring agent, window 1

2. Select **Configure Tivoli Enterprise Monitoring Agent (TEMA)** and click **Next**.
3. In the Agent Configuration window, you can set an alternative Node ID for identifying the agent. This is the identifier that determines how the agent is displayed in the Tivoli Enterprise Portal navigation tree. The default is `Primary`, which is used in conjunction with the host name of the computer where the agent is installed. In the **Port** field, you can specify a TCP socket port that the

monitoring agent uses to listen for connection requests from the data collectors. Normally, do not change this value. The port is used only for local communication on the host.

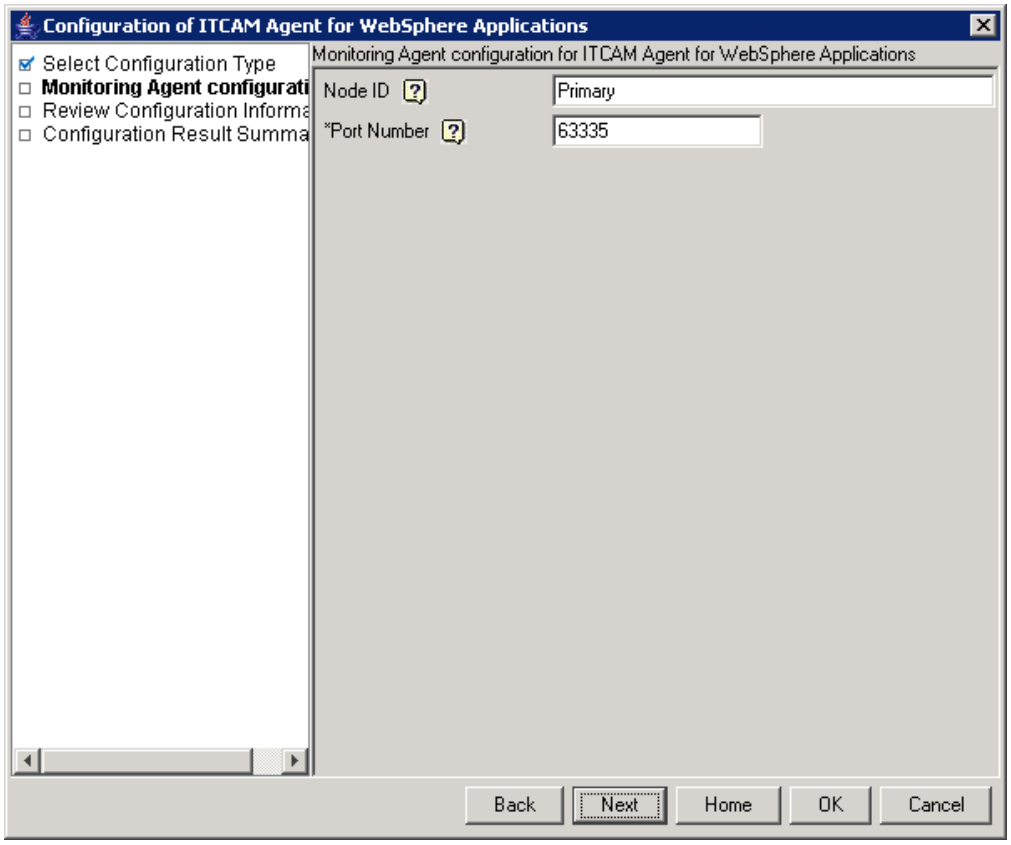

Figure 17. Configuring Communication to the monitoring agent, window 2

Enter the Node ID if necessary; change the port number if necessary.

Important: Valid characters for the node ID include A-z, a-z, 0-9, underscore (_), dash (-), and period (.); do not use other characters.
Click **Next**.

4. In the next step, you can choose to create a response file to save your configuration settings. You can use the response file to perform a silent configuration with the same parameters.

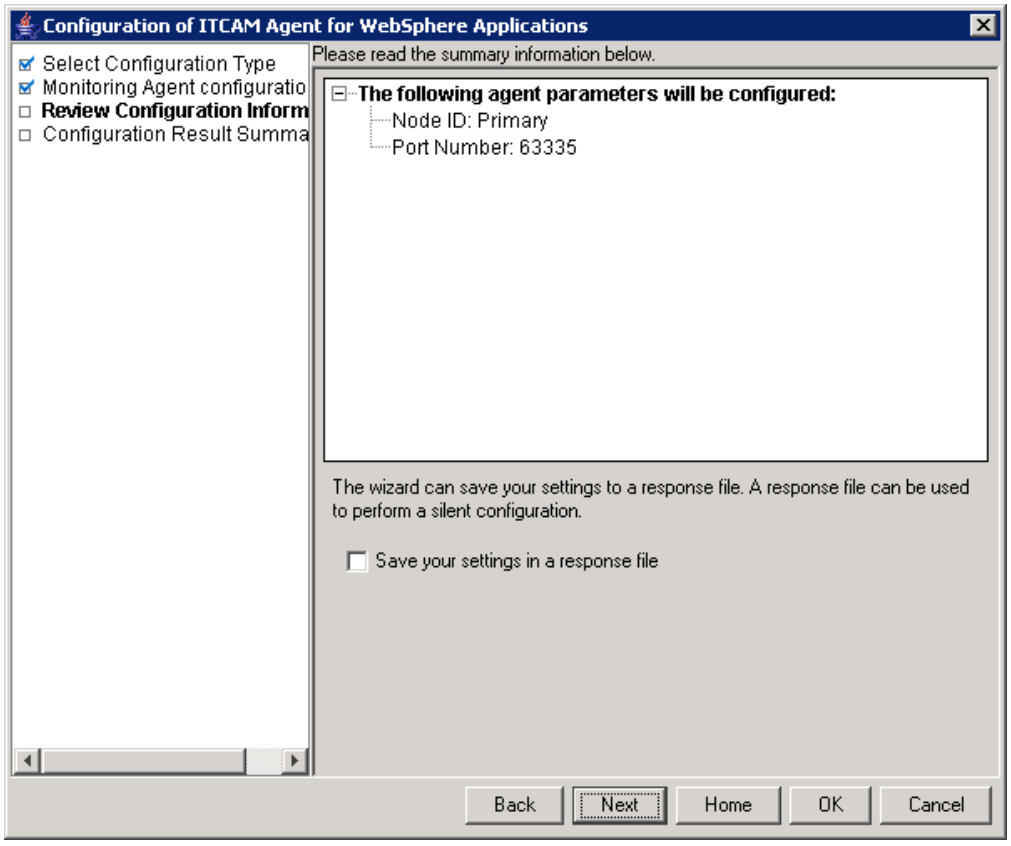

Figure 18. Configuring Communication to the monitoring agent, window 3

If you need to create a response file, select the **Save your settings in a response file** check box and click **Browse** to select the file location, then click **Next**. Otherwise, leave the box unchecked and click **Next**.

5. A message is displayed to indicate that the monitoring agent is successfully configured.

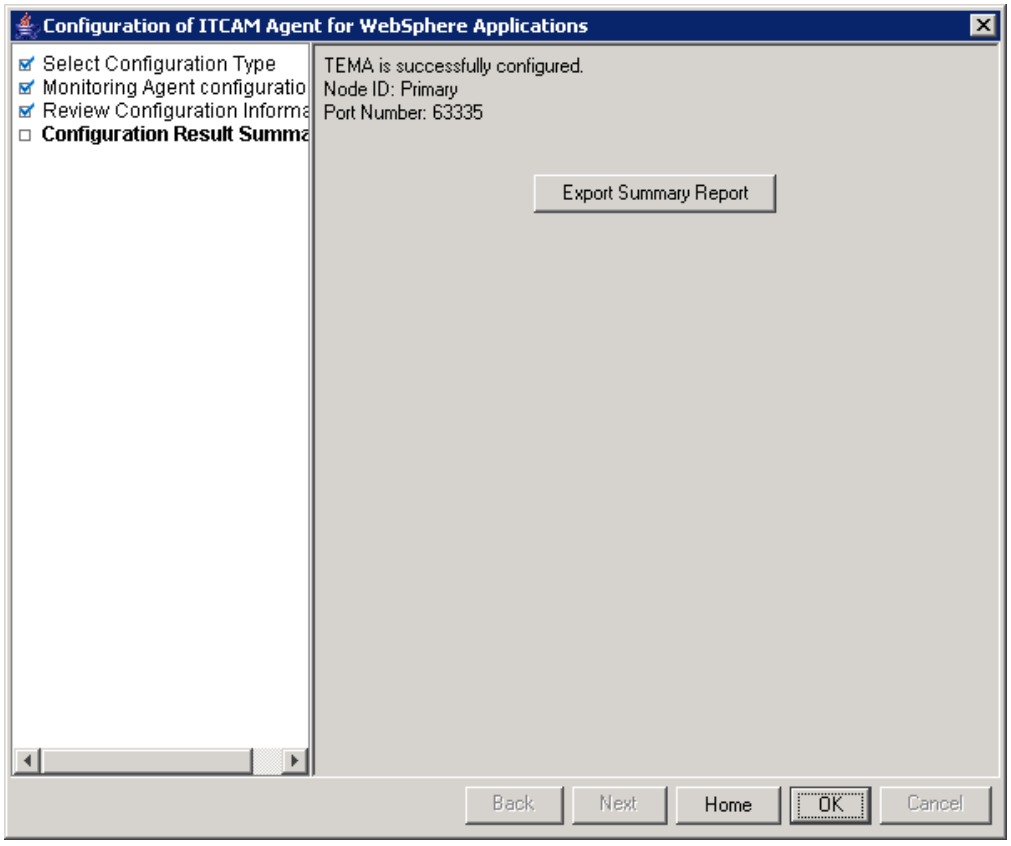

Figure 19. Configuring Communication to the monitoring agent, window 4

Click **Home** to return to the Agent Configuration window, or click **OK** to complete the configuration process.

Before configuring the data collector on Windows systems

Before configuring the data collector using the configuration utilities interactively or in silent mode, ensure that you have the necessary permissions to perform the configuration tasks.

Permissions required for configuration tasks

If you are configuring the data collector to monitor instances of the application server, the user must also have privileges (read, write, and execute) for the application server directory.

If you are migrating an older version of the data collector to ITCAM Data Collector for WebSphere, the user must have read/write privileges for the home directory of the previous version of the data collector.

The user must have permission to execute scripts in the *DC_home*\bin directory.

The user must run the configuration utilities using a Windows operating system user ID that owns the WebSphere Application Server profile that is being configured. If the WebSphere Application Server installer and profile owner do not map to the same Windows operating system user ID, follow the steps in the

WebSphere Application Server information center about configuring the profile user. For more information, see the WebSphere Application Server information center.

If WebSphere global security is enabled, the configuration utilities prompt you for a WebSphere administrative user ID with login privileges to the wsadmin tool. Specify a user ID that is the primary administrative user for the WebSphere Application Server.

Configuring the data collector interactively

There are a number of command-line configuration utilities to configure, reconfigure, unconfigure, and migrate ITCAM Data Collector for WebSphere.

The following table provides a description of the configuration tasks supported by the utilities.

Table 3. Configuration tasks

Configuration task	Where to find the procedure
Configure the data collector to monitor application server instances within a WebSphere Application Server profile. This configuration utility is started automatically when you install the monitoring agent.	"Configuring ITCAM Data Collector for WebSphere" on page 39
Modify the configuration of the data collector for application server instances that were already configured by the ITCAM Data Collector for WebSphere Configuration utility.	"Reconfiguring ITCAM Data Collector for WebSphere" on page 48
Unconfigure the data collector.	"Unconfiguring ITCAM Data Collector for WebSphere" on page 46
Migrate an older version of the data collector to ITCAM Data Collector for WebSphere or update the maintenance level of ITCAM Data Collector for WebSphere.	"Migrating data collectors to ITCAM Data Collector for WebSphere" on page 54
Migrate the WebSphere Application Server data collector provided by ITCAM for SOA version 7.1.1 to ITCAM Data Collector for WebSphere.	"Migrating ITCAM for SOA version 7.1.1 data collector to ITCAM Data Collector for WebSphere" on page 57

Important: To change to a later maintenance level of ITCAM Agent for WebSphere Applications, use the migration utility (see "Migrating data collectors to ITCAM Data Collector for WebSphere" on page 54).

Guidelines on which configuration utility to run

Use the following guidelines to determine whether to run the configuration or reconfiguration utility to configure application servers:

- If the application servers you plan to configure are not yet configured for data collection, use the configuration utility.

  If you run the configuration utility on any application servers that are already configured for data collection, your data collector configuration settings are overwritten.
- If the application servers that you plan to configure are already configured for data collection, use the reconfiguration utility to retain your existing data collector configuration settings.

- If some of the application servers you plan to configure are already configured and others are not yet configured, complete either of the following steps:
  - Use the configuration utility to configure the application servers. The data collection settings of the applications servers are overwritten.
  - Alternatively, run the configuration utility for the set of servers that have not yet been configured and run the reconfiguration utility for the servers that are already configured.

To apply different configuration settings to sets of application servers, run either utility for each set of servers separately.

Configuring ITCAM Data Collector for WebSphere

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

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

If you are installing the data collector, the installer automatically launches the configuration utility.

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

Remember: If you have already configured the data collector and you want to reconfigure it, start the ITCAM Data Collector for WebSphere Reconfiguration utility. Otherwise, the changes you made are lost.

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

1. If you are installing the monitoring agent where the ITCAM Data Collector for WebSphere Configuration utility is started automatically by the installer, proceed to step 4. Otherwise, from the command line, navigate to the *DC_home*\bin directory.
2. Set the location of the Java home directory before you run the utility, for example:

   ```
   set JAVA_HOME=C:\Progra~1\IBM\WebSphere\AppServer80\java
   ```
3. Run the following command to start the configuration utility.

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

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

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

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

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

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

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

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

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

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

   If global security is not enabled, skip to step 9

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

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

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

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

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

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

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

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

   Remember:

   - For a stand-alone environment, application server instances must be running during the configuration.
   - For a Network Deployment, WebSphere Virtual Enterprise, or WebSphere Compute Grid environment, the Node Agent and Deployment Manager must be running.

- Ensure that the application server instances that you select are the actual servers that host the applications or services that you want to monitor.

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

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

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

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

    When configuring data collection for ITCAM Agent for WebSphere Applications, you can integrate the data collector with the ITCAM Agent for WebSphere Applications monitoring agent, or with the ITCAM for Application Diagnostics Managing Server, or with both.

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

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

    Important: When you configure data collection for ITCAM Agent for WebSphere Applications for applications servers in a profile where data collection is configured for application servers for ITCAM for SOA version 7.2, you must reconfigure and restart the Tivoli Enterprise Portal Server to capture ITCAM Agent for WebSphere Applications data in the topology views of ITCAM for SOA.
13. Enter 1 to integrate the data collector with the ITCAM Agent for WebSphere Applications. Otherwise, enter 2 and skip to step 16 on page 42.

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

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

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

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

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

15. Enter the port number of the monitoring agent.

    If you are configuring the Data Collector shipped with ITCAM Agent for WebSphere Applications version 7.2 ifix 1 or later, the utility prompts you for the server alias. The alias is the name of the node in Tivoli Enterprise Portal that contains the monitoring information for this application server instance. The default is the node name combined with the server name.

    ```
    Enter the server alias for server server1 in node node1  [default is: node1server1]:
    ```

    Accept the default or enter another alias.

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

    You are prompted to specify whether you want to integrate the data collector with a managing server.

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

    Remember:

    - To integrate the data collector with ITCAM for Application Diagnostics Managing Server for deep-dive analysis, you must have ITCAM for Application Diagnostics version 7.1.0.3 or later installed.
    - If you decide not to configure the managing server at this time, you can still configure the data collector to communicate with the managing server later.

17. Enter 1 to integrate with the managing server. Otherwise, enter 2 and skip to step 20 on page 43.

    You are prompted to specify the host name of the managing server:

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

18. Enter the fully qualified host name of the managing server.

    You are prompted to specify the port number of the managing server:

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

    The port number is codebase port on which the managing server is listening.

    Tip: The port number is specified in the key `PORT_KERNEL_CODEBASE01` in the `ITCAM61_MS_CONTEXT.properties` file in the managing server home directory. For more information, see *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

    The configuration tool attempts to connect to the managing server and retrieve the value for the managing server home directory. If successful, the tool displays a message similar to the following message:

```
MS home directory is: C:\IBM\itcam\WebSphere\MS
```

19. If the connection to the managing server is *not* successful, you are prompted to enter the value of the managing server home directory:

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

    If prompted, enter the value of the managing server home directory.

20. The utility prompts you to specify whether you want to configure advanced settings for the managing server.

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

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

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

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

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

    Enter the RMI port numbers.

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

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

    Enter the RMI Controller port numbers.

23. You are prompted to enter the Remote File Sharing (RFS) port number of the managing server:

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

    The RFS server in the managing server kernel listens to the RFS port to accept incoming requests. Enter the RFS port number.

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

    Remember: To integrate the data collector with ITCAM for Transactions, you must install ITCAM for Transactions version 7.3 or later within an IBM Tivoli Monitoring environment.
    You are prompted to specify whether you want to integrate with ITCAM for Transactions:

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

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

25. Enter 1 to integrate the data collector with ITCAM for Transactions. Otherwise, enter 2 and skip to step 30 on page 44.

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

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

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

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

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

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

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

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

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

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

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

    Application Performance Diagnostics Lite is a tool for diagnostic investigation of applications running on WebSphere Application Server and WebSphere Portal Server. Using this tool, you can analyze data in real time or you can save diagnostic information to a file for later analysis. For more information about installing and using Application Performance Diagnostics Lite, see the Application Performance Diagnostics Lite product documentation.

    In the version of the Data Collector shipped with ITCAL Agent for Websphere versions prior to 7.2 ifix 1, the name *ITCAM diagnostics tool* is used for Application Performance Diagnostics Lite.

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

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

    Enter 1 to select a garbage collection log path. Otherwise, enter 2 and skip to step 34 on page 45.
33. You are prompted to specify the garbage collection log path:

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

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

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

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

```
 1) List of servers selected

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

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

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

                    WAS version : 8.0.0.0
                     Deployment : Standalone
                       JVM mode : 32
                Configuration home : C\IBM\ITM\dchome\7.2.0.0.1

 2) Integrate with ITCAM for SOA Agent : Yes

 3) Integrate with ITCAM Agent for WebSphere Applications : Yes

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

 4) Integrate with ITCAM for AD Managing Server : No

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

 5) Integrate with ITCAM for Transactions : Yes

       Transaction Collector hostname : 127.0.0.1
       Transaction Collector port number : 5455

 6) Integrate with Tivoli Performance Viewer : No

 7) Integrate with ITCAM diagnostics tool : No

 8) Advanced settings :

       Set Garbage Collection log path : No

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

```
 8) Advanced settings

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

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

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

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

36. Enter 1 to create a backup of the current configuration. Otherwise, enter 2.
37. The utility applies the changes and presents a status message to indicate that the configuration of the data collector for the profile is complete:

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

38. After configuring the data collector to monitor application server instances, you must restart the instances as directed by the utility. The data collector configuration takes effect when the application server instances are restarted.

Data collection is configured for the specified application server instances.

Unconfiguring ITCAM Data Collector for WebSphere

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

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

To unconfigure the data collector, complete the following procedure:

1. From a command line, navigate to the *DC_home*\bin directory.
2. Set the location of the Java home directory before you run the script. For example:

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

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

   DC_home\bin\unconfig.bat

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

   Remember:

   - Application server instances must be running during the unconfiguration procedure.
   - For Network Deployment environment, the Node Agent and Deployment Manager must also be running.

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

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

4. Enter the number that corresponds to the application server instance to unconfigure for data collection or enter an asterisk (*) to unconfigure data collection for all application server instances. To specify a subset of servers, enter the numbers, separated by commas, that represent the servers. For example: 1,2,3.
5. The utility prompts you to specify whether you want to create a backup of your current WebSphere Application Server configuration:

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

   Enter 1 to create a backup of the current configuration. Otherwise, enter 2 and skip to step 8.
6. The utility prompts you to specify the directory in which to store the backup of the configuration. For example:

   ```
   Enter backup directory  [default is: C:\IBM\ITM_DC\dchome\7.2.0.0.1\data]:
   ```

   Specify a directory in which to store the backup of the configuration or accept the default directory.
7. The utility displays the name of the WebSphere home directory and the WebSphere profile for which a backup is created. For example:

   ```
   WebSphere Home:C:\Program Files (x86)\IBM\WebSphere\AppServer
   WebSphere Profile:AppSrv01
   ```
8. The utility indicates whether WebSphere Global Security is enabled for the WebSphere Application profile that you specified:

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

   If global security is not enabled, skip to step 11 on page 48.
9. The utility prompts you to specify whether to retrieve security settings from a client properties file:

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

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

   Enter 1 to allow the utility to retrieve the user name and password from the appropriate client properties file and skip to step 11 on page 48. Otherwise, enter 2 to enter the user name and password.

   ```
   Enter WebSphere admin user name:
   Enter WebSphere admin user password:
   ```
10. If you selected the option to back up the current WebSphere configuration, the utility starts backing up the configuration. For example:

```
Backing up profile: AppSrv01 home: C:\Program Files
(x86)\IBM\WebSphere\AppServer\bin ...  Backup file
C:\IBM\ITM_DC\dchome\7.2.0.0.1\data\v525400e96601Cell01.
v525400e96601Node01.AppSrv01.WebSphereConfig_20120716161102.zip
is successfully created
```

11. The utility unconfigures the data collector for the specified application server instances. A status message is displayed to indicate that the data collector was successfully unconfigured. For example:

    ```
    Successfully executed Unconfiguring for Cell: v525400597750Node01Cell
    Node: v525 400597750Node01 Profile: AppSrv01
    ```

12. After unconfiguring the data collector to monitor application server instances, you must restart the instances as directed by the utility. The data collector unconfiguration takes effect when the application server instances are restarted.

Data collection is unconfigured for the specified application server instances.

Reconfiguring ITCAM Data Collector for WebSphere

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

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

- ITCAM Agent for WebSphere monitoring agent
- ITCAM for Application Diagnostics Managing Server
- ITCAM for SOA monitoring agent
- ITCAM for Transactions
- Tivoli Performance Viewer, available from the WebSphere administrative console
- ITCAM Diagnostic Tool that is previewed in the ITCAM for Application Diagnostics beta

You can also reconfigure garbage collection settings.

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

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

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

3. Run the following command to start the ITCAM Data Collector for WebSphere Reconfiguration utility.

   ```
   DC_home\bin\reconfig.bat
   ```

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

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

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

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

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

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

Remember:

- For a stand-alone environment, application server instances must be running during the configuration.
- For a Network Deployment, WebSphere Virtual Enterprise, or WebSphere Compute Grid environment, the Node Agent and Deployment Manager must be running.
- Ensure that the application server instances that you select are the actual servers that host the applications or services that you want to monitor.

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

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

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

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

   When configuring data collection for ITCAM Agent for WebSphere Applications, you can integrate the data collector with ITCAM Agent for WebSphere Applications monitoring agent, or with the ITCAM for Application Diagnostics Managing Server, or with both.

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

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

   Important: When you configure data collection for ITCAM Agent for WebSphere Applications for applications servers in a profile where data collection is configured for application servers for ITCAM for SOA version 7.2, you must reconfigure and restart the Tivoli Enterprise Portal Server to capture ITCAM Agent for WebSphere Applications data in the topology views of ITCAM for SOA.

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

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

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

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

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

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

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

11. Enter the port number of the monitoring agent.

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

    You are prompted to specify whether you want to integrate the data collector with a managing server.

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

    Remember:

    - To integrate with ITCAM for Application Diagnostics Managing Server for deep-dive analysis, you must have ITCAM for Application Diagnostics version 7.1.0.3 or later installed.
    - If you decide not to configure the managing server at this time, you can still configure the data collector to communicate with the managing server later.

13. Enter 1 to integrate with the managing server. Otherwise, enter 2 and skip to step 16 on page 51.

    You are prompted to specify the host name of the managing server:

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

14. Enter the fully qualified host name of the managing server.

    You are prompted to specify the port number of the managing server:

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

    The port number is codebase port on which the managing server is listening.

    Tip: The port number is specified in the key `PORT_KERNEL_CODEBASE01` in the `ITCAM61_MS_CONTEXT.properties` file in the managing server home directory. See *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

The configuration utility attempts to connect to the managing server and retrieve the value for the managing server home directory. If successful, the utility displays a message similar to the following message:

```
MS home directory is: C:\IBM\itcam\WebSphere\MS
```

15. If the connection to the managing server is *not* successful, you are prompted to enter the value of the managing server home directory:

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

    If prompted, enter the value of the managing server home directory.

16. The utility prompts you to specify whether you want to configure advanced settings for the managing server.

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

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

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

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

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

    Enter the RMI port numbers.

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

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

    Enter the RMI Controller port numbers.

19. You are prompted to enter the Remote File Sharing (RFS) port number of the managing server:

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

    The RFS server in the managing server kernel listens to the RFS port to accept incoming requests. Enter the RFS port number.

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

    Remember: To integrate the data collector with ITCAM for Transactions, you must install ITCAM for Transactions version 7.3 or later within an IBM Tivoli Monitoring environment.
    You are prompted to specify whether you want to integrate with ITCAM for Transactions:

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

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

21. Enter 1 to integrate the data collector with ITCAM for Transactions. Otherwise, enter 2 and skip to step 26 on page 52.

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

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

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

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

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

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

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

    ITCAM for WebSphere Application Server 7.2 support for WebSphere Application Server version 8.5 includes ITCAM Data Collector for WebSphere. Enter 1 to integrate ITCAM Data Collector for WebSphere with the Tivoli Performance Viewer. Otherwise, enter 2 and skip to step 27.
27. In the **Integration with ITCAM diagnostics tool** section, the utility provides an option for integrating the data collector with the ITCAM diagnostics tool.

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

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

    Enter 1 to integrate ITCAM Data Collector for WebSphere with the ITCAM Diagnostics Tool. Otherwise, enter 2 and skip to step 28.
28. In the **Advanced Settings** section, the utility provides options for performing advanced configuration of the data collector. The utility prompts you to specify whether to change the garbage collection log path:

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

    Enter 1 to select a garbage collection log path. Otherwise, enter 2 and skip to step 30 on page 53.
29. You are prompted to specify the garbage collection log path:

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

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

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

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

```
 1) List of servers selected

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

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

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

                    WAS version : 8.0.0.0
                     Deployment : Standalone
                       JVM mode : 32
                Configuration home : C\IBM\ITM\dchome\7.2.0.0.1


 2) Integrate with ITCAM for SOA Agent : Yes

 3) Integrate with ITCAM Agent for WebSphere Applications : Yes

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

 4) Integrate with ITCAM for AD Managing Server : No

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

 5) Integrate with ITCAM for Transactions : Yes

       Transaction Collector hostname : 127.0.0.1
       Transaction Collector port number : 5455

 6) Integrate with Tivoli Performance Viewer : No

 7) Integrate with ITCAM diagnostics tool : No

 8) Advanced settings :

       Set Garbage Collection log path : No

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

```
 7) Integrate with ITCAM diagnostics tool
 8) Advanced settings

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

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

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

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

32. Enter `1` to create a backup of the current configuration. Otherwise, enter `2`.
33. The utility applies the changes and presents a status message to indicate that the reconfiguration of the data collector for the profile is complete:

    ```
    Successfully executed Reconfiguring for Cell: v525400597750Node01Cell
    Node: v525
    400597750Node01 Profile: AppSrv01
    ```

34. After reconfiguring the data collector to monitor application server instances, you must restart the instances as directed by the utility. The data collector configuration takes effect when the application server instances are restarted.

Data collection is reconfigured for the specified application server instances.

Migrating data collectors to ITCAM Data Collector for WebSphere

A previous version or an earlier maintenance level of ITCAM Data Collector for WebSphere can be migrated interactively with the ITCAM Data Collector for WebSphere Migration utility. If you want to migrate many application server instances, it might be more convenient to migrate the application servers using the migration utility in silent mode.

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

1. ITCAM for WebSphere version 6.1.0.4 or later
2. WebSphere Data Collector version 6.1.0.4 or later included in ITCAM for Web Resources version 6.2.0.4 or later
3. ITCAM Agent for WebSphere Applications version 7.1 included in ITCAM for Applications Diagnostics version 7.1
4. ITCAM for WebSphere Application Server version 7.2
5. ITCAM for SOA version 7.1.1

You can also use the migration utility to update ITCAM Data Collector for WebSphere to a new maintenance level.

For the procedure for migrating the ITCAM for SOA version 7.1.1 WebSphere Application Server data collector to ITCAM Data Collector for WebSphere, see "Migrating ITCAM for SOA version 7.1.1 data collector to ITCAM Data Collector for WebSphere" on page 57.

To upgrade the monitoring of server instances to ITCAM Data Collector for WebSphere or to update the maintenance level of the data collector, complete the following procedure:

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

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

2. Run the following command to start the migration utility.

   On Windows systems:

   DC_home\bin\migrate.bat

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

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

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

   The utility prompts you to specify from the type of agent that you want to upgrade to ITCAM Data Collector for WebSphere. If you are configuring the Data Collector shipped with ITCAM Agent for WebSphere Applications version 7.2 ifix 1 or later, the following list is displayed.

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

   1. ITCAM for WebSphere 6.1.0.4 or later
   2. ITCAM WebSphere Agent 6.2.0.4 or later [ITCAM for Web Resources 6.2]
   3. ITCAM Agent for WebSphere Applications 7.1 [ITCAM for Application Diagnostics 7.1]
   4. ITCAM for WebSphere Application Server 7.2
   5. ITCAM for SOA 7.1.1.x
   6. Maintenance level update for ITCAM Data Collector for WebSphere 7.2 and later [ITCAM
     Agent for WebSphere Applications 7.2 and later, ITCAM for SOA 7.2 and later, IBM
     Application Performance Diagnostics Lite]
   Enter the number [default is: 1]:
   ```

   In older Data Collector versions, the following list is displayed:

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

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

   Enter the number that represents the agent.

   Attention: To update the maintenance level of ITCAM Data Collector for WebSphere, enter 4.

For the procedure for migrating the ITCAM for SOA version 7.1.1 WebSphere Application Server data collector to version 7.2, see "Migrating ITCAM for SOA version 7.1.1 data collector to ITCAM Data Collector for WebSphere" on page 57.

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

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

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

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

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

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

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

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

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

   Enter the port number of the monitoring agent.

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

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

   ```
   Choose a Server or Servers to be migrate
    1. x336r1s37-vn01Cell01.x336r1s36-vn01Node03.server3
    2. x336r1s37-vn01Cell01.x336r1s36-vn01Node03.server5
    3. x336r1s37-vn01Cell01.x336r1s36-vn01Node03.server1
   Enter a number or numbers separated by a comma, enter '*' to select all
   servers listed, or enter 'q' to quit the selection.
   ```

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

   Remember:

   - For a stand-alone environment, application server instances must be running during the configuration.
   - For a Network Deployment, WebSphere Virtual Enterprise, or WebSphere Compute Grid environment, the Node Agent and Deployment Manager must be running.

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

12. If WebSphere Global Security is enabled on one or more profiles, the utility prompts you to specify whether to retrieve security settings from a client properties file:

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

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

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

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

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

    ```
    Migration of the Data Collector has successfully completed with return code 0.
    ```
15. After migrating the data collector, you must restart the instances as directed by the utility. The data collector configuration takes effect when the application server instances are restarted.

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

You can also configure or reconfigure integration with ITCAM for SOA, ITCAM Agent for WebSphere Applications monitoring agent, ITCAM for Application Diagnostics Managing Server, Tivoli Performance Viewer, and ITCAM Diagnostics Tool for the application server instances. For more information, see "Reconfiguring ITCAM Data Collector for WebSphere" on page 48.

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

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

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

For the procedure for migrating the following data collector components to ITCAM Data Collector for WebSphere, see "Migrating data collectors to ITCAM Data Collector for WebSphere" on page 54:

- ITCAM for WebSphere version 6.1.0.4 or later
- WebSphere Data Collector version 6.1.0.4 or later included in ITCAM for Web Resources version 6.2.0.4 or later
- ITCAM Agent for WebSphere Applications version 7.1 included in ITCAM for Applications Diagnostics version 7.1
- ITCAM for WebSphere Application Server version 7.2

To update the maintenance level of any products that have ITCAM Data Collector for WebSphere as a component, including ITCAM for SOA, follow the procedure in "Migrating data collectors to ITCAM Data Collector for WebSphere" on page 54.

Important: If an older version of ITCAM Agent for WebSphere Applications is configured for application servers in the same profile as ITCAM for SOA version 7.1.1, migrate the data collector provided with ITCAM Agent for WebSphere Applications. Then, reconfigure the data collector to integrate it with the ITCAM for SOA monitoring agent. You must not run the migration utility to migrate the older version of the ITCAM for SOA WebSphere Application Server data collector.

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

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

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

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

   DC_home\bin\migrate.bat

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

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

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

   The utility prompts you to specify from the type of agent that you want to upgrade to ITCAM Data Collector for WebSphere. If you are configuring the Data Collector shipped with ITCAM Agent for WebSphere Applications version 7.2 ifix 1 or later, the following list is displayed.

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

   1. ITCAM for WebSphere 6.1.0.4 or later
   2. ITCAM WebSphere Agent 6.2.0.4 or later [ITCAM for Web Resources 6.2]
   3. ITCAM Agent for WebSphere Applications 7.1 [ITCAM for Application Diagnostics 7.1]
   4. ITCAM for WebSphere Application Server 7.2
   5. ITCAM for SOA 7.1.1.x
   6. Maintenance level update for ITCAM Data Collector for WebSphere 7.2 and later [ITCAM
     Agent for WebSphere Applications 7.2 and later, ITCAM for SOA 7.2 and later, IBM
     Application Performance Diagnostics Lite]
   Enter the number [default is: 1]:
   ```

   In older Data Collector versions, the following list is displayed:

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

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

Enter 5 to migrate ITCAM for SOA version 7.1.1.x.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Important:

- For a stand-alone environment, application server instances must be running during the configuration.
- For a Network Deployment, WebSphere Virtual Enterprise, or WebSphere Compute Grid environment, the Node Agent and Deployment Manager must be running.
- Ensure that the application server instances that you select are the actual servers that host the BPM applications or services that you want to monitor.

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

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

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

Each of the servers will be configured for data collection

 1) List of servers selected

   - WAS server: IBM-6DA7F9C6EE6Node02Cell.IBM-6DA7F9CNode02.server1
(AppSrv02)
       WAS cell: IBM-6DA7F9C6EE6Node02Cell
        WAS node: IBM-6DA7F9C6EE6Node02

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

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

                    WAS version : 8.0.0.0
                     Deployment : Standalone
                       JVM mode : 32
              Configuration home : C\IBM\ITM\dchome\7.2.0.0.1

 2) Integrate with ITCAM for SOA Agent : Yes

 3) Integrate with ITCAM Agent for WebSphere Applications : No

 4) Integrate with ITCAM for AD Managing Server : No

 5) Integrate with ITCAM for Transactions : No

 6) Integrate with Tivoli Performance Viewer : No

 7) DE Integrate with ITCAM diagnostics tool : No

 8) Advanced settings :

       Set Garbage Collection log path : No

Configuration sections:

 1) List of servers selected
 2) Integrate with ITCAM for SOA Agent
```

```
 3) Integrate with ITCAM Agent for WebSphere Applications
 4) Integrate with ITCAM for AD Managing Server
 5) Integrate with ITCAM for Transactions
 6) Integrate with Tivoli Performance Viewer
 7) DE Integrate with ITCAM diagnostics tool
 8) Advanced settings

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

11. To enable integration with products and components other than ITCAM for SOA, select the corresponding number. For details on the configuration, see "Configuring ITCAM Data Collector for WebSphere" on page 39. Otherwise, to accept the configuration, enter `a`.

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

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

12. Enter 1 to create a backup of the current configuration. Otherwise, enter 2.
13. The utility applies the changes and presents a status message to indicate that the configuration of the data collector for the profile is complete:

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

14. After migrating the data collector, you must restart the instances as directed by the utility. The data collector configuration takes effect when the application server instances are restarted.

You can also configure or reconfigure integration with ITCAM for SOA, ITCAM Agent for WebSphere Applications monitoring agent, ITCAM for Application Diagnostics Managing Server, Tivoli Performance Viewer, and ITCAM Diagnostics Tool for the application server instances at the same time. For more information about reconfiguring application server instances, see "Reconfiguring ITCAM Data Collector for WebSphere" on page 48.

Enabling application support on Windows systems

To ensure that ITCAM Agent for WebSphere Applications works within your Tivoli Monitoring infrastructure, you must enable application support for it on every hub and remote monitoring server, portal server, and portal client. After configuring the agent on the monitored host, you must also enable Tivoli Monitoring history collection. If Tivoli Monitoring is not used (in a deep-dive diagnostics-only installation), you do not have to install application support files.

Tip: Enabling application support is sometimes referred to as adding or activating application support.

If self-description is enabled on the Tivoli Monitoring components and on ITCAM Agent for WebSphere Applications, application support files are automatically installed and enabled on the monitoring server and the portal server without the need to recycle the monitoring server or the portal server. The conditions that must be met for self-description to operate are specified in "Enabling application support through self-description" on page 62.

If the agent and the Tivoli Monitoring components are not enabled for self-description, you must manually install application support files on the Tivoli Monitoring components. For more information, see "Manually installing application support" on page 63.

Enabling application support through self-description

IBM Tivoli Monitoring version 6.2.3 or later agents, which are enabled for self-description, install application support files and enable application support on the IBM Tivoli Monitoring infrastructure automatically.

ITCAM Agent for WebSphere Applications is enabled by default for self-description. When ITCAM Agent for WebSphere Applications is installed and the hub and remote monitoring servers are enabled for self-description, application support files are automatically installed on the hub monitoring server, the remote monitoring server, and the portal server, without the need to recycle the monitoring server or the portal server. Application support files must be installed manually on the portal client.

Although the self-describing agent is enabled by default for ITCAM Agent for WebSphere Applications, a number of conditions apply:

- All Tivoli Management Services server components must be at version 6.2.3 or higher.
- The agent framework must be at version 6.2.3 or higher. In ITCAM Agent for WebSphere Applications version 7.2, agent framework 6.2.2 is installed a part of an installation or upgrade of ITCAM Agent for WebSphere Applications. However, if you install another IBM Tivoli Monitoring agent, such as an OS agent, and its agent framework is at version 6.2.3, its installation could upgrade the agent framework of ITCAM Agent for WebSphere Applications to version 6.2.3.

  Remember: Not all OS agents running version 6.2.3, which share the same IBM Tivoli Monitoring home directory as ITCAM Agent for WebSphere Applications, upgrade the agent framework to 6.2.3. You must verify that the agent framework has been upgraded to version 6.2.3 before using self-description for ITCAM Agent for WebSphere Applications.

  To identify the agent framework version after installing or upgrading the agent, complete the following steps:

  1. From the command prompt, navigate to *ITM_Home*\bin directory.
  2. Run the following command:

     ```
     Kincinfo -t
     ```

  3. Locate the line for the agent framework in the output and note the version. For example:

     ```
     PC    PRODUCT        DESC      PLAT      VER          BUILD     INSTALL DATE
     GL  Tivoli Enterprise Monitoring Agent Framework   WIX64  06.23.02.00
     d2215a
     20120816 1412
     ```

You must verify that these conditions are met before you can use self-description for deploying application support to the monitoring server and the portal server.

After the self-describing application update is complete, and the application support files are manually installed on the portal client, you should see the following new agent data in the portal client:

- Historical Configuration is updated with any new attributes

- Workspaces are updated
- New or updated situations, policies, and take actions
- Queries are updated
- Help server files are updated

The self-describing agent feature is disabled by default on the hub monitoring server. The procedure for enabling self-description on the hub monitoring server is documented in the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Manually installing application support

If you have not enabled self-description on Tivoli Monitoring components and on ITCAM Agent for WebSphere Applications, you must install and enable application support manually on every hub and remote monitoring server, portal server, and portal client.

Multiple versions of ITCAM Agent for WebSphere Applications (version 6.2 and later) can be integrated with Tivoli Monitoring. If self-description is not enabled, you must install application support files from the agent that is at the latest version. For example, if your environment has ITCAM Agent for WebSphere Applications versions 7.2 and 7.1, ensure you install the application support files for the latest version, in this case version 7.2.

You must stop the monitoring server, portal server, or portal client when installing the support files.

Installing and enabling application support on Tivoli Enterprise Monitoring Server

1. Stop Tivoli Enterprise Monitoring Server.

   The installer automatically stops the Tivoli Enterprise Monitoring Server; you can also choose to stop the server manually before starting the installer. To stop the Tivoli Enterprise Monitoring Server manually, complete the following steps:

   a. Click **Start** > **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Monitoring Services**.
   b. Right-click Tivoli Enterprise Monitoring Server.
   c. In the menu, select **Stop**.
2. When you load the application support installation media, locate and double-click the `setup.exe` file within the WINDOWS directory.
3. On the Welcome window, click **Next**.
4. The Software License Agreement window is displayed. Select **I accept the terms in the license agreement** and click **Next**.
5. Select **Tivoli Enterprise Monitoring Server - TEMS** and click **Next**.

   Important: If you have other components installed on the same computer, such as the desktop client, also select those components to install the component-specific application support.
6. If you want to install the agent remotely, select the agent to add it to the remote deployment depot and click **Next**. Otherwise, click **Next** without selecting any agents.
7. Review the installation summary details. Click **Next** to start the installation.
8. Select the setup type that best suits your needs.

In the following steps, you are prompted for the information that is required to configure the items that are listed in the **Setup Type** window. You can clear the check box to delay the configuration until the installation is complete. Configuration items that are mandatory are preceded by an asterisk (*) and cannot be cleared.

9. Specify the location of the monitoring server. Choose **On this computer** to install application support on the host you are running the setup file on; alternatively, choose **On a different computer**. Click **OK**.
10. Select the application support to add to the monitoring server and click **OK**. By default, application supports which are not yet installed on this server are selected.
11. Review the application support addition details and click **Next**.
12. Specify the default values for the agent to use when it communicates with the monitoring server and click **OK**.

    Tip:

    - You can specify three methods for communication to set up backup communication methods. If the method that you identified as Protocol 1 fails, Protocol 2 is used.
    - You can specify the default values for a backup communication between the agent and the monitoring server by selecting **Option Secondary TEMS Connection**.

    a. If the agent must cross a firewall to access the monitoring server, select **Connection must pass through firewall**.

    b. Identify the type of protocol that the agent uses to communicate with the monitoring server. You have five choices: `IP.UDP`, `IP.PIPE`, `IP.SPIPE`, `SNA`, `No TEMS`.
13. Define the communications between agents and the monitoring server and click **OK**. For more details about the information, see Table 2 on page 33.
14. Click **Finish**.
15. If the Tivoli Enterprise Monitoring Server does not restart automatically, open **Manage Tivoli Enterprise Monitoring Services**.
16. Right-click the monitoring server and click **Start**.

Installing and enabling application support on Tivoli Enterprise Portal server

1. Open **Manage Tivoli Enterprise Monitoring Services.**
2. Right-click the portal server and click **Stop**.
3. On the application support installation media, access the `\WINDOWS` subdirectory.
4. Double-click **`setup.exe`**.
5. On the Welcome window, click **Next**.
6. The Software License Agreement window is displayed. Select **I accept the terms in the license agreement** and click **Next**.
7. Select **Tivoli Enterprise Portal Server - TEPS** and click **Next**.

   Important: If other components are installed on the same computer, such as the desktop client, also select those components to install the component-specific application support.

8. If you need remote configuration in the future, select the agent to add it to the remote deployment depot and click **Next**. Otherwise, click **Next** without selecting any agents.
9. Review the installation summary details. To start the installation, click **Next**.
10. Select the setup type that best suits your needs.

    In the following steps, you are prompted for the information that is required to configure the items that are listed in the **Setup Type** window. You can clear the check box to delay the configuration until the installation is complete. Configuration items that are mandatory are preceded by an asterisk (*) and cannot be cleared.
11. Type the host name for the portal server and click **Next**.
12. Click **Finish**.
13. If the Tivoli Enterprise Portal server does not restart automatically, open **Manage Tivoli Enterprise Monitoring Services**.
14. Right-click the portal server and click **Start**.

Important: If the Tivoli Enterprise Portal Server provides the browser client, check that the Eclipse help server is configured. For more information, see "Ensuring that the Eclipse server is configured" on page 66.

Installing and enabling application support on Tivoli Enterprise Portal desktop client

1. Open **Manage Tivoli Enterprise Monitoring Services.**
2. Right-click the desktop client and click **Stop**.
3. On the application support installation media, access the `\WINDOWS` subdirectory.
4. Double-click **`setup.exe`**.
5. On the Welcome window, click **Next**.
6. The Software License Agreement window is displayed. Select **I accept the terms in the license agreement** and click **Next**.
7. Select **TEP Desktop Client - TEPD** and click **Next**.
8. If you need remote configuration in the future, select the agent to add it to the remote deployment depot and click **Next**. Otherwise, click **Next** without selecting any agents.
9. Review the installation summary details. To start the installation, click **Next**.
10. Select the setup type that best suits your needs.

    In the following steps, you are prompted for the information that is required to configure the items that list in the **Setup Type** window. You can clear the check box to delay the configuration until the installation is complete. Configuration items that are mandatory are preceded by an asterisk (*) and cannot be cleared.
11. Type the host name for the portal server and click **Next**.
12. To complete the installation, click **Finish**.
13. If the Tivoli Enterprise Portal desktop client does not restart automatically, open **Manage Tivoli Enterprise Monitoring Services**.
14. Right-click the desktop client and click **Start**.

Important: Check that the Eclipse help server is configured for the client. For more information, see "Ensuring that the Eclipse server is configured" on page 66.

Ensuring that the Eclipse server is configured

After installing application support files on a Tivoli Enterprise Portal Server that provides the browser client or on a Tivoli Enterprise Portal desktop client, you must check the Eclipse help server for the portal client to ensure that it is configured.

Start Manage Tivoli Enterprise Monitoring Services (**Start** > **All Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Monitoring Services**), and ensure that the **Eclipse Help Server** entry indicates **Yes** in the Configured column.

If **No** is indicated, you must configure the Eclipse server. To do this, right-click the entry. From the menu, select **Configure Using Defaults**.

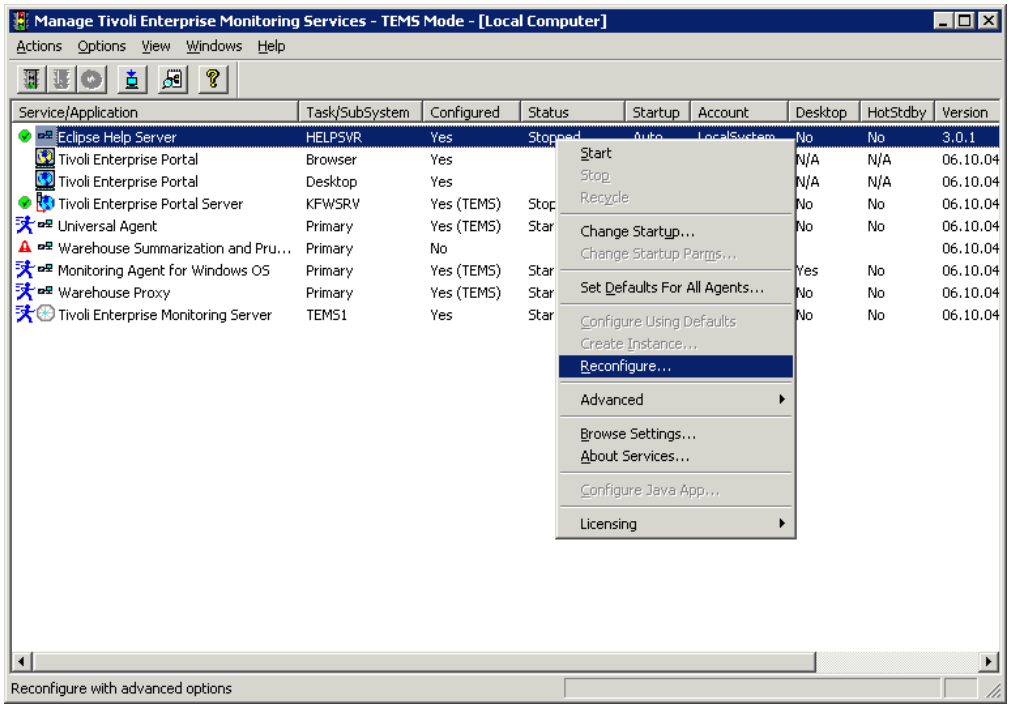

Figure 20. Configuring the Eclipse server

You are prompted for the port number that the Eclipse Help Server is to use:

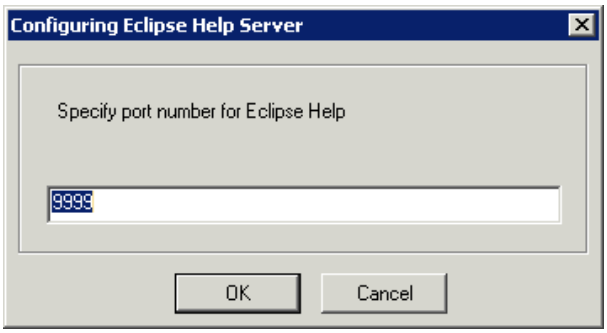

Figure 21. Defining the port number for the Eclipse Help Server

Ensure that this value is set to the same port number that you specified when installing IBM Tivoli Monitoring. Click **OK**.

If you want the Eclipse help server to start automatically whenever this node is started, right-click the **Eclipse Help Server** entry, and select **Change Startup** from the menu. The Eclipse servers startup parameters are displayed:

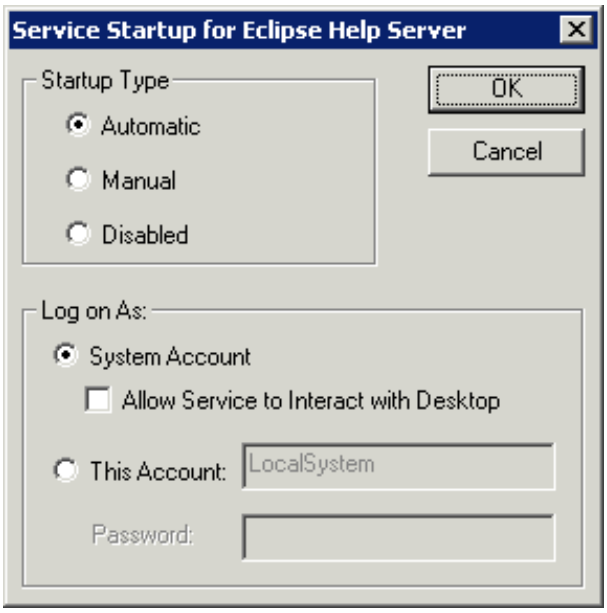

Figure 22. Specifying Eclipse help server startup type

In the **Startup Type** field, select **Automatic**. Click **OK**.

Upgrading the Tivoli Date Warehouse database tables

If you upgrading to ITCAM Agent for WebSphere Applications version 7.2, you might have configured history collection and summarization and pruning for the following tables in the Tivoli Data Warehouse for the older version of the agent:

- `"DC_Messages_-_WebSphere"`
- `"DC_Messages_-_WebSphere_H"`
- `"DC_Messages_-_WebSphere_D"`
- `"DC_Messages_-_WebSphere_W"`
- `"DC_Messages_-_WebSphere_M"`
- `"DC_Messages_-_WebSphere_Q"`
- `"DC_Messages_-_WebSphere_Y"`

You must run the database tables upgrade script provided with ITCAM Agent for WebSphere Applications version 7.2 to upgrade the database tables.

You must run the script before you enable historical data collection for version 7.2.

Important: If you run the upgrade script, but one or more of the tables did not exist in the Tivoli Data Warehouse, the upgrade script does not create them.

The upgrade script increases the size of the tables so that they can store data provided by ITCAM Agent for WebSphere Applications version 7.2.

The scripts are located in the *ITM_Home*/TMAITM6 directory. The name of the script indicates the database type it supports.

To upgrade the database tables, complete the following steps:

1. (Optional) Back up the Tivoli Data Warehouse or the tables to be upgraded before running the script. For more information about backing up IBM Tivoli Monitoring components, see *IBM Tivoli Monitoring: Installation and Configuration Guide*.
2. Disable the Warehouse Proxy agent and the Summarization and Pruning agent. Complete the following steps:
   a. Launch the Manage Tivoli Monitoring Services utility. To open the utility, enter the Windows **Start Menu** and click **Programs** > **IBM Tivoli Monitoring** > **Manage Tivoli Monitoring Services** to launch the utility.
   b. Right-click the Summarization and Pruning agent in the `Service/Application` column.
   c. Select **Stop**.
   d. Right-click the Warehouse Proxy agent in the `Service/Application` column.
   e. Select **Stop**.
3. If the Tivoli Data Warehouse is running a DB2 database, complete the following steps:
   a. Open a DB2 command line processor windows. Click **Start** > **Run** and enter the `db2cmd.exe` command.
   b. In the DB2 command-line processor window, connect to the Tivoli Data Warehouse by issuing the following command:

      ```
      db2 CONNECT TO database USER db_user USING db_password
      ```

      Where:

      database
      Specifies the name of the Tivoli Data Warehouse database server.

      db_user
      Specifies the user who owns the Tivoli Data Warehouse database tables.

      db_password
      Specifies the database password for the specified *db_user*.
   c. Navigate to the *ITM_Home*`/TMAITM6` directory. Run the following script to upgrade the database tables:

      ```
      db2 -td@ -f yn_072000000_warehouse_changes_DB2.sql -x -z log_file
      ```

      Where *log_file* is the name of the log file used to log the output of the script.
   d. Wait for the database upgrade process to complete.
   e. Close the DB2 command-line window.
4. If the Tivoli Data Warehouse is using a Microsoft SQL Server database, complete the following steps:
   a. Navigate to the path where the `sqlcmd` utility is located. Run the following command to connect to the SQL server instance that hosts the Tivoli Data Warehouse and to run the script to upgrade the database tables:

      ```
      sqlcmd.exe -S [protocol:]server[\instance_name][,port]
      -U db_user -P db_password -d database
      -I -i yn_072000000_warehouse_changes_MSSQL.sql -o log_file
      ```

      Where:

protocol
Specifies the protocol used to connect to the database. You can specify TCP/IP, shard memory, or named pipes as the protocol. Valid values are `tcp`, `lpc`, or `np`.

server Specifies the IP address or host name of the computer where the database server resides.

instance_name
Specifies the instance of the SQL server to which to connect.

port Specifies the port used by the SQL server instance.

db_user
Specifies the user who owns the Tivoli Data Warehouse database tables.

db_password
Specifies the database password for the specified *userID*.

database
Specifies the name of the Tivoli Data Warehouse.

log_file
Specifies the name of the log file which the script uses to log the output of the upgrade script.

b. Wait for the database update process to complete and for the script to return to the command prompt.

5. If the Tivoli Data Warehouse is using an Oracle database, complete the following steps:
   a. Navigate to the path where the `sqlplus` utility is located. Run the following command to connect to the instance of the database server that hosts the Tivoli Data Warehouse and to run the script to upgrade the database tables:

```
sqlplus.exe db_user/db_password@db_connection
@yn_072000000_warehouse_changes_ORACLE.sql > log_file
```

Where:

db_user
Specifies the user who owns the Tivoli Data Warehouse database tables.

db_password
Specifies the database password for the specified *userID*.

db_connection
Specifies the net service name of the Oracle instance used for the Tivoli Data Warehouse.

log_file
Specifies the name of the log file which the script uses to log the output of the upgrade script.

   b. Wait for the database update process to complete and for the script to return to the command prompt.

Enabling history collection

Some ITCAM Agent for WebSphere Applications workspaces require collection of historical data. You must enable historical collection by using a script on the Tivoli Enterprise Portal Server.

The `kynHistoryConfigure.bat` script is installed with the agent support files. It requires the IBM Tivoli Monitoring user interface component (`tacmd` command).

You must run the script after the support files have been installed.

You must run the script every time a node of one or more new affinity types is connected to the IBM Tivoli Monitoring infrastructure. A node represents an application server instance. The following affinity types are available:

- WebSphere Application Server (AFF_CAM_WAS_SERVER)
- WebSphere Portal Server (AFF_CAM_WAS_PORTAL_SERVER)
- WebSphere ESB Server (AFF_CAM_WAS_ESB_SERVER)
- IBM Business Process Server (AFF_CAM_WAS_PROCESS_SERVER)
- WebSphere Workplace Server (AFF_CAM_WAS_WORKPLACE_SERVER)

At least one server instance of the new affinity type must be running and connected to the IBM Tivoli Monitoring infrastructure when the script is started.

Run this script when the agents on the monitored servers are already configured and connected to the Tivoli Enterprise Monitoring Server. In this way, history is enabled for all of the affinity types that are used in the environment. If a new affinity type is added to the environment, run the script again.

To run the script, you must know the name of the Tivoli Enterprise Monitoring Server, as configured on the Tivoli Enterprise Portal Server. If there is more than one hub Tivoli Enterprise Monitoring Server, you must run the script for each of the Tivoli Enterprise Monitoring Servers.

The script is located in the *ITM_home*`\bin` directory. Run it with the following command:

`kynHistoryConfigure.bat` *username password TEMS_name*

Where:

username
: Name of a Tivoli Enterprise Portal user with administrative privileges (for example, SYSADMIN).

password
: Password for this user.

TEMS_name
: Name of the Tivoli Enterprise Monitoring Server, as configured on the Tivoli Enterprise Portal Server.

Silent installation of the monitoring agent on Windows systems

The installer support a *silent* mode. In this mode, no user interaction is required for an installation. Instead, the parameters are taken from a *response file*. You can install and uninstall the agent and install the application support files.

Response files have a text format. You can create a response file based on one of the samples provided on the installation DVD or image.

You can also create a response file during the installation, modify it if necessary, and then use it for a silent installation. In this way, you can quickly reproduce similar installations many times, for example, on different hosts.

Performing a silent installation or uninstallation of the monitoring agent on Windows systems

You can use the installer to install or uninstall ITCAM Agent for WebSphere Applications monitoring agent and ITCAM Data Collector for WebSphere in silent mode. You can also install support files for the Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal client on Windows in silent mode. To do this, modify the sample files that are provided on the installation DVD or image. Then, run the installer from the command-prompt.

To complete a silent installation or uninstallation, first you must prepare the response file. Then, run the installer, supplying the name of the response file.

Preparing a response file for an ITCAM Agent for WebSphere Applications installation

To prepare a response file for installing the monitoring agent, complete the following procedure:

1. On the product installation DVD or image, in the `WINDOWS` directory, locate the `silent.txt` file.
2. Make a copy of this file, and open it in a text editor.
3. Modify any of the following properties, if necessary. Do not modify any other properties.

Table 4. Agent installation response file properties

Response file property	Meaning
License Agreement	Uncomment the line that contains the License Agreement. You must agree to the license agreement and uncomment this parameter to be able to proceed with the installation procedure.
Install Directory	Uncomment the line that contains the Install Directory parameter and specify the directory in which you want to install the agent. The property defaults to `C:\IBM\ITM`. **Important:** If you are installing an agent on a system where IBM Tivoli Monitoring is already installed, the agent is installed in the IBM Tivoli Monitoring installation directory, regardless of this parameter.
Install Folder	If you do not want the agent to be given the default name specified by the `Install Folder` property, uncomment the parameter and enter a new name. The property defaults to `IBM Tivoli Monitoring`.
EncryptionKey	The 32-character encryption key used to secure password transmission and other sensitive data across your IBM Tivoli Monitoring environment. For more information, see IBM Tivoli Monitoring: Installation and Setup Guide for details about the encryption key.
KGLWICMA	Uncomment the line `KGLWICMA=Tivoli Enterprise Monitoring Agent Framework` to install the agent framework.
KYNWICMA	Uncomment the line `KYNWICMA=ITCAM Agent for WebSphere Applications (TEMA)` to install the agent.
KYN_PORT	Specifies the port number of the TCP socket port that the monitoring agent uses to listen for connection requests from the data collectors. The default is 63335.

Table 4. Agent installation response file properties (continued)

Response file property	Meaning
KYN_ALT_NODEID	Specifies an Alternative Node ID for identifying the agent. This identifier determines how the agent is displayed in the Tivoli Enterprise Portal navigator tree. The default is "Primary", which is used with the host name of the computer where the agent is installed.
configure_type	Uncomment the line that contains the configure type. The property defaults to `tema_configure`. Do not modify the value of this property.
KYNWICMA_FILE	Specifies the location of the ITCAM Data Collector for WebSphere silent response file, `silent_exit.txt`. For example, `C:\Temp\silent_exit.txt`. The location must be specified as an absolute path. The file `silent_exit.txt` must contain the `ITCAM_CONFIGHOME` parameter.

Important: The `silent.txt` file contains the parameters required for installing and configuring the ITCAM Agent for WebSphere Applications monitoring agent.

4. Save the edited copy in a work directory, for example, as `C:\TEMP\SILENT.TXT`.

Preparing a response file for an ITCAM Data Collector for WebSphere installation

To prepare a response file for installing the data collector, complete the following procedure:

1. On the product installation DVD or image, in the `WINDOWS` directory, locate the `silent_exit.txt` file.
2. Make a copy of this file, and open it in a text editor.
3. Modify the following property.

Table 5. Data Collector installation response file properties

Response file property	Meaning
ITCAM_CONFIGHOME	Specifies the location of the ITCAM Data Collector for WebSphere home directory, for example `C:\IBM\ITM\dchome\7.2.0.0.1`. The location must be specified as an absolute path. The data collector home directory must exist. Beginning with ITCAM Agent for WebSphere Applications version 7.2, ITCAM Data Collector for WebSphere is a shared component with the following products: • ITCAM for SOA 7.2 • ITCAM for WebSphere Application Server 7.2 support for WebSphere Application Server 8.5 • ITCAM Diagnostics Tool that is previewed in the ITCAM for Application Diagnostics beta If ITCAM Data Collector for WebSphere is installed at this location and is found to be of the same version, release, and maintenance level, it is not replaced. If ITCAM Data Collector for WebSphere is installed at this location and is found to be of a different version, release, and maintenance level, a new directory, `dc_version`, is created in the data collector home directory. For example, *DC_home*`\7.2.0.0.1`. The data collector is installed in this location.

4. Save the edited copy in a work directory, for example, as `C:\Temp\silent_exit.txt`. The absolute path to this file must be the location referenced by the `KYNWICMA_FILE` parameter of the monitoring agent response file.

Preparing the response file for a monitoring agent uninstallation

To prepare a response file for uninstalling the monitoring agent and data collector, complete the following procedure:

1. In the *ITM_HOME*`\Config` directory, locate the `YN_Silent_Uninstall.txt` file.
2. Copy the file to a work directory, for example, as `C:\TEMP\silent_uninstall.TXT`. Do not modify the copy.

This response file contains the configuration for uninstalling the monitoring agent and ITCAM Data Collector for WebSphere.

Important: If ITCAM Data Collector for WebSphere home directory was specified to be outside of IBM Tivoli Monitoring home directory, the data collector home directory is not removed during the uninstallation.

Preparing the response file for support files installation

To prepare a response file for installing the application support files on a Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, or Tivoli Enterprise Portal client, complete the following procedure:

1. On the product installation DVD or image, in the `WINDOWS` directory, locate the `silent.txt` file.
2. Make a copy of this file, and open it in a text editor.

3. Find the following lines, and comment out (by adding ; as the first character) the lines that do not apply to the host that you are installing on:

```
KYNWICMS=ITCAM Agent for WebSphere Applications Support ( TEMS )
KYNWIXEW=ITCAM Agent for WebSphere Applications Support ( TEP Workstation )
KYNWICNS=ITCAM Agent for WebSphere Applications Support ( TEP Server )
```

4. Save the edited copy in a work directory, for example, as `C:\TEMP\SILENT.TXT`.

Running the installer in silent mode

After preparing the response file for your installation and uninstallation, run the installer and specify the path and name of the response file. Complete the following procedure:

1. Open a Windows command-prompt window, and change to the WINDOWS directory on the installation DVD or image.
2. Run setup in the following way, specifying the parameters in the order that is shown:

   ```
   start /wait setup /z"/sfresponse_file_name" /s /f2"log_file_name"
   ```

   Where:

   response_file_name
   The name of the response file that you prepared (with full path).

   log_file_name
   The name of the log file that the installer writes (with full path).

   For example:

   ```
   start /wait setup /z"/sfC:\TEMP\SILENT.TXT" /s /f2"C:\TEMP\INSTALL.LOG"
   ```

Important: If you are completing an upgrade, and the monitoring agent is currently running, silent installation is aborted.

You can find complete information about silent IBM Tivoli Monitoring installation in "Appendix B. Performing a silent installation of IBM Tivoli Monitoring"of the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Configuring the data collector is silent mode

The ITCAM Data Collector for WebSphere configuration utilities support a *silent* mode. In this mode, no user interaction is required for configuration. Instead, the parameters are taken from a *response file*.

The following table provides a description of the configuration tasks that can be performed in silent mode by the utilities.

Table 6. Configuration tasks

Configuration task	Where to find the procedure
Configure the data collector to monitor application server instances within a WebSphere Application Server profile in silent mode.	"Configuring ITCAM Data Collector for WebSphere in silent mode" on page 75
Unconfigure the data collector in silent mode.	"Unconfiguring ITCAM Data Collector for WebSphere in silent mode" on page 80

Table 6. Configuration tasks (continued)

Configuration task	Where to find the procedure
Migrate an older version of the data collector to ITCAM Data Collector for WebSphere in silent mode or update the maintenance level of ITCAM Data Collector for WebSphere in silent mode.	"Migrating ITCAM Data Collector for WebSphere in silent mode" on page 82
Migrate the WebSphere Application Server data collector provided by ITCAM for SOA version 7.1.1 to ITCAM Data Collector for WebSphere in silent mode.	"Migrating ITCAM for SOA version 7.1.1 data collector to ITCAM Data Collector for WebSphere in silent mode" on page 85

Important: When you create or edit a silent response file that contains unicode characters, make sure the file is saved using UTF-8 encoding. If you save the file using a different encoding scheme, for example ISO-8858, an error is displayed during the configuration task that indicates that the utility was unable to access the file.

Configuring ITCAM Data Collector for WebSphere in silent mode

ITCAM Data Collector for WebSphere can be configured interactively with the ITCAM Data Collector for WebSphere Configuration utility. If you want to configure many application server instances, it might be more convenient to configure the data collector in silent mode.

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

When you configure the data collector in silent mode, you first specify configuration options in a properties file. A sample properties file, `sample_silent_config.txt`, is packaged with the configuration utility. The file is available in the *DC_home*`\bin` directory. The *DC_home* variable is the location where the data collector is installed.

A sample of a properties file is displayed in "Sample properties file" on page 78.

Complete the following steps to perform a silent configuration:

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

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

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

Properties file

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

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

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

  property
  Name of property. The list of valid properties that you can configure is shown in Table 7.

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

Table 7 describes the properties that are available when configuring the data collector in silent mode:

Table 7. Available properties for running the configuration utility in silent mode

Property	Comment
default.hostip	If the computer system uses multiple IP addresses, specify the IP address for the data collector to use.
Integration of the data collector with the ITCAM for Application Diagnostics Managing Server	
ms.connect	Specifies whether the data collector is configured to connect to the managing server in an ITCAM for Application Diagnostics environment. Valid values are `True` and `False`.
ms.kernel.host	Specifies the fully qualified host name of the managing server.
ms.kernel.codebase.port	Specifies the codebase port on which the managing server is listening.
ms.am.home	Specifies the managing server home directory.
ms.am.socket.bindip	Specifies the IP address or host name to be used by the data collector to communicate with the managing server. If more than one network interface or IP address is configured on data collector computer system, choose one of them.
ms.firewall.enabled	Specifies whether a firewall is enabled on the data collector host or you have special requirements to change the RMI ports for the data collector. Valid values are *True* and *False*.
ms.probe.controller.rmi.port	If the data collector is behind a firewall or you have special requirements to change the Controller RMI port of data collector, set this port number range. Configure this port number as permitted by the firewall for the data collector host. For example: `ms.probe.controller.rmi.port=8300-8399` or ms.probe.controller.rmi.port=8300.
ms.probe.rmi.port	If the data collector is behind a firewall, or you have special requirements to change the RMI port of data collector, set this port number range. Configure this port number as permitted by the firewall for the data collector host. For example: `ms.probe.rmi.port=8200-8299` or `ms.probe.rmi.port=8200`.
Integration of the data collector with the ITCAM for Transactions	
ttapi.enable	Specifies whether the data collector communicates with ITCAM for Transactions using the Transaction Tracking API (TTAPI). Valid values are `True` and `False`.
ttapi.host	Specifies the host name of the ITCAM for Transactions Transaction Collector to connect to.
ttapi.port	Specifies the port of the Transaction Collector to connect to.
Integration of the data collector with the ITCAM for SOA	
soa.enable	Specifies whether to integrate the data collector with ITCAM for SOA. The ITCAM for SOA agent must be installed to complete the configuration.

Table 7. Available properties for running the configuration utility in silent mode (continued)

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

Table 7. Available properties for running the configuration utility in silent mode (continued)

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

Sample properties file

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

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

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

```
################################################################################

[DEFAULT SECTION]

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

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

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

#  ITCAM for SOA agent:
soa.enable=False

#  Tivoli Performance Viewer:
tpv.enable=True

#  ITCAM Diagnostics Tool:
de.enable=False

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

#  Create a backup of WebSphere Application Server:
was.backup.configuration=False
was.backup.configuration.dir=C:\IBM\ITM\dchome\7.2.0.0.1

#  Modify Garbage Collection log path:
#was.gc.custom.path=False
#was.gc.file=C:\test.log

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

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

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

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

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

Unconfiguring ITCAM Data Collector for WebSphere in silent mode

ITCAM Data Collector for WebSphere can be unconfigured interactively with the ITCAM Data Collector for WebSphere Unconfiguration utility. If you want to unconfigure many application server instances, it might be more convenient to unconfigure ITCAM Data Collector for WebSphere in silent mode.

When you unconfigure the data collector in silent mode, you first specify configuration options in a properties file. A sample properties file, `sample_silent_unconfig.txt`, is packaged with the unconfiguration utility. The file is available in the *DC_home*`\bin` directory. The *DC_home* variable is the location where the data collector is installed.

A sample of a properties file is presented in Table 8.

Complete the following steps to perform a silent unconfiguration:

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

   `unconfig.bat -silent [`*dir_path*`]\`*silent file*
4. After unconfiguring the data collector to monitor application server instances, you must restart the instances. The data collector configuration takes effect when the application server instances are restarted.

Properties file

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

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

  property
  : This is the name of property. The list of valid properties that you can configure is shown in Table 8.

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

Table 8 describes the properties that are available when unconfiguring the data collector in silent mode:

Table 8. Available properties for running the unconfiguration utility in silent mode

Property	Comment
WebSphere Application Server connecting settings	

Table 8. Available properties for running the unconfiguration utility in silent mode (continued)

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

Sample properties file

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

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

[DEFAULT SECTION]

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

```
was.wsadmin.password=

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

#  Create a backup of WebSphere Application Server:
was.backup.configuration=False
was.backup.configuration.dir=C:\Program Files\IBM\ITM\dchome\7.2.0.0.1\data

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

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

Migrating ITCAM Data Collector for WebSphere in silent mode

A previous version or an earlier maintenance level of ITCAM Data Collector for WebSphere can be migrated interactively with the ITCAM Data Collector for WebSphere Migration utility. If you want to migrate many application server instances, it might be more convenient to migrate the application servers using the migration utility in silent mode.

To migrate ITCAM for SOA WebSphere Application Server version 7.1.1 using the migration utility in silent mode, see "Migrating ITCAM for SOA version 7.1.1 data collector to ITCAM Data Collector for WebSphere in silent mode" on page 85.

When you migrate the data collector in silent mode, you first specify configuration options in a properties file. A sample properties file, `sample_silent_migrate.txt`, is packaged with the migration utility. The file is available in the *DC_home*`\bin` directory . The *DC_home* variable is the location where the data collector is installed. A sample of a properties file is presented in "Sample properties file" on page 84.

Complete the following steps to perform a silent migration:

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

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

During a silent migration, you can also configure or reconfigure integration with: ITCAM for SOA, ITCAM Agent for WebSphere Applications monitoring agent, ITCAM for Application Diagnostics Managing Server, ITCAM for WebSphere Application Server, and ITCAM Diagnostics Tool. Use the silent configuration parameters for these components, as described in "Configuring ITCAM Data Collector for WebSphere in silent mode" on page 75.

Properties file

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

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

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

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

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

Table 9 describes the properties that are available when migrating the data collector in silent mode:

Table 9. Properties for the migration utility in silent mode

Property	Comment
default.hostip	If the computer system uses multiple IP addresses, specify the IP address for the data collector to use.
migrate.type	Type of agent whose data collector you want to migrate to ITCAM Data Collector for WebSphere. The value must be set to `AD`. **Important:** For all products, to update a maintenance level, set the `migrate.type` property to AD.
Location of data collector to be migrated	
itcam.migrate.home	Specifies the data collector home directory of the old version of the data collector. The directory is not deleted as part of the migration.
ITCAM Agent for WebSphere Applications monitoring agent settings	
temaconnect	Specifies whether the data collector connects to the ITCAM Agent for WebSphere Applications monitoring agent. Set this property to `False` if you do not want to connect the ITCAM Agent for WebSphere Applications with the monitoring agent, if you plan to connect the ITCAM Agent for WebSphere Applications with the managing server only, or if you do not have the ITCAM Agent for WebSphere Applications installed. Valid values are `True` and `False`. **Remember:** The managing server is not a component of ITCAM for Applications.
tema.host	Specifies the fully qualified host name or IP address of the ITCAM for Agent for WebSphere Applications monitoring agent.
tema.port	Specifies the port number of the ITCAM for Agent for WebSphere Applications monitoring agent.
WebSphere Application Server connection settings	
was.wsadmin.connection.host	Specifies the name of the host to which the wsadmin tool is connecting. In a Network Deployment environment, specify the wsadmin connection to the Deployment Manger. In a stand-alone environment, specify the wsadmin connection to the server.
WebSphere Application Server global security settings	

Table 9. Properties for the migration utility in silent mode (continued)

Property	Comment
was.wsadmin.username	Specifies the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server.
was.wsadmin.password	Specifies the password that corresponds to the user specified in the `was.wsadmin.username` property.
WebSphere Application Server settings	
was.appserver.profile.name	Specifies the name of the application server profile you want to configure.
was.appserver.home	Specifies the WebSphere Application Server home directory.
was.appserver.cell.name	Specifies the WebSphere Application Server cell name.
was.appserver.node.name	Specifies the WebSphere Application Server node name.
WebSphere Application Server runtime instance settings	
was.appserver.server.name	Specifies the application server instance within the application server profile to migrate to the new version of the data collector. **Tip:** The silent response file can have multiple instances of this property.

Sample properties file

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

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

```
[DEFAULT SECTION]

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

#Migration type:
migrate.type=AD

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

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

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

#  WebSphere Application Server details:
was.appserver.profile.name=AppSrv01
was.appserver.home=C:\Program Files\IBM\WebSphere\AppServer
was.appserver.cell.name=yourCellName
was.appserver.node.name=yourNodeName

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

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

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

The ITCAM for SOA version 7.1.1 WebSphere Application Server data collector can be migrated to ITCAM Data Collector for WebSphere interactively with the ITCAM Data Collector for WebSphere Migration utility. If you want to migrate many application server instances, it might be more convenient to migrate the application servers using the migration utility in silent mode.

For the procedure for migrating the following data collector components to the ITCAM Data Collector for WebSphere, see "Migrating ITCAM Data Collector for WebSphere in silent mode" on page 82:

- ITCAM for WebSphere version 6.1.0.4 or later
- WebSphere Data Collector version 6.1.0.4 or later included in ITCAM for Web Resources version 6.2.0.4 or later
- ITCAM Agent for WebSphere Applications version 7.1 included in ITCAM for Applications Diagnostics version 7.1
- ITCAM for WebSphere Application Server version 7.2

The procedure in "Migrating ITCAM Data Collector for WebSphere in silent mode" on page 82 can also be followed to update the maintenance level of any products that have ITCAM Data Collector for WebSphere as a component, including ITCAM for SOA.

Important: If an older version of ITCAM Agent for WebSphere Applications is configured for application servers in the same profile as ITCAM for SOA version 7.1.1, migrate the data collector provided with ITCAM Agent for WebSphere Applications. Then, reconfigure the data collector to integrate it with the ITCAM

for SOA monitoring agent. You must not run the migration utility to migrate the older version of the ITCAM for SOA WebSphere Application Server data collector.

When you migrate the ITCAM for SOA version 7.1.1 WebSphere Application Server data collector in silent mode, you first specify configuration options in a properties file. A sample properties file, `sample_silent_migrate_soa.txt`, is packaged with the migration utility. The file is available in the *DC_home*`\bin` directory . The *DC_home* variable is the location where the data collector is installed. A sample of a properties file is presented in "Sample properties file" on page 88.

Complete the following steps to perform a silent migration:

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

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

While you are performing a silent migration, , you can also configure or reconfigure integration with ITCAM for SOA, ITCAM Agent for WebSphere Applications monitoring agent, ITCAM for Application Diagnostics Managing Server, Tivoli Performance Viewer, and the ITCAM Diagnostics Tool for the application server instances at the same time. To do this, use the silent configuration parameters for these components, as described in "Migrating ITCAM Data Collector for WebSphere in silent mode" on page 82.

Properties file

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

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

  property
  : This is the name of property. The list of valid properties that you can configure is shown in: Table 10 on page 87.

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

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

Table 10 on page 87 describes the properties that are available when migrating the data collector in silent mode:

Table 10. Available properties for running the migration utility in silent mode

Property	Comment
default.hostip	If the computer system uses multiple IP addresses, specify the IP address for the data collector to use.
migrate.type	Type of agent whose agent you want to migrate to ITCAM Data Collector for WebSphere. The value must be set to `SOA`.
was.appserver.home	Location of the WebSphere Application Server home directory where the ITCAM for SOA version 7.1.1 WebSphere Application Server data collector is configured. For example: `C:\Program Files\IBM\WebSphere\AppServer`.
ms.connect	Specifies whether the data collector is configured to connect to the managing server in an ITCAM for Application Diagnostics environment. For a migration from ITCAM for SOA version 7.1.1 where the data collector is not being integrated with another product, ignore this parameter.
ttapi.enable	Specifies whether the data collector communicates with ITCAM for Transactions using the Transaction Tracking API (TTAPI). Valid values are `True` and `False`.
soa.enable	Specifies whether to integrate the data collector with ITCAM for SOA. The ITCAM for SOA agent must be installed to complete the configuration.
tpv.enable	Specifies whether to integrate the data collector with the Tivoli Performance Viewer when the data collector is included as part of ITCAM for WebSphere Application Server 8.5. Tivoli Performance Viewer is accessed with the WebSphere Application Server administrative console. For a migration from ITCAM for SOA version 7.1.1 where the data collector is not being integrated with another product, ignore this parameter.
de.enable	Specifies whether to integrate the data collector with the ITCAM Diagnostics Tool. The ITCAM Diagnostics Tool is built on Eclipse. It is a tool for diagnostic investigation of applications that are running on WebSphere Application Server. For a migration from ITCAM for SOA version 7.1.1 where the data collector is not being integrated with another product, ignore this parameter.
temaconnect	Specifies whether the data collector connects to the ITCAM Agent for WebSphere Applications monitoring agent. For a migration from ITCAM for SOA version 7.1.1 where the data collector is not being integrated with another product, ignore this parameter.
was.backup.configuration	Specifies whether to back up the current configuration of the WebSphere Application Server configuration before applying the new configuration. Valid values are `True` and `False`.
was.gc.custom.path	Specifies the path to the custom Garbage Collection log. For a migration from ITCAM for SOA version 7.1.1 where the data collector is not being integrated with another product, ignore this parameter.
WebSphere Application Server connection settings	

Table 10. Available properties for running the migration utility in silent mode (continued)

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

Sample properties file

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

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

```
#If the utility cannot determine the values, uncomment and override the default values.
#
#Servers:
#You can migrate the data collector for multiple servers in the same profile.
#Uncomment the second [SERVER] and add the server name.
#Repeat for each additional server.
################################################################################


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

#  Migration type:
migrate.type=SOA

#  Old WebSphere Application Server home directory:
was.appserver.home=C:\Program Files\IBM\WebSphere\AppServer80\AppServer

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

#  ITCAM for Transactions:
ttapi.enable=False

#  ITCAM for SOA agent:
soa.enable=True

#  Tivoli Performance Viewer:
tpv.enable=False

#  ITCAM Diagnostics Tool:
de.enable=False

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

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

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

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

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

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

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

Additional steps for configuring the data collector on Windows systems

For every application server instance where the data collector was configured, complete the following steps, as applicable.

Setting up a secure connection to the Managing Server

If the data collector is to communicate with ITCAM for Application Diagnostics Managing Server, you might have to set up a secure connection.

Important: The Managing Server deep-dive functionality is not available in ITCAM for Applications 7.2; if you do not have ITCAM for Application Diagnostics installed in your environment, please ignore all references to this functionality in this document.

See Appendix A, "Setting up a secure connection to the Managing Server," on page 275 for more information about setting up a secure (SSL) connection between the data collector and the Managing Server.

Connecting to an ITCAM for SOA version 7.1.1 monitoring agent

When you integrate ITCAM Data Collector for WebSphere with ITCAM for SOA for applications servers within a profile where ITCAM for SOA is not already installed and configured, and you later install ITCAM for SOA 7.1.1, you must add additional properties to the `KD4.dc.properties` file.

To add the additional properties to the `KD4.dc.properties` file, complete the following steps:

1. Navigate to the *ITCAM4SOA_Home*`\KD4\config` directory.
2. Add the following properties to the `KD4.dc.properties` file with any text editor:

```
1.server_instance.monitor=on
1.server_instance.log=info
1.server_instance.trace=off
1.server_instance.monitor.control.count=1
1.server_instance.monitor.control.1=*;*;*;*;*;none
1.server_instance.filter.control.count=0
```

3. Save the file.

Displaying data in ITCAM for SOA topology views

When you configure data collection for applications servers for ITCAM Agent for WebSphere Applications, data collection might be configured for ITCAM for SOA version 7.2 for application servers in the same profile. You must reconfigure and restart the Tivoli Enterprise Portal Server to capture ITCAM Agent for WebSphere Applications data in the topology views of ITCAM for SOA.

After you integrate the data collector with the ITCAM Agent for WebSphere Applications monitoring agent, complete the following steps:

1. Wait until at least one of the application servers that you are monitoring processes transaction data.
2. Rebuild the Tivoli Enterprise Portal Server on Linux or AIX® systems or reconfigure the Tivoli Enterprise Portal Server on Windows systems.
3. Restart the Tivoli Enterprise Portal Server.

For more information about reconfiguring and restarting the Tivoli Enterprise Portal Server, see the *IBM Tivoli Composite Application Manager for SOA Installation Guide*.

Completing and verifying data collector configuration

To complete and verify that configuration of the data collector for an application server instance, complete the following steps:

1. If any of the following problems occur, you know that the data collector configuration has failed:
   - After the configuration, the application server fails to restart.
   - During a command-line configuration, the configuration tool indicates that the configuration failed.
   - During a silent configuration, the command line indicates a message that the configuration failed.
   - After the configuration, there are messages in the Tivoli common log file that indicates that configuration has failed.

   If the data collector configuration failed:
   - Restore the application server configuration that you had before you attempted the failed configuration. For more information, see "Restoring the application server configuration from a backup" on page 321.
   - Run the command-line or silent configuration again.
   - If the configuration fails repeatedly, contact IBM Support. If directed by IBM Support, configure the application server instance manually; for more information, see "Manually removing data collector configuration from an application server instance" on page 329.
2. If Terminal Services are enabled on a Windows 2008 Server, run the following command:

   ```
   change user /execute
   ```
3. If you use the IBM Tivoli Monitoring infrastructure, start a Tivoli Enterprise Portal client and verify that you can see the monitored data for the application server instance.
4. If you use the ITCAM for Application Diagnostics Managing Server infrastructure, access the visualization engine and verify that you can see monitored data for the application server instance.

Uninstalling ITCAM Agent for WebSphere Applications on Windows systems

To remove ITCAM Agent for WebSphere Applications on a Windows system, complete these steps:

1. Unconfigure the data collector from all of the application server instances.

   For more information, see "Unconfiguring ITCAM Data Collector for WebSphere" on page 46.
2. Uninstall IBM Tivoli Monitoring:
   a. To access the Control Panel **Add or Remove Programs** option, complete these steps:
      - For Windows 2003, from the desktop, click **Start** > **Control Panel**.
      - For Windows 2008, from the desktop, click **Start** > **Control Panel** > **Programs and Features**.
      - For Windows 7, from the desktop, click **Start** > **Control Panel** > **Programs** > **Programs and Features**.

   b. Click **Add or Remove Programs**.

   c. Select **IBM Tivoli Monitoring**.

d. Click **Change**.
e. Complete one of the following procedures:
   - If you want to remove all IBM Tivoli Monitoring components, including the agent, select **Remove** and click **Next**. To confirm the uninstallation, click **OK**
   - If you want to remove the agent but not other IBM Tivoli Monitoring components, select **Modify** and click **Next**. Deselect the agent. Then, to complete the uninstallation, click **Next** several times.
f. Click **Finish**.

Important:

- If you uninstalled the agent without unconfiguring the data collector for any application server instance, see "Manually removing data collector configuration from an application server instance" on page 329.
- If the home directory of ITCAM Data Collector for WebSphere was specified to be outside of the IBM Tivoli Monitoring home directory, the data collector home directory is not removed during the uninstallation and must be removed manually.

Installing and uninstalling a language pack on Windows systems

A language pack enables user interaction with the agent in a language other than English. For example, when a Spanish language pack is installed, the Tivoli Enterprise Portal workspaces and the internal messages of the agent are displayed in Spanish.

To enable full support for a language, you must install the language pack on the agent host and all hosts where the Tivoli monitoring support files for the agent are installed (hub and remote Tivoli Enterprise Monitoring Servers, all Tivoli Enterprise Portal Servers, and all Tivoli Enterprise Portal desktop clients).

If you no longer want to use a language, uninstall the language pack for it.

Before installing or uninstalling a language pack, ensure that:

- The agent and the Tivoli Enterprise Portal Support Files are installed.
- The Java runtime environment (JRE) is available on every host where you are planning to install the language pack. (The JRE is required by IBM Tivoli Monitoring).

Installing a language pack on Windows systems

To install a language pack on a Windows system, you must use the installer on the language pack DVD. The procedure is the same on the agent host, hub Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal desktop client.

Complete the following procedure:

1. Start `lpinstaller.bat` from the 7.2 folder on the language pack DVD.
2. Select the language of the installer and click **OK**.

   Important: In this step, you select the language for the installer user interface, not the language pack that will be installed.
3. On the introduction window, click **Next**.

4. Select **Add/Update** and click **Next**.
5. In the `nlspackage` folder on the language pack DVD, select the folder where the National Language Support package (NLSPackage) files are located.
6. Select language support for **ITCAM Agent for WebSphere Applications** and click **Next**.
7. Select the languages that you want to install and click **Next**.
8. Examine the installation summary page. To begin the installation, click **Next**.
9. To exit the installer, click **Finish**.
10. If you are installing the language pack on a Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, or Tivoli Enterprise Portal desktop client, start the **Manage Tivoli Monitoring Services** utility, and use it to restart the server or client. If the Eclipse Help Server is running, restart it as well.

Uninstalling a language pack on Windows systems

To uninstall a language pack on a Windows system, you must use the installer on the language pack DVD. The procedure is the same on the agent host, hub Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal desktop client.

Complete the following procedure:

1. From the 7.2 folder on the language pack DVD, start `lpinstaller.bat`.
2. Select the language of the installer and click OK.

   Important: In this step, you select the language for the installer user interface, not the language pack that is to be installed.
3. On the introduction window, click **Next**.
4. Select **Remove** and click **Next**.
5. Select **ITCAM Agent for WebSphere Applications**.
6. Select the languages to uninstall and click **Next**.

   Tip: To select multiple languages at the same time, you can hold down the **Ctrl** key and select the languages that you want.
7. Examine the installation summary page. To begin the installation, click **Next**.
8. To exit the installer, click **Finish**.
9. If you are uninstalling a language pack from Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, or Tivoli Enterprise Portal desktop client, start the **Manage Tivoli Monitoring Services** utility, and use it to restart the server or client. If the Eclipse Help Server is running, restart it as well.

Part 3. Installing and Configuring ITCAM Agent for WebSphere Applications on UNIX and Linux

Chapter 4. Prerequisites and pre-installation tasks for ITCAM Agent for WebSphere Applications on Linux and UNIX systems

You must complete certain tasks before installing ITCAM Agent for WebSphere Applications on UNIX and Linux systems.

System and software prerequisites

See the Software product compatibility reports website to generate a variety of reports related to product and component requirements.

Tip: ITCAM Agent for WebSphere Applications version 7.2 is a component of ITCAM for Applications version 7.2. To run a report specific to ITCAM for Applications version 7.2, specify Tivoli Composite Application Manager for Applications as the product name and 7.2 as the version.

To view the system requirements for ITCAM Agent for WebSphere Applications version 7.2, see the Detailed software requirements report.

Required tasks before installation

Complete the tasks in each of the following sections before you install the data collector.

Permissions

If the IBM Tivoli Monitoring framework is being installed on the host for the first time, root privileges are required for installation. Otherwise, a non-root user account can be used, but it must meet certain requirements.

The agent requires the IBM Tivoli Framework; the agent installer installs this framework by default. The framework includes Global Security Kit (GSKit); installation of GSKit requires root permissions. Therefore, if the IBM Tivoli Monitoring framework was not installed on the host, you must use a root account to install the agent.

However, if the IBM Tivoli Framework is already installed on the host, you can use a non-root account for installation. This must be the account that owns all the application server profiles that are monitored by the data collector. The account must meet the following requirements for every application server profile that is monitored:

- The user must be able to start and stop WebSphere Application Server using the standard `startServer.sh` and `stopServer.sh` scripts.
- The user must have privileges (read, write, and execute) for accessing the application server directory tree.
- The files in the `AppServer_home` directory must be owned by this user.
- The user must have read/write permission for the IBM Tivoli Monitoring home directory (by default, `/opt/IBM/ITM`) and the `logs` subdirectory in it.

- The user must have read and write privileges to the application server log directory: *AppServer_home*/profiles/*profile_name*/logs; if the wsadmin.traceout and wsadmin.valout files exist in this directory, the user must have read/write permission for these files.
- If you are performing an upgrade of the agent, this installation user must have read/write permission for the home directory for the previous versions of the monitoring agent and data collector.

Important: If IBM WebSphere Application Server was installed by root, but all the instances to be monitored are owned by a non-root account, you must complete the following procedure before using this non-root account to install the agent:

1. As the root user, run the following commands:

   ```
   chown -R wasuser:wasgroup AppServer_home/properties/version/history
   chown wasuser:wasgroup AppServer_home/properties/version
   ```

   The *wasuser* and the *wasgroup* are the user and group of the application server instance.
2. As your non-root user, run the following command from the *profile_home*/bin directory:

   ```
   ./versionInfo.sh
   ```

   If the application server version (not an error message) is displayed, you have completed the change successfully, and can use the non-root account to install the agent.

For information about the permissions required to run the data collector configuration, reconfiguration, migration, and unconfiguration utilities in interactive mode and silent mode, see "Permissions required for configuration tasks" on page 121.

Adjusting for ports that are blocked by your firewall or that are used by other applications

During the installation, you must specify or accept the defaults for port numbers that are used by ITCAM Agent for WebSphere Applications.

By default, the ITCAM Agent for WebSphere Applications communicates in the following ways:

- If the IBM Tivoli Monitoring infrastructure is used, the agent makes outbound connections to the Tivoli Enterprise Monitoring Server host.
- If an ITCAM for Application Diagnostics Managing Server is used, and the data collector is configured for one or more application server instances, it opens ports in the 8200 - 8399 range for inbound communication.
- With WebSphere Network Deployment, WebSphere Virtual Enterprise, or WebSphere Compute Grid environments, the agent makes outbound connections to the deployment manager host. The port number is available in the deployment manager administrative console.

  Remember: WebSphere Virtual Enterprise functions in Network Deployment version 8.5 are characterized as intelligent management capabilities. WebSphere Compute Grid functions in Network Deployment version 8.5 are characterized as WebSphere batch capabilities.

You must ensure that these connections are not blocked by a firewall. If they are blocked, you must either modify the communication settings during installation

and configuration of the data collector, or change the settings of the firewall. To determine the connections that your firewall might block, see the documentation that is supplied with the firewall.

If you use the managing server, you must also make sure that ports that are used for inbound communication are not used by other applications. If they are used by other applications, you must change the ports for data collector inbound communication when configuring the data collector. For more information, see "Configuring ITCAM Data Collector for WebSphere" on page 122. To list the ports that are used by other applications, run the `netstat -a` command; In its output, look for lines that include `LISTENING`.

Increasing the heap size

To increase the heap size configuration to 128 MB greater than the current configuration, complete these steps from the WebSphere administrative console for each server that you want to configure for data collection:

1. Log in to the IBM WebSphere Application Server administrative console.
2. Click **Server** > **Server Types** > **WebSphere Application Servers** and select the *server_name*.
3. In the **Configuration** tab, go to **Server Infrastructure** > **Java and Process Management** > **Process Definition** > **Additional Properties: Java Virtual Machine**.
4. Edit the **Maximum Heap Size** field. If the default is not specified, then it assumes `256`.

HP-UX: tuning HotSpot JVM garbage collection

For HotSpot JVM, the default NewSize and MaxNewSize might be too small for some applications if these applications allocate large numbers of short living objects. Some tuning is recommended for an application that allocates many short living objects:

```
-XX:+DisableExplicitGC -XX:NewSize=128m -XX:MaxNewSize=256m
```

Also, the default MaxPermSize might be small for some applications. It is recommended to use `-XX:MaxPermSize=128m or -XX:MaxPermSize=256m`

Important: Change the NewSize, MaxNewSize, and MaxPermSize based on the Maximum (-Xmx) and Minimum (-Xms) heap settings of the JVM. Before you modify these parameters, consult the Tuning hotspot Java virtual machines section of the
IBM WebSphere Application Server Express® information center.

Making sure that there are no invalid mounted file systems

Some file systems might be incorrectly specified as mounted in the `/etc/file_systems` file. Such files are not mounted, or might have lost connection with the computer on which the agent is being installed. In this case, the installation might hang without producing any error messages.

To prevent this, complete the following steps:

1. Either mount all of the file systems that are listed in the `/etc/file_systems` file, or comment out all of the file systems that are listed in the `/etc/file_systems` files that are not mounted.

   The variable *file_systems* is the file that lists the mounted file systems. For example, on **AIX** it is called `filesystems`, and on Linux it is called `fstab`.

2. Verify that the following commands can be run successfully, without error messages:

```
df -a
df -k
```

WebSphere Global Security: setting the user name and password in client properties files

The data collector must communicate with WebSphere Administrative Services using the Remote Method Invocation (RMI) or the Simple Object Access Protocol (SOAP) protocol. If WebSphere Global Security is enabled, this communication requires a user name and password. You can set them when configuring the data collector to monitor an application server instance. For security reasons, you might prefer to encrypt the user name and password and store them in client properties files before configuring the data collector.

Use the `sas.client.props` file for an RMI connection, or the `soap.client.props` file for a SOAP connection.

Important: If you complete this operation, you must do it separately for each monitored application server profile.

Enabling user ID and password input from the sas.client.props file for RMI connector types

When you use an RMI connection to WebSphere Application Server and global security is enabled, you can use the ITCAM Data Collector for WebSphere configuration utilities to retrieve the user ID and password from a `sas.client.props` file.

To retrieve the user ID and password from the `sas.client.props` file, complete the following steps:

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

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

2. Run the following command to encrypt the password:

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

   Run it from the *AppServer_home*`/profiles/`*profile_name*`/bin` directory.

Enabling user ID and password input from the soap.client.props file for SOAP connector types

When you use a SOAP connection to WebSphere Application Server and global security is enabled, you can use the ITCAM Data Collector for WebSphere configuration utilities to retrieve the user ID and password from a `soap.client.props` file.

To retrieve the user ID and password from the `soap.client.props` file, complete these steps:

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

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

2. Run the following command to encrypt the password:

```
./PropFilePasswordEncoder.sh
  AppServer_home/profiles/profile_name/properties/soap.client.props
  com.ibm.SOAP.loginPassword
```

Run it from the *AppServer_home*/profiles/*profile_name*/bin directory.

Linux: timezone setting for historical data collection

If your site uses Linux as its WebSphere Application Server operating environment, you must synchronize historical data collection at the agent with the timezone of the Tivoli Enterprise Portal client. To do this, set a time zone variable in the Linux /etc/profile file. For example, to set the Linux time zone to the U.S. Pacific time zone, complete the following steps:

1. Complete one of the following actions:
   - For Red Hat Linux, set:

     ```
     ZONE="US/Pacific"
     export ZONE
     ```

   - For SuSE and Novell Linux, set:

     ```
     TIMEZONE="US/Pacific"
     export TIMEZONE
     ```

2. Reboot your Linux computer.

HP-UX: Mounting the agent installation DVD

If you plan to use the DVD to install the agent on HP-UX, run this command when mounting the DVD:

```
mount -F cdfs -o ro,cdcase,rr /dev/dsk/dvd_device /mnt/cdrom
```

Make sure the value for *dvd_device* corresponds to your particular DVD device.

Verify that prerequisite packages have been installed correctly.

Optionally, verify that the prerequisite packages for ITCAM Agent for WebSphere Applications are installed correctly before launching the installer.
The Environment Checking Utility (ECU) generates a report of the operating-system packages and libraries installed. From the report, you can determine if the system prerequisites have been met. For more information about generating an ECU report, see the *IBM Tivoli Composite Application Manager Agents for WebSphere Applications, J2EE, and HTTP Servers Troubleshooting Guide*.

What to do next

For more information, see Chapter 5, “Installing and configuring ITCAM Agent for WebSphere Applications on Linux and UNIX systems,” on page 103

Chapter 5. Installing and configuring ITCAM Agent for WebSphere Applications on Linux and UNIX systems

Instructions are provided for installing and configuring ITCAM Agent for WebSphere Applications on any supported UNIX or Linux environment, including:

- Linux running on Intel platforms
- Linux running on pSeries platforms
- Linux running on zSeries platforms
- AIX
- HP-UX
- Solaris

In older versions of ITCAM Agent for WebSphere Applications, you install the data collector when installing the monitoring agent. Beginning with version 7.2, you install the monitoring agent first. After you install the monitoring agent, you install ITCAM Data Collector for WebSphere in a location that you specify. A configuration tool, ITCAM Data Collector for WebSphere Configuration utility (`config.sh`), is used to configure the data collector.

With the configuration utility, you can integrate the data collector with the following components:

- ITCAM for SOA monitoring agent
- ITCAM Agent for WebSphere Applications monitoring agent
- ITCAM for Application Diagnostics Managing Server
- Tivoli Performance Viewer, available from the WebSphere administrative console
- ITCAM Diagnostics Tool that is previewed in the ITCAM for Application Diagnostics beta

If you integrate the data collector with the managing server only, you must configure the monitoring agent so that it does *not* communicate with a Tivoli Enterprise Monitoring Server, and ensure that the monitoring agent is not started automatically.

New utilities are also provided for configuring the data collector. The utilities that you use and the configuration options that you choose in each utility depend on whether you are installing or upgrading the data collector and whether the same version or an older version of the data collector is configured for the same WebSphere profile in which you plan to enable data collection.

If you are performing an installation of ITCAM Agent for WebSphere Applications, review the installation scenarios. See the "Installing ITCAM Agent for WebSphere Applications version 7.2 and configuring ITCAM Data Collector for WebSphere" section in *IBM Tivoli Composite Application Manager Agents for WebSphere Applications, J2EE, and HTTP Servers: Planning an Installation* guide.

If you are performing an upgrade of ITCAM Agent for WebSphere Applications, review the upgrade scenarios. See the "Upgrading to ITCAM Agent for WebSphere Applications version 7.2 and configuring ITCAM Data Collector for WebSphere" section in *IBM Tivoli Composite Application Manager Agents for WebSphere Applications, J2EE, and HTTP Servers: Planning an Installation* guide.

Installing the agent on Linux and UNIX systems

If ITCAM Agent for WebSphere Applications version 7.2 is already installed on the host, you can use this process to reinstall it. You are not prompted to specify the installation directory, the encryption key, and the program folder; the reinstallation uses the same settings as the existing installation.

Use the same process to upgrade the monitoring agent, if a monitoring agent is already installed on the host by any of the following products:

- ITCAM for WebSphere version 6.1.0.4 or later
- WebSphere Tivoli Enterprise Monitoring Agent version 6.2.0.4 or later included in ITCAM for Web Resources version 6.2.0.4 or later
- ITCAM Agent for WebSphere Applications version 7.1 included in ITCAM for Applications Diagnostics version 7.1

To upgrade to the data collector component of ITCAM Agent for WebSphere Applications version 7.2, you must upgrade monitoring of application server instances to use the ITCAM Data Collector for WebSphere using the migration command-line utility. For more information about migrating the data collector, see "Migrating data collectors to ITCAM Data Collector for WebSphere" on page 137.

Before starting the process, make sure the Manage Tivoli Enterprise Monitoring Services (MTMS) utility is not running. If it is running, stop it. If the utility is running, the upgrade or installation might fail.

To install ITCAM Agent for WebSphere Applications on a Linux or UNIX system, complete the following steps:

Step 1: Start the installer

After loading the ITCAM Agent for WebSphere Applications installation media for Linux or UNIX systems and changing to its root directory, locate the installation script, `install.sh`, and start it:

```
./install.sh
```

Step 2: Supply the name of the installation directory

The install script prompts you for the name of the installation directory where ITCAM Agent for WebSphere Applications will be installed.

```
Enter the name of the IBM Tivoli Monitoring directory
[ default = /opt/IBM/ITM ]:
```

The directory (*ITM_home*) can be shared with other IBM Tivoli Monitoring products. When you install ITCAM Agent for WebSphere Applications 7.2, if the monitoring agent component of any of the following products was installed on this computer, use the same installation directory:

- ITCAM for WebSphere version 6.1.0.4 or later
- WebSphere Tivoli Enterprise Monitoring Agent version 6.2.0.4 or later included in ITCAM for Web Resources version 6.2.0.4 or later
- ITCAM Agent for WebSphere Applications version 7.1 included in ITCAM for Applications Diagnostics version 7.1

In all cases, the monitoring agent is upgraded automatically.

Specify the absolute or relative directory name, or, to accept the default, press Enter. The installer searches for the directory name that you specified and, if it does not exist, prompts you with the following message:

```
"/opt/IBM/ITM" does not exist
Try to create it [ y or n; "y" is default ]?
```

Press Enter.

If the monitoring agent is running, the installer warns that it will restart during the installation. To continue, press Enter.

Step 3: Select installation options

The installer displays background information about installation requirements, searches the DVD or image for the components available for installation, and prompts you about the available installation options:

```
Select one of the following:

1) Install products to the local host.
2) Install products to depot for remote deployment (requires TEMS).
3) Install TEMS support for remote seeding.
4) Exit install.

Please enter a valid number:  1
```

Important: Option 2 works only if the version of Tivoli Enterprise Monitoring Server is 6.2.2.2 or higher.

Enter 1. The installer starts initializing.

Important:

- Option 2 applies to remote agent deployment. If you want to add installation files for this agent to your site deployment depot, run `install.sh` on the hub Tivoli Enterprise Monitoring Server (TEMS) host, and start this option.
- Option 3 applies to the installation of Tivoli Enterprise Monitoring Server support files. For more information about these files, see "Enabling application support on Linux and UNIX systems" on page 145.

Step 4: Accept the product license agreement

After the initialization, the product license agreement is displayed:

```
International Program License Agreement

Part 1 - General Terms

BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, OR USING
THE PROGRAM YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF
YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON
OR A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND
WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON,
COMPANY, OR LEGAL ENTITY TO THESE TERMS. IF YOU DO NOT
AGREE TO THESE TERMS,

- DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, OR USE THE
PROGRAM; AND

Press Enter to continue viewing the license agreement, or
enter "1" to accept the agreement, "2" to decline it, "3"
to print it, "4" to read non-IBM terms, or "99" to go back
to the previous screen.
```

If you accept the license agreement, enter 1.

Step 5: Enter the IBM Tivoli Monitoring encryption key

In an upgrade installation or a reinstallation, or when some IBM Tivoli Monitoring components are already installed, the data encryption key is already set, and this step is skipped. On a new installation, you are prompted for the 32-character encryption key that is used to secure password transmission and other sensitive data across your IBM Tivoli Monitoring environment:

```
Enter a 32-character encryption key, or just press Enter to use the default
        Default = IBMTivoliMonitoringEncryptionKey
....+....1....+....2....+....3..
```

For more information about the encryption key, see *IBM Tivoli Monitoring: Installation and Setup Guide*.

Supply the 32-character key, or accept the default. The key information is displayed:

```
GSkit encryption key is set.
Key File directory: /opt/IBM/ITM/keyfiles
```

Step 6: Install prerequisites and specify the component to install

The installer displays the installed components of IBM Tivoli Monitoring., for example:

```
The following products are currently installed in "/opt/IBM/TEMA:"

 IBM GSKit Security Interface V07.40.27.00 @ Linux Intel R2.4 (32 bit)/Intel
  R2.6 (32 bit)/x86_64 R2.6 (32 bit)
```

If any prerequisites for the agent are not installed, the installer prompts you to install them. If you have to install any prerequisites, press Enter. If you are prompted to install prerequisites but choose not to install them, the installer does not continue.

The installer displays the components that are available for the version of the operating system (Linux, AIX, HP-UX, or Solaris) that you are installing on, for example:

```
Product packages are available for this operating system and component support
categories:

 1) IBM Tivoli Monitoring components for this operating system
 2) Tivoli Enterprise Portal Browser Client support
 3) Tivoli Enterprise Portal Desktop Client support
 4) Tivoli Enterprise Portal Server support
 5) Tivoli Enterprise Monitoring Server support
 6) Other operating systems

Type the number or type "q" to quit selection
[ number "1" or "IBM Tivoli Monitoring components for this operating system" is
default]:
```

Enter 1. The installer prompts you with the following message:

```
The following products are available for installation:

 1) IBM Tivoli Composite Application Manager Agent for WebSphere
 Applications  V07.20.00.00
 2) all of the above
```

```
Type the numbers for the products you want to install, type "b" to
 change operating system, or type "q" to quit selection.
If you enter more than one number, separate the numbers by a comma
 or a space.

Type your selections here:
```

Enter 1. The installer displays a confirmation prompt:

```
The following products will be installed:

  IBM Tivoli Composite Application Manager Agent for WebSphere Applications
  V07.20.00.00

Are your selections correct [ 1=Yes, 2=No ; default is "1" ] ?
```

Enter 1 (or press Enter to accept the default).

Step 7: Install the product software

The installer displays several status messages as the product files are installed. When that installation completes, you are prompted to specify whether you want to install additional packages:

```
Do you want to install additional products or product support packages [ 1=Yes,
2=No; default is "2" ]?
```

When you have installed additional products or product support packages, enter 2 to complete the installation. The installer confirms that the installation is complete:

```
... postprocessing please wait.
... finished postprocessing
Installation step complete.
```

Step 8: Installing the data collector

A message is displayed to indicate that the installer has identified additional procedures that need to be performed to complete the installation of the ITCAM Agent for WebSphere Applications. The additional procedures involve the installation of ITCAM Data Collector for WebSphere.

Important: ITCAM Data Collector for WebSphere in ITCAM Agent for WebSphere Applications version 7.2 is a component that is shared with the following products:

- ITCAM for SOA version 7.2
- ITCAM for WebSphere Application Server version 7.2 support for WebSphere Application Server version 8.5
- ITCAM Diagnostics Tool that is previewed in the ITCAM for Application Diagnostics beta

If ITCAM for SOA version 7.2 is already installed under the *ITM_home* directory or if you are performing a reinstallation, the same version, release, and maintenance level of ITCAM Data Collector for WebSphere might be installed under *ITM_home*. If the installer detects that the same version of ITCAM Data Collector for WebSphere is already installed under *ITM_home*, the installation of the data collector is skipped and the data collector configuration utility is displayed. Skip to step “Step 9: Configuring the data collector” on page 108.

Remember: The same version, release, and maintenance level of ITCAM Data Collector for WebSphere might be installed and configured for the same WebSphere profile, but the data collector installation might not be under the *ITM_home* directory:

- If the data collector is installed by ITCAM for WebSphere Application Server version 7.2 support for WebSphere Application Server version 8.5 or the ITCAM Diagnostics Tool that is previewed in the ITCAM for Application Diagnostics beta, the data collector installation is outside of the *ITM_home* directory. The installer does not detect that the data collector already exists. When prompted, you must specify the location of the data collector installation.
- If the data collector is installed by ITCAM for SOA version 7.2 outside of *ITM_home*, the installer does not detect that the data collector exists. When prompted, you must specify the location of the data collector installation.

When the same version, release, and maintenance level of the data collector is not already installed under the *ITM_home* directory, the installer opens a command-line window.

The installer prompts you to specify whether you want to:

- Install the data collector in the `DC_home` directory (default install)
- Reuse an existing data collector home directory (custom install)
- Create a new data collector home directory (custom install)

```
Choose the type of install to perform.
      1. default install
      2. custom install
[default is: 1]:
```

Enter `1` to install the data collector in the *DC_home* directory.

Otherwise, enter `2` and specify the location of the data collector home directory. If the installer finds that the data collector home directory does not exist, it asks you whether you want to create the directory.

```
Directory /opt/IBM/ITM/dchome/7.2.0.0.1 does not exist.  Is it ok to create?
[1 - YES, 2 - NO]
```

Enter `1` to create the directory. If you enter `2`, you can enter a different data collector home directory or exit the command prompt.

If the data collector installation does not already exist, the installer starts the installation of the data collector.

Step 9: Configuring the data collector

Once you have installed the data collector, the ITCAM Data Collector for WebSphere Configuration utility is launched for configuring the data collector.

Before you configure the data collector, ensure that you have sufficient permissions to run the data collector configuration utilities (see “Permissions required for configuration tasks” on page 121).

For information about using the utility, see “Configuring ITCAM Data Collector for WebSphere” on page 122.

If you are installing ITCAM Agent for WebSphere Applications and you want to postpone the configuration of ITCAM Data Collector for WebSphere until later, exit the utility. At a later time, use the ITCAM Data Collector for WebSphere Configuration utility to configure the data collector.

You must migrate the data collector components of following products to the ITCAM Data Collector for WebSphere before you enable data collection for ITCAM Agent for WebSphere Applications version 7.2 within the same profile:

- ITCAM for SOA version 7.1.1
- ITCAM for WebSphere Application Server version 7.2

If an older version of the ITCAM Agent for WebSphere Applications is configured for the same profile, exit the utility and migrate the data collector.

For more information about migrating the data collector, see "Migrating data collectors to ITCAM Data Collector for WebSphere" on page 137.

Step 10: Verify completion of installation procedure

In a pristine installation or an upgrade, when you complete the installation of the monitoring agent, exit the ITCAM Data Collector for WebSphere Configuration utility, and close the command-line window, a confirmation message is presented to indicate that the installation and configuration tasks have completed successfully.

```
Exit point procedures for following agents were executed:
  *) IBM Tivoli Composite Application Manager Agent for
WebSphere Applications [Success]
```

Important: If you cancel the configuration of the ITCAM Data Collector for WebSphere after the data collector has been installed but before the data collector is configured, the message displays the value [*Error*]. This message indicates that the data collector has been installed but has yet to be configured.

Additional procedure for Security Enhanced Linux (SELinux)

After installing ITCAM Data Collector for WebSphere on SELinux, for example, Red Hat Enterprise Linux Version 5 or SUSE Linux Enterprise Server Version 11, you must complete an additional procedure to identify the data collector shared libraries.

To identify the data collector shared libraries on SELinux, run the following command as root, substituting the installation directory for *DC_home* and the Tivoli Monitoring architecture identifier for *DC_architecture_code*:

```
chcon -R -t texrel_shlib_t

DC_home/toolkit/lib/DC_architecture_code
```

For information about resolving directory path variables, see "Operating system-dependent variables and paths" on page xvii.

The architecture code identifiers for Linux systems are:

- `li6263`: Linux Intel R2.6 (32 bit)
- `lx8266`: Linux x86_64 R2.6 (64 bit)
- `lpp263`: Linux ppc R2.6 (32 bit)
- `lpp266`: Linux ppc R2.6 (64 bit)
- `ls3263`: Linux S390 R2.6 (32 bit)
- `ls3266`: Linux S390 R2.6 (64 bit)

For 64-bit systems, you must run the command twice in order to identify shared libraries for both 32-bit and 64-bit versions of the data collector.

Deep-dive diagnostics-only installation: disabling monitoring agent autostart

If you are performing a deep-dive diagnostics-only installation, where IBM Tivoli Monitoring is *not* used, disable monitoring agent autostart. If Tivoli Monitoring is used, do not disable it.

Remember: The managing server deep-dive functionality is not available in ITCAM for Applications version 7.2; unless you have ITCAM for Application Diagnostics installed in your environment, ignore all references to this functionality in this document.

To disable monitoring agent autostart, complete the following procedure:

1. Check the contents of the file *ITM_home*/registry/AutoStart, and get the number from that file. Use this number as *NUM* in the following step.
2. Edit the autostart file for the operating system:
   - On AIX: /etc/rc.itm*NUM*
   - On HP-UX: /sbin/init.d/ITMAgents*NUM*
   - On Linux: /etc/init.d/ITMAgents*NUM*
   - On Solaris: /etc/init.d/ITMAgents*NUM*

   In this file, find and comment out (using the # symbol) the lines with the itmcmd agent start yn and itmcmd agent stop yn commands.

   Example:

```
start_all()
{
/bin/su - root -c " /opt/IBM/YN1024/bin/itmcmd agent start yn >/dev/null 2>&1"
}

stop_all()
{
/bin/su - root -c " /opt/IBM/YN1024/bin/itmcmd agent stop yn >/dev/null 2>&1"
}
```

   In this example, you must comment out both lines that start with /bin/su.

What to do next

On AIX, if the version of IBM Development Kit is earlier than SR10, you must issue one forced stop command for the agent after installing it:

ITM_home/bin/itmcmd agent -f stop yn

If you use IBM Tivoli Monitoring infrastructure, you must enable application support files on hub and remote Tivoli Enterprise Monitoring Servers, and all Tivoli Enterprise Portal Servers and Tivoli Enterprise Portal desktop clients. For a detailed description of the procedure, see “Enabling application support on Linux and UNIX systems” on page 145.

Important: If you are planning to use ITCAM Agent for WebSphere Applications to monitor WebSphere Extrene Scale (WXS) in a WebSphere Application Server environment with enabled security, you must complete additional configuration steps. See Appendix B, “Configuring the agent for to monitor WebSphere Extreme Scale in security-enabled WebSphere environments,” on page 285.

Configuring the monitoring agent on Linux and UNIX systems

This section provides instructions for configuring the ITCAM Agent for WebSphere Applications monitoring agent.

On UNIX and Linux platforms, you can configure the monitoring agent settings and communication with the monitoring server using the command line or the GUI.

In ITCAM Agent for WebSphere Applications version 7.2, a GUI is no longer provided for configuring the data collector. Instead, you can use the new ITCAM Data Collector for WebSphere Configuration utility in console mode or silent mode.

Configuring monitoring agent settings and communication with the monitoring server using the command line

If the IBM Tivoli Monitoring infrastructure is used, you *must* configure monitoring agent settings before you configure the data collector to monitor any application server instances. You must also configure monitoring agent communication to the monitoring server. Do not complete this configuration in a deep-dive diagnostics-only installation, where IBM Tivoli Monitoring is not used.

You can change the port that is used for communication between the data collector and the monitoring agent. This communication is on the local host. The default port is 63335. You can also set an alternate node name that determines how the agent is displayed in the Tivoli Enterprise Portal navigation tree. Although you can change these values at a later time, it is most convenient to set them when you configure the communication.

To configure monitoring agent settings and communication with the monitoring server on UNIX or Linux systems using the command line, complete the following procedure:

1. Change to the *ITM_home*/bin directory (by default, /opt/IBM/ITM/bin) and run the following command:

   ```
   ./itmcmd config -A yn
   ```

   The itmcmd utility prompts you whether you want to change agent configuration:

   ```
   Agent configuration started...
   Edit "ITCAM Agent for WebSphere Applications" settings? [ 1=Yes, 2=No ]
    (default is: 1):
   ```

   Enter 1, or press Enter to accept the default.

2. The utility prompts you to select the configuration type:

   ```
   Select Configuration Type :
   Choose the configuration type:

   Configuration type description:
   1.Use this option to configure the Tivoli Enterprise Monitoring Agent (TEMA)
    port number or Agent ID. If you modify the Tivoli Monitoring Agent
   port, all Application Servers with Data
   Collectors must be restarted to complete the
   reconfiguration.
   Choose the configuration type: [ 1=Configure Tivoli Enterprise
   Monitoring Agent (TEMA), 2=Exit ] (default is: 1):
   ```

   To start configuring the data collector communication to the monitoring agent, type 1 and press Enter.

3. The configuration utility prompts you for an alternative node ID for identifying the agent. This identifier determines how the agent is displayed in the Tivoli Enterprise Portal navigation tree. The default is `Primary` and is used with the host name of the computer where the agent is installed.

   Important: If you install more than one copy of the monitoring agent on a single host, you must set the Alternative Node ID parameter to different values for each of the copies. Otherwise, the multiple copies of the monitoring agent do not work correctly with Tivoli Monitoring.

   ```
   Alternative Node ID for identifying the Agent.
   This is a unique id that will determine how the agent will appear in
   the Tivoli Enterprise Portal navigation tree. The max Node ID length
   is 24 characters.
   Node ID (default is: Primary):
   ```

   Restriction: Valid characters for the node ID include A - Z, a - z, 0 - 9, underline (_), dash (-), and period (.); do not use other characters.
   If you want to use an alternative node ID, enter it and press Enter. Otherwise, press Enter.
4. The configuration utility prompts you for the TCP socket port to listen for communication from the data collectors:

   ```
   Monitoring Agent listening Port.
   The Monitoring Agent will use this TCP socket port to listen for
   connection requests coming from the Data Collector(s).
   Port number (default is: 63335):
   ```

   Enter the port number or press Enter to accept the default.
5. The configuration utility prompts you to save your settings to a response file:

   ```
   Save Response File:

   The wizard can save your settigns to a response file.  A response file can
   be used to perform a silent configuraiton.
   Save Configuration setting in a Response File
   [1=true, 2=false] (default is 2):
   ```
6. To save the settings to a response file, enter 1 and specify the full path name of the response file. Otherwise, enter 2.
7. The configuration utility prompts you to specify whether the monitoring agent will connect with a Tivoli Enterprise Monitoring Server:

   ```
   Will this agent connect to a TEMS? [1=YES, 2=NO) (Default is 1):
   ```

   Enter 1 to connect the monitoring agent to the monitoring server. Otherwise, enter 2 and skip to step 14 on page 113.
8. The configuration utility prompts you for the Tivoli Enterprise Monitoring Server host name:

   ```
   TEMS Host Name (Default is: LLVMRH5):
   ```

   Type the correct host name and press Enter.
9. The configuration utility prompts you to choose a network protocol that the monitoring agent is to use to communicate with the hub monitoring server:

   ```
   Network Protocol [ip, sna, ip.pipe or ip.spipe] (Default is: ip.pipe):
   ```

   Select the protocol that was selected when the Tivoli Enterprise Monitoring Server was installed, and press Enter.
10. The configuration utility prompts you to select a second (backup) protocol).

```
     Now choose the next protocol number from one of these:
     - ip
     - sna
     - ip.spipe
     - 0 for none
Network Protocol 2 (Default is: 0):
```

If a backup protocol was selected when the Tivoli Enterprise Monitoring Server was installed, enter that protocol and press Enter. Otherwise, press Enter.

11. The configuration utility prompts you for the settings for each selected protocol. For example, if you selected IP.PIPE, it prompts you for the port number:

    ```
    IP.PIPE Port Number (Default is: 1918):
    ```

    Type the port number and press Enter, or, to accept the default, press Enter.

    Also, for some protocols that include IP.PIPE, the configuration utility prompts you for the KDC_PARTITION name:

    ```
    Enter name of KDC_PARTITION (Default is: null):
    ```

    You can specify the partition name if it is available, or press Enter without specifying it. You can configure the partition name at a later time.

12. The configuration utility prompts you whether you want to configure a connection for a secondary Tivoli Enterprise Monitoring Server:

    ```
    Configure connection for a secondary TEMS? [1=YES, 2=NO] (Default is:2):
    ```

    If your environment includes a Tivoli Enterprise Monitoring Server for a failover connection, select 1. In this case, you must enter its host name and settings for communication with it. For more information, see steps 8 on page 112 to 11. Otherwise, press Enter.

13. The configuration utility displays the following message:

    ```
    Enter Optional Primary Network Name or 0 for "none" (Default is: 0):
    ```

    Press Enter.

14. The configuration utility displays the message:

    ```
    Agent configuration completed...
    ```

Configuring the Monitoring Agent using a GUI

To configure the monitoring agent using the graphical user interface, use the Manage Tivoli Enterprise Monitoring Services utility.

Entering the agent configuration window

To complete all the configuration procedures described in this section, you must start from the **Agent Configuration** window.

Change to the *ITM_home*/bin directory (by default, /opt/IBM/ITM/bin) and run the following command:

```
./itmcmd manage
```

The Manage Tivoli Enterprise Monitoring Services utility opens.

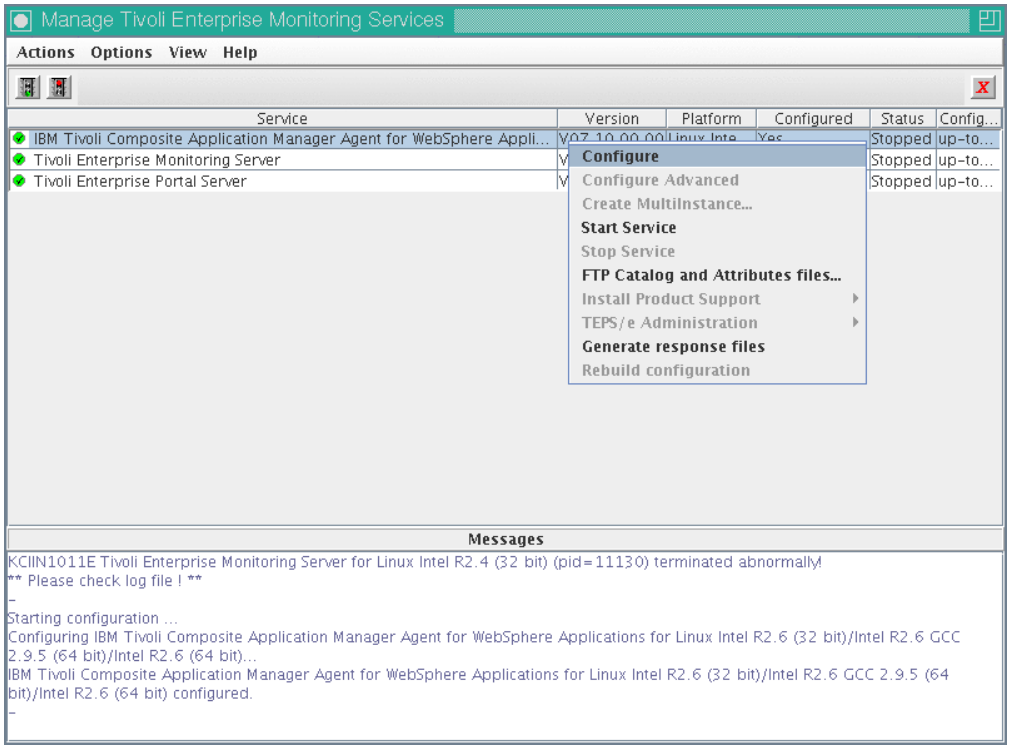

Figure 23. Manage Tivoli Enterprise Monitoring Services window on UNIX and Linux

Right-click **IBM Tivoli Composite Application Manager Agent for WebSphere Applications** and then click **Configure**. The agent configuration window opens.

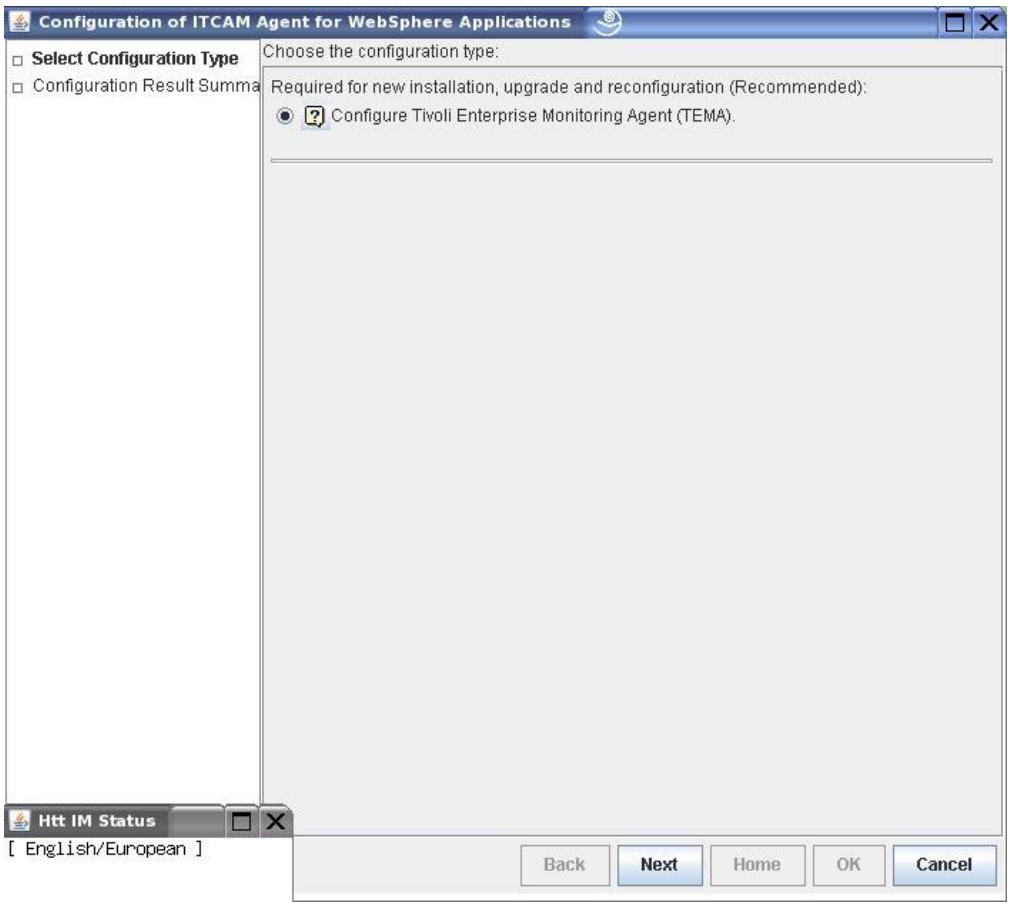

Figure 24. Agent Configuration window

Important: On Linux and UNIX systems, the window for configuring monitoring agent configuration to the Tivoli Enterprise Monitoring Server is always displayed at the end of the configuration process. This is different from a Windows systems, where this window is always displayed at the beginning of the configuration process.

Configuring monitoring agent settings and communication with the monitoring server using a GUI

If the IBM Tivoli Monitoring infrastructure is used, you *must* configure monitoring agent settings before configuring the data collector to monitor any application server instances. You may also want to configure monitoring agent communication to the monitoring server. Do not complete this configuration in a deep-dive diagnostics-only installation, where IBM Tivoli Monitoring is not used.

You can change the port that is used for communication between the data collector and the monitoring agent (this communication is on the local host). The default port is 63335. You can also set an alternative node name that determines how the agent is displayed in the Tivoli Enterprise Portal navigation tree. Although you can change these settings at a later time, it is usually convenient to set them when you configure the communication initially.

To configure monitoring agent settings and communication with the monitoring server, complete the following procedure:

1. Open the Agent Configuration window. For more information, see “Entering the agent configuration window” on page 113.

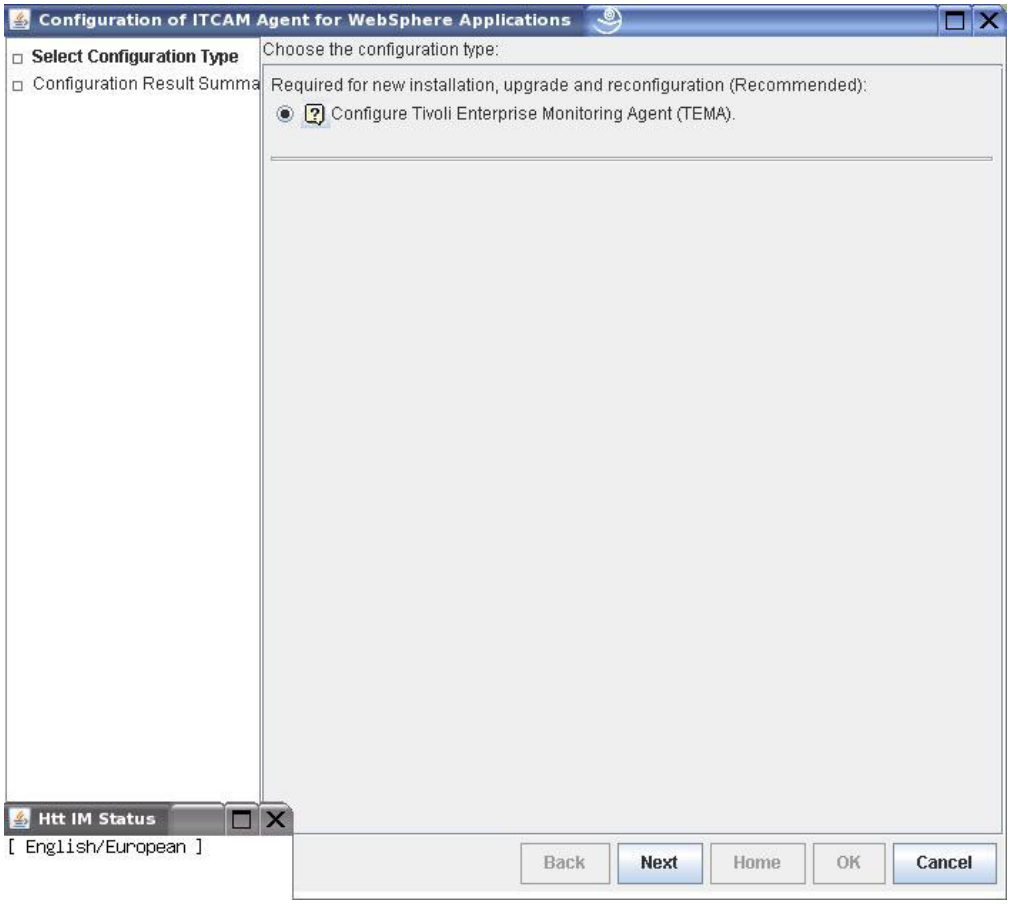

Figure 25. Configuring Communication to the monitoring agent, window 1

2. Select **Configure Tivoli Enterprise Monitoring Agent (TEMA)** and click **Next**.
3. In the Agent Configuration page, you can set an alternative Node ID for identifying the agent. The Node ID is the identifier that determines how the agent is displayed in the Tivoli Enterprise Portal navigation tree. The default is `Primary`, and is used with the host name of the computer where the agent is installed. In the **Port** field, you can specify a TCP socket port that the monitoring agent is to use to listen for connection requests from the data collectors. Normally, do not change this value. The port is used only for local communication on the host

   Important: If you install more than one copy of the monitoring agent on a single host, you must set the Alternative Node ID parameter to different values for each of the copies. Otherwise, the multiple copies of the monitoring agent do not work correctly with Tivoli Monitoring.

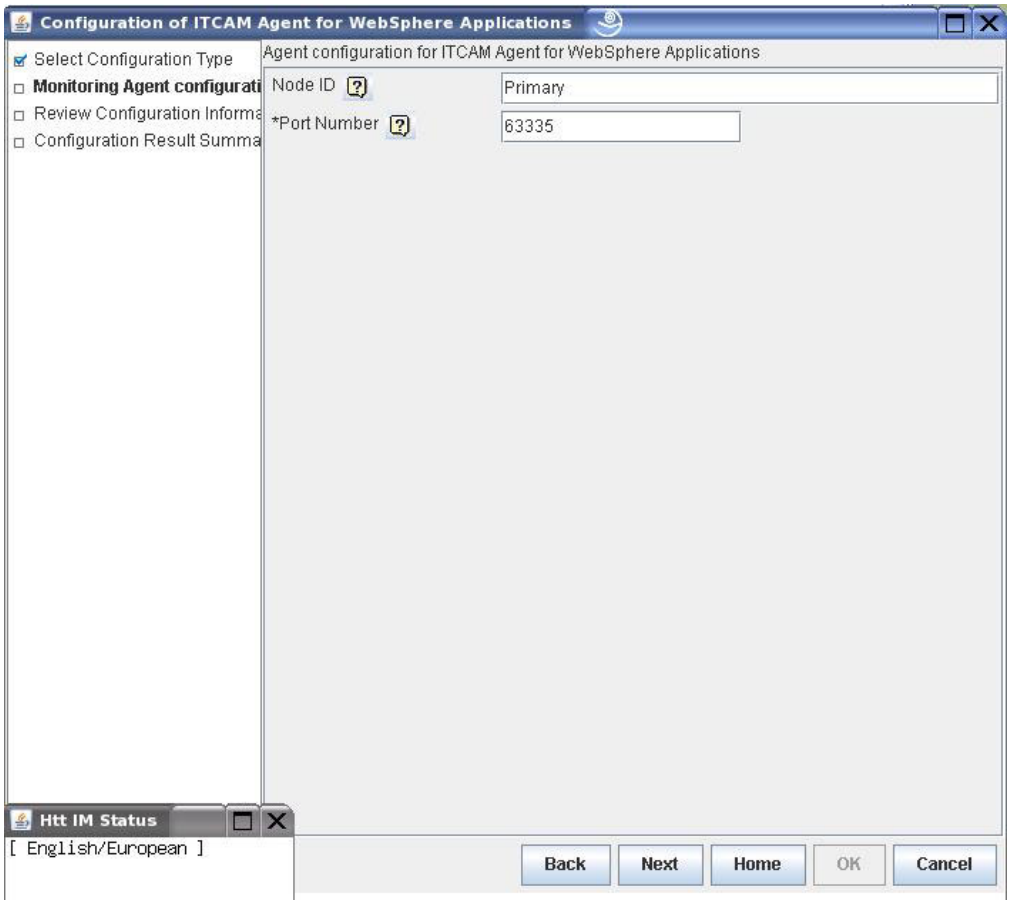

Figure 26. Configuring Communication to the Monitoring Agent, window 2

Restriction: Valid characters for the node ID include A - Z, a - z, 0 - 9, underline (_), dash (-), and period (.). Do not use other characters.
If necessary, enter the Node ID or the port number, or both. Click **Next**.

4. You can create a response file to save your configuration settings. You can use the response file to complete a silent configuration with the same parameters.

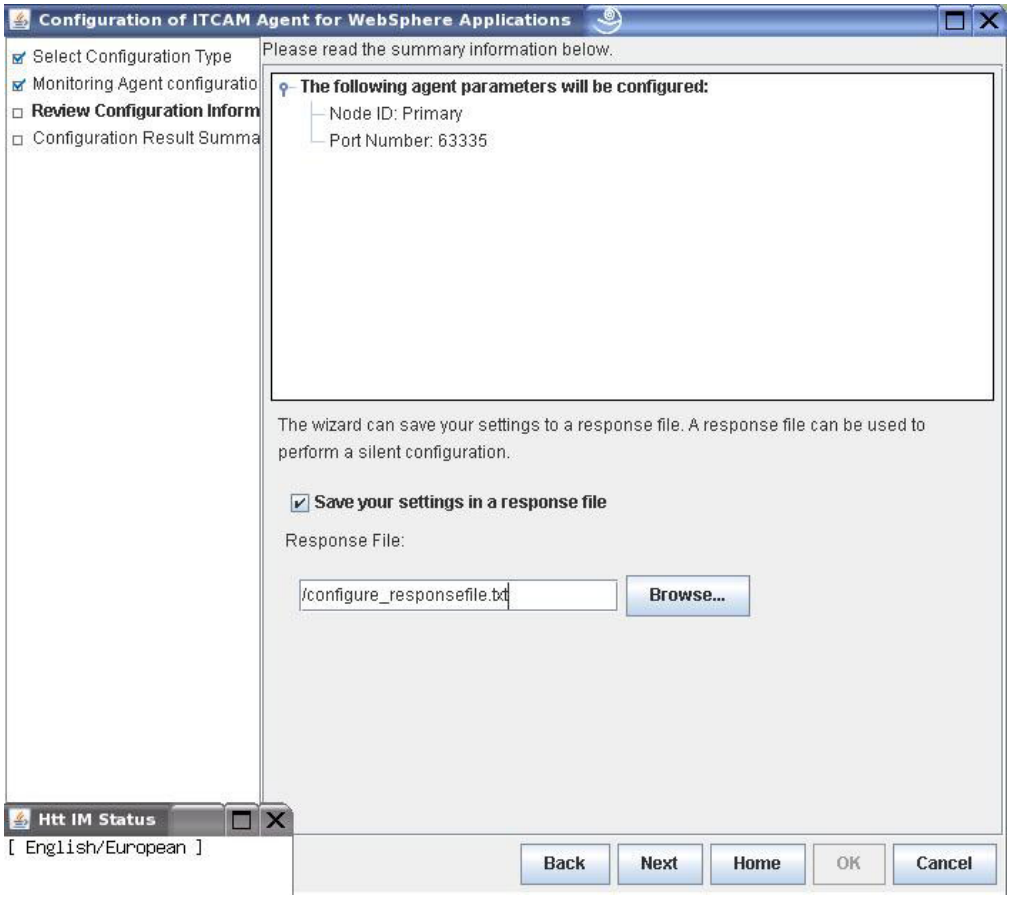

Figure 27. Configuring Communication to the Monitoring Agent, window 3

If you want to create a response file, select **Save your settings in a response file**. To select the file location, click **Browse**. Click **Next**. Otherwise, leave the check box cleared and click **Next**.

5. The utility indicates that the monitoring agent is successfully configured.

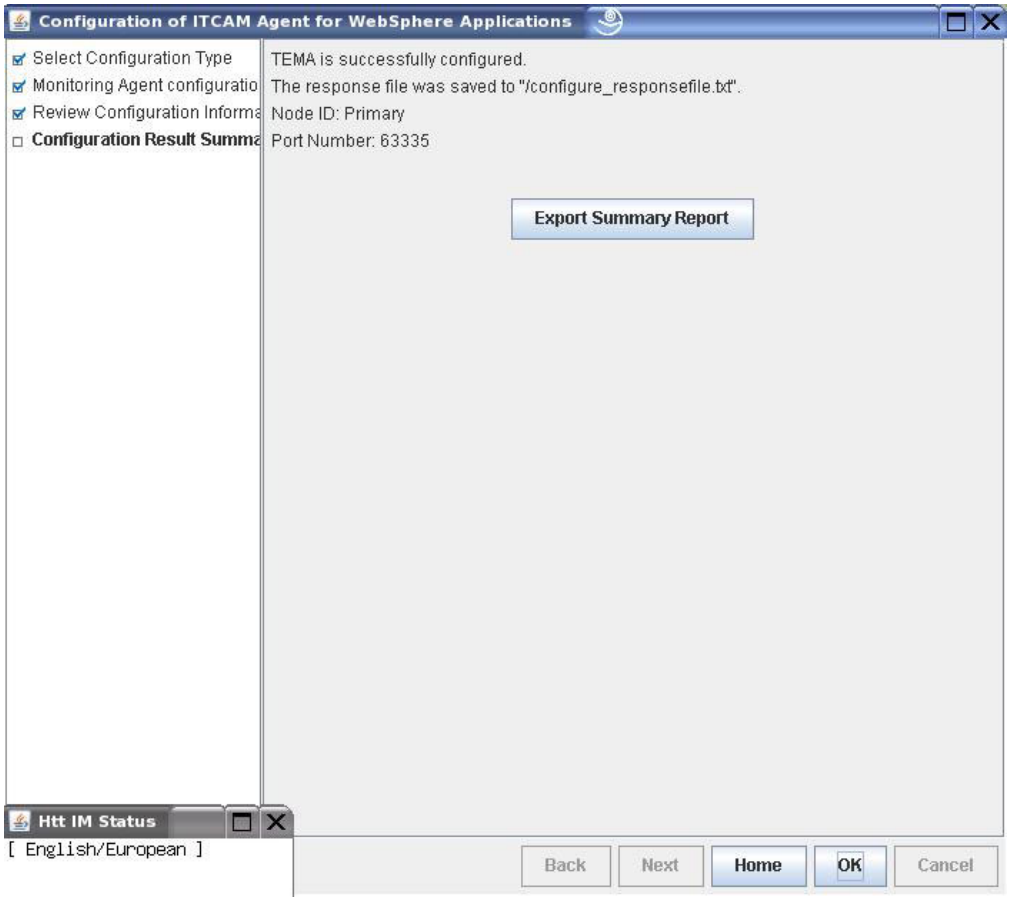

Figure 28. Configuring Communication to the Monitoring Agent, window 4

Click **OK**.

6. The **TEMS Connection** window is displayed.

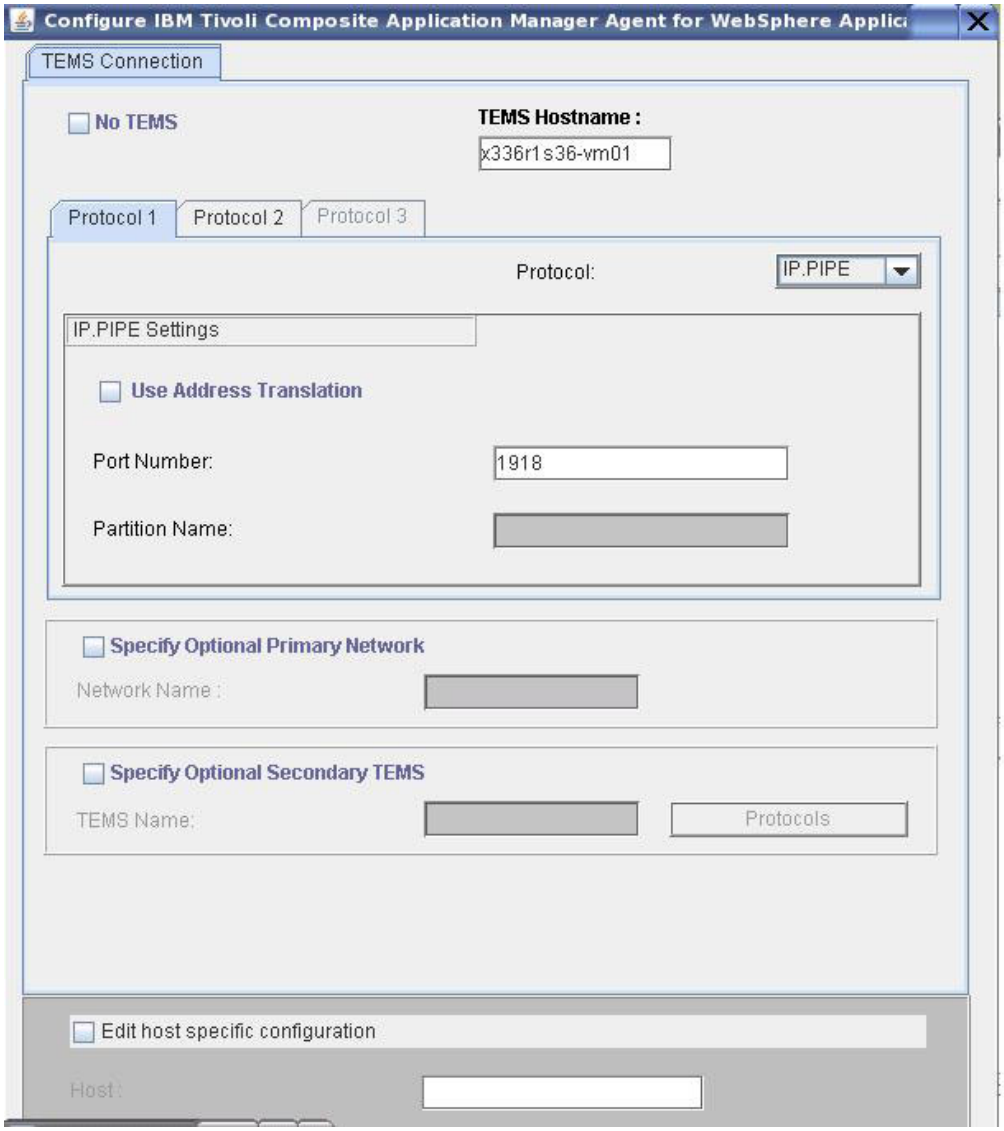

Figure 29. Configuring Communication to the Monitoring Agent, window 5

7. Enter the Tivoli Enterprise Monitoring Server (TEMS) host name, and select the protocol for connecting with the Tivoli Enterprise Monitoring Server. If the connection must pass-through a firewall with address translation, select **IP.PIPE** and select **Use Address Translation**.

   Specify protocol parameters and, if necessary the secondary protocols and secondary Tivoli Enterprise Monitoring Server host. For more information, see *IBM Tivoli Monitoring: Installation and Setup Guide* for details.

   Important: If IBM Tivoli Monitoring is not used (in a deep-dive diagnostics-only installation), the **No TEMS** check box is selected this window.
8. Click **Save**.

Before configuring the data collector on Linux and UNIX systems

Before configuring the data collector using the configuration utilities iteratively or in silent mode, ensure that you have the necessary permissions to perform the configuration tasks.

Permissions required for configuration tasks

If you are configuring the data collector to monitor instances of the application server, the user must also have privileges (read, write, and execute) for the application server directory.

To run the configuration scripts, the user must have permission to execute scripts in the *dc_home*/bin directory.

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

If WebSphere global security is enabled, the configuration utilities prompt you for a WebSphere administrative user ID with login privileges to the wsadmin tool. Specify a user ID that is the primary administrative user for the WebSphere Application Server.

Configuring the data collector on Linux and UNIX

There are a number of command-line configuration utilities to configure, reconfigure, unconfigure, and migrate ITCAM Data Collector for WebSphere.

The following table provides a description of the configuration tasks supported by the utilities.

Table 11. Configuration tasks

Configuration task	Where to find the procedure
Configure the data collector to monitor application server instances within a WebSphere Application Server profile. This configuration utility is started automatically when you install the monitoring agent.	"Configuring ITCAM Data Collector for WebSphere" on page 122
Modify the configuration of the data collector for application server instances that were already configured by the ITCAM Data Collector for WebSphere Configuration utility.	"Reconfiguring ITCAM Data Collector for WebSphere" on page 131
Unconfigure the data collector.	"Unconfiguring ITCAM Data Collector for WebSphere" on page 129
Migrate an older version of the data collector to ITCAM Data Collector for WebSphere or update the maintenance level of ITCAM Data Collector for WebSphere.	"Migrating data collectors to ITCAM Data Collector for WebSphere" on page 137
Migrate the data collector provided by ITCAM for SOA version 7.1.1 to ITCAM Data Collector for WebSphere.	"Migrating ITCAM for SOA version 7.1.1 data collector to ITCAM Data Collector for WebSphere" on page 140

Important: To change to a later maintenance level of ITCAM Agent for WebSphere Applications, use the migration utility (see "Migrating data collectors to ITCAM Data Collector for WebSphere" on page 137).

Guidelines on which configuration utility to run

Use the following guidelines to determine whether to run the configuration or reconfiguration utility to configure application servers:

- If the application servers you plan to configure are not yet configured for data collection, use the configuration utility.

  If you run the configuration utility on any application servers that are already configured for data collection, your data collector configuration settings are overwritten.
- If the application servers that you plan to configure are already configured for data collection, use the reconfiguration utility to retain your existing data collector configuration settings.
- If some of the application servers you plan to configure are already configured and others are not yet configured, complete either of the following steps:
  - Use the configuration utility to configure the application servers. The data collection settings of the applications servers are overwritten.
  - Alternatively, run the configuration utility for the set of servers that have not yet been configured and run the reconfiguration utility for the servers that are already configured.

To apply different configuration settings to sets of application servers, run either utility for each set of servers separately.

Configuring ITCAM Data Collector for WebSphere

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

The ITCAM Data Collector for WebSphere Configuration utility is a menu driven command-line utility for configuring ITCAM Data Collector for WebSphere. If you are installing the data collector, the installer automatically starts the configuration utility.

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

Remember: If you have already configured the data collector and you want to reconfigure it, start the ITCAM Data Collector for WebSphere Reconfiguration utility. Otherwise, the changes you made are lost.

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

1. If you are installing the monitoring agent where the ITCAM Data Collector for WebSphere Configuration utility is started automatically by the installer, proceed to step 4 on page 123. Otherwise, from the command line, navigate to the *DC_home*/bin directory.
2. Set the location of the Java home directory before you run the utility, for example:

```
export JAVA_HOME=/opt/IBM/AppServer80/java
```

3. Run the following command to start the ITCAM Data Collector for WebSphere Configuration utility.

   DC_home/bin/config.sh

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

```
List of TCP/IP interfaces discovered:
  1. 9.1100.98.108/www.example.com
Enter a number [default is: 1]:
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Remember:

- For a stand-alone environment, application server instances must be running during the configuration.
- For a Network Deployment, WebSphere Virtual Enterprise, or WebSphere Compute Grid environment, the Node Agent and Deployment Manager must be running.
- Ensure that the application server instances that you select are the actual servers that host the applications or services that you want to monitor.

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

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

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

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

    When configuring data collection for ITCAM Agent for WebSphere Applications, you can integrate the data collector with the ITCAM Agent for WebSphere Applications monitoring agent, or with the ITCAM for Application Diagnostics Managing Server, or with both.

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

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

    Important: When you configure data collection for ITCAM Agent for WebSphere Applications for applications servers in a profile where data collection is configured for application servers for ITCAM for SOA version 7.2, you must reconfigure and restart the Tivoli Enterprise Portal Server to capture ITCAM Agent for WebSphere Applications data in the topology views of ITCAM for SOA.

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

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

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

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

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

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

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

15. Enter the port number of the monitoring agent.

    If you are configuring the Data Collector shipped with ITCAM Agent for WebSphere Applications version 7.2 ifix 1 or later, the utility prompts you for the server alias. The alias is the name of the node in Tivoli Enterprise Portal that contains the monitoring information for this application server instance. The default is the node name combined with the server name.

    ```
    Enter the server alias for server server1 in node node1  [default is: node1server1]:
    ```

    Accept the default or enter another alias.

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

    You are prompted to specify whether you want to integrate the data collector with a managing server.

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

    Remember:

    - To integrate the data collector with ITCAM for Application Diagnostics Managing Server for deep-dive analysis, you must have ITCAM for Application Diagnostics version 7.1.0.3 or later installed.
    - If you decide not to configure the managing server at this time, you can still configure the data collector to communicate with the managing server later.

17. Enter 1 to integrate with the managing server. Otherwise, enter 2 and skip to step 20 on page 126.

    You are prompted to specify the host name of the managing server:

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

18. Enter the fully qualified host name of the managing server.

You are prompted to specify the port number of the managing server:

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

The port number is codebase port on which the managing server is listening.

Tip: The port number is specified in the key `PORT_KERNEL_CODEBASE01` in the `ITCAM61_MS_CONTEXT.properties` file located under the managing server home directory. See *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

The configuration tool attempts to connect to the managing server and retrieve the value for the managing server home directory. If successful, the tool displays a message similar to the following message:

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

19. If the connection to the managing server is *not* successful, you are prompted to enter the value of the managing server home directory:

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

    If prompted, enter the value of the managing server home directory.

20. The utility prompts you to specify whether you want to configure advanced settings for the managing server.

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

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

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

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

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

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

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

    Enter the RMI Controller port numbers.

23. You are prompted to enter the Remote File Sharing (RFS) port number of the managing server:

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

    The RFS server in the managing server kernel listens to the RFS port to accept incoming requests. Enter the RFS port number.

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

    Remember: To integrate the data collector with ITCAM for Transactions, you must install ITCAM for Transactions version 7.3 or later within an IBM Tivoli Monitoring environment.
    You are prompted to specify whether you want to integrate with ITCAM for Transactions:

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

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

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

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

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

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

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

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

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

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

    Application Performance Diagnostics Lite is a tool for diagnostic investigation of applications running on WebSphere Application Server and WebSphere Portal Server. Using this tool, you can analyze data in real time or you can save diagnostic information to a file for later analysis. For more information about installing and using Application Performance Diagnostics Lite, see the Application Performance Diagnostics Lite product documentation.

In the version of the Data Collector shipped with ITCAL Agent for Websphere versions prior to 7.2 ifix 1, the name *ITCAM diagnostics tool* is used for Application Performance Diagnostics Lite.

Enter 1 to integrate ITCAM Data Collector for WebSphere with Application Performance Diagnostics Lite. Otherwise, enter 2.

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

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

Enter 1 to select a garbage collection log path. Otherwise, enter 2 and skip to step 34.

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

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

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

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

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

```
 1) List of servers selected

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

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


       wsadmin location          :
        /opt/IBM/WebSphere/AppServer/bin/wsadmin.sh

                    WAS version : 8.0.0.0
                     Deployment : Standalone
                       JVM mode : 32
              Configuration home : /opt/IBM/ITM/dchome/7.2.0.0.1

 2) Integrate with ITCAM for SOA Agent : Yes

 3) Integrate with ITCAM Agent for WebSphere Applications : Yes

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

 4) Integrate with ITCAM for AD Managing Server : No

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

```
 5) Integrate with ITCAM for Transactions : Yes

       Transaction Collector hostname : 127.0.0.1
       Transaction Collector port number : 5455

 6) Integrate with Tivoli Performance Viewer : No

 7) Integrate with ITCAM diagnostics tool : No

 8) Advanced settings :

       Set Garbage Collection log path : No

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

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

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

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

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

36. Enter `1` to create a backup of the current configuration. Otherwise, enter `2`.
37. The utility applies the changes and presents a status message to indicate that the configuration of the data collector for the profile is complete:

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

38. After configuring the data collector to monitor application server instances, you must restart the instances as directed by the utility. The data collector configuration takes effect when the application server instances are restarted.

Data collection is configured for the specified application server instances.

Unconfiguring ITCAM Data Collector for WebSphere

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

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

To unconfigure the data collector, complete the following procedure:

1. From the command line, navigate to the *DC_home*`/bin` directory.

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

   ```
   export JAVA_HOME=/opt/IBM/AppServer80/java
   ```

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

   DC_home/bin/unconfig.sh

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

   Remember:

   - Application server instances must be running during the unconfiguration procedure.
   - For Network Deployment environment, the Node Agent and Deployment Manager must also be running.

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

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

4. Enter the number that corresponds to the application server instance to unconfigure for data collection or enter an asterisk (*) to unconfigure data collection for all application server instances. To specify a subset of servers, enter the numbers, separated by commas, that represent the servers. For example: 1,2,3.
5. The utility prompts you to specify whether you want to create a backup of your current WebSphere Application Server configuration:

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

   Enter 1 to create a backup of the current configuration. Otherwise, enter 2 and skip to step 8.
6. The utility prompts you to specify the directory in which to store the backup of the configuration. For example:

   ```
   Enter backup directory  [default is: /opt/IBM/ITM_DC/dchome/7.2.0.0.1/data]:
   ```

   Specify a directory in which to store the backup of the configuration or accept the default directory.
7. The utility displays the name of the WebSphere home directory and the WebSphere profile for which a backup is created. For example:

   ```
   WebSphere Home:/opt/IBM/WebSphere/AppServer/profiles/AppSrv01
   WebSphere Profile:AppSrv01
   ```

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

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

   If global security is not enabled, skip to step 11 on page 131.
9. The utility prompts you to specify whether to retrieve security settings from a client properties file:

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

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

Enter `1` to allow the utility to retrieve the user name and password from the appropriate client properties file and skip to step 11. Otherwise, enter `2` to enter the user name and password.

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

10. If you selected the option to back up the current WebSphere configuration, the utility starts backing up the configuration. For example:

```
Backing up profile: AppSrv01 home: /opt/IBM/WebSphere/AppServer/bin ...
Backup file /opt/IBM/ITM_DC/dchome/7.2.0.0.1/data/v525400e96601Cell01.
v525400e96601Node01.AppSrv01.WebSphereConfig_20120716161102.zip is
successfully created
```

11. The utility unconfigures the data collector for the specified application server instances. A status message is presented to indicate that the data collector was successfully unconfigured:

```
Successfully executed Unconfiguring for Cell: v525400e96601Cell01 Node:
v525400e96601Node01 Profile: AppSrv01
```

12. After unconfiguring the data collector to monitor application server instances, you must restart the instances as directed by the utility. The data collector unconfiguration takes effect when the application server instances are restarted.

Data collection is unconfigured for the specified application server instances.

Reconfiguring ITCAM Data Collector for WebSphere

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

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

- ITCAM Agent for WebSphere monitoring agent
- ITCAM for Application Diagnostics Managing Server
- ITCAM for SOA monitoring agent
- ITCAM for Transactions
- Tivoli Performance Viewer, available from the WebSphere administrative console
- ITCAM Diagnostic Tool that is previewed in the ITCAM for Application Diagnostics beta

You can also reconfigure garbage collection settings.

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

1. From the command line, navigate to *DC_home*`/bin` directory.
2. Set the location of the Java home directory before you run the utility:
3. Run the following command to start the ITCAM Data Collector for WebSphere Reconfiguration utility:

DC_home/bin/reconfig.sh

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

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

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

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

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

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

   Remember:

   - For a stand-alone environment, application server instances must be running during the configuration.
   - For a Network Deployment, WebSphere Virtual Enterprise, or WebSphere Compute Grid environment, the Node Agent and Deployment Manager must be running.
   - Ensure that the application server instances that you select are the actual servers that host the applications or services that you want to monitor.

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

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

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

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

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

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

   When configuring data collection for ITCAM Agent for WebSphere Applications, you can integrate the data collector with ITCAM Agent for WebSphere Applications monitoring agent, or with the ITCAM for Application Diagnostics Managing Server, or with both.

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

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

Important: When you configure data collection for ITCAM Agent for WebSphere Applications for applications servers in a profile where data collection is configured for application servers for ITCAM for SOA version 7.2, you must reconfigure and restart the Tivoli Enterprise Portal Server to capture ITCAM Agent for WebSphere Applications data in the topology views of ITCAM for SOA.

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

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

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

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

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

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

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

11. Enter the port number of the monitoring agent.

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

    You are prompted to specify whether you want to integrate the data collector with a managing server.

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

    Remember:

    - To integrate with ITCAM for Application Diagnostics Managing Server for deep-dive analysis, you must have ITCAM for Application Diagnostics version 7.1.0.3 or later installed.
    - If you decide not to configure the managing server at this time, you can still configure the data collector to communicate with the managing server later.

13. Enter 1 to integrate with the managing server. Otherwise, enter 2 and skip to step 16 on page 134.

    You are prompted to specify the host name of the managing server:

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

14. Enter the fully qualified host name of the managing server.

    You are prompted to specify the port number of the managing server:

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

    The port number is codebase port on which the managing server is listening.

    Tip: The port number is specified in the key `PORT_KERNEL_CODEBASE01` in the `ITCAM61_MS_CONTEXT.properties` file in the managing server home directory. See *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

    The configuration utility attempts to connect to the managing server and retrieve the value for the *MS_home* directory. If successful, the utility displays a message similar to the following message:

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

15. If the connection to the managing server is *not* successful, you are prompted to enter the value of the managing server home directory:

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

    If prompted, enter the value of the managing server home directory.

16. The utility prompts you to specify whether you want to configure advanced settings for the managing server.

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

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

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

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

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

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

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

    Enter the RMI Controller port numbers.

19. You are prompted to enter the Remote File Sharing (RFS) port number of the managing server:

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

    The RFS server in the managing server kernel listens to the RFS port to accept incoming requests. Enter the RFS port number.

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

    Remember: To integrate the data collector with ITCAM for Transactions, you must install ITCAM for Transactions version 7.3 or later within an IBM Tivoli

Monitoring environment.
You are prompted to specify whether you want to integrate with ITCAM for Transactions:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    Enter 1 to select a garbage collection log path. Otherwise, enter 2 and skip to step 31.

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

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

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

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

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

    ```
    1) List of servers selected

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

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

          wsadmin location          :
            /opt/IBM/WebSphere/AppServer/bin/wsadmin.sh

                       WAS version : 8.0.0.0
                        Deployment : Standalone
                          JVM mode : 32
                 Configuration home : /opt/IBM/ITM/dchome/7.2.0.0.1


    2) Integrate with ITCAM for SOA Agent : Yes

    3) Integrate with ITCAM Agent for WebSphere Applications : Yes

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

    4) Integrate with ITCAM for AD Managing Server : No

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

    5) Integrate with ITCAM for Transactions : Yes

          Transaction Collector hostname : 127.0.0.1
          Transaction Collector port number : 5455
    ```

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

 7) Integrate with ITCAM diagnostics tool : No

 8) Advanced settings :

       Set Garbage Collection log path : No

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

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

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

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

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

33. Enter `1` to create a backup of the current configuration. Otherwise, enter `2`.
34. The utility applies the changes and presents a status message to indicate that the reconfiguration of the data collector for the profile is complete:

    ```
    Successfully executed Reconfiguring for Cell: v525400597750Node01Cell
    Node: v525400597750Node01 400597750Node01
    Profile: AppSrv01
    ```

35. After reconfiguring the data collector to monitor application server instances, you must restart the instances as directed by the utility. The data collector configuration takes effect when the application server instances are restarted.

Data collection is reconfigured for the specified application server instances.

Migrating data collectors to ITCAM Data Collector for WebSphere

A previous version or an earlier maintenance level of ITCAM Data Collector for WebSphere can be migrated interactively with the ITCAM Data Collector for WebSphere Migration utility. If you want to migrate many application server instances, it might be more convenient to migrate the application servers using the migration utility in silent mode.

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

1. ITCAM for WebSphere version 6.1.0.4 or later
2. WebSphere Data Collector version 6.1.0.4 or later included in ITCAM for Web Resources version 6.2.0.4 or later

3. ITCAM Agent for WebSphere Applications version 7.1 included in ITCAM for Applications Diagnostics version 7.1
4. ITCAM for WebSphere Application Server version 7.2
5. ITCAM for SOA version 7.1.1

You can also use the migration utility to update ITCAM Data Collector for WebSphere to a new maintenance level.

For the procedure for migrating the ITCAM for SOA version 7.1.1 WebSphere Application Server data collector to ITCAM Data Collector for WebSphere, see "Migrating ITCAM for SOA version 7.1.1 data collector to ITCAM Data Collector for WebSphere" on page 140.

To upgrade the monitoring of server instances to ITCAM Data Collector for WebSphere or to update the maintenance level of the data collector, complete the following procedure:

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

   ```
   export JAVA_HOME=/opt/IBM/AppServer80/java
   ```

2. Run the following command to start the migration utility.

   DC_home/bin/migrate.sh

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

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

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

   The utility prompts you to specify from the type of agent that you want to upgrade to ITCAM Data Collector for WebSphere. If you are configuring the Data Collector shipped with ITCAM Agent for WebSphere Applications version 7.2 ifix 1 or later, the following list is displayed.

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

   1. ITCAM for WebSphere 6.1.0.4 or later
   2. ITCAM WebSphere Agent 6.2.0.4 or later [ITCAM for Web Resources 6.2]
   3. ITCAM Agent for WebSphere Applications 7.1 [ITCAM for Application Diagnostics 7.1]
   4. ITCAM for WebSphere Application Server 7.2
   5. ITCAM for SOA 7.1.1.x
   6. Maintenance level update for ITCAM Data Collector for WebSphere 7.2 and later [ITCAM
     Agent for WebSphere Applications 7.2 and later, ITCAM for SOA 7.2 and later, IBM
     Application Performance Diagnostics Lite]
   Enter the number [default is: 1]:
   ```

   In older Data Collector versions, the following list is displayed:

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

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

5. Enter the number that represents the agent.

   Attention: In older Data Collector versions, to update the maintenance level of ITCAM Data Collector for WebSphere, enter 4.

   For the procedure for migrating the ITCAM for SOA version 7.1.1 data collector to version 7.2, see "Migrating ITCAM for SOA version 7.1.1 data collector to ITCAM Data Collector for WebSphere" on page 140.
6. The utility prompts you to specify the home directory of the previous version of the data collector.

   ```
   Enter the home directory of the data collector to be upgraded:
   ```
7. Enter the home directory of the previous version of the data collector. For example, `/opt/IBM/ITM/li6263/yn/wasdc/7.1.0.2`.

   If you are migrating ITCAM for WebSphere Application Server version 7.2, skip to step 10.
8. If the data collector was integrated with the ITCAM Agent for WebSphere monitoring agent, you are prompted to reenter the host name and port of the monitoring agent. If more than one version of the monitoring agent is available, you can connect the data collector to the correct version. On Linux and UNIX systems, you can install several versions of the monitoring agent on the same host, using different ports.

   ```
   Enter the host name or IP address of the ITCAM Agent for
   WebSphere Applications TEMA: [default is: 127.0.0.1]:
   ```
9. Enter the fully qualified host name or IP address of the ITCAM Agent for WebSphere Applications monitoring agent. It is on the local host, so the default is correct.

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

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

   Enter the port number of the monitoring agent.
10. The utility searches for the list of application server instances that are configured by the specified data collector installation.

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

    ```
    Choose a Server or Servers to be migrate
     1. x336r1s37-vn01Cell01.x336r1s36-vn01Node03.server3
     2. x336r1s37-vn01Cell01.x336r1s36-vn01Node03.server5
     3. x336r1s37-vn01Cell01.x336r1s36-vn01Node03.server1
    Enter a number or numbers separated by a comma, enter '*' to select all
    servers listed, or enter 'q' to quit the selection.
    ```

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

    Remember:

    - For a stand-alone environment, application server instances must be running during the configuration.
    - For a Network Deployment, WebSphere Virtual Enterprise, or WebSphere Compute Grid environment, the Node Agent and Deployment Manager must be running.
11. Enter the number that corresponds to the application server instance whose data collector is to be migrated or enter an asterisk (*) to migrate the data

collector of all application server instances. To specify a subset of servers, enter the numbers, separated by commas, that represents the servers. For example: `1,2,3`.

12. The utility determines whether WebSphere Global Security was enabled for each of the profiles that are impacted by the migration task.
13. If WebSphere Global Security is enabled on one or more profiles, the utility prompts you to specify whether to retrieve security settings from a client properties file:

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

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

    Enter `1` to allow the utility to retrieve the user name and password from the appropriate client properties file and skip to step 14. Otherwise, enter `2` to enter the user name and password.

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

    Important: It may take some time to log in to the WebSphere Application Server administrative console.
    The utility prompts you for the user name and password for each profile whether WebSphere Global Security is enabled.
14. The utility migrates data collection for each selected application server instance and displays a status message that indicates whether the migration of each server completed successfully.
15. When the utility completes the migration of all application server instances configured by the previous version of the data collector, it displays the following message:

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

16. After migrating the data collector, you must restart the instances as directed by the utility. The data collector configuration takes effect when the application server instances are restarted.

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

You can also configure or reconfigure integration with ITCAM for SOA, ITCAM Agent for WebSphere Applications monitoring agent, ITCAM for Application Diagnostics Managing Server, Tivoli Performance Viewer, and ITCAM diagnostics tool for the application server instances. For more information, see “Reconfiguring ITCAM Data Collector for WebSphere” on page 131.

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

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

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

For the procedure for migrating the following data collector components to ITCAM Data Collector for WebSphere, see "Migrating data collectors to ITCAM Data Collector for WebSphere" on page 137:

- ITCAM for WebSphere version 6.1.0.4 or later
- WebSphere Data Collector version 6.1.0.4 or later included in ITCAM for Web Resources version 6.2.0.4 or later
- ITCAM for WebSphere Application Server version 7.1 included in ITCAM for Applications Diagnostics version 7.1
- ITCAM for WebSphere Application Server version 7.2. Data Collector

To update the maintenance level of any products that have ITCAM Data Collector for WebSphere as a component, including ITCAM for SOA, follow the procedure in "Migrating data collectors to ITCAM Data Collector for WebSphere" on page 137.

Important:

If an older version of ITCAM Agent for WebSphere Applications is configured for application servers in the same profile as ITCAM for SOA version 7.1.1, migrate the data collector provided with ITCAM Agent for WebSphere Applications. Then, reconfigure the data collector to integrate it with the ITCAM for SOA monitoring agent. You must not run the migration utility to migrate the older version of the ITCAM for SOA WebSphere Application Server data collector.

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

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

   ```
   export JAVA_HOME=/opt/IBM/AppServer80/java
   ```

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

   DC_home/bin/migrate.sh

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

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

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

   The utility prompts you to specify from the type of agent that you want to upgrade to ITCAM Data Collector for WebSphere. If you are configuring the Data Collector shipped with ITCAM Agent for WebSphere Applications version 7.2 ifix 1 or later, the following list is displayed.

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

   1. ITCAM for WebSphere 6.1.0.4 or later
   2. ITCAM WebSphere Agent 6.2.0.4 or later [ITCAM for Web Resources 6.2]
   3. ITCAM Agent for WebSphere Applications 7.1 [ITCAM for Application Diagnostics 7.1]
   4. ITCAM for WebSphere Application Server 7.2
   5. ITCAM for SOA 7.1.1.x
   ```

```
6. Maintenance level update for ITCAM Data Collector for WebSphere 7.2 and later [ITCAM
  Agent for WebSphere Applications 7.2 and later, ITCAM for SOA 7.2 and later, IBM
  Application Performance Diagnostics Lite]
Enter the number [default is: 1]:
```

In older Data Collector versions, the following list is displayed:

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

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

Enter 5 to migrate ITCAM for SOA version 7.1.1.

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

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

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

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

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

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

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

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

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

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

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

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

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

9. The utility searches for all application server instances under the specified profile. The utility displays all servers that are not configured yet for data

collection and all servers that have been configured to use the same maintenance level of ITCAM Data Collector for WebSphere.

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

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

Important:

- For a stand-alone environment, application server instances must be running during the configuration.
- For a Network Deployment, WebSphere Virtual Enterprise, or WebSphere Compute Grid environment, the Node Agent and Deployment Manager must be running.
- Ensure that the application server instances that you select are the actual servers that host the BPM applications or services that you want to monitor.

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

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

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

Each of the servers will be configured for data collection

 1) List of servers selected

   - WAS server: IBM-6DA7F9C6EE6Node02Cell.IBM-6DA7FNode02.server1(AppSrv02)
       WAS cell: IBM-6DA7F9C6EE6Node02Cell
        WAS node: IBM-6DA7F9C6EE6Node02

       WebSphere Profile home    :
         /opt/IBM/WebSphere/AppServer80/profiles/AppSrv02

       wsadmin location          :
         /opt/IBM/WebSphere/AppServer80/bin/wsadmin.bat

                    WAS version : 8.0.0.0
                     Deployment : Standalone
                       JVM mode : 32
              Configuration home : /opt/IBM/ITM/dchome/7.2.0.0.1

 2) Integrate with ITCAM for SOA Agent : Yes

 3) Integrate with ITCAM Agent for WebSphere Applications : No

 4) Integrate with ITCAM for AD Managing Server : No

 5) Integrate with ITCAM for Transactions : No

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

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

 8) Advanced settings :

       Set Garbage Collection log path : No

Configuration sections:

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

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

11. To enable integration with products and components other than ITCAM for SOA, select the corresponding number. For details on the configuration, see "Configuring ITCAM Data Collector for WebSphere" on page 122. Otherwise, to accept the configuration, enter `a`.

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

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

12. Enter 1 to create a backup of the current configuration. Otherwise, enter 2.
13. The utility applies the changes and presents a status message to indicate that the configuration of the data collector for the profile is complete:

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

14. After migrating the data collector, you must restart the instances as directed by the utility. The data collector configuration takes effect when the application server instances are restarted.

You can also configure or reconfigure integration with ITCAM for SOA, ITCAM Agent for WebSphere Applications monitoring agent, ITCAM for Application Diagnostics Managing Server, Tivoli Performance Viewer, and ITCAM diagnostics tool for the application server instances at the same time. For more information, see "Reconfiguring ITCAM Data Collector for WebSphere" on page 131.

Starting ITCAM Agent for WebSphere Applications

To start ITCAM Agent for WebSphere Applications, start the following command on the computer where it is installed:

```
./itmcmd agent start yn
```

Where `yn` is the two-character product code for the ITCAM Agent for WebSphere Applications.

The installer also adds the agent to system startup scripts. To remove it from the scripts, see "Deep-dive diagnostics-only installation: disabling monitoring agent autostart" on page 110.

Enabling application support on Linux and UNIX systems

To ensure that ITCAM Agent for WebSphere Applications works within your Tivoli Monitoring infrastructure, you must install application support files and enable application support for it on every hub and remote monitoring server, portal server, and portal client. After configuring the agent on the monitored host, you must also enable Tivoli Monitoring history collection. If Tivoli Monitoring is not used (in a deep-dive diagnostics-only installation), you do not have to install application support files.

Tip: Enabling application support is sometimes referred to as adding or activating application support. On the portal server and portal client, application support is enabled when you configure the portal server. On the monitoring server, application support is enabled when you seed the monitoring server database.

If self-description is enabled on the Tivoli Monitoring components and on ITCAM Agent for WebSphere Applications, application support files are automatically installed and enabled on the monitoring server and the portal server without the need to recycle the monitoring server or the portal server. The conditions that must be met for self-description to operate are specified in "Enabling application support through self-description."

If the agent and the Tivoli Monitoring components are not enabled for self-description, you must manually install application support files on the Tivoli Monitoring components. For more information, see "Manually installing application support" on page 146.

Enabling application support through self-description

IBM Tivoli Monitoring version 6.2.3 or later agents, which are enabled for self-description, install application support files and enable application support on the IBM Tivoli Monitoring infrastructure automatically. ITCAM Agent for WebSphere Applications is enabled by default for self-description. When the ITCAM Agent for WebSphere Applications is installed, and the hub and remote monitoring servers are enabled for self-description, application support files are automatically installed on the hub monitoring server, the remote monitoring server, and the portal server, without the need to recycle the monitoring server or the portal server. Application support files must be installed manually on the portal client.

Although the self-describing agent is enabled by default for ITCAM Agent for WebSphere Applications, a number of conditions apply:

- All Tivoli Management Services server components must be at version 6.2.3 or higher.
- The agent framework must be at version 6.2.3 or higher. In ITCAM Agent for WebSphere Applications version 7.2, agent framework version 6.2.2 is installed during the installation or upgrade of ITCAM Agent for WebSphere Applications. However, if you install another IBM Tivoli Monitoring agent, such as an OS agent, and its agent framework is at version 6.2.3, its installation may upgrade the agent framework of ITCAM Agent for WebSphere Applications to version 6.2.3.

  Remember: Not all OS agents running version 6.2.3, which share the same IBM Tivoli Monitoring home directory as ITCAM Agent for WebSphere Applications,

upgrade the agent framework to 6.2.3. You must verify that the agent framework has been upgraded to version 6.2.3 before using self-description for ITCAM Agent for WebSphere Applications.

To identify the agent framework version after installing or upgrading ITCAM Agent for WebSphere Applications, complete the following steps:

1. From the command-line, navigate to *ITM_Home*/bin directory.
2. Run the following command:

   ```
   ./cinfo -t
   ```

3. Locate the line for the agent framework in the output and note the version. For example:

   ```
   ax IBM Tivoli Monitoring Shared Libraries li6263 06.22.02.00
   d0126a 20120716 1412
   ```

You must verify that these conditions are met before you can use self-description for deploying application support to the monitoring server and the portal server.

After the self-describing application update is complete, and the application support files are manually installed on the portal client, you should see the following new agent data in the portal client:

- Historical Configuration is updated with any new attributes
- Workspaces are updated
- New or updated situations, policies, and take actions
- Queries are updated
- Help server files are updated

The self-describing agent feature is disabled by default on the hub monitoring server. The procedure for enabling self-description on the hub monitoring server is documented in the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Manually installing application support

If you have not enabled self-description on Tivoli Monitoring components and on ITCAM Agent for WebSphere Applications, you must install and enable application support manually on every hub and remote monitoring server, portal server, and portal client.

Multiple versions of ITCAM Agent for WebSphere Applications (version 6.2 and later) can be integrated with Tivoli Monitoring. If self-description is not enabled, you must install application support files from the agent that is at the latest version. For example, if your environment has ITCAM Agent for WebSphere Applications versions 7.2 and 7.1, ensure you install the application support files for the latest version, in this case version 7.2.

You must stop the monitoring server, portal server, or portal client when installing the support files.

Installing and enabling application support on Tivoli Enterprise Monitoring Server

1. To stop the monitoring server, run the following command:

   ```
   ./itmcmd server stop tems_name
   ```

2. After loading the application support installation media for Linux or UNIX systems and changing to its root directory, locate the installation script, `install.sh`, and start it:

```
./install.sh
```

3. To accept the default directory (/opt/IBM/ITM), press Enter, or type the full path to the installation directory you used when the software asks for the IBM Tivoli Monitoring home directory.

   The following prompt is displayed:

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

   Please enter a valid number:
   ```

4. Type 1 and press Enter.
5. The software license agreement is displayed after the initialization. To accept the agreement, enter 1 and press Enter.
6. Type the 32 character encryption key that was specified during the installation of the monitoring server and press Enter.

   Important: If you already installed another IBM Tivoli Monitoring component on this computer or you are installing support for an agent from an agent installation image, this step does not occur.

   Information about installed products is displayed.

7. To continue the installation, press Enter. The installer prompts you with the following message:

   ```
   Product packages are available for the following operating systems and
   component support categories:

    1) IBM Tivoli Monitoring components for this operating system
    2) Tivoli Enterprise Portal Browser Client support
    3) Tivoli Enterprise Portal Desktop Client support
    4) Tivoli Enterprise Portal Server support
    5) Tivoli Enterprise Monitoring Server support
    6) Other operating systems

   Type the number or type "q" to quit selection
   [ number "1" or "IBM Tivoli Monitoring components for this operating system"
   is default ]:
   ```

8. To install the application support on the Tivoli Enterprise Monitoring Server, type 5. Then, press Enter. The following message is displayed:

   ```
   You selected number "5" or "Tivoli Enterprise Monitoring Server support"

   Is the selection correct [ 1=Yes, 2=No; default is "1"]?
   ```

9. To confirm the selection, type 1 and press Enter. The following message is displayed:

   ```
   The following products are available for installation:

    1) IBM Tivoli Composite Application Manager Agent for WebSphere
      Applications v07.20.00.00
    2) all of the above

   Type the numbers for the products you want to install,
   type "b" to change operating system, or type "q" to quit selection.
   If you enter more than one number, separate the numbers by a comma or a space.

   Type you selections here:
   ```

10. Type 1 and press Enter. The installer prompts you with the following message:

```
The following application supports are available for installation:

1) IBM Tivoli Composite Application Manager Agent for WebSphere Applications
V07.20.00.00
2) all of the above

Type the numbers for the products you want to install,
type "b" to change operating system, or type "q" to quit selection.
If you enter more than one number, separate the numbers by a comma or a space.

Type you selections here:
```

11. Type 1 and press Enter to confirm your selection and start the installation.
12. After installing all of the components, the following message is displayed to ask you whether you want to install additional Tivoli Monitoring components or application support files:

    ```
    Do you want to install additional products or product support packages
     [ 1=Yes, 2=No; default is "2" ]?
    ```

    Type 2 and press Enter.
13. The installation step completes and the information about installed application support files for Tivoli Enterprise Monitoring Server is displayed:

    ```
    *) IBM Tivoli Composite Application Manager Agent for WebSphere Applications
    ```

    The installer also prompts you with the following message to enable application support for the Tivoli Enterprise Monitoring Server:

    ```
    Note: This operation causes the monitoring server to restart.
    Do you want to seed product support on the Tivoli Enterprise Monitoring Server?
    [ 1=Yes, 2=No; default is "1" ]?
    ```
14. To use the default choice, press Enter.
15. After starting the Tivoli Enterprise Monitoring Server, the message about enabling application support is displayed:

    ```
    The following new Tivoli Enterprise Monitoring Server product support packages
    will be seeded:
     *) IBM Tivoli Composite Application Manager Agent for WebSphere Applications
    ```
16. To use the default choice, press Enter.
17. When application support is enabled and the monitoring server is stopped, the following message is displayed to remind you about configuring Tivoli Monitoring components:

    ```
    You may now configure any locally installed IBM Tivoli Monitoring product via
    the "/opt/IBM/ITM/bin/itmcmd config" command.
    ```
18. The monitoring server is restarted automatically.

Installing and enabling application support on Tivoli Enterprise Portal Server

On a Tivoli Enterprise Portal Server, you must install and enable application support files both for the server itself and for the desktop client.

Stop the portal server before you complete this procedure.

1. After loading the application support installation media for Linux or UNIX systems and changing to its root directory, locate the installation script, `install.sh`, and start it:

   ```
   ./install.sh
   ```

2. To accept the default directory, (/opt/IBM/ITM) press Enter, or type the full path to the installation directory you used when the software asks for the IBM Tivoli Monitoring home directory.

   The software displays the following prompt:

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

   Please enter a valid number:
   ```

3. Type 1 and press Enter.
4. The software license agreement is displayed after the initialization. To accept the agreement, type 1 and press Enter.
5. Type the 32-character encryption key that was specified during the installation of the monitoring server. Then, press Enter.

   Important: If you already installed another IBM Tivoli Monitoring component on this computer or you are installing support for an agent from an agent installation image, this step does not occur.

   The information about installed products is displayed.
6. To continue the installation, press Enter. The installer prompts you with the following message:

   ```
   Product packages are available for the following operating systems and
   component support categories:

    1) IBM Tivoli Monitoring components for this operating system
    2) Tivoli Enterprise Portal Browser Client support
    3) Tivoli Enterprise Portal Desktop Client support
    4) Tivoli Enterprise Portal Server support
    5) Tivoli Enterprise Monitoring Server support
    6) Other operating systems

   Type the number or type "q" to quit selection
   [ number "1" or "IBM Tivoli Monitoring components for this operating system"
   is default ]:
   ```

7. Type 4 and press Enter to install the application support on the Tivoli Enterprise Portal server. The following message is displayed:

   ```
   You selected number "4" or "Tivoli Enterprise Portal Server support"

   Is the selection correct [ 1=Yes, 2=No; default is "1"]?
   ```

8. Type 1 and press Enter to confirm the selection. The following message about the application support files to install is displayed:

   ```
   The following application supports are available for installation:

   1) IBM Tivoli Composite Application Manager Agent for WebSphere Applications
   V07.20.00.00
   2) all of the above

   Type the numbers for the products you want to install,
   type "b" to change operating system, or type "q" to quit selection.
   If you enter more than one number, separate the numbers by a comma or a space.

   Type you selections here:
   ```

9. Type 1 and press Enter. The installer prompts you with the following message to ask you to confirm your selection:

```
The following products will be installed:

 IBM Tivoli Composite Application Manager Agent for WebSphere
    Applications v07.20.00.00

Are your selections correct [ 1=Yes, 2=No; default is "1" ]?
```

10. Type 1 and press Enter to confirm your selection and start the installation.
11. After installing all of the components, the following message is displayed to ask you whether you want to install additional Tivoli Monitoring components or application support files:

    ```
    Do you want to install additional products or product support
       packages [ 1=Yes, 2=No; default is "2" ]?
    ```

    Type 1 to confirm that you want to install additional application support files and press Enter.
12. The following message is displayed:

    ```
    Product packages are available for the following operating systems and
    component support categories:

    1) IBM Tivoli Monitoring components for this operating system
    2) Tivoli Enterprise Portal Browser Client support
    3) Tivoli Enterprise Portal Desktop Client support
    4) Tivoli Enterprise Portal Server support
    5) Tivoli Enterprise Monitoring Server support
    6) Other operating systems
    Type the number for the OS you want, or type "q" to quit selection:
    ```
13. Type 2 and press Enter to install application support on the Tivoli Enterprise Portal browser client. The following message is displayed:

    ```
    You selected number "1" or "Tivoli Enterprise Portal Browser Client support"

    Is the selection correct [ 1=Yes, 2=No; default is "1"]?
    ```
14. Type 1 and press Enter to confirm the selection. The message about the products to install is displayed:

    ```
    The following application supports are available for installation:

     1) IBM Tivoli Composite Application Manager Agent for WebSphere Applications
    V07.20.00.00
     2) all of the above

    Type the numbers for the products you want to install,
    type "b" to change operating system, or type "q" to quit selection.
    If you enter more than one number, separate the numbers by a comma or a space.

    Type you selections here:
    ```
15. Type 1 and press Enter. The installer prompts you with the following message to ask you to confirm your selection:

    ```
    The following products will be installed:

     IBM Tivoli Composite Application Manager Agent for WebSphere
       Applications v07.20.00.00

    Are your selections correct [ 1=Yes, 2=No; default is "1" ]?
    ```
16. Type 1 and press Enter to confirm your selection and start the installation.
17. After installing all of the components, the following message is displayed to ask you whether you want to install other components:

    ```
    Do you want to install additional products or product support packages
     [ 1=Yes, 2=No; default is "2" ]?
    ```

    Type 2 and press Enter.

18. The installation program completes the installation and exits. After this, reconfigure the portal server and browser client to enable application support by running the following command:

    ```
    itmcmd config -A cq
    ```

    At any prompts, to accept the default values, press Enter.

Important: If the Tivoli Enterprise Portal Server provides the browser client, check that the Eclipse help server is configured. For more information, see "Ensure that the Eclipse server is configured" on page 152.

Installing and enabling application support on Tivoli Enterprise Portal desktop client

Stop the desktop client before you complete this procedure.

1. After loading the application support installation media for Linux or UNIX systems and changing to its root directory, locate the installation script, `install.sh`, and start it:

   ```
   ./install.sh
   ```

2. To accept the default directory (`/opt/IBM/ITM`) press Enter, or when the software asks for the IBM Tivoli Monitoring home directory, type the full path to the installation directory that you used. The following prompt is displayed:

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

   Please enter a valid number:
   ```

3. Type 1 and press Enter.
4. The software license agreement is displayed after the initialization. To accept the agreement, type 1 and press Enter.
5. Type the 32-character encryption key that was specified during the installation of the monitoring server and press Enter.

   Important: If you already installed another IBM Tivoli Monitoring component on this computer, or if you are installing support for an agent from an agent installation image, this step does not occur.

   Information about the installed products is displayed.
6. To continue the installation, press Enter. The installer prompts you with the following message:

   ```
   Product packages are available for the following operating systems and
   component support categories:

    1) IBM Tivoli Monitoring components for this operating system
    2) Tivoli Enterprise Portal Browser Client support
    3) Tivoli Enterprise Portal Desktop Client support
    4) Tivoli Enterprise Portal Server support
    5) Tivoli Enterprise Monitoring Server support
    6) Other operating systems

   Type the number or type "q" to quit selection
   [ number "1" or "IBM Tivoli Monitoring components for this operating system"
   is default ]:
   ```

7. To install the application support on the Tivoli Enterprise Portal desktop client, type 3 and press Enter. The following message is displayed:

```
You selected number "3" or "Tivoli Enterprise Portal Desktop Client support"

Is the selection correct [ 1=Yes, 2=No; default is "1"]?
```

8. To confirm the selection, type 1 and press Enter. The following message about the application support files available for installation is displayed:

```
The following application supports are available for installation:

 1) IBM Tivoli Composite Application Manager Agent for WebSphere
   Applications v07.20.00.00
 2) all of the above

Type the numbers for the products you want to install,
type "b" to change operating system, or type "q" to quit selection.
If you enter more than one number, separate the numbers by a comma or a space.

Type you selections here:
```

9. Type 1 and press Enter. The installer prompts you with the following message to ask you to confirm your selection:

```
The following products will be installed:

 IBM Tivoli Composite Application Manager Agent for WebSphere
   Applications v07.20.00.00

Are your selections correct [ 1=Yes, 2=No; default is "1" ]?
```

10. To confirm your selection and start the installation, type 1 and press Enter.
11. After installing all of the components, the following message is displayed to ask you whether you want to install additional Tivoli Monitoring components or application support files:

```
Do you want to install additional products or product support packages
 [ 1=Yes, 2=No; default is "2" ]?
```

    Type 2 and press Enter.
12. The installer prompts you with the following message for the configuration:

```
You may now configure any locally intalled IBM Tivoli Monitoring product via
the "/opt/IBM/ITM/bin/itmcmd config" command.
```

13. The installation program completes the installation and exits. Next, reconfigure the desktop client to enable application support by running the following command:

```
itmcmd config -A cj
```

    At any prompts, to accept the default values, press Enter.

Important: Check that the Eclipse help server is configured for the client. For more information, see "Ensure that the Eclipse server is configured."

Ensure that the Eclipse server is configured

After you install application support files on a Tivoli Enterprise Portal Server that provides the browser client or on a Tivoli Enterprise Portal desktop client, you must check the Eclipse help server for the portal client to ensure that it is configured.

To check that the Eclipse help server is configured, complete the following procedure:

1. Start Manage Tivoli Enterprise Monitoring Services:

```
./itmcmd manage
```

   The Manage Tivoli Enterprise Monitoring Services window opens.

2. Verify that the Eclipse Help Server entry indicates `Yes` in the configured column. If it does not, right-click the entry, and select **Configure** from the menu.
3. You are prompted for the port number that the Eclipse Help Server is to use. Verify that this value is set to the same port number that you specified when you installed IBM Tivoli Monitoring. Click **OK**.

Upgrading the Tivoli Date Warehouse database tables

If you upgrading to ITCAM Agent for WebSphere Applications version 7.2, you might have configured history collection and summarization and pruning for the following tables in the Tivoli Data Warehouse for the older version of the agent:

- `"DC_Messages_-_WebSphere"`
- `"DC_Messages_-_WebSphere_H"`
- `"DC_Messages_-_WebSphere_D"`
- `"DC_Messages_-_WebSphere_W"`
- `"DC_Messages_-_WebSphere_M"`
- `"DC_Messages_-_WebSphere_Q"`
- `"DC_Messages_-_WebSphere_Y"`

You must run the database tables upgrade script provided with ITCAM Agent for WebSphere Applications version 7.2 to upgrade the database tables.

You must run the script before you enable historical data collection for version 7.2.

Important: If you run the upgrade script, but one or more of the tables did not exist in the Tivoli Data Warehouse, the upgrade script does not create them.

The upgrade script increases the size of the tables so that they can store data provided by ITCAM Agent for WebSphere Applications version 7.2.

The scripts are located in the *ITM_home*`/samples` directory. The name of the script indicates the database type it supports.

To upgrade the database tables, complete the following steps:

1. (Optional) Back up the Tivoli Data Warehouse or the tables to be upgraded before running the script. For more information about backing up IBM Tivoli Monitoring components, see *IBM Tivoli Monitoring: Installation and Configuration Guide*.
2. Disable the Warehouse Proxy agent and the Summarization and Pruning agent:
   a. Start the Manage Tivoli Monitoring Services utility. To start the utility, issue the command *ITM_home*`/bin/itmcmd mange`.
   b. Right-click the Summarization and Pruning agent in the `Service/Application` column.
   c. Select **Stop**.
   d. Right-click the Warehouse Proxy agent in the `Service/Application` column.
   e. Select **Stop**.
3. If the Tivoli Data Warehouse is running a DB2 database, complete the following steps:
   a. Connect to the Tivoli Data Warehouse by issuing the following command:
      `db2 CONNECT TO` *database* `USER` *db_user* `USING` *db_password*

      Where:

database
Specifies the name of the Tivoli Data Warehouse database server.

db_user
Specifies the user who owns the Tivoli Data Warehouse database tables.

db_password
Specifies the database password for the specified *db_user*.

b. Navigate to the *ITM_home*/samples directory. Run the following script to upgrade the database tables:

```
db2 -td@ -f yn_072000000_warehouse_changes_DB2.sql -x -z log_file
```

Where *log_file* is the name of the log file used to log the output of the script.

c. Wait for the database upgrade process to complete.

d. Close the DB2 command-line window.

4. If the Tivoli Data Warehouse is using an Oracle database, complete the following steps:

a. Navigate to the path where the sqlplus utility is located. Run the following command to connect to the instance of the database server that hosts the Tivoli Data Warehouse and to run the script to upgrade the database tables:

```
sqlplus db_user/db_password@db_connection
@yn_072000000_warehouse_changes_ORACLE.sql > log_file
```

Where:

db_user
Specifies the user who owns the Tivoli Data Warehouse database tables.

db_password
Specifies the database password for the specified *userID*.

db_connection
Specifies the net service name of the Oracle instance used for the Tivoli Data Warehouse.

log_file
Specifies the name of the log file which the script uses to log the output of the upgrade script.

b. Wait for the database update process to complete and for the script to return to the command-line.

Enabling history collection

Some ITCAM Agent for WebSphere Applications workspaces require collection of historical data. You must enable historical collection by using a script on the Tivoli Enterprise Portal Server.

The kynHistoryConfigure.sh script is installed with the agent support files. It requires the IBM Tivoli Monitoring user interface component (tacmd command).

You must run the script after the support files have been installed.

You must run the script every time a node of one or more new affinity types is connected to the IBM Tivoli Monitoring infrastructure. A node represents an application server instance. The following affinity types are available:

- WebSphere Application Server (AFF_CAM_WAS_SERVER)

- WebSphere Portal Server (AFF_CAM_WAS_PORTAL_SERVER)
- WebSphere ESB Server (AFF_CAM_WAS_ESB_SERVER)
- IBM Business Process Server (AFF_CAM_WAS_PROCESS_SERVER)
- WebSphere Workplace Server (AFF_CAM_WAS_WORKPLACE_SERVER)

At least one server instance of the new affinity type must be running and connected to the IBM Tivoli Monitoring infrastructure when the script is started.

Run this script when the agents on the monitored servers are already configured and connected to the Tivoli Enterprise Monitoring Server. In this way, history is enabled for all of the affinity types that are used in the environment. If a new affinity type is added to the environment, run the script again.

To run the script, you must know the name of the Tivoli Enterprise Monitoring Server, as configured on the Tivoli Enterprise Portal Server. If agents for WebSphere Applications are connected to more than one Tivoli Enterprise Monitoring Server, you must run the script for each of the Tivoli Enterprise Monitoring Servers.

The script is located in the *ITM_home*/*architecture*/bin directory. Run it with the following command:

```
./kynHistoryConfigure.sh username password TEMS_name
```

Where:

username
: Name of a Tivoli Enterprise Portal user with administrative privileges (for example, SYSADMIN).

TEMS_name
: Name of the Tivoli Enterprise Monitoring Server

password
: Password as configured on the Tivoli Enterprise Portal Server.

Silent installation of the monitoring agent on Linux and UNIX systems

The installer support a *silent* mode. In this mode, no user interaction is required for an installation. Instead, the parameters are taken from a *response file*. You can install and uninstall the agent and install application support files.

Response files have a text format. You can create a response file based on one of the samples provided on the installation DVD or image.

You can also create a response file during the installation, modify it if necessary, and then use it for a silent installation. In this way, you can quickly reproduce similar installations many times, for example, on different hosts.

Performing a silent installation or uninstallation of the monitoring agent on Linux or UNIX

You can use the installer to install or uninstall the ITCAM Agent for WebSphere Applications monitoring agent and ITCAM Data Collector for WebSphere in silent mode. You can also install support files for the Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal client in silent mode. To do this, modify the sample files that are provided on the installation DVD or image. Then, run the installer from the command-line.

To complete a silent installation or uninstallation, first you must prepare the response file. Then, run the installer, supplying the name of the response file.

Preparing a response file for an ITCAM Agent for WebSphere Applications installation

To prepare a response file for installing the agent, complete the following procedure:

1. On the product installation DVD or image, in the top-level directory, locate the `silent_install.txt` file.
2. Make a copy of this file, and open it in a text editor.
3. Modify the following properties, if necessary. Do not modify any other properties.

Table 12. Agent installation response file properties

Response file property	Meaning
EncryptionKey	The 32-character encryption key used to secure password transmission and other sensitive data across your IBM Tivoli Monitoring environment. For more information, see *IBM Tivoli Monitoring: Installation and Setup Guide* for details about the encryption key.
INSTALL_FOR_PLATFORM	(Optional) The operating system for which to install the components, represented by an architecture code. If you do not specify an architecture code, the operating system for the current computer is used. You can find a list of the architecture codes for the supported architectures in `archdsc.tbl` in the registry directory; they are also listed, see Appendix D in the *IBM Tivoli Monitoring: Installation and Setup Guide*.
INSTALL_PRODUCT	The product code for the components (or "products") that you want to install. For a list of product codes for the base components, see Appendix D in the *IBM Tivoli Monitoring: Installation and Setup Guide*. You can use the **`./cinfo`** command to view the product codes for the applications installed on this computer. You can also find a list of the product codes in the registry directory in `proddsc.tbl`.
EP_RSP_FILE_YN	Specify the location of the ITCAM Data Collector for WebSphere silent response file, `silent_exit.txt`. For example, `/tmp/silent_exit.txt`. The location must be specified as an absolute path. The file `silent_exit.txt` must contain the `ITCAM_CONFIGHOME` parameter.

4. Save the edited copy in a work directory, for example, as `/tmp/silent.txt`.

Preparing a response file for an ITCAM Data Collector for WebSphere installation

To prepare a response file for installing ITCAM Data Collector for WebSphere, complete the following procedure:

1. On the product installation DVD or image, locate the `silent_exit.txt` file.
2. Make a copy of this file, and open it in a text editor.
3. Modify the following property:

Table 13. Data collector installation response file properties

Response file property	Meaning
ITCAM_CONFIGHOME	Specifies the location of the ITCAM Data Collector WebSphere home directory, for example `/opt/ibm/itm/dchome/7.2.0.0.1`. The location must be specified as an absolute path. The data collector home directory must already exist. Beginning with ITCAM Agent for WebSphere Applications version 7.2, ITCAM Data Collector for WebSphere is a shared component with the following products: • ITCAM for SOA 7.2 • ITCAM for WebSphere Application Server 7.2 support for WebSphere Application Server 8.5 • ITCAM Diagnostics Tool that is previewed in the ITCAM for Application Diagnostics beta If ITCAM Data Collector for WebSphere is installed at this location and is found to be of the same version, release, and maintenance level, it is not replaced. If ITCAM Data Collector for WebSphere is installed at this location and is found to be of a different version, release, and maintenance level, a new directory, `dc_version`, is created in the data collector home directory. For example, *DC_home*`/7.2.0.0.1`. The data collector is installed in this location.

4. Save the edited copy in a work directory, for example, as `/tmp/silent.txt`. The absolute path to this file must be the location referenced by the `EP_RSP_FILE_YN` parameter of the monitoring agent response file.

Running the installer in silent mode

After preparing the response file for your installation and uninstallation, run the installer, specifying the path and name for the response file. Complete the following procedure:

1. Change to the directory where the installation DVD or image is mounted.
2. Start `install.sh`:

   ```
   ./install.sh -q -h ITM_home -p response_file_name
   ```

   Where

   ITM_home
   : The destination directory where the agent is to be installed (by default it is `/opt/IBM/ITM`; you can use different destination directories to install several copies of the agent on the same host).

   response_file_name
   : The name of the response file that you prepared (with full path). For example:

   ```
   ./install.sh -q -h /opt/IBM/ITM -p /tmp/silent.txt
   ```

Important: If you are completing an upgrade and the monitoring agent is currently running, silent installation is aborted.

Performing a silent uninstallation

To uninstall ITCAM Agent for WebSphere Applications in silent mode, complete the following procedure:

1. Change to the *ITM_home*/bin directory.
2. Run the command:

   ```
   uninstall.sh -f yn platform_code
   ```

Important: If the ITCAM Data Collector for WebSphere home directory was specified to be outside of IBM Tivoli Monitoring home directory, the data collector home directory is not removed during the uninstallation.

You can find complete information about silent Tivoli Monitoring installation in "Appendix B. Performing a silent installation of IBM Tivoli Monitoring" of the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Configuring the monitoring agent in silent mode

You can use the configuration utility in silent mode to configure the ITCAM Agent for WebSphere Applications monitoring agent. To do this, prepare the response file by modifying a sample that was provided with the agent, or use a response file that was saved during interactive configuration.

The sample response file, `silent_config.txt`, is in the top-level directory on the installation DVD or image.

To complete a configuration task, you must prepare a response file, and then start the configuration utility. This is useful for large-scale deployments.

Preparing a response file

To prepare a response file for configuring the agent, complete the following procedure:

1. On the product installation DVD, in the top-level directory, locate the `silent_config.txt` file.
2. Make a copy of this file, and open it in a text editor.
3. Modify the follow properties, if necessary:

Table 14. Agent configuration response file properties

Response file property	Meaning
KYN_PORT	Specifies the port number of the TCP socket port that the monitoring agent uses to listen for connection requests from the data collectors. The default is 63335.
KYN_ALT_NODEID	Specifies an Alternative Node ID for identifying the agent. This identifier determines how the agent is displayed in the Tivoli Enterprise Portal navigator tree. The default is "Primary", used with the host name of the computer where the agent is installed is used.

4. Save the edited copy in a work directory, for example, as `/tmp/silent.txt`.

Running the Configuration utility in silent mode

After preparing the response file for a configuration task, run the configuration utility, specifying the path and name for the response file. Complete the following procedure:

1. Change to the *ITM_home*/bin directory.
2. Start the configuration utility as follows. Specify the parameters in the exact order shown:

   ```
   itmcmd config -A -p response_file_name yn
   ```

   Where *response_file_name* is the name of the response file that you prepared (with full path). For example:

   ```
   itmcmd config -A -p /tmp/silent.txt yn
   ```

Configuring the data collector in silent mode

The ITCAM Data Collector for WebSphere configuration utilities support a *silent* mode. In this mode, no user interaction is required for configuration. Instead, the parameters are taken from a *response file*.

The following table provides a description of the configuration tasks that can be performed in silent mode by the utilities.

Table 15. Configuration tasks

Configuration task	Where to find the procedure
Configure the data collector to monitor application server instances within a WebSphere Application Server profile in silent mode.	"Configuring ITCAM Data Collector for WebSphere in silent mode"
Unconfigure the data collector in silent mode.	"Unconfiguring ITCAM Data Collector for WebSphere in silent mode" on page 164
Migrate an older version of the data collector to ITCAM Data Collector for WebSphere in silent mode or update the maintenance level of ITCAM Data Collector for WebSphere in silent mode.	"Migrating ITCAM Data Collector for WebSphere in silent mode" on page 166
Migrate the WebSphere Application Server data collector provided by ITCAM for SOA version 7.1.1 to ITCAM Data Collector for WebSphere in silent mode.	"Migrating ITCAM for SOA 7.1.1 data collector to ITCAM Data Collector for WebSphere in silent mode" on page 169

Important: When you create or edit a silent response file that contains unicode characters, make sure the file is saved using UTF-8 encoding. If you save the file using a different encoding scheme, for example ISO-8858, an error is displayed during the configuration task that indicates that the utility was unable to access the file.

Configuring ITCAM Data Collector for WebSphere in silent mode

ITCAM Data Collector for WebSphere can be configured interactively with the ITCAM Data Collector for WebSphere Configuration utility. If you want to configure many application server instances, it might be more convenient to configure ITCAM Data Collector for WebSphere in silent mode.

Important: In an ITCAM for Application Diagnostics deployment, do not configure the data collector to monitor an instance of WebSphere Application

Server that hosts the Managing Server Visualization Engine (MSVE). However, you can use the data collector to monitor any other WebSphere Application Server instances that are on the same node.

When you configure the data collector in silent mode, you first specify configuration options in a properties file. A sample properties file, `sample_silent_config.txt`, is packaged with the ITCAM Data Collector for WebSphere Configuration utility. The file is available in *DC_home*`/bin`. The variable *DC_home* is the location where the data collector is installed. A sample of a properties file is presented in "Sample properties file" on page 162.

Complete the following steps to perform a silent configuration:

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

Properties file

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

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

  property
  : Name of property. The list of valid properties that you can configure is shown in Table 16.

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

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

Table 16 describes the properties that are available when configuring the data collector in silent mode:

Table 16. Available properties for running the configuration utility in silent mode

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

Table 16. Available properties for running the configuration utility in silent mode (continued)

Property	Comment
ms.am.home	Specifies the managing server home directory.
ms.am.socket.bindip	Specifies the IP address or host name to be used by the data collector to communicate with the managing server. If more than one network interface or IP address is configured on data collector computer system, choose one of them.
ms.firewall.enabled	Specifies whether a firewall is enabled on the data collector host or you have special requirements to change the RMI ports for the data collector. Valid values are `True` and `False`.
ms.probe.controller.rmi.port	If the data collector is behind a firewall or you have special requirements to change the Controller RMI port of data collector, set this port number range. Configure this port number as permitted by the firewall for the data collector host. For example: `ms.probe.controller.rmi.port=8300-8399` or `ms.probe.controller.rmi.port=8300`.
ms.probe.rmi.port	If the data collector is behind a firewall, or you have special requirements to change the RMI port of data collector, set this port number range. Configure this port number as permitted by the firewall for the data collector host. For example: `ms.probe.rmi.port=8200-8299` or `ms.probe.rmi.port=8200`.
Integration of the data collector with the ITCAM for Transactions	
ttapi.enable	Specifies whether the data collector communicates with ITCAM for Transactions using the Transaction Tracking API (TTAPI). Valid values are `True` and `False`.
ttapi.host	Specifies the host name of the ITCAM for Transactions Transaction Collector to connect to.
ttapi.port	Specifies the port of the Transaction Collector to connect to.
Integration of the data collector with the ITCAM for SOA	
soa.enable	Specifies whether to integrate the data collector with ITCAM for SOA. The ITCAM for SOA agent must be installed to complete the configuration.
Integration of the data collector with the Tivoli Performance Monitoring	
tpv.enable	Specifies whether to integrate the data collector with the Tivoli Performance Monitoring when the data collector is included as part of ITCAM for WebSphere Application Server version 8.5. Tivoli Performance Monitoring is accessed with the WebSphere Application Server administrative console. Valid values are `True` and `False`.
Integration of the data collector with the ITCAM Diagnostics Tool	
de.enable	Specifies whether to integrate the data collector with the ITCAM Diagnostics Tool that is previewed in the ITCAM for Application Diagnostics beta. The ITCAM Diagnostics Tool is a tool for diagnostic investigation of applications that are running on WebSphere Application Server. Valid values are `True` and `False`.
Integration of the data collector with the ITCAM Agent for WebSphere Applications monitoring agent	
temaconnect	Specifies whether the data collector connects to ITCAM Agent for WebSphere Applications monitoring agent. Valid values are `True` and `False`. Set this property to `False` if you plan to connect ITCAM Agent for WebSphere Applications with the managing server only or you do not have ITCAM Agent for WebSphere Applications installed and do not plan to install it.
tema.host	Specifies the fully qualified host name or IP address of the ITCAM Agent for WebSphere Applications monitoring agent.
tema.port	Specifies the port number of the ITCAM Agent for WebSphere Applications monitoring agent.

Table 16. Available properties for running the configuration utility in silent mode (continued)

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

Sample properties file

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

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

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

[DEFAULT SECTION]

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

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

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

#  ITCAM for SOA agent:
soa.enable=False

#  Tivoli Performance Viewer:
tpv.enable=True

#  ITCAM Diagnostics Tool:
de.enable=False

#  ITCAM Agent for WebSphere Applications monitoring agent:
temaconnect=True
```

```
tema.host=127.0.0.1
tema.port=63335

#  Create a backup of WebSphere Application Server:
was.backup.configuration=False
was.backup.configuration.dir=/opt/IBM/ITM/dchome/7.2.0.0.1

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

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

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

#  WebSphere Application Server details:
was.appserver.profile.name=AppSrv02
was.appserver.home=/opt/IBM/WebSphere/AppServer
was.appserver.cell.name=yourITCAMCell
was.appserver.node.name=yourITCAMNode

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

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

Unconfiguring ITCAM Data Collector for WebSphere in silent mode

ITCAM Data Collector for WebSphere can be unconfigured interactively with the ITCAM Data Collector for WebSphere Unconfiguration utility. If you want to unconfigure many application server instances, it might be more convenient to unconfigure ITCAM Data Collector for WebSphere in silent mode.

When you unconfigure the data collector in silent mode, you first specify configuration options in a properties file. A sample properties file, `sample_silent_unconfig.txt`, is packaged with the unconfiguration utility. The file is available in *DC_home*`/bin`.

The variable *DC_home* is the location where the data collector is installed. A sample of a properties file is presented in "Sample properties file" on page 166.

Complete the following steps to perform a silent unconfiguration:

1. Specify configuration options in the properties file.
2. Go to the *DC_home*`/bin` directory.
3. Run the command `unconfig.sh -silent [`*dir_path*`]/`*silent file*
4. After unconfiguring the data collector to monitor application server instances, you must restart the instances. The data collector configuration takes effect when the application server instances are restarted.

Properties file

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

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

  property
  This is the name of property. The list of valid properties that you can configure is shown in Table 17.

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

Table 17 describes the properties that are available when unconfiguring the data collector in silent mode:

Table 17. Available properties for running the unconfiguration utility in silent mode

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

Sample properties file

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

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

[DEFAULT SECTION]

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

#  WebSphere Application Server details:
was.appserver.profile.name=AppSrv02
was.appserver.home=/opt/IBM/WebSphere/AppServer
was.appserver.cell.name=yourITCAMCell
was.appserver.node.name=yourITCAMNode

#  Create a backup of WebSphere Application Server:
was.backup.configuration=False
was.backup.configuration.dir=/opt/IBM/ITM/dchome/7.2.0.0.1/data

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

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

Migrating ITCAM Data Collector for WebSphere in silent mode

A previous version or an earlier maintenance level of ITCAM Data Collector for WebSphere can be migrated interactively with the ITCAM Data Collector for WebSphere Migration utility. If you want to migrate many application server instances, it might be more convenient to migrate the application servers using the migration utility in silent mode.

To migrate ITCAM for SOA WebSphere Application Server version 7.1.1 using the migration utility in silent mode, see "Migrating ITCAM for SOA 7.1.1 data collector to ITCAM Data Collector for WebSphere in silent mode" on page 169.

When you migrate the data collector in silent mode, you first specify configuration options in a properties file. A sample properties file, `sample_silent_migrate.txt`, is

packaged with the migration utility. The file is available in *DC_home*/bin. A sample of a properties file is available in "Sample properties file" on page 168.

Complete the following steps to perform a silent migration:

1. Specify configuration options in the properties file.
2. Go to the *DC_home*/bin directory.
3. Run the command migrate.sh -silent [*dir_path*]/*silent_file*

During a silent migration, you can also configure or reconfigure integration with: ITCAM for SOA, ITCAM Agent for WebSphere Applications monitoring agent, ITCAM for Application Diagnostics Managing Server, ITCAM for WebSphere Application Server, and ITCAM Diagnostics Tool. Use the silent configuration parameters for these components, as described in Table 18.

Properties file

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

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

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

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

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

Table 18 describes the properties that are available when migrating the data collector in silent mode:

Table 18. Available properties for running the migration utility in silent mode

Property	Comment
default.hostip	If the computer system uses multiple IP addresses, specify the IP address for the data collector to use.
migrate.type	Type of agent whose data collector you want to migrate to ITCAM Data Collector for WebSphere. The value must be set to AD. **Important:** For all products, to update a maintenance level, set the migrate.type property to AD.
Location of data collector to be migrated	
itcam.migrate.home	Specifies the data collector home directory of the old version of the data collector. The directory is not deleted as part of the migration.
ITCAM Agent for WebSphere Applications monitoring agent settings	

Table 18. Available properties for running the migration utility in silent mode (continued)

Property	Comment
temaconnect	Specifies whether the data collector connects to the ITCAM Agent for WebSphere Applications monitoring agent. Set this property to `False` if you do not want to connect the ITCAM Agent for WebSphere Applications with the monitoring agent, if you plan to connect the ITCAM Agent for WebSphere Applications with the managing server only, or if you do not have the ITCAM Agent for WebSphere Applications installed. Valid values are `True` and `False`. **Remember:** The managing server is not a component of ITCAM for Applications.
tema.host	Specifies the fully qualified host name or IP address of the ITCAM for Agent for WebSphere Applications monitoring agent.
tema.port	Specifies the port number of the ITCAM for Agent for WebSphere Applications monitoring agent.
WebSphere Application Server connection settings	
was.wsadmin.connection.host	Specifies the name of the host to which the wsadmin tool is connecting. In a Network Deployment environment, specify the wsadmin connection to the Deployment Manger. In a stand-alone environment, specify the wsadmin connection to the server.
WebSphere Application Server global security settings	
was.wsadmin.username	Specifies the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server.
was.wsadmin.password	Specifies the password that corresponds to the user specified in the `was.wsadmin.username` property.
WebSphere Application Server settings	
was.appserver.profile.name	Specifies the name of the application server profile you want to configure.
was.appserver.home	Specifies the WebSphere Application Server home directory.
was.appserver.cell.name	Specifies the WebSphere Application Server cell name.
was.appserver.node.name	Specifies the WebSphere Application Server node name.
WebSphere Application Server runtime instance settings	
was.appserver.server.name	Specifies the application server instance within the application server profile to migrate to the new version of the data collector. **Tip:** The silent response file can have multiple instances of this property.

Sample properties file

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

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

```
#
#This file has 2 sections; [DEFAULT SECTION] and [SERVER].
#You can have one instance of [DEFAULT].
#You can have multiple instances of [SERVER].
#
#Use this sample file to migrate the data collector of any of the following products:
#  ITCAM for WebSphere 6.1 (fix pack 4 or later)
#  WebSphere Data Collector 6.1 (fix pack 4 or later)
#  ITCAM Agent for WebSphere Applications 7.1
#  ITCAM for WebSphere Application Server 7.2
#
#Considerations:
#IP address to use:
#Uncomment and specify an IP address to use, if the system has multiple IP addresses.
#
#Migration type:
#Important: Do not modify this value.
#
#Servers:
#You can migrate the data collector for multiple servers in the same profile.
#Uncomment the second [SERVER] and add the server name.
#Repeat for each additional server.
#
#
################################################################################

[DEFAULT SECTION]

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

#Migration type:
migrate.type=AD

#  Old data collector home directory:
itcam.migrate.home=/opt/IBM/ITM/tmaitm6/wsdc/71

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

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

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

#Note: As of now, was.appserver.server.name is the only supported parameter in this section
[SERVER]
was.appserver.server.name=server1


#Note: As of now, was.appserver.server.name is the only supported parameter in this section
##[SERVER]
#was.appserver.server.name=server2
```

Migrating ITCAM for SOA 7.1.1 data collector to ITCAM Data Collector for WebSphere in silent mode

The ITCAM for SOA version 7.1.1 WebSphere Application Server data collector can be migrated to ITCAM Data Collector for WebSphere interactively with the ITCAM Data Collector for WebSphere Migration utility. If you want to migrate many

application server instances, it might be more convenient to migrate the application servers using the migration utility in silent mode.

For the procedure for migrating the following data collector components to ITCAM Data Collector for WebSphere, see "Migrating ITCAM Data Collector for WebSphere in silent mode" on page 166:

- ITCAM for WebSphere version 6.1.0.4 or later
- WebSphere Data Collector version 6.1.0.4 or later included in ITCAM for Web Resources version 6.2.0.4 or later
- ITCAM Agent for WebSphere Applications version 7.1 included in ITCAM for Applications Diagnostics version 7.1
- ITCAM for WebSphere Application Server version 7.2

The procedure in "Migrating ITCAM Data Collector for WebSphere in silent mode" on page 166 can also be followed to update the maintenance level of any products, including ITCAM for SOA, that have ITCAM Data Collector for WebSphere as a component.

Important: If an older version of ITCAM Agent for WebSphere Applications is configured for application servers in the same profile as ITCAM for SOA version 7.1.1, migrate the data collector provided with ITCAM Agent for WebSphere Applications. Then, reconfigure the data collector to integrate it with the ITCAM for SOA monitoring agent. You must not run the migration utility to migrate the older version of the ITCAM for SOA WebSphere Application Server data collector.

When you migrate the ITCAM for SOA version 7.1.1 data collector in silent mode, you first specify configuration options in a properties file. A sample properties file, `sample_silent_migrate_soa.txt`, is packaged with the migration utility. The file is available in *DC_home*`/bin`. A sample of a properties file is presented in "Sample properties file" on page 172.

Complete the following steps to perform a silent migration:

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

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

While you are performing a silent migration, you can also configure or reconfigure integration with ITCAM for SOA, ITCAM Agent for WebSphere Applications monitoring agent, ITCAM for Application Diagnostics Managing Server, Tivoli Performance Viewer, and the ITCAM Diagnostics Tool for the application server instances at the same time. To do this, use the silent configuration parameters for these components, as described in . Table 19 on page 171.

Properties file

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

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

property
This is the name of property. The list of valid properties that you can configure is shown in: Table 19.

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

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

Table 19 describes the properties that are available when migrating the data collector in silent mode:

Table 19. Available properties for running the migration utility in silent mode

Property	Comment
default.hostip	If the computer system uses multiple IP addresses, specify the IP address for the data collector to use.
migrate.type	Type of agent whose agent you want to migrate to ITCAM Data Collector for WebSphere. The value must be set to `SOA`.
was.appserver.home	Location of the WebSphere Application Server home directory where the ITCAM for SOA version 7.1.1 data collector is configured. For example: `/opt/IBM/WebSphere70/AppServer`
ms.connect	Specifies whether the data collector is configured to connect to the managing server in an ITCAM for Application Diagnostics environment. For a migration from ITCAM for SOA version 7.1.1, ignore this parameter.
ttapi.enable	Specifies whether the data collector communicates with ITCAM for Transactions using the Transaction Tracking API (TTAPI). Valid values are *True* and *False*.
soa.enable	Specifies whether to integrate the data collector with ITCAM for SOA. The ITCAM for SOA agent must be installed to complete the configuration.
tpv.enable	Specifies whether to integrate the data collector with the Tivoli Performance Viewer when the data collector is included as part of ITCAM for WebSphere Application Server 8.5. Tivoli Performance Viewer is accessed with the WebSphere Application Server administrative console. For a migration from ITCAM for SOA 7.1.1, ignore this parameter.
de.enable	Specifies whether to integrate the data collector with the ITCAM Diagnostics Tool previewed in the ITCAM for Application Diagnostics beta. The ITCAM Diagnostics Tool is an Eclipse-based tool for diagnostic investigation of applications that are running on WebSphere Application Server. For a migration from ITCAM for SOA version 7.1.1, ignore this parameter.

Table 19. Available properties for running the migration utility in silent mode (continued)

Property	Comment
temaconnect	Specifies whether the data collector connects to the ITCAM Agent for WebSphere Applications monitoring agent. For a migration from ITCAM for SOA version 7.1.1 where the data collector is not being integrated with another product, ignore this parameter.
was.backup.configuration	Specifies whether to back up the current configuration of the WebSphere Application Server configuration before applying the new configuration. Valid values are *True* and *False*.
was.gc.custom.path	Specifies the path to the custom Garbage Collection log. For a migration from ITCAM for SOA version 7.1.1, ignore this parameter.
WebSphere Application Server connection settings	
was.wsadmin.connection.host	Specifies the name of the host to which the wsadmin tool is connecting. In a Network Deployment environment, specify the wsadmin connection to the Deployment Manger. In a stand-alone environment, specify the wsadmin connection to the server.
was.wsadmin.connection.type	Specifies the connection protocol for the wsadmin tool to use.
was.wsadmin.connection.port	Specifies the port that the wsadmin tool must use to connect to the WebSphere Application Server.
WebSphere Application Server global security settings	
was.wsadmin.username	Specifies the user ID of a user who is authorized to log on to the IBM WebSphere Application Server administrative console. This user must have the agent role on the application server.
was.wsadmin.password	Specifies the password that corresponds to the user specified in the `was.wsadmin.username` property.
WebSphere Application Server settings	
was.appserver.profile.name	Specifies the name of the application server profile you want to configure.
was.appserver.cell.name	Specifies the WebSphere Application Server cell name.
was.appserver.node.name	Specifies the WebSphere Application Server node name.
WebSphere Application Server runtime instance settings	
was.appserver.server.name	Specifies the application server instance within the application server profile to configure. **Important:** The silent response file can have multiple instances of this property.

Sample properties file

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

```
################################################################################
#
#Comments:
#Locate the ITCAM Data Collector for WebSphere Migration Utility (migrate.sh|bat) in
<dc_home>/bin.
#Run migrate.sh|bat -silent [dir_path]/<properties_file> to migrate an older version of the
data collector silently.
```

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


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

#  Migration type:
migrate.type=SOA

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

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

#  ITCAM for Transactions:
ttapi.enable=False

#  ITCAM for SOA agent:
soa.enable=True

#  Tivoli Performance Viewer:
tpv.enable=False

#  ITCAM Diagnostics Tool:
de.enable=False

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

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

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

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

#  WebSphere Application Server details:
was.appserver.profile.name=AppSrv01
```

```
was.appserver.cell.name=yourITCAMCell
was.appserver.node.name=yourITCAMNode

#Note: As of now, was.appserver.server.name is the only supported parameter in this section
[SERVER]
was.appserver.server.name=server1

#Note: As of now, was.appserver.server.name is the only supported parameter in this section
#[SERVER]
#was.appserver.server.name=server2
```

Additional steps for configuring the data collector on Linux and UNIX systems

For every application server instance where the data collector was configured, complete the following steps, as applicable.

Generating your own .jks key files and trust files

This product provides default Secure Socket Layer (SSL) certificates so that you can set up a secure environment without customization. These .jks files are for test purposes only and expire shortly after deployment. These files are not recommended for use in a production environment. For more information about setting up SSL, see Appendix A, "Setting up a secure connection to the Managing Server," on page 275.

If you used the root ID for the data collector installation and the application server is not owned and operated by the root ID

The installer can use whatever directories and files it requires. In addition, the installer can find most application server installations on the computer. But, if the application server is not owned and operated by root ID, you must complete the following tasks for the data collector to work correctly:

1. Use the chown command to change ownership of the data collector installation from root to the application server owner ID:

   ```
   chown -R wasOwnerId:wasGroupId DC_home
   ```

2. Make sure that the application server owner ID can write to the `DC_home/logs/CYN` directory:

   ```
   chown -R wasOwnerId:wasGroupId /opt/IBM/ITM/dchome/7.2.0.0.1/logs/CYN
   ```

Connecting to an ITCAM for SOA 7.1.1 monitoring agent

When you integrate ITCAM Data Collector for WebSphere with ITCAM for SOA for applications servers within a profile where ITCAM for SOA is not already installed and configured, and you later install ITCAM for SOA 7.1.1, you must add additional properties to the `KD4.dc.properties` file.

To add the additional properties to the `KD4.dc.properties` file, complete the following steps:

1. Navigate to the *ITCAM4SOA_Home*`/KD4/config` directory.
2. Add the following properties to the `KD4.dc.properties` file with any text editor:

```
1.server_instance.monitor=on
1.server_instance.log=info
1.server_instance.trace=off
1.server_instance.monitor.control.count=1
1.server_instance.monitor.control.1=*;*;*;*;*;none
1.server_instance.filter.control.count=0
```

3. Save the file.

Displaying data in ITCAM for SOA topology views

When you configure data collection for applications servers for ITCAM Agent for WebSphere Applications, data collection might be configured for ITCAM for SOA version 7.2 for application servers in the same profile. You must reconfigure and restart the Tivoli Enterprise Portal Server to capture ITCAM Agent for WebSphere Applications data in the topology views of ITCAM for SOA.

After you integrate the data collector with the ITCAM Agent for WebSphere Applications monitoring agent, complete the following steps:

1. Wait until at least one of the application servers that you are monitoring processes transaction data.
2. Rebuild the Tivoli Enterprise Portal Server on Linux or AIX systems or reconfigure the Tivoli Enterprise Portal Server on Windows systems.
3. Restart the Tivoli Enterprise Portal Server.

For more information about reconfiguring and restarting the Tivoli Enterprise Portal Server, see the *IBM Tivoli Composite Application Manager for SOA Installation Guide*.

Completing and verifying data collector configuration

To finish and verify the configuration of the data collector for an application server instance, complete the following steps:

1. If any of the following problems occur, you know that the data collector configuration has failed:
   - After the configuration, the application server fails to restart.
   - During a silent configuration, the displayed text indicates that the configuration failed.
   - After the configuration, messages in the Tivoli common log file indicate that configuration failed.

   If the data collector configuration has failed:
   - Restore the application server configuration that you had before you attempted the failed configuration. For more information, see “Restoring the application server configuration from a backup” on page 321.
   - Run the command line or silent configuration again.
   - If the configuration fails repeatedly, contact IBM Support. If directed by IBM Support, configure the application server instance manually; see “Manually configuring the data collector to monitor an application server instance” on page 323.
2. If you use the IBM Tivoli Monitoring infrastructure, start a Tivoli Enterprise Portal client and verify that you can see monitored data for the application server instance.
3. If you use the ITCAM for Application Diagnostics Managing Server infrastructure, access the visualization engine and verify that you can see monitored data for the application server instance.

Uninstalling ITCAM Agent for WebSphere Applications on Linux and UNIX systems

To remove ITCAM Agent for WebSphere Applications on UNIX and Linux systems, complete these steps:

1. Unconfigure the data collector from all of the application server instances.

   For more information, see "Unconfiguring ITCAM Data Collector for WebSphere" on page 129.
2. To change to the appropriate `/bin` directory, from a command line, run the following command:

   ```
   cd ITM_home/bin
   ```
3. Run the following command:

   ```
   ./uninstall.sh
   ```

   A numbered list of product codes, architecture codes, version and release numbers, and product titles is displayed for all installed products.
4. Type the number for the monitoring agent. Repeat this step for each additional installed product that you want to uninstall.

Important: If the home directory of ITCAM Data Collector for WebSphere was specified to be outside of the IBM Tivoli Monitoring home directory, the data collector home directory is not removed during the uninstallation and must be removed manually.

Installing and uninstalling a language pack on Linux and UNIX systems

A language pack allows users to interact with the agent in a language other than English. For example, when a Spanish language pack is installed, the Tivoli Enterprise Portal workspaces and the internal messages of the agent are displayed in Spanish.

To enable full support for a language, you must install the language pack on the agent host and all hosts where the Tivoli monitoring support files for the agent are installed (hub Tivoli Enterprise Monitoring Servers, all Tivoli Enterprise Portal Servers, and all Tivoli Enterprise Portal desktop clients).

If you no longer want to use a language, uninstall the language pack for it.

Before you install or uninstall a language pack, ensure that:

- The agent and the Tivoli Enterprise Portal support files are installed.
- The Java runtime environment (JRE) is available on every host where you are planning to install the language pack. (The JRE is required by IBM Tivoli Monitoring).
- You know the installation directories (*ITM_home*) for the agent and all other Tivoli monitoring components on which you plan to install the agent. The default installation directory is `/opt/IBM/ITM`.

Installing a language pack on Linux and UNIX systems

To install a language pack on Linux and UNIX systems, you must use the installer on the language pack DVD. The procedure is the same on the agent host, hub Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal desktop client.

Complete the following procedure:

1. Mount the language pack DVD. Make sure that the full path to the mount directory does not include spaces.
2. To start the installer from the 7.2 folder on the language pack DVD, use the following commands:

   ```
   cd dir_name
   ./lpinstaller.sh -c ITM_home
   ```

3. Select the language of the installer and click **OK**.

   Important: In this step, you select the language for the installer user interface, not the language pack that is to be installed.
4. On the introduction window, click **Next**.
5. Select **Add/Update** and click **Next**.
6. Select the directory where the National Language Support package (NLSPackage) files are located. This is the `nlspackage` directory on the language pack DVD.
7. Select language support for **ITCAM Agent for WebSphere Applications** and click **Next**.
8. Select the languages to install and click **Next**.

   Tip: You can hold down the **Ctrl** key for multiple selections.
9. Examine the installation summary page. To begin installation, click **Next**.
10. Click **Next**.
11. Click **Finish** to exit the installer.
12. If you are installing the language pack on a Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, or Tivoli Enterprise Portal desktop client, start the **Manage Tivoli Monitoring Services** utility, and use it to restart the server or client. If the Eclipse Help Server is running, restart it as well.

Uninstalling a language pack on Linux and UNIX systems

To uninstall a language pack on Linux and UNIX systems, you must use the installer on the language pack DVD. The procedure is the same on the agent host, hub Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal desktop client.

Complete the following procedure:

1. Mount the language pack DVD. Make sure that the full path to the mount directory does not include spaces.
2. To start the installer from the 7.2 folder on the language pack DVD, use the following commands:

   ```
   cd dir_name
   ./lpinstaller.sh -c ITM_home
   ```

3. Select the language of the installer and click **OK**.

   Important: In this step, you select the language for the installer user interface, not the language pack that is to be installed.
4. On the introduction window, click **Next**.
5. Select **Remove** and click **Next**.
6. Select **ITCAM Agent for WebSphere Applications**.
7. Select the languages to uninstall and click **Next**.

Tip: You can hold down the **Ctrl** key for multiple selections.

8. Examine the installation summary page. To begin the installation, click **Next**.
9. Click **Next**.
10. To exit the installer, click **Finish**.
11. If you are uninstalling a language pack from Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, or Tivoli Enterprise Portal desktop client, start the **Manage Tivoli Monitoring Services** utility, and use it to restart the server or client. If the Eclipse Help Server is running, restart it as well.

Part 4. Installing and configuring the Agent on WebSphere Application Server Hypervisor Edition

Chapter 6. Installing and configuring the agent on WebSphere Application Server Hypervisor Edition

On WebSphere Application Server Hypervisor Edition in the VMWare ESX environment, you can install ITCAM Agent for WebSphere Applications on the initial image. Then, when a server is instantiated from the copy of the image, you can configure the agent within the server configuration.

To use ITCAM Agent for WebSphere Applications on WebSphere Application Server Hypervisor Edition in VMWare ESX, complete the following procedures:

1. Create a WebSphere Application Server Hypervisor Edition image and install ITCAM Agent for WebSphere Applications on it. For more information, see "Installing ITCAM Agent for WebSphere Applications on a WebSphere Application Server Hypervisor Edition image."
2. When creating an instance of the server, do the following tasks if the situation applies:
   - If you use interactive configuration, configure ITCAM Agent for WebSphere Applications. For more information, see "Configuring ITCAM Agent for WebSphere Applications on an image in interactive mode" on page 183.
   - If you use silent configuration, edit the silent configuration parameters file to include ITCAM Agent for WebSphere Applications data. For more information, see "Configuring ITCAM Agent for WebSphere Applications on an image in silent mode" on page 185.

Installing ITCAM Agent for WebSphere Applications on a WebSphere Application Server Hypervisor Edition image

You can install ITCAM Agent for WebSphere Applications on a WebSphere Application Server Hypervisor Edition image. Then, when you create servers from this image, the agent is installed on them automatically. After configuration within the standard WebSphere Application Server Hypervisor Edition process, the servers are monitored by the agent immediately.

Procedure

1. Create a WebSphere Application Server Hypervisor Edition image. For more information about creating an image, see the "Installing virtual images for VMware ESX" section in the WebSphere Application Server Hypervisor Edition information center.
2. Start the virtual machine with this image.
3. Enter the default login and password (root/password).
4. Select the default language and press F10.
5. Accept licenses, and choose the network protocol and parameters.
6. Enter new root and virtuser passwords. Then, the WebSphere Application Server Hypervisor Edition Configuration is started.
7. In **Environment type**, select **None** to bypass the configuration of the WebSphere Application Server.
8. With an SSH client or an X Window System, connect to the virtual server host using the network parameters specified in step 5 and open a console.
9. Create a directory on the virtual host.

10. Upload the ITCAM Agent for WebSphere Applications Linux x86 version 7.2 installation image into the directory that was specified in step 9 on page 181. You can download this image from IBM Passport Advantage®. Use the package language of your choice.
11. Change to the directory specified in step 9 on page 181, and unzip the image.
12. Extract the Hypervisor bootstrap elements from the installation tar file by running the following command:

    ```
    tar xf installation_tar_file hypervisor silent*
    ```

13. In the sample response file, `silent_install.txt`, specify the location of the data collector silent response file in the property `EP_RSP_FILE_YN`. For example:

    ```
    EP_RSP_FILE_YN=path_to_dc_silent/silent_exit.txt
    ```

    The property `EP_RSP_FILE_YN` is commented out by default.
14. In the sample response file for the data collector, `silent_exit.txt`, specify the data collector installation directory in the property `ITCAM_CONFIGHOME` and specify the version and maintenance level of the data collector in the property `ITCAM_VERSION`. For example:

    ```
    ITCAM_CONFIGHOME=/opt/IBM/ITM/dchome/7.2.0.0.1
    ITCAM_VERSION=7.2.0.0.1
    ```

    The properties `ITCAM_CONFIGHOME` and `ITCAM_VERSION` are commented out by default.
15. From the directory, run the following installation script: `hypervisor/installITCAMforHypervisor.sh`. Specify the name of the agent version 7.2 installation image as a parameter. For example:

    ```
    ./hypervisor/installITCAMforHypervisor.sh ../installation_tar_file
    ```

16. When prompted, enter the name of the IBM Tivoli Monitoring home directory.

    ```
    Enter the name of the IBM Tivoli Monitoring Directory
    [ default = /opt/IBM/ITM ]:
    /opt/IBM/ITM
    ```

17. The installer presents the progress of the installation. For example:

    ```
    Extracting ynv720-201208152100.xlinux.tar.
    Installing ...

    Preparing ITCAM for Hypervisor environment.

    Done.

    You can change the default configuration parameters stored in the
    /opt/IBM/ITM/hypervisor/*.properties
    ```

18. When the installation is complete, review and edit the default configuration settings for the agent, as required. The setting files are located in the *ITM_home*`/hypervisor` directory:
    - `yn.properties`: settings for the monitoring agent
    - `wasdc.properties`: settings for the data collector

    All settings are explained in the comments within the files.
19. Using the script provided by WebSphere Application Server Hypervisor Edition image, reset the virtual machine:

    ```
    /var/adm/ibmvmcoc-postinstall/resetvm.sh -notools -resetip
    ```

    This command closes the virtual machine and makes the image a template.

Results

You created a master image of WebSphere Application Server Hypervisor Edition, with ITCAM Agent for WebSphere Applications installed. You can create virtual servers by copying and configuring this image. These servers are monitored by the agent.

Configuring ITCAM Agent for WebSphere Applications on an image in interactive mode

If you use interactive configuration to create a virtual server based on the WebSphere Application Server Hypervisor Edition template image, configure the monitoring agent and data collector by replying to additional prompts within the interactive configuration process.

About this task

You must install and configure ITCAM Agent for WebSphere Applications manually on the template image before you create the server. For more information, see "Installing ITCAM Agent for WebSphere Applications on a WebSphere Application Server Hypervisor Edition image" on page 181.

If no ISO image with a silent activation file (`ovf-env.xml`) is connected to the virtual machine during its first startup, interactive console configuration starts.

Procedure

1. Start the virtual machine.
2. Enter the default login and password (root/password).
3. Select the default language and press F10.
4. Accept licenses, set the network parameters for the virtual server, and enter the new root and virtuser passwords. For more information about passwords, see the WebSphere Application Server Hypervisor Edition documentation, in the chapter describing configuration. Then, prompts for configuring ITCAM Agent for WebSphere Applications are displayed, under the heading **IBM Tivoli Composite Application Manager for Application Diagnostics**.
5. In the **Protocol** prompt, set the protocol for communication with the Tivoli Enterprise Monitoring Server (IP.PIPE, IP.SPIPE, or IP.UDP),
6. In the **Protocol-specific** prompt, set the host name and port number for the Tivoli Enterprise Monitoring Server.
7. In the **Configure Tivoli Enterprise Monitoring Agent?** prompt, optionally change the node ID for this server and the port number for communication with the data collector. The node ID determines how the agent is displayed in the Tivoli Enterprise Portal navigation tree. The default is Primary, used with the host name of the computer where the agent is installed.
8. In the **Configure communication to Managing Server?** prompt, select whether the data collector connects to an ITCAM for Application Diagnostics Managing Server.

   Important: If you have an ITCAM for Application Diagnostics 7.1.0.3 installation in your environment, you can integrate the data collector with the ITCAM for Application Diagnostics Managing Server.
   If you select **Yes**, do the following tasks:

a. In the **Agent configuration for the Managing Server** prompt, set the parameters for communication with the managing server:
   - The fully qualified host name for the managing server (its kernel component).
   - The Codebase port set on the managing server.
   - The managing server home directory.

     Important: Double any backslash (\) characters for Windows systems, for example, `C:\\IBM\\MS`.
   - The host name or IP address for the data collector. By default, this is the host name for the virtual server. You can edit it to use the IP address or an alternative host name that is configured on the same server.
   - The port range that can be used for the RMI port of the data collector. If some of the ports are not available, for example, if the virtual server is behind a firewall, you might have to change the port range.
   - The port range that can be used for the Controller RMI port of the data collector. If some of the ports are not available, for example, if the virtual server is behind a firewall, you might have to change the port range.

9. In the **Configure ITCAM for SOA agent?** prompt, select whether the data collector communicates with ITCAM for SOA monitoring agent. To integrate the data collector with the ITCAM for SOA monitoring agent, select **Yes**. Otherwise, select **No**. You must install and configure the ITCAM for SOA agent manually. For more information about installing and configuring the ITCAM for SOA agent, see *IBM Tivoli Composite Application Manager for SOA Installation Guide*.
10. In the **Configure Tivoli Performance Viewer?** prompt, select whether the agent communicates with Tivoli Performance Viewer. To integrate the data collector with the Tivoli Performance Viewer, select **Yes**. Otherwise, select **No**. ITCAM for WebSphere Application Server version 7.2 can be used to monitor the performance of the WebSphere Application Server. Performance monitoring infrastructure (PMI) metrics are gathered using ITCAM Data Collector for WebSphere and are displayed in the Tivoli Performance Viewer (TPV). The TPV is accessible from the WebSphere Application Server administrative console. For information about using ITCAM for WebSphere Application Server, see *IBM Tivoli Composite Application Manager for WebSphere Application Server version 7.2 Support for WebSphere Application Server version 8.5 Installation and User Guide*.
11. In the **Configure ITCAM Diagnostics Tool?** prompt, select whether the data collector communicates with the ITCAM Diagnostics Tool that is previewed in the ITCAM for Application Diagnostics beta. To integrate the data collector with the ITCAM Diagnostics Tool, select **Yes**. Otherwise, select **No**. ITCAM Diagnostics Tool is built on Eclipse. The tool is used for diagnostic investigation of applications that are running on the WebSphere Application Server. Using this tool, you can analyze data in real time or you can save diagnostic information to a file for later analysis. For information about using the ITCAM Diagnostics Tool, see *ITCAM Diagnostic Tool Installation Guide*.
12. In the **Configure integration with ITCAM for Transactions?** prompt, select whether the data collector communicates with ITCAM for Transactions using Transaction Tracking API (TTAPI). If you select **Yes**, do the following tasks:
    a. In the **Agent configuration for integration with ITCAM for Transactions** prompt, set the host name and port of the Transaction Collector that the agent is to communicate with. To integrate the data collector with ITCAM

for Transactions, you must install ITCAM for Transactions version 7.3 or later within an IBM Tivoli Monitoring environment.

Otherwise, select **No**.

13. In the **Garbage Collection (GC) configuration** prompt, choose **Custom** to modify the garbage collection settings. Otherwise, choose **Default** to accept the default parameter settings for garbage collection and skip to step 15.
14. Specify the absolute path to the garbage collection log. The full path to the garbage collection log must exist. The server name, cell name, and node name are appended to the garbage collection log file name.
15. If WebSphere Global Security is enabled, for each profile that is configured on the server, in the **Use the user name and password in *.client.props** prompt, select whether to use the logon credentials that are saved in properties files. WebSphere Application Server Hypervisor Edition configuration saves the correct credentials in these files automatically. Unless you have special requirements, select **Yes**.
16. If you selected **No** in step 15, enter the administrative user name and password for the profile:
    a. In the **Input user name** prompt, enter the user name.
    b. In the **Input password** prompt, enter the password.
    c. In the **Verify password** prompt, enter the same password again.
17. In the **Confirm** prompt, review the configuration information. If it is correct, select **Yes** to complete the configuration process. Otherwise, select **No** to enter the configuration information again.

Results

You configured a single virtual machine with WebSphere Application Server that is running and available for use. The server is monitored by ITCAM Agent for WebSphere Applications.

Configuring ITCAM Agent for WebSphere Applications on an image in silent mode

If you use silent configuration to create a virtual server based on the WebSphere Application Server Hypervisor Edition template image, configure the agent within the silent configuration process.

About this task

You must install ITCAM Agent for WebSphere Applications on the template image before you create the server. For more information, see “Installing ITCAM Agent for WebSphere Applications on a WebSphere Application Server Hypervisor Edition image” on page 181.

Procedure

1. Prepare the silent activation file (`ovf-env.xml`) for WebSphere Application Server Hypervisor Edition, as described in the WebSphere Application Server Hypervisor Edition documentation. The documentation is available in the WebSphere Application Server Hypervisor Edition version 8.0. To find information about the silent configuration procedure, search for “Silently installing WebSphere Application Server Hypervisor Edition”. To find the format of the `ovf-env.xml` file, search for "ovf-env.xml".

2. Add configuration parameters to the ovf-env.xml file. All parameters are optional; if any parameter is not present, the values from *ITM_home*/hypervisor/yn.properties and *ITM_home*/hypervisor/wasdc.properties are used. The parameters for ovf-env.xml are described in Table 20. Sample configuration XML code is provided in with the image in the file hypervisor/samples/ovf_env.xml.

Table 20. Silent configuration parameters for ITCAM Agent for WebSphere Applications.

Property	Valid values	Description
Primary Tivoli Enterprise Monitoring Server configuration		
<Property ovfenv:key="ConfigITCAM.CMSCONNECT" ovfenv:value="yes"/>	yes or no	Specify whether the agent connects to a Tivoli Enterprise Monitoring Server. Set to no for deep-dive-only configuration.
<Property ovfenv:key="ConfigITCAM.FIREWALL" ovfenv:value="no"/>	yes or no	Specify whether the agent must cross a firewall to connect to Tivoli Enterprise Monitoring Server. If set to yes, NETWORKPROTOCOL must be set to ip.pipe.
<Property ovfenv:key="ConfigITCAM.NETWORKPROTOCOL" ovfenv:value="ip.pipe"/>	ip, sna,ip.pipe, or ip.spipe	The method to use for communication with the Tivoli Enterprise Monitoring Server. **Tip:** Use ip for UDP communication.
<Property ovfenv:key="ConfigITCAM.IPPIPEPORTNUMBER" ovfenv:value="1918"/>	Any valid IP port number.	Tivoli Enterprise Monitoring Server IP port number. Used for ip.pipe.
<Property ovfenv:key="ConfigITCAM.IPSPIPEPORTNUMBER" ovfenv:value="3660"/>	Any valid IP port number.	IP Port number. Used for ip.spipe.
<Property ovfenv:key="ConfigITCAM.HOSTNAME" ovfenv:value="gd-119.ibm.ti"/>	Any valid IP address or host name.	The host name or IP address of the Tivoli Enterprise Monitoring Server to connect to. Used for ip.
<Property ovfenv:key="ConfigITCAM.PORTNUMBER" ovfenv:value="1918"/>	Any valid IP port number.	IP Port number. Used for ip.
<Property ovfenv:key="ConfigITCAM.BK1NETWORKPROTOCOL" ovfenv:value="none"/>	ip, sna,ip.pipe, ip.spipe, or none	The first backup network protocol used for connecting to the Tivoli Enterprise Monitoring Server.

Table 20. Silent configuration parameters for ITCAM Agent for WebSphere Applications. (continued)

Property	Valid values	Description
<Property ovfenv:key="ConfigITCAM.BK2NETWORKPROTOCOL" ovfenv:value="none"/>	ip, sna,ip.pipe, ip.spipe, or none	The second backup network protocol used for connecting to the Tivoli Enterprise Monitoring Server.
<Property ovfenv:key="ConfigITCAM.KDC_PARTITIONNAME" ovfenv:value="null"/>	Any valid partition name.	The ip.pipe partition name.
<Property ovfenv:key="ConfigITCAM.KDC_PARTITIONFILE" ovfenv:value="null"/>	Any valid partition file name.	The partition file. The file enables the agent to connect to the monitoring server through a firewall.
Secondary Tivoli Enterprise Monitoring Server configuration		
<Property ovfenv:key="ConfigITCAM.FTO" ovfenv:value="no"/>	yes or no	Specify whether the agent connects to a secondary Tivoli Enterprise Monitoring Server. Set to no for deep-dive-only configuration.
<Property ovfenv:key="ConfigITCAM.MIRROR" ovfenv:value="tems.mirror.domain.com"/>	Any valid IP address or host name.	The host name or IP address of the secondary Tivoli Enterprise Monitoring Server to connect to. This parameter is required if ConfigITCAM.FTO is set to yes.
<Property ovfenv:key="ConfigITCAM.FIREWALL2" ovfenv:value="no"/>	yes or no	Specify whether the agent must cross a firewall to connect to the secondary Tivoli Enterprise Monitoring Server.
<Property ovfenv:key="ConfigITCAM.HSNETWORKPROTOCOL" ovfenv:value="ip.pipe"/>	ip, sna, or ip.pipe	The method to use for communication with the secondary Tivoli Enterprise Monitoring Server.
<Property ovfenv:key="ConfigITCAM. BK1HSNETWORKPROTOCOL" ovfenv:value="none"/>	ip, sna,ip.pipe, or none	The first backup network protocol used for connecting to the secondary Tivoli Enterprise Monitoring Server.
<Property ovfenv:key="ConfigITCAM. BK2HSNETWORKPROTOCOL" ovfenv:value="none"/>	ip, sna,ip.pipe, or none	The second backup network protocol used for connecting to the secondary Tivoli Enterprise Monitoring Server.

Table 20. Silent configuration parameters for ITCAM Agent for WebSphere Applications. (continued)

Property	Valid values	Description
`<Property ovfenv:key="ConfigITCAM. HSIPPIPEPORTNUMBER" ovfenv:value="1918"/>`	Any valid IP port number.	IP port number for secondary Tivoli Enterprise Monitoring Server. Used for ip.pipe.
`<Property ovfenv:key="ConfigITCAM. HSPORTNUMBER" ovfenv:value="1918"/>`	Any valid IP port number.	IP port number for secondary Tivoli Enterprise Monitoring Server. Used for ip. A port number and or one or more pools of port numbers can be specified. The format for a pool is `#-#` with no embedded blanks.
Optional Primary Network Name configuration		
`<Property ovfenv:key="ConfigITCAM. PRIMARYIP" ovfenv:value="none"/>`	Any valid IP port number.	If the system is equipped with dual network host adapter cards, you can designate the primary network name.
Monitoring Agent configuration		
`<Property ovfenv:key="ConfigITCAM.KYN_ALT_NODEID" ovfenv:value="Primary"/>`	String, up to 24 characters in length.	Alternative Node ID for identifying this agent. This identifier determines how the agent is displayed in the Tivoli Enterprise Portal navigation tree. The default is "Primary", used with the host name of the computer where the agent is installed. **Important:** If you install more than one copy of the monitoring agent on a single host, you must set the Alternative Node ID parameter to different values for each of the copies. Otherwise, the multiple copies of the monitoring agent do not work correctly with Tivoli Monitoring.
`<Property ovfenv:key="ConfigITCAM.KYN_PORT" ovfenv:value="63335"/>`	Any valid IP port number.	Monitoring agent listening port for communication with the data collector.
ITCAM for Application Diagnostics Managing Server Configuration		

Table 20. Silent configuration parameters for ITCAM Agent for WebSphere Applications. (continued)

Property	Valid values	Description
`<Property ovfenv:key="ConfigITCAM.ITCAM_MSCONNECT" ovfenv:value="True"/>`	`True` or `False`	Specify whether the agent connects to an ITCAM for Application Diagnostics Managing Server. Set to `False` for an IBM Tivoli Monitoring only configuration.
`<Property ovfenv:key="ConfigITCAM.ITCAM_KERNELIP" ovfenv:value="servername.yourcompany.com "/>`	Fully qualified host name.	The host name of the managing server to connect to.
`<Property ovfenv:key="ConfigITCAM.ITCAM_KERNELPORT01" ovfenv:value="9122"/>`	Any valid IP port number.	The IP port that the managing server listens on for connection requests from data collectors.
`<Property ovfenv:key="ConfigITCAM.ITCAM_MS_AM_HOME" ovfenv:value="/opt/IBM/itcam/WebSphere/MS"/>`	A valid directory.	The installation location of the ITCAM for Application Diagnostics Managing Server. **Important:** Use double backslash (\) characters, for example, `C:\\IBM\\MS`.
`<Property ovfenv:key="ConfigITCAM.ITCAM_BINDIP" ovfenv:value="localhostname"/>`	Any valid IP address or host name.	The IP address or host name to be used by the data collector to communicate with the managing server. If more than one network interface or IP address is configured on data collector system, choose one of them.
`<Property ovfenv:key="ConfigITCAM.ITCAM_ PROBECONTROLLERRMIPORT" ovfenv:value="8300-8399"/>`	Range of valid IP port numbers.	If the data collector is behind a firewall or you have special requirements to change the RMI port of data collector, set this port number range. Configure this port number as permitted by the firewall for the data collector host. For example: `"ConfigITCAM.ITCAM_ PROBECONTROLLERRMIPORT" ovfenv:value="8300-8399"` or `"ConfigITCAM.ITCAM_ PROBECONTROLLERRMIPORT" ovfenv:value="8300""`.

Table 20. Silent configuration parameters for ITCAM Agent for WebSphere Applications. (continued)

Property	Valid values	Description
`<Property ovfenv:key="ConfigITCAM.ITCAM_PROBERMIPORT" ovfenv:value="8200-8299"/>`	Range of valid IP port numbers.	If the data collector is behind a firewall, or you have special requirements to change the RMI port of data collector, set this port number range. Configure this port number as permitted by the firewall for the data collector host. For example: `ConfigITCAM.ITCAM_ PROBERMIPORT" ovfenv: value="8200-8299"` or `PConfigITCAM.ITCAM_ PROBERMIPORT" ovfenv: value="8200"`.
Enable integration with ITCAM for Transactions		
`<Property ovfenv:key="ConfigITCAM.ITCAM_TTAPI" ovfenv:value="False"/>`	`True` or `False`.	Specify whether the data collector communicates with ITCAM for Transactions using Transaction Tracking API (TTAPI).
`<Property ovfenv:key="ConfigITCAM.ITCAM_TTTCHOST" ovfenv:value="servername.yourcompany.com"/>`	Fully qualified host name.	The host name of the ITCAM for Transactions Transaction Collector to connect to.
`<Property ovfenv:key="ConfigITCAM.ITCAM_TTTCPORT" ovfenv:value="5455"/>`	Any valid IP port number.	The port of the Transaction Collector to connect to.
Enable integration with ITCAM for SOA		
`<Property ovfenv:key="ConfigITCAM.ITCAM_SOADC" ovfenv:value="False"/>`	`True` or `False`.	Specify whether to integrate the data collector with the ITCAM for SOA agent. You must install the ITCAM for SOA version 7.1.1 or version 7.2 to complete the integration.
Enable integration with Tivoli Performance Viewer		

Table 20. Silent configuration parameters for ITCAM Agent for WebSphere Applications. (continued)

Property	Valid values	Description
`<Property ovfenv:key="ConfigITCAM.ITCAM_TPVDC" ovfenv:value="False"/>`	`True` or `False`.	Specify whether to integrate the data collector with the Tivoli Performance Viewer. For information about using ITCAM for WebSphere Application Server, see *IBM Tivoli Composite Application Manager for WebSphere Application Server version 7.2 Support for WebSphere Application Server version 8.5 Installation and User Guide*.
Enable integration with ITCAM Diagnostics Tool		
`<p><Property ovfenv:key="ConfigITCAM.ITCAM_DEDC" ovfenv:value="False"/>`	`True` or `False`.	Specify whether to integrate the data collector with the ITCAM Diagnostics Tool. For information about using the ITCAM Diagnostics Tool, see *ITCAM Diagnostic Tool Installation Guide*.
Modify Garbage Collection log path		
`<Property ovfenv:key="ConfigITCAM.ITCAM_GCOUTPUTDIST" ovfenv:value="True"/>`	`True` or `False`.	Specify whether to configure garbage collection.
`<Property ovfenv:key="ConfigITCAM.ITCAM_GCLOGPATH" ovfenv:value="/opt/IBM/WebSphere/AppServer/itcam_gc.log"/>`	Any valid path.	Modify the garbage collection log path. The full path to the garbage collection log file must exist. The server name, cell name, and node name are appended to the garbage collection log file name.
WebSphere Global Security configuration		

Table 20. Silent configuration parameters for ITCAM Agent for WebSphere Applications. (continued)

Property	Valid values	Description
`<Property ovfenv:key="ConfigITCAM.ITCAM_USE_ CLIENT_PROPS" ovfenv:value="Yes"/>`	`Yes` or `No`	Specify whether to use the user name and password stored in `soap.client.props` or `sas.client.props` of WebSphere Application Server. Set this property to `Yes` if WebSphere Application Server Global Security is enabled. In this case, WebSphere Application Server Hypervisor Edition automatically stores the user name and the password in `soap.client.props` or `sas.client.props`.
`<Property ovfenv:key="ConfigITCAM.ITCAM_USER" ovfenv:value="virtuser"/>`	`virtuser`	WebSphere Application Server administrative user name.
`<Property ovfenv:key="ConfigITCAM.ITCAM_PASSWORD" ovfenv:value="Virtuser01"/>`	Any valid password.	WebSphere Application Server administrative user password.

3. Create the ISO image. The ISO image can be created using any standard ISO creation software. Below is an example of the ISO image being created using the `mkisofs` utility. For example:

   ```
   mkdir /tmp/ovfenv
   cp ovf-env.xml /tmp/ovfenv
   mkisofs –J –r –o activation.iso /tmp/ovfenv
   ```

4. Transfer the ISO image to the data store where the IBM WebSphere Application Server Hypervisor Edition virtual image disks are located. Transfer the ISO image to the data store in the same way as the virtual image disks were transferred in step 1 on page 185.
5. Confirm that the ISO image file is attached to the virtual image. Using the VMware Infrastructure Client, click **Edit Settings** and verify that the ISO image is the primary iCD image for the virtual machine.
6. Start the virtual machine by right-clicking the virtual machine name and selecting **Power On**.

Results

After completing these steps, you have configured a single virtual machine with WebSphere Application Server that is running and available for use. The server is monitored by ITCAM Agent for WebSphere Applications.

Part 5. Configuring server templates for WebSphere Virtual Enterprise dynamic clusters

Chapter 7. Configuring server templates for WebSphere Virtual Enterprise dynamic clusters

In WebSphere Virtual Enterprise (VE) environments or environments with intelligent management capabilities, dynamic clusters use workload management to balance the workload of its members dynamically. Membership of dynamic clusters expands and contracts depending on the workload in the environment.

To create a dynamic cluster in the WebSphere Administrative Console, you can either choose to create servers based on a pre-configured template or you can use an existing server in your environment as a template. ITCAM Agent for WebSphere Applications provides support for creating a dynamic cluster template in which ITCAM Data Collector for WebSphere is pre-configured

Creating a server template

ITCAM Agent for WebSphere Applications provides a `configtemplate` script to create an ITCAM server template and to add it to the WebSphere template repository.

Before running the script, you must have installed ITCAM Agent for WebSphere Applications on the computer system where the Deployment Manager is installed. For more information about installing the agent, see Chapter 3, "Installing and configuring ITCAM Agent for WebSphere Applications on Windows systems," on page 19 or Chapter 5, "Installing and configuring ITCAM Agent for WebSphere Applications on Linux and UNIX systems," on page 103.

Tip: This section describes paths in a syntax that is valid on Linux and UNIX systems. On a Windows system, use \ instead of / in paths.

To create a server template and add it to the repository, complete these steps:

1. Navigate to the *DC_home*`/bin` directory on the computer system where the Deployment Manager is installed and run the `configtemplate` script.
2. Respond to each of the prompts listed in Table 21:

Table 21. Prompts presented by the `configtemplate` script

Prompt	Description
List of WebSphere Application Server home directories discovered:	Choose the WebSphere home directory which contains the Deployment Manager profile from the list of WebSphere Application Server home directories found.
List of WebSphere profiles discovered:	Choose a Deployment Manager profile from the list of profiles under the WebSphere Application Server home directory.
Specify Config home:	Specify the home directory of the ITCAM installation. For example, `C:\IBM\ITM\dchome\7.2.0.0.1` on Windows systems or `/opt/IBM/ITM/dchome/7.2.0.0.1` on Linux or UNIX systems.

Table 21. Prompts presented by the `configtemplate` script (continued)

Prompt	Description
Specify Operating System type	Choose the type of operating system on which the ITCAM Agent for WebSphere Applications is installed.
Specify JDK version	Choose a JDK from the list of valid JDKs.
Do you want to integrate with an ITCAM for SOA Agent?	Specify whether to integrate the data collector with the ITCAM for SOA agent.
Do you want to integrate with an ITCAM Agent for WebSphere Applications?	Specify whether to integrate the data collector with the ITCAM Agent for WebSphere Applications monitoring agent. If you choose `yes`, you are prompted for the host name or IP address and port of the monitoring agent.
Do you want to integrate with an MS?	Specify whether to integrate the data collector with an ITCAM for Application Diagnostics Managing Server. If you choose `yes`, you are prompted for the host name or IP address and port of the Managing Server.
Do you want to integrate with ITCAM for TT?	Specify whether to integrate the data collector with the ITCAM for Transactions using the Transaction Tracking API (TTAPI). If you choose `yes`, you are prompted for the host name or IP address and port of the Transactions Collector.
Do you want to integrate with Tivoli Performance Viewer?	Specify whether to integrate the data collector with the Tivoli Performance Monitoring when the data collector is included as part of ITCAM for WebSphere Application Server version 8.5. Tivoli Performance Monitoring is accessed from the WebSphere Application Server administrative console.
Do you want to integrate with ITCAM diagnostics tool?	Specify whether to integrate the data collector with the ITCAM Diagnostics Tool that is previewed in the ITCAM for Application Diagnostics beta. The ITCAM Diagnostics Tool is a tool for diagnostic investigation of applications that are running on WebSphere Application Server.

3. The template is created and is named *OSname_JDKversion*_itcam, where

   OSname
   Name of the operating system

   JDKversion
   Version of the JDK.

   The *OSname_JDKversion*_itcam template is created and is added to the WebSphere Virtual Environment template repository. The template is available from the list of dynamic cluster templates from the WebSphere Administrative Console. Dynamic clusters can be created using this template as the basis for each new server that is created.
4. If an application server has not yet been configured for data collection on the computer system that is running the dynamic cluster, complete these steps:

a. Create the directory wsBundleMetaData in the DC_home/runtime directory.
b. Copy the file itcam_wsBundleMetaData_template.xml from the *DC_home*/itcamdc/etc/was directory to the *DC_home*/runtime/wsBundleMetaData directory and rename it to itcam_wsBundleMetaData.xml.
c. Edit the file itcam_wsBundleMetaData.xml. Set the @{CONFIGHOME} property to point to the data collector home directory.

5. Copy the file *OSname*_Template_DCManualInput.txt (for example, win64_Template_DCManualInput.txt) from the *DC_home*/runtime directory on the computer system that is running the Deployment Manager to the *DC_home*/runtime directory where the dynamic cluster is running. The variable *OSname* is the name of the operating system for which you created the template.

Restriction: On every computer system on which the dynamic cluster is running, ITCAM Agent for WebSphere Applications must be installed using the configuration home directory that you specified when you ran the configtemplate script. Also, servers in the dynamic cluster can only run on the same operating system. Each *OSname_JDKversion*_itcam template is based on a specific operating system.

Deleting a server template

ITCAM Agent for WebSphere Applications provides a deletetemplate script to remove the ITCAM template from the WebSphere template repository.

To delete a server template from the repository, complete these steps:

1. Navigate to the *DC_home*\bin directory on the computer system where the Deployment Manager is installed and run the script deletetemplate.
2. Respond to each of the prompts listed in Table 22:

Table 22. Prompts presented by the deletetemplate script

Prompt	Description
List of WebSphere Application Server home directories discovered:	Choose the WebSphere home directory which contains the Deployment Manager profile from the list of WebSphere Application Server home directories found.
List of WebSphere profiles discovered:	Choose a Deployment Manager profile from the list of profiles under the WebSphere Application Server home directory.
Select the XD templates for deletion:	If an ITCAM template is found, choose a template from the list.

The ITCAM template is removed from the WebSphere template repository.

Part 6. Installing and Configuring ITCAM Agent for WebSphere Applications on a Remote Computer

Chapter 8. Installing and configuring ITCAM Agent for WebSphere Applications remotely

IBM Tivoli Monitoring supports remote installation and configuration of agents, including ITCAM Agent for WebSphere Applications. This section contains instructions for remote installation and configuration specific to this agent.

For details about remote agent deployment in IBM Tivoli Monitoring, see *IBM Tivoli Monitoring: Installation and Setup Guide*.

This capability requires IBM Tivoli Monitoring. If Tivoli Monitoring is not used (in a deep-dive diagnostics-only installation), remote installation and configuration is not supported.

Pre-installation task for remote installation of ITCAM Agent for WebSphere Applications on Linux or UNIX systems using a non-root user

Configure the `sudo` command for remote installation of ITCAM Agent for WebSphere Applications on Linux or UNIX systems using a non-root user.

If you remotely install ITCAM Agent for WebSphere Applications using a non-root user, the agent cannot be installed correctly because the OS agent is running as a user other than root.

The `sudo` command on Linux and UNIX systems provides a way to address this issue.

The `sudo` command must be configured before a remote installation using a non-root user is performed. The `sudo` command is then started when the agent is started. The following section provides an example; in this example, the following assumptions are made:

- The OS agent user 'itmuser' is a member of a group called 'itm'.
- The Agent Management Services are not prompted for a password.

```
# sudoers file.
#
# This file MUST be edited with the 'visudo' command as root.
# Failure to use 'visudo' may result in syntax or file permission errors
# that prevent sudo from running.
#
# For more information, see the sudoers man page for the details on how to
write a sudoers file.
#

# Host alias specification

# User alias specification

# Cmnd alias specification
Cmnd_Alias AMSAGENTSTART = /opt/PAS/ITMTEST/bin/itmcmd agent -[po] [[\:alnum\:]_]*
start [[\:alnum\:]][[\:alnum\:]],/opt/PAS/ITMTEST/bin/itmcmd agent start
[[\:alnum\:]][[\:alnum\:]]
```

```
Cmnd_Alias AMSAGENTSTOP = /opt/PAS/ITMTEST/bin/itmcmd agent -[po] [[\:alnum\:]_]*
stop [[\:alnum\:]][[\:alnum\:]],/opt/PAS/ITMTEST/bin/itmcmd agent stop
[[\:alnum\:]][[\:alnum\:]]
Cmnd_Alias ITMAMSCMD = AMSAGENTSTART,AMSAGENTSTOP
# Defaults specification

# Runas alias specification

Runas_Alias ITMAGENTIDS = itmuser

# Same thing without a password
%itmusers ALL=( ITMAGENTIDS ) NOPASSWD: ITMAMSCMD
```

This is just one possible example. The `sudo` command has many advanced capabilities that include the ability to audit and to alert administrators of usage of the `sudo` command by unauthorized users. For more information, see your operating system sudo man pages for more information. In the *ITM_home*/*platform*/lz/bin/agentInstanceCommand.sh script, replace calls to 'su' with calls to 'sudo'. For example:

```
if [  -z "$USR" ]; then
 $START_CMD
else
 # su - $USR -c "$START_CMD"
   sudo -u $USR $START_CMD
fi
...
if [ -z "$USR" ]; then
 $STOP_CMD
else
   # su - $USR -c "$STOP_CMD"
 sudo -u $USR $STOP_CMD
fi
```

Also, because ITCAM Agent for WebSphere Applications remote configuration runs under the same user as the OS agent, you must ensure that this user has write access to the WebSphere Application Server profile home directory trees for all the profiles that the agent is to monitor.

Installing, upgrading, and configuring ITCAM Agent for WebSphere Application monitoring agent remotely from the command-line

You can use the `tacmd` command on a hub Tivoli Enterprise Monitoring Server host to install the monitoring agent remotely on any host that runs the IBM Tivoli Monitoring OS agent. You can also use this command to upgrade the remote monitoring agent and to configure the monitoring agent settings.

You can upgrade the monitoring agent of the following products to the ITCAM Agent for WebSphere Applications version 7.2 monitoring agent:

- ITCAM for WebSphere version 6.1.0.4 or later
- WebSphere Tivoli Enterprise Monitoring Agent version 6.2.0.4 or later included in ITCAM for Web Resources version 6.2.0.4 or later
- ITCAM Agent for WebSphere Applications version 7.1 included in ITCAM for Applications Diagnostics 7.1

The following procedure presents the steps for installing and upgrading the monitoring agent.

For information about installing ITCAM Data Collector for WebSphere, see "Installing and configuring ITCAM Data Collector for WebSphere on Windows systems" on page 206.

For information about migrating to ITCAM Data Collector for WebSphere, see "Migrating to ITCAM Data Collector for WebSphere on Windows systems" on page 211.

Application support files must be installed on the monitoring server, portal server, and portal clients to view monitoring data in the Tivoli Enterprise Portal after remote deployment.

The application support files are automatically installed on the monitoring server and the portal server, if the following conditions are met:

- Self-description is enabled on the hub and remote monitoring servers.
- All Tivoli Management Services server components are at version 6.2.3 or higher.
- The agent framework is at version 6.2.3 or higher.

Self-description is enabled by default for ITCAM Agent for WebSphere Applications. For more information about the conditions that must be met for self-description, see "Enabling application support through self-description" on page 62 on Windows systems and "Enabling application support through self-description" on page 145 on Linux or UNIX systems.

For more information about manually installing application support files, see "Enabling application support on Windows systems" on page 61 on Windows systems and "Enabling application support on Linux and UNIX systems" on page 145 on Linux or UNIX systems.

Before you install or upgrade the agent, you must add its installation bundles to the monitoring server.

For details on using `tacmd`, and for other available options (including installation from a remote monitoring server), see *IBM Tivoli Monitoring Command Reference*.

Important: This section describes commands in a syntax that is valid on Linux and UNIX systems. On a Windows monitoring server host, use `tacmd` instead of `./tacmd`, and use `\` instead of `/` in paths.

Adding the installation bundles

In most cases, it is recommended that you add both the Windows bundle and the Linux and UNIX systems bundle to a monitoring server host. In this way, you can deploy the agent on hosts with both platform types. However, you can choose to add only the Windows system bundle or only the Linux and UNIX systems bundle.

Complete the following procedure:

1. Copy or mount the agent installation images on the Tivoli Enterprise Monitoring Server host.
2. Change to the *ITM_home*`/bin` directory.
3. Use the following command to log on:

   ```
   ./tacmd login -s localhost -u sysadmin -p password
   ```

   Use the password for the `SYSADMIN` user of IBM Tivoli Monitoring.

4. To add the installation bundle for Windows target hosts, enter the command:
   ```
   ./tacmd addBundles -i path_to_Windows_image/WINDOWS/Deploy -t yn
   ```
5. To add the installation bundle for Linux or UNIX hosts, enter the command:
   ```
   ./tacmd addBundles -i path_to_Linux_UNIX_package/unix -t yn
   ```

Installing the agent on a remote host

To install the agent on a remote host, complete the following procedure on the Tivoli Enterprise Monitoring Server host:

1. Change to the *ITM_home*/bin directory.
2. Use the following command to log on:
   ```
   ./tacmd login -s localhost -u sysadmin -p password
   ```
   Use the password for the SYSADMIN user of IBM Tivoli Monitoring.
3. To list the available Operating System agents on remote hosts, enter the command:
   ```
   ./tacmd listSystems -t UX LZ NT
   ```
   Find the necessary remote host in the list, and note the name of the Operating System agent that is on it.

   Important: The Operating System agent must be running. This is indicated by Y in the list. If the Operating System agent on the target host is not running, start it before you attempt the installation.
4. To install ITCAM Agent for WebSphere Applications on a remote host, enter the command:
   ```
   ./tacmd addSystem -t yn -n OS_agent_name
   ```
   OS_agent_name is the name of the Operating System agent, for example, lrtx228:LZ. The node identifier displayed in the Tivoli Enterprise Portal navigation tree is set to "Primary", and the port for incoming data collector connections is set to 63335.

   Alternatively, you can install ITCAM Agent for WebSphere Applications on a remote host and configure custom settings for the node identifier and port at the same time. To do this, enter the command:
   ```
   ./tacmd addSystem -t yn -n OS_agent_name  --properties
     CONFIGURATION_TYPE.configure_type="tema_configure"
     KYN_Tema_Config.KYN_ALT_NODEID="node_id"
     KYN_Tema_Config.KYN_PORT=port_number
   ```
   OS_agent_name
   : Name of the Operating System agent, for example, lrtx228:LZ.

   node_id
   : An alternative Node ID for identifying the agent. This identifier determines how the agent is displayed in the Tivoli Enterprise Portal navigation tree. The default is "Primary", used with the host name of the computer where the agent is installed.

   port_number
   : The TCP socket port that the monitoring agent uses to listen for connection requests from the data collectors. The default is 63335. The port is used only for local communication on the host.

If you want to monitor the remote deployment status, enter the command:

```
./tacmd getDeployStatus
```

When the agent is successfully installed, it automatically connects to the Tivoli Enterprise Monitoring Server, and the Tivoli Enterprise Portal shows it.

Upgrading the agent on a remote host

To upgrade the agent on a remote host, complete the following procedure:

1. Change to the *ITM_home*/bin directory.
2. To log on, use the following command:

   ```
   ./tacmd login -s localhost -u sysadmin -p password
   ```

   Use the password for the SYSADMIN user of IBM Tivoli Monitoring.
3. To list the available Operating System agents on remote hosts, enter the command:

   ```
   ./tacmd listSystems -t UX LZ NT
   ```

   Find the necessary remote host in the list, and note the name of the Operating System agent on it.

   Important: The Operating System agent must be running. This is indicated by Y in the list. If the Operating System agent on the target host is not running, start it before you attempt the installation.
4. To upgrade ITCAM Agent for WebSphere Applications on a remote host, enter the command:

   ```
   ./tacmd updateagent -t yn -n OS_agent_name
   ```

   OS_agent_name
   Name of the Operating System agent, for example, lrtx228:LZ.
5. If you want to monitor the remote deployment status, enter the command:

   ```
   ./tacmd getDeployStatus
   ```

When the ITCAM Agent for WebSphere Applications monitoring agent is s successfully installed, it automatically connects to the Tivoli Enterprise Monitoring Server, and it is displayed in the Tivoli Enterprise Portal.

Configuring the agent on a remote host

To configure monitoring agent settings on a remote host where the agent is installed, on the Tivoli Enterprise Monitoring Server host, complete the following procedure:

1. Change to the *ITM_home*/bin directory.
2. To log on, use the following command:

   ```
   ./tacmd login -s localhost -u sysadmin -p password
   ```

   Use the password for the SYSADMIN user of IBM Tivoli Monitoring.
3. To list the available agents on remote hosts, enter the command:

   ```
   ./tacmd listSystems -t yn
   ```

   Find the necessary remote host in the list, and note the name of the agent on it.

   Important:
   - The ITCAM Agent for WebSphere Applications must be running.
   - This is indicated by Y in the list. If the Operating System agent on the target host is not running, start it before performing the installation.

4. To configure ITCAM Agent for WebSphere Applications on a remote host, enter the command:

```
./tacmd configureSystem --system Agent_name --properties
  CONFIGURATION_TYPE.configure_type="tema_configure"
  KYN_Tema_Config.KYN_ALT_NODEID="node_id"
  KYN_Tema_Config.KYN_PORT=port_number
```

Agent_name
: Name of ITCAM Agent for WebSphere Applications on the remote host, for example, `Primary:tivm40:KYNA`

node_id
: An alternative Node ID for identifying the agent. This identifier that determines how the agent is displayed in the Tivoli Enterprise Portal navigation tree. The default is "Primary", used with the host name of the computer where the agent is installed.

port_number
: The TCP socket port that is used by the monitoring agent to listen for connection requests from the data collectors. The default is 63335. The port is used only for local communication on the host.

Alternatively, you can create a response file with the settings, and then run the `tacmd` command on the response file. The content of the response file is:

```
--system
Agent_name
--properties
CONFIGURATION_TYPE.configure_type="tema_configure"
KYN_Tema_Config.KYN_ALT_NODEID="node_id"
KYN_Tema_Config.KYN_PORT=port_number
```

For example:

```
--system
Primary:tivm40:KYNA
--properties
CONFIGURATION_TYPE.configure_type="tema_configure"
KYN_Tema_Config.KYN_ALT_NODEID="mynode"
KYN_Tema_Config.KYN_PORT=63336
```

To use the response file, enter the following command:

```
./tacmd configureSystem response_file_name
```

When the agent is successfully configured, it automatically connects to the Tivoli Enterprise Monitoring Server using the new settings and it is displayed in the Tivoli Enterprise Portal.

To complete other configuration tasks on a remote agent installation, see “Configuring ITCAM Agent for WebSphere Applications remotely using Tivoli Enterprise Portal” on page 217.

Installing and configuring ITCAM Data Collector for WebSphere on Windows systems

You can install and configure ITCAM Data Collector for WebSphere on a remote system using `tacmd` commands from the command prompt of the Tivoli Enterprise Monitoring Server.

You must install the monitoring agent on the remote system from the Tivoli Enterprise Monitoring Server before you install ITCAM Data Collector for WebSphere.

When you install monitoring agent on the remote system, ITCAM Data Collector for WebSphere installation files are placed in the *ITM_HOME*\TMAITM6\yn\wasdc*dc_version* directory. For example, C:\IBM\ITM\TMAITM6\yn\wasdc\7.2.0.0.1. The directory contains the following files:

- Data collector installation files, gdc.zip.
- A script to extract and install the installation files, gdc_extract.bat.

For more information about operating system-dependent variables, see "Operating system-dependent variables and paths" on page xvii.

Tip: In the following procedure, if the Tivoli Enterprise Monitoring Server is on a Windows system, use the tacmd command. If the Tivoli Enterprise Monitoring Server is on a Linux or UNIX system, use the ./tacmd command.

You can use tacmd executecommand to install the data collector and configure it in silent mode. To use the tacmd executecommand command, the hub and remote Tivoli Enterprise Monitoring Servers must be at version 6.2.2 fix pack 2 or later. For details about using tacmd commands, see *IBM Tivoli Monitoring Command Reference*.

To install the ITCAM Data Collector for WebSphere from the command line, complete the following procedure on the Tivoli Enterprise Monitoring Server:

1. Change to *ITM_HOME*\bin directory.
2. Use the following command to log in to the Tivoli Enterprise Monitoring Server:

   ```
   tacmd login -s TEMS_hostname -u userid -p password
   ```

   Use the SYSADMIN user of IBM Tivoli Monitoring and password. For example:

   ```
   tacmd login -s machine01.raleigh.ibm.com -u user01 -p a1b2c3d4
   ```
3. Set the KT1_TEMS_SECURE configuration parameter in the hub Tivoli Enterprise Monitoring Server's configuration file to specify that the hub supports the tacmd commands:
   - Navigate to the file *ITM_HOME*\CMS\KBBENV.
   - Add the property KT1_TEMS_SECURE='YES', if it does not exist.
   - Recycle the hub Tivoli Enterprise Monitoring Server
4. Set the location of the Java home directory, the Tivoli Monitoring home directory, and the data collector home directory. Extract the data collector installation files to the data collector home directory.

```
tacmd executecommand -m System -c "set JAVA_HOME=path_to_java_home&set CANDLE_HOME=path_to_ITM_home&
gdc_extract.bat -d path_to_dc_home full_path_to_archive_file" -w ITM_Home\TMAITM6\yn\wasdc\dc_version
```

Where:

-m | --system
Specifies on which managed system to run the command.

-c | --commandstring
Specifies the command to run. Use double quotation marks for commands with parameters. You must escape back slashes when defining a Windows directory path. For more information, see the "Escaping backslashes, spaces, and double quotation marks" section in the *Tivoli Monitoring Command Reference* guide.

-w | --workingdir
Specifies the working directory that is switched to before the command is run. When running this command between a UNIX or Linux system and targeting a Windows monitoring agent, you must replace the backslashes with forward slashes in the path definitions for the source parameter. It is best to use forward slashes for tolerance with Windows systems. If the working directory contains spaces, you must include double quotation marks around the directory location.

For example:

```
tacmd executecommand -m Primary:WINDOWS:NT -c "set JAVA_HOME=C:\IBM\WebSphere\AppServer\java&set
CANDLE_HOME=C:\IBM\ITM&gdc_extract.bat -d C:\\IBM\\ITM\\dchome c:\\IBM\\ITM\\TMAITM6\\yn\\wasdc\\
7.2.0.0.1\\gdc.zip"
-w C:\\IBM\\ITM\\TMAITM6\\yn\\wasdc\\7.2.0.0.1
```

Important: In interactive mode, the user is expected to press any prompt to continue to indicate to the batch file that the script is complete. The command might return a non-zero when it is run in console mode on a remote system, although the `gdc.zip` file is extracted successfully.

5. Specify the data collector configuration in a properties file on the Tivoli Enterprise Monitoring Server. A sample properties file, `sample_silent_config.txt`, is available from *DC_home*`\bin` on any local system where you installed the agent.
6. Copy the *silent_file* from the Tivoli Enterprise Monitoring Server to the remote system using the `tacmd putfile` command.

```
tacmd putfile -m System -s local_dir_path\silent_file -d remote_dir_path\silent_file -t text
```

Where:

-m | --system
Specifies on which managed system to run the command.

-s | --source
Specifies the local file name.

-d | --destination
Specifies the remote file name.

-t | --text
Specifies the mode of transfer.

For example:

```
tacmd putfile -m Primary:WINDOWS:NT -s /opt/IBM/ITM/dchome/silent_file.txt
-d c:\\temp\\silent_file.txt -t text
```

7. Configure the data collector using the response silent response file:

```
tacmd executecommand -m System -c "config.bat -silent full_path_to_silent_file\\silent_file.txt" -w path_to_DC_home\bin
```

For example:

```
tacmd executecommand -m Primary:WINDOWS:NT -c "config.bat -silent C:\\temp\\silent_file.txt"
-w C:\\IBM\\ITM\\dchome\\7.2.0.0.1\\bin
```

8. Restart the application server instances.
   a. Stop the application server.

```
tacmd executecommand -m System -c "stopServer.bat server_name" -w profile_home\bin
```

For example:

```
tacmd executecommand -m Primary:WINDOWS:NT -c "stopServer.bat server1"
-w C:\\Program Files\\IBM\\WebSphere\\AppServer\\profiles\\AppSrv01\\bin
```

b. Start the application server:

```
tacmd executecommand -m System -c "startServer.bat server_name -w profile_home\bin"
```

For example:

```
tacmd executecommand -m Primary:WINDOWS:NT -c "startServer.bat server1"
-w C:\\Program Files\\IBM\\WebSphere\\AppServer\\profiles\\AppSrv01\\bin
```

For more information about remote deployment, see the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Installing and configuring ITCAM Data Collector for WebSphere on Linux and UNIX systems

You can install and configure ITCAM Data Collector for WebSphere using `tacmd` commands on a remote system from the command prompt of the Tivoli Enterprise Monitoring Server.

You must install the monitoring agent on the remote system from the Tivoli Enterprise Monitoring Server before you install ITCAM Data Collector for WebSphere.

When you install monitoring agent on the remote system, ITCAM Data Collector for WebSphere installation files are placed in the *ITM_Home*`/arch/yn/wasdc/`*dc_version* directory. The directory contains the following files:

- Data collector installation files, `gdc.tar.gz`.
- A script to extract and install the installation files, `gdc_extract.sh`.

For more information about operating system-dependent variables, see "Operating system-dependent variables and paths" on page xvii.

Tip: In the following procedure, if the Tivoli Enterprise Monitoring Server is on a Windows system, use the `tacmd` command. If the Tivoli Enterprise Monitoring Server is on a Linux or UNIX system, use the `./tacmd` command.

You can use `tacmd executecommand` to install the data collector and configure it in silent mode. To use the `tacmd executecommand` command, the hub and remote Tivoli Enterprise Monitoring Servers must be at version 6.2.2 fix pack 2 or later. For details about using `tacmd` commands, see *IBM Tivoli Monitoring Command Reference*.

To install the ITCAM Data Collector for WebSphere from the command line, complete the following procedure from the Tivoli Enterprise Monitoring Server:

1. Change to *ITM_HOME*`/bin` directory.
2. Use the following command to log in to the Tivoli Enterprise Monitoring Server:

   ```
   ./tacmd login -s TEMS_hostname -u userid -p password
   ```

   Use the SYSADMIN user of IBM Tivoli Monitoring and password. For example:

   ```
   ./tacmd login -s machine01.raleigh.ibm.com -u user01 -p a1b2c3d4
   ```

3. Set the `KT1_TEMS_SECURE` configuration parameter in the hub Tivoli Enterprise Monitoring Server's configuration file to specify that the hub Tivoli Enterprise Monitoring Server supports the `tacmd` commands:
   - Navigate to the file *ITM_Home*`/config/ms.ini`.
   - Set the property to `KT1_TEMS_SECURE='YES'`.

- Recycle the Tivoli Enterprise Monitoring Server.

4. Set the location of the Java home directory, the Tivoli Monitoring home directory, and the data collector home directory. Extract the data collector installation files to the data collector home directory.

```
 ./tacmd  executecommand -m System -c "export JAVA_HOME=path_to_java_home&&export CANDLE_HOME=path_to_ITM_home&&
./gdc_extract.sh -d path_to_dc_home full_path_to_archive_file"
-w ITM_Home/arch/yn/wasdc/dc_version
```

Where:

-m|--system
Specifies on which OS agent to run the command. Run the **tacmd listSystems** command to list the OS agents that you are monitoring. For example:

```
./tacmd listSystems -t UX LZ NT
```

-c|--commandstring
Specifies the command to run. Use double quotation marks for commands with parameters. You must escape back slashes when defining a Windows directory path. For more information, see the "Escaping backslashes, spaces, and double quotation marks" section in the *Tivoli Monitoring Command Reference* guide.

-w|--workingdir
Specifies the working directory that is switched to before the command is run. When running this command between a UNIX or Linux system and targeting a Windows monitoring agent, you must replace the backslashes with forward slashes in the path definitions for the source parameter. It is best to use forward slashes for tolerance with Windows systems. If the working directory contains spaces, you must include double quotation marks around the directory location

For example:

```
./tacmd executecommand -m v5254005b0186:LZ -c "export JAVA_HOME=/opt/IBM/ITM/JRE/li6263&&export
CANDLE_HOME=/opt/IBM/ITM&&./gdc_extract.sh -d /opt/IBM/ITM/dchome1 /opt/IBM/ITM/li6263/yn/wasdc/
7.2.0.0.1/gdc.tar.gz"
-w /opt/IBM/ITM/li6263/yn/wasdc/7.2.0.0.1
```

On Solaris systems:

```
 ./tacmd  executecommand -m v5254005b0186:KUX -c "JAVA_HOME=/opt/IBM/ITM/JRE/sol283&&export JAVA_HOME&&
./gdc_extract.sh -d /opt/IBM/ITM/dchome1 /opt/IBM/ITM/sol283/yn/wasdc/7.2.0.0.1/gdc_tar.gz"
-w /opt/IBM/ITM/sol283/yn/wasdc/7.2.0.0.1
```

5. Specify the data collector configuration in a properties file on the Tivoli Enterprise Monitoring Server. A sample properties file, `sample_silent_config.txt`, is available from *DC_home*`/bin` on any local system where you installed the agent.
6. Copy the *silent_file* from the Tivoli Enterprise Monitoring Server to the remote system using the `tacmd putfile` command.

```
./tacmd putfile -m System -s local_dir_path/silent_file -d remote_dir_path/silent_file -t text
```

Where:

-m|--system
Specifies on which OS agent to run the command. Run the **tacmd listSystems** command to list the OS agents that you are monitoring. For example:

```
./tacmd listSystems -t UX LZ NT
```

-s | --source
Specifies the local file name.

-d | --destination
Specifies the remote file name.

-t | --text
Specifies the mode of transfer.

For example:

```
./tacmd putfile -m v5254005b0186:LZ -s dc_config.txt -d /opt/IBM/ITM/dchome1/7.2.0.0.1/bin/dc_config.txt -t text
```

7. Configure the data collector using the silent response file:

```
./tacmd executecommand -m System -c "./config.sh -silent /full_path_to_silent_file/silent_file.txt"
-w path_to_DC_home/bin
```

For example:

```
./tacmd executecommand -m v5254005b0186:LZ -c "./config.sh -silent /opt/IBM/ITM/dchome1/7.2.0.0.1/bin/dc_config.txt"
-w /opt/IBM/ITM/dchome1/7.2.0.0.1/bin
```

8. Restart the application server instances.
   a. Stop the application server.

```
./tacmd executecommand -m System -c "./stopServer.sh server_name" -w profile_home/bin
```

For example:

```
./tacmd executecommand -m v5254005b0186:LZ -c "./stopServer.sh server3" -w /opt/IBM/WAS8/profiles/AppSrv01/bin
```

   b. Start the application server:

```
./tacmd executecommand -m System -c "./startServer.sh server_name" -w profile_home\bin
```

For example:

```
./tacmd executecommand -m v5254005b0186:LZ -c "./startServer.sh server3" -w /opt/IBM/WAS8/profiles/AppSrv01/bin
```

For more information about remote deployment, see the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Migrating to ITCAM Data Collector for WebSphere on Windows systems

When you upgrade to Agent for WebSphere Applications version 7.2 or later on the remote system, there may be other older versions of the data collector installed and configured for the same profile in which you plan to configure ITCAM for SOA.

These older versions of the data collector must be migrated to the ITCAM Data Collector for WebSphere after you install ITCAM Data Collector for WebSphere. The ITCAM for SOA 7.1.1 data collector for the WebSphere Application Server is upgraded automatically as part of the migration of these older versions of the data collector.

When an earlier maintenance level of the ITCAM Data Collector for WebSphere is installed and configured for the same profile, you can migrate it to the latest maintenance level using the ITCAM Data Collector for WebSphere Migration utility.

You can use `tacmd executecommand` to migrate older versions and earlier maintenance levels of the data collector in silent mode. For details about using `tacmd` commands, see *IBM Tivoli Monitoring Command Reference*.

In the following procedure, if the Tivoli Enterprise Monitoring Server is on a Windows system, use the `tacmd` command. If the Tivoli Enterprise Monitoring Server is on a Linux or UNIX system, use the `./tacmd` command.

To migrate an older version or an earlier maintenance level of the data collector to the latest ITCAM Data Collector for WebSphere, complete the following procedure from the command prompt of the Tivoli Enterprise Monitoring Server:

1. Change to *ITM_HOME*`\bin` directory.
2. Use the following command to log in to the Tivoli Enterprise Monitoring Server:

   `tacmd login -s` *TEMS_hostname* `-u` *userid* `-p` *password*

   Use the SYSADMIN user of IBM Tivoli Monitoring and password. For example:

   ```
   tacmd login -s machine01.raleigh.ibm.com -u user01 -p a1b2c3d4
   ```
3. Set the `KT1_TEMS_SECURE` configuration parameter in the hub 's configuration file to specify that the hub supports the `tacmd` commands:
   - Navigate to the file *ITM_HOME*`\CMS\KBBENV`.
   - Add the property `KT1_TEMS_SECURE='YES'`, if it does not exist.
   - Recycle the hub
4. Set the location of the Java home directory, the Tivoli Monitoring home directory, and the data collector home directory. Extract the data collector installation files to the data collector home directory.

```
tacmd executecommand -m System -c "set JAVA_HOME=path_to_java_home&set CANDLE_HOME=path_to_ITM_home&
gdc_extract.bat -d path_to_dc_home full_path_to_archive_file" -w ITM_Home\TMAITM6\yn\wasdc\dc_version
```

Where:

-m | --system
Specifies on which managed system to run the command.

-c | --commandstring
Specifies the command to run. Use double quotation marks for commands with parameters. You must escape back slashes when defining a Windows directory path. For more information, see the "Escaping backslashes, spaces, and double quotation marks" section in the *Tivoli Monitoring Command Reference* guide.

-w | --workingdir
Specifies the working directory that is switched to before the command is run. When running this command between a UNIX or Linux system and targeting a Windows monitoring agent, you must replace the backslashes with forward slashes in the path definitions for the source parameter. It is best to use forward slashes for tolerance with Windows systems. If the working directory contains spaces, you must include double quotation marks around the directory location.

For example:

```
tacmd executecommand -m Primary:WINDOWS:NT -c "set JAVA_HOME=C:\IBM\WebSphere\AppServer\java&set
CANDLE_HOME=C:\IBM\ITM&gdc_extract.bat -d C:\\IBM\\ITM\\dchome c:\\IBM\\ITM\\TMAITM6\\yn\\wasdc\\
7.2.0.0.1\\gdc.zip"
-w C:\\IBM\\ITM\\TMAITM6\\yn\\wasdc\\7.2.0.0.1
```

Important: In interactive mode, the user is expected to press any key to continue to indicate to the batch file that the script is complete. The command might return a non-zero when it is run in console mode on a remote system, although the `gdc.zip` file is extracted successfully.

5. Specify the migration details in a properties file on the Tivoli Enterprise Monitoring Server. Two sample properties file are available from *DC_home*\bin on any local system where you installed the agent.

   The file, `sample_silent_migrate.txt`, can be used when you migrate the data collector of the following products to the ITCAM Data Collector for WebSphere:

   - ITCAM for WebSphere 6.1.0.4 or later
   - WebSphere Data Collector 6.1.0.4 or later included in ITCAM for Web Resources 6.2.0.4 or later
   - ITCAM Agent for WebSphere Applications 7.1 included in ITCAM for Applications Diagnostics 7.1
   - ITCAM for WebSphere Application Server 7.2

   The file, `sample_silent_migrate_soa.txt`, can be used when you migrate the ITCAM for SOA 7.1.1 data collector to the ITCAM Data Collector for WebSphere.

6. Copy the *silent_file* from the managing server to the remote system using the `tacmd putfile` command.

```
tacmd putfile -m System -s local_dir_path\silent_file -d remote_dir_path\silent_file -t text
```

Where:

-m | --system
Specifies on which managed system to run the command.

-s | --source
Specifies the local file name.

-d | --destination
Specifies the remote file name.

-t | --text
Specifies the mode of transfer.

For example:

```
tacmd putfile -m Primary:WINDOWS:NT -s /opt/IBM/ITM/dchome/silent_file.txt
-d c:\\temp\\silent_file.txt -t text
```

7. Migrate the data collector using the silent response file:

```
tacmd executecommand -m System -c "migrate.bat -silent full_path_to_silent_file\\silent_file.txt"
-w path_to_DC_home\bin
```

For example:

```
tacmd executecommand -m Primary:WINDOWS:NT -c "migrate.bat -silent C:\\temp\\silent_file.txt"
-w C:\\IBM\\ITM\\dchome\\7.2.0.0.1\\bin
```

8. Restart the application server instances.
   a. Stop the application server.

```
tacmd executecommand -m System -c "stopServer.bat server_name" -w profile_home\bin
```

For example:

```
tacmd executecommand -m Primary:WINDOWS:NT -c "stopServer.bat server1"
-w C:\\Program Files\\IBM\\WebSphere\\AppServer\\profiles\\AppSrv01\\bin
```

   b. Start the application server:

```
tacmd executecommand -m System -c "startServer.bat server_name -w profile_home\bin"
```

For example:

```
tacmd executecommand -m Primary:WINDOWS:NT -c "startServer.bat server1"
-w C:\\Program Files\\IBM\\WebSphere\\AppServer\\profiles\\AppSrv01\\bin
```

For more information about remote deployment, see the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Migrating to the ITCAM Data Collector for WebSphere on Linux and UNIX systems

When you upgrade to Agent for WebSphere Applications version 7.2 or later on the remote system, there may be other older versions of the data collector installed and configured for the same profile in which you plan to configure the agent.

These older versions of the data collector must be migrated to the ITCAM Data Collector for WebSphere after you install ITCAM Data Collector for WebSphere. The ITCAM for SOA 7.1.1 data collector for the WebSphere Application Server is upgraded automatically as part of the migration of these older versions of the data collector.

When an earlier maintenance level of the ITCAM Data Collector for WebSphere is installed and configured for the same profile, you can migrate it to the latest maintenance level using the ITCAM Data Collector for WebSphere Migration utility.

You can use `tacmd executecommand` to migrate older versions and earlier maintenance levels of the data collector in silent mode. For details about using `tacmd` commands, see *IBM Tivoli Monitoring Command Reference*.

In the following procedure, if the Tivoli Enterprise Monitoring Server is on a Windows system, use the `tacmd` command. If the Tivoli Enterprise Monitoring Server is on a Linux or UNIX system, use the `./tacmd` command.

Remember: You must upgrade the monitoring agent on the remote system before you upgrade the data collector.

To migrate an older version or an earlier maintenance level of the data collector to the latest ITCAM Data Collector for WebSphere with the command prompt, complete the following procedure on the Tivoli Enterprise Monitoring Server:

1. Change to *ITM_HOME*`/bin` directory.
2. Use the following command to log in to the Tivoli Enterprise Monitoring Server:

   ```
   ./tacmd  login -s TEMS_hostname -u userid -p password
   ```

   Use the SYSADMIN user of IBM Tivoli Monitoring and password. For example:

   ```
   ./tacmd  login -s machine01.raleigh.ibm.com -u user01 -p a1b2c3d4
   ```
3. Set the `KT1_TEMS_SECURE` configuration parameter in the hub 's configuration file to specify that the hub supports the `tacmd` commands:
   - Navigate to the file *ITM_Home*`/config/ms.ini`.
   - Set the property to `KT1_TEMS_SECURE='YES'`.
   - Recycle the Tivoli Enterprise Monitoring Server.

4. Set the location of the Java home directory, the Tivoli Monitoring home directory, and the data collector home directory. Extract the data collector installation files to the data collector home directory.

```
 ./tacmd  executecommand -m System -c "export JAVA_HOME=path_to_java_home&&export CANDLE_HOME=path_to_ITM_home&&
./gdc_extract.sh -d path_to_dc_home full_path_to_archive_file" -w ITM_Home/arch/yn/wasdc/dc_version
```

Where:

-m|--system
Specifies on which OS agent to run the command. Run the **tacmd listSystems** command to list the OS agents that you are monitoring. For example:

```
./tacmd listSystems -t UX LZ NT
```

-c|--commandstring
Specifies the command to run. Use double quotation marks for commands with parameters. You must escape back slashes when defining a Windows directory path. For more information, see the "Escaping backslashes, spaces, and double quotation marks" section in the *Tivoli Monitoring Command Reference* guide.

-w|--workingdir
Specifies the working directory that is switched to before the command is run. When running this command between a UNIX or Linux system and targeting a Windows monitoring agent, you must replace the backslashes with forward slashes in the path definitions for the source parameter. It is best to use forward slashes for tolerance with Windows systems. If the working directory contains spaces, you must include double quotation marks around the directory location

For example:

```
./tacmd executecommand -m v5254005b0186:LZ -c "export JAVA_HOME=/opt/IBM/ITM/JRE/li6263&&export
CANDLE_HOME=/opt/IBM/ITM&&./gdc_extract.sh -d /opt/IBM/ITM/dchome1 /opt/IBM/ITM/li6263/yn/wasdc/
7.2/gdc.tar.gz"
-w /opt/IBM/ITM/li6263/yn/wasdc/7.2.0.0.1
```

On Solaris systems:

```
./tacmd  executecommand -m v5254005b0186:KUX -c "JAVA_HOME=/opt/IBM/ITM/JRE/sol283&&export JAVA_HOME&&
./gdc_extract.sh -d /opt/IBM/ITM/dchome1 /opt/IBM/ITM/sol283/yn/wasdc/7.2.0.0.1/gdc_tar.gz"
-w /opt/IBM/ITM/sol283/yn/wasdc/7.2.0.0.1
```

5. Specify the migration details in a properties file on the Tivoli Enterprise Monitoring Server. Two sample properties file are available from *DC_home*/bin on any local system where you installed the agent.

   The file, sample_silent_migrate.txt, can be used when you migrate the data collector of the following products to the ITCAM Data Collector for WebSphere:

   - ITCAM for WebSphere 6.1.0.4 or later
   - WebSphere Data Collector 6.1.0.4 or later included in ITCAM for Web Resources 6.2.0.4 or later
   - ITCAM Agent for WebSphere Applications 7.1 included in ITCAM for Applications Diagnostics 7.1
   - ITCAM for WebSphere Application Server 7.2

   The file, sample_silent_migrate_soa.txt, can be used when you migrate the ITCAM for SOA 7.1.1 data collector to the ITCAM Data Collector for WebSphere.

6. Copy the *silent_file* from the Tivoli Enterprise Monitoring Server to the remote system using the tacmd putfile command.

```
./tacmd putfile -m System -s local_dir_path/silent_file -d remote_dir_path/silent_file -t text
```

Where:

-m | --system
Specifies on which OS agent to run the command. Run the **tacmd listSystems** command to list the OS agents that you are monitoring. For example:

```
./tacmd listSystems -t UX LZ NT
```

-s | --source
Specifies the local file name.

-d | --destination
Specifies the remote file name.

-t | --text
Specifies the mode of transfer.

For example:

```
./tacmd putfile -m v5254005b0186:LZ -s dc_config.txt -d /opt/IBM/ITM/dchome1/7.2.0.0.1/bin/dc_config.txt
-t text
```

7. Migrate the data collector using the silent response file:

```
./tacmd executecommand -m System -c "./migrate.sh -silent /full_path_to_silent_file/silent_file.txt"
-w path_to_DC_home/bin
```

For example:

```
./tacmd executecommand -m v5254005b0186:LZ -c "./migrate.sh -silent /opt/IBM/ITM/dchome1/7.2.0.0.1/bin/dc_config.txt"
-w /opt/IBM/ITM/dchome1/7.2.0.0.1/bin
```

8. Restart the application server instances.
   a. Stop the application server.

```
./tacmd executecommand -m System -c "./stopServer.sh server_name" -w profile_home/bin
```

For example:

```
./tacmd executecommand -m v5254005b0186:LZ -c "./stopServer.sh server3" -w /opt/IBM/WAS8/profiles/AppSrv01/bin
```

   b. Start the application server:

```
./tacmd executecommand -m System -c "./startServer.sh server_name" -w profile_home\bin
```

For example:

```
./tacmd executecommand -m v5254005b0186:LZ -c "./startServer.sh server3" -w /opt/IBM/WAS8/profiles/AppSrv01/bin
```

For more information about remote deployment, see the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Installing ITCAM Agent for WebSphere Applications remotely using Tivoli Enterprise Portal

You can use Tivoli Enterprise Portal to install ITCAM Agent for WebSphere Applications remotely. Before this installation, the agent support files must be installed on the Tivoli Enterprise Portal Server (including browser client support files), hub and remote Tivoli Enterprise Monitoring Servers, and Tivoli Enterprise Portal desktop clients.

These sections describe the steps for installing and upgrading the monitoring agent.

Adding the agent to the remote deployment depot

To make a remote installation available, you must first add ITCAM Agent for WebSphere Applications to the remote deployment depot on the remote Tivoli Enterprise Monitoring Server.

On Windows systems, see "Enabling application support on Windows systems" on page 61; be sure to select the agent for the remote deployment depot in Step 6 on page 63.

Performing a remote installation

You might have to prepare the host computer for installation of the agent. For more information, see Chapter 2, "Prerequisites and pre-installation tasks for ITCAM Agent for WebSphere Applications on Windows systems," on page 15 and Chapter 4, "Prerequisites and pre-installation tasks for ITCAM Agent for WebSphere Applications on Linux and UNIX systems," on page 97.

To install ITCAM Agent for WebSphere Applications remotely using IBM Tivoli Monitoring, complete the following procedure:

1. Select the node for installation in Tivoli Enterprise Portal. (The node must already be a part of IBM Tivoli Monitoring infrastructure; for details about setting up a node in IBM Tivoli Monitoring, see *IBM Tivoli Monitoring: Installation and Setup Guide*).
2. Right-click the name of the node, and select **Add Managed System...**
3. In the **Select a monitoring Agent** window, select **IBM Tivoli Composite Application Manager Agent for WebSphere Applications** and click **OK**.
4. The agent configuration window is displayed. Select **Configure Tivoli Enterprise Monitoring Agent**, and configure the monitoring agent settings. For more information, see "Configuring monitoring agent settings" on page 34. Other configuration options are not available before installation is complete.

   Important: While you create a response file, the **Browse** button is disabled. Therefore, you must enter the path name for the response file manually. The file is saved on the host where the agent is installed.
5. Click **Finish**. The agent installation process is started. You can track its progress in the **Deployment Status** workspace.

Configuring ITCAM Agent for WebSphere Applications remotely using Tivoli Enterprise Portal

You can use Tivoli Enterprise Portal to configure ITCAM Agent for WebSphere Applications remotely. You cannot configure the data collector remotely using the Tivoli Enterprise Portal.

To configure the data collector on a remote system from a command-line window, see "Installing and configuring ITCAM Data Collector for WebSphere on Windows systems" on page 206.

To configure ITCAM Agent for WebSphere Applications remotely using IBM Tivoli Monitoring, select the agent in the Tivoli Enterprise Portal. Right click it, and select **Configure**.

The **Managed System Configuration** window is displayed.

This window is the same as the agent configuration window that is available on the host where the agent is installed. Using this window, you can complete agent configuration. For more information, see “Configuring the monitoring agent on Windows systems” on page 32 for the configuration procedures.

Important: While you create a response file, the **Browse** button is disabled. Therefore, you must enter the path name for the response file manually. The file is saved on the host where the agent is installed.

Part 7. Advanced configuration of the Agent

Chapter 9. Customization and advanced configuration for the data collector

You can complete additional customization for your configuration of the data collector.

Properties files for the Data Collector

Several properties files control data collector configuration and behavior.

The properties files, and other files that are used by the data collector, are located under the *DC_home* directory.

For most common changes to this configuration, you must edit the data collector properties file and the toolkit properties file.

Important: After changing a configuration file, restart the monitored application server instance. Then the changes will take effect.

The Data Collector properties file

The data collector properties file is automatically created by the data collector, and is unique for every application server instance that is monitored by the data collector. Its name is *DC_home*/runtime/*appserver_version.node_name.server_name*/datacollector.properties.

However, to facilitate future upgrades, do not change this file.

Instead, add the settings that you want to modify to the data collector custom properties file. This file is named *DC_home*/runtime/*app_server_version.node_name.server_name*/custom/datacollector_custom.properties. Settings in the data collector custom properties file override the values that are in the data collector properties file.

Important: If the *DC_home*/runtime/*app_server_version.node_name.server_name*/custom/datacollector_custom.properties file does not exist, create it when you want to make changes. You might also have to create the custom directory.

The toolkit properties file

The toolkit properties file is automatically created by the data collector at startup, using various input files. It is unique for every application server instance monitored by the data collector. Its name is *DC_home*/runtime/*appserver_version.node_name.server_name*/toolkit.properties.

Because this file is re-created at each data collector startup, **do not make any changes** to this file; if you do, they will be overwritten.

Instead, add the settings that you want to modify to the toolkit custom properties file. This file is named *DC_home*/runtime/

app_server_version.*node_name*.*server_name*/custom/toolkit_custom.properties. Settings in the toolkit custom properties file override the values in the toolkit properties file.

You can also set toolkit properties for all the application server instances that are monitored by this installation of the data collector. To do this, add the settings to the global toolkit custom properties file: *DC_home*/runtime/custom/toolkit_global_custom.properties. However, if a property is set in the instance-specific toolkit_custom.properties file, it overrides the value in the global file for this instance.

Important: If the *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom/toolkit_custom.properties or *DC_home*/runtime/custom/toolkit_custom.properties file does not exist, create it when you want to make changes. You might also have to create the custom directory.

Other properties files

The following properties files are unique for every application server instance monitored by the data collector:

- *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/cynlogging.properties defines the log file names and logging details for the Java portion of the data collector.
- *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/cyncclog.properties defines the log file names and logging details for the C++ portion of the data collector.
- *DC_home*/runtime/*appserver_version*.*node_name*.*server_name*/kwjdc.properties defines communication with the monitoring agent, including the host name and port for the monitoring agent host.

Important: You can integrate the data collector with ITCAM for Transactions using the configuration utilities. You can modify these settings using the toolkit_custom.properites file. For more information about configuring the transaction tracking API (TTAPI), see *IBM Tivoli Composite Application Agent for WebSphere Applications: Configuring and using TTAPI*.

Data collector log files

The default location for the log files generated by the data collector configuration utility is *DC_home*\data on Windows systems and *DC_home*/data on Linux and UNIX systems.

The following table describes log files generated before and during the configuration process

Table 23. Log files generated before and during the configuration process

Full path name	Description
DC_home/data/config-console.log	User input while the config or reconfig script is running.
DC_home/data/config-message.log	Messages generated while the config or reconfig script is running.
DC_home/data/config-trace.log	Debug messages generate while the config or reconfig script is running.

Table 23. Log files generated before and during the configuration process (continued)

Full path name	Description
DC_home/data/reconfig.log	Log written during the reconfiguration of data collector for application servers.
DC_home/data/unconfig-console.log	User input while the unconfig script is running.
DC_home/data/unconfig-message.log	Messages generated while the unconfig script is running.
DC_home/data/unconfig-trace.log	Debug messages generated while the unconfig script is running.
DC_home/data/ profile.cell.node.configdatacollector.log For example: default.beta85.tvt6080. configdatacollector.log	Log written by the wsadmin script (configDataCollector.py) during configuration updates to WebSphere Application Server.
DC_home/data/ profile.cell.node.unconfigdatacollector.log For example: default.beta85.tvt6080. unconfigdatacollector.log	Log written by the wsadmin script (unconfigDataCollector.py) during unconfiguration updates to WebSphere Application Server.
DC_home/data/profile.findservers.log For example: default.findservers.log	Log generated by findSevers.py. The file is used for diagnosing problems with the find servers process.
DC_home/data/node.server_valCheck.log For example: tvt6080_rd-test_valCheck.log	Log generated by WebSphere Application Sever validity checking.

The data collector trace files are stored by default in the following locations:

- On Windows systems: *DC_home*\logs\CYN\logs.
- On Linux and UNIX systems: *DC_home*/logs/CYN/logs.

Restriction: For log and trace file names that include *profile*, *cell*, *node*, or *server* variables, when any of these variables includes non-ascii characters, the non-ascii characters are converted to ascii characters.

Tuning data collector performance and monitoring scope

The data collector monitors the performance of the application server in several ways. This monitoring introduces a performance overhead. The scope and accuracy of the monitoring can vary; but, when more information is gathered, the performance overhead is increased.

The monitoring scope is broadly determined by the monitoring level, which the user can set as necessary.

In the Tivoli Enterprise Portal, the available monitoring levels are L1 and L2. In the ITCAM for Application Diagnostics Managing Server Visualization Engine (MSVE), monitoring levels (known as Monitoring On Demand, or MOD, levels) are L1, L2, and L3. The MSVE is the user interface of the managing server which provides deep-dive diagnostics information.

This level is set independently for IBM Tivoli Monitoring and the managing server. For example, the user can set monitoring level L1 for Tivoli monitoring from the

Tivoli Enterprise Portal, and at the same time set MOD L2 in the MSVE. In this case, only L1 data is available in the Tivoli Enterprise Portal, but L2 information is displayed in the MSVE.

Important: In ITCAM for Applications version 7.2, the managing server (deep-dive) functionality is not available. Unless you have ITCAM for Application Diagnostics version 7.1 installed in your environment, you can ignore all references to this function.

You can also set the *sampling rate* for the managing server and monitoring agent independently. For the managing server, the sampling rate determines the percentage of monitored requests that are archived in the database. Irrespective of the sampling rate, all data is sent to the managing server, so the resource usage of the data collector is not affected by it. The sampling rate is set separately for every data collector installation. Having a low sampling rate does not prevent the user from seeing requests that have hung in-flight, nor does it prevent managing server traps and Tivoli Enterprise Portal situations from working on all requests. Generally, a 2% sampling rate is suggested for MOD L1 Tivoli monitoring data collection in a production environment where data is often stored for 15 to 30 days or more.

Important: For managing server data collection, the sampling rate does not apply to custom request and nested request monitoring.

You can also fine-tune the data collector monitoring process using the properties files. This affects the performance overhead, and the scope and accuracy of the monitoring. Although the default configuration is broadly acceptable for common situations, you can use the properties files to reach the performance and monitoring that closely match the requirements of your environment.

Data collector internal buffering settings

The following parameters affect buffering in communication between the data collector and ITCAM for Application Diagnostics Managing Server. In most cases, the default settings are appropriate. Do not change these parameters unless directed by IBM Software Support. These settings do not affect communication with the monitoring agent.

Remember: If you use ITCAM for Applications, the managing server (deep-dive) functionality is not available, so you can ignore all references to this function.

Internal Buffering settings

The following parameters in the data collector properties file control internal buffering in the data collector. For more information about data collector properties, see "The Data Collector properties file" on page 221.

internal.memory.limit

The default value is `100` (MB). This property limits the amount of memory that the data collector can use for all of its buffering needs. Reducing this setting can lower the memory overhead that is introduced by the data collector. However, a reduced setting can also increase the probability of buffer overflow at MOD L2 or L3 during periods of high transaction volume. You can also reduce buffer load by limiting the monitoring scope for MOD L2 and L3, using the settings in the rest of this chapter, especially "Controlling instrumentation of application classes for lock analysis, memory leak analysis, and method profiling and tracing" on page 227.

internal.memory.accept.threshold
The default value is 2 (MB). When the amount of memory specified in `internal.memory.limit` is reached, a buffer overflow state happens, and data is not buffered. This property specifies the minimum amount of free memory to be reached before buffering is resumed.

internal.url.limit
The default value is `1000`. This property controls the maximum URL length that is accepted by the data collector. If your URL length typically exceeds this value, increase it to avoid display truncation.

internal.sql.limit
The default value is `5000`. This property controls the maximum SQL length that is accepted by the data collector. If your SQL statement length is typically greater than this value, increase it to avoid display truncation.

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.

internal.probe.event.packet.size
The default value is `5000` Kbytes. Changing the default is not recommended. Valid values are `1` to `4000000` (or up to available process memory on the server). This property specifies the size of the data collector 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, because the default send buffer size is adequate.

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

If the data collector is to communicate with ITCAM for Application Diagnostics Managing Server, and two or more application servers use Remote Method Invocation over Internet InterORB Protocol (RMI/IIOP), you must enable instrumentation and monitoring of RMI/IIOP requests in order to view composite requests (via correlation icons) in the visualization engine.

Remember: If you use ITCAM for Applications, the managing server (deep-dive) functionality is not available, so you can ignore all references to this function.

All of the servers must be instrumented by data collectors connected to the same Managing Server.

For all the application servers, in the toolkit custom properties file, add or uncomment the following property:

```
org.omg.PortableInterceptor.ORBInitializerClass.com.ibm.tivoli.itcam.toolkit.
   ai.orbinterceptor.Initializer=true
```

For information about properties files, see “The toolkit properties file” on page 221.

Disabling various types of Byte Code Instrumentation for JEE APIs

In Byte Code Instrumentation (BCI), the data collector intercepts method entry and exit calls for various types of Java APIs in order to create an execution flow of each application request. Some resources are used for the monitoring. You can tune the data collector so that some of the APIs are not monitored, reducing resource use.

For some APIs, you can also disable collection of BCI information for MOD L1, reducing resource use for this level (typically enabled most of the time on production systems).

To disable BCI monitoring for JEE APIs, add the following properties to the toolkit custom properties file. For more information about this file, see "The toolkit properties file" on page 221.

Table 24. Adding lines to the toolkit custom properties file

Type of JEE 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`
Web containers for Servlets/ JavaServer Pages (JSP)	`com.ibm.tivoli.itcam.dc.was.webcontainer=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	`com.ibm.tivoli.itcam.toolkit.ai.axis.enablewebservice=false`
Remote Method Invocation (RMI)	`am.ejb.rmilistener.enable=false`
IBM WebSphere Application Server EJB container	`com.ibm.tivoli.itcam.dc.was.enableEJBContainer=false`

BCI nested request information is only collected for MOD levels L2 and L3. If the MOD Level is set to L1, only edge request information is collected by BCI. (The MOD Level set for IBM Tivoli Monitoring does not affect the data sent to the managing server, and vice versa).

For the following API types, BCI information (if it is not disabled completely) is also collected at MOD L1. For performance reasons, you can disable it only for L1

monitoring, while keeping it enabled for L2 and L3. To do this, add (or uncomment) the following lines in the toolkit custom properties file:

Table 25. Modifying lines in the toolkit custom properties file

Type of JEE 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`

Important: Setting any of these properties to `false` can result in missing data when MOD Level is switched from L1 to L2. For example, the data collector might be unable to determine the data source names for JDBC requests.
For more information about the toolkit properties file, see "The toolkit properties file" on page 221).

Controlling instrumentation of application classes for lock analysis, memory leak analysis, and method profiling and tracing

The data collector can use Byte Code Instrumentation (BCI) to collect lock analysis information, memory leak analysis information (at MOD L3), method profiling (at MOD L2) and application method entry and exit (at MOD L3). Instrumentation for this data is disabled by default, and you must enable it if the information is required. This information is only displayed in the visualization engine of ITCAM for Application Diagnostics Managing Server.

Remember: If you use ITCAM for Applications, the managing server (deep-dive) functionality is not available, so you can ignore all references to this function.

To enable BCI for lock analysis, Level 3 memory leak analysis, and Level 3 method entry and exit tracing, you must adjust the toolkit custom properties file. For information about this file, see "The toolkit properties file" on page 221.

Making these adjustments activates the use of one or more configuration files in the *DC_home*`/itcamdc/etc` directory. These files contain the default settings to control BCI. The configuration files and default settings are described in the following table:

Table 26. Byte Code Instrumentation configuration files

File name	Purpose	Default behavior
`lock_analysis.xml`	Defines application lock analysis BCI. Specific behavior in each MOD level is determined by settings in the data collector properties file.	Lock acquisition and release requests for all application classes are Byte-Code-Instrumented. Lock event, lock contention, and lock reporting information is provided in MOD L2 and MOD L3. (You can enable lock analysis for MOD L1 as well; see "Customizing lock analysis" on page 228).
`memory_leak_diagnosis.xml`	Defines application Memory Leak Diagnosis BCI.	Heap allocations for all classes instantiated by all application classes are Byte-Code-Instrumented. Leak Analysis data is collected at MOD L3.

Table 26. Byte Code Instrumentation configuration files (continued)

File name	Purpose	Default behavior
`method_entry_exit.xml`	Defines application method entry and exit BCI.	All non-trivial methods for all application classes, subject to certain thresholds and limits, are Byte-Code-Instrumented. Method profiling data is collected at MOD L2; method entry and exit analysis data is collected at MOD L3.

If you want to enable one or more of the BCI features with the default settings, for more information, see "Enabling Byte Code Instrumentation features with default settings."

If you want to customize the default settings and make more granular choices for what classes and methods to modify, see the following sections for more information:

- "Customizing lock analysis"
- "Customizing memory leak diagnosis" on page 231
- "Customizing method profiling and method entry and exit tracing" on page 232

Important: Enabling Byte Code Instrumentation for any of these features slightly increases resource usage even on monitoring levels where no data is collected for them.

Enabling Byte Code Instrumentation features with default settings

To enable one or more of the BCI features (lock analysis, Level 3 memory leak analysis, and method profiling and entry and exit tracing,) with the default settings, complete the following procedure. Method profiling at MOD L2 and method entry and exit tracing at MOD L3 are enabled by the same properties.

1. In the 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.lock=DC_home/itcamdc/etc/lock_analysis.xml
   am.camtoolkit.gpe.customxml.leak=DC_home/itcamdc/etc/memory_leak_diagnosis.xml
   am.camtoolkit.gpe.customxml.L3=DC_home/itcamdc/etc/method_entry_exit.xml
   ```

   For more information about the toolkit properties file, see "The toolkit properties file" on page 221. For more information about Byte Code Instrumentation configuration files, see Table 26 on page 227 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.enablelockanalysis=true
   com.ibm.tivoli.itcam.toolkit.ai.enablememoryleakdiagnosis=true
   com.ibm.tivoli.itcam.toolkit.ai.methodentryexittrace=true
   ```

Customizing lock analysis

By default, if lock analysis is enabled, lock acquisition and release requests for all application classes are Byte-Code-Instrumented. With default settings, lock contention information is provided in MOD L2 and MOD L3. You may configure the data collector to modify the lock information provided on the different MOD levels, and to exclude some classes from BCI for lock analysis.

Configuring lock analysis information for MOD levels

The following properties in the data collector properties file control the lock analysis information provided by the data collector. For more information about properties files, see "Properties files for the Data Collector" on page 221.

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

This property controls whether lock acquisition and release events are collected and passed to the managing server. (If the managing server is not used, this parameter is ignored). The variable *n* can represent MOD L1, L2 or L3. Possible values are `true` or `false`. In most cases, the recommended setting at all levels is `false` because there is little benefit in displaying lock acquisition events if they do not involve contention; lock contention events are collected separately. However, you might want to enable lock event collection for some development tasks.

Example:

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

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

This property controls whether lock contention events are collected and passed to the managing server. (If the managing server is not used, this parameter is ignored). The variable *n* can represent MOD L1, L2 or L3. Possible values are `true`, `false` or `justone`.

`True` indicates contention records are collected. For each lock acquisition request that results in contention, a pair of contention 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, regardless of how many threads actually acquired the lock before the requesting thread.

Setting this property to `true` enables you to determine whether 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 helps you to collect just one pair of contention records for each lock acquisition that encountered contention. The recommended setting at L3 is `true`. In order to identify every thread that acquired the lock ahead of the requesting thread, this setting has a high performance cost, which is common for L3 monitoring. To reduce performance impact, enable L3 for a limited time only.

Example:

```
internal.lockanalysis.collect.L2.contend.events = justone
```

internal.lockanalysis.collect.L*n*.contention.inflight.reports

This parameter controls whether data is collected for the Lock Contention report, available in the visualization engine of the managing server. (If the managing server is not used, this parameter is ignored). The variable *n* can represent Mod L1, L2, or L3. Possible values are `true` or `false`. 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
```

Setting classes for lock analysis instrumentation

To set classes for lock analysis instrumentation, complete the following procedure:

1. Make a copy of the *DC_home*/itcamdc/etc/lock_analysis.xml file in a temporary location. Open the copy in a text editor.
2. Modify the lockingClasses specification in the file.

   This element defines the classes for which lock requests are 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 element 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. It matches any sequence of characters that starts and ends with the package separator (.).

     For example, java..String matches java.lang.String and com.ibm..* matches any declaration beginning with com.ibm.
   - If the locking class name begins with an exclamation point (!), any classes matching the classes that are 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 excluded.

   In the following example, an application with a package name of com.mycompany.myapp has the following requirements:

   - Only classes that begin with Cus or Sup must be Byte-Code-Instrumented for lock analysis.
   - The Supplier class must not be Byte-Code-Instrumented for lock analysis.

   The following example shows 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 the *DC_home*/runtime/*app_server_version.node_name.server_name*/custom directory, then complete the following steps:
     a. In the toolkit custom properties file, set the property am.camtoolkit.gpe.customxml.lock to the name (without path) of the file that you modified in Step 2. For more information about toolkit custom properties files, see "The toolkit properties file" on page 221.
     b. In the same toolkit custom properties file, set the following property to true:

        com.ibm.tivoli.itcam.toolkit.ai.enablelockanalysis=true

- Save the file in any directory on the monitored host. Complete the following steps:
  a. In the toolkit custom properties file, set the property `am.camtoolkit.gpe.customxml.lock` to the path and name for the file that you modified in Step 2 on page 230. For more information about the toolkit custom properties file, see "The toolkit properties file" on page 221.
  b. In the same toolkit custom properties file, set the following property to `true`:

     ```
     com.ibm.tivoli.itcam.toolkit.ai.enablelockanalysis=true
     ```

Customizing memory leak diagnosis

By default, if memory leak analysis is enabled, all application classes are Byte-Code-Instrumented for memory leak analysis and all information is collected in MOD L3. You can configure the data collector to exclude some classes from BCI for memory leak analysis.

To set classes for Memory Leak Diagnosis, complete the following procedure:

1. Make a copy of the *DC_home*`/itcamdc/etc/memory_leak_diagnosis.xml` file in a temporary location. Then, open the copy in a text editor.
2. Modify the parameters in the file. The following table describes the tags that you can modify:

Table 27. Parameters for the memory leak diagnosis configuration file

Tag name	Description
`heapAllocationTarget`	Defines the allocating and allocated classes for which heap allocations are 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 `allocatingClassName` and `allocatedClassName` tags can include wildcard characters. The following description is a summary of 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. It matches any sequence of characters that starts and ends with the package separator (.).

  For example, `java..String` matches `java.lang.String` and `com.ibm..*` matches any declaration beginning with `com.ibm.`
- 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 excluded.

For example, an application with a package name of `com.mycompany.myapp` has the following requirements:

- Within the `Customer` class, all heap allocations must be Byte-Code-Instrumented.
- Within the `Supplier` class, all heap allocations must be Byte-Code-Instrumented except for allocations for classes beginning with `java.lang.String`.

The following example shows 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 the *DC_home*`/runtime/`*app_server_version*`.`*node_name*`.`*server_name*`/custom` directory. Complete the following steps:
     a. In the toolkit custom properties file, set the property `am.camtoolkit.gpe.customxml.leak` to the name (without path) of the file that you modified in Step 2 on page 231. For more information about the toolkit custom properties file, see "The toolkit properties file" on page 221.
     b. In the same toolkit custom properties file, set the following property to `true`:

        ```
        com.ibm.tivoli.itcam.toolkit.ai.enablememoryleakdiagnosis=true
        ```
   - Save the file in any directory on the monitored host. Complete the following steps:
     a. In the toolkit custom properties file, set the property `am.camtoolkit.gpe.customxml.leak` to the path and name for the file that you modified in Step 2 on page 231. For more information about the toolkit custom properties file, see "The toolkit properties file" on page 221.
     b. In the same toolkit custom properties file, set the following property to `true`:

        ```
        com.ibm.tivoli.itcam.toolkit.ai.enablememoryleakdiagnosis=true
        ```

Customizing method profiling and method entry and exit tracing

Method profiling and method entry and exit tracing are enabled together and use the same call interceptions. Method profiling is performed at MOD L2, and method

entry and exit tracing is performed at MOD L3. You can configure the data collector to change the thresholds and limits for method profiling, and to exclude some classes and methods for method entry and exit tracing.

Customizing thresholds for Level 2 method profiling

The data collector only instruments method profiling data when the method exceeds certain thresholds of processor time and real ("wall clock") time usage. The total number of methods, stack size, and running thread size are also limited. You can customize the thresholds and limits.

The following properties in the data collector properties file control the thresholds and limits for method profiling. For more information about properties files, see "The Data Collector properties file" on page 221.

am.mp.cpuThreshold
The default is `30` milliseconds. Only the methods that take at least the minimum amount of processor time specified in this property are captured for method profiling data. This avoids unnecessary clutter. Generally, methods with greater than the value that is specified in this property are considered useful. Customers can reduce or increase this value if required.

am.mp.clockThreshold
The default is `30` milliseconds. Only the methods that take at least the minimum amount of wall clock time specified in this property are captured for method profiling data. This avoids unnecessary clutter. Generally, methods with greater than the value that is specified in this property are considered useful. Customers can reduce or increase this value if required.

am.mp.leagueTableSize
The default is `1000`. This is the maximum number of methods that are monitored for method profiling data. Customers can reduce or increase this value if required. Decreasing it helps to reduce memory requirements.

am.mp.methodStackSize
The default is `100`. This is the maximum stack size of any running thread that is recorded in method profiling.

Setting classes and methods for Level 3 method entry and exit tracing

By default, method entry and exit tracing on MOD L3 is performed for all classes and methods. To set specific classes and methods for method entry and exit analysis, complete the following procedure:

1. Make a copy of the *DC_home*`/itcamdc/etc/method_entry_exit.xml` file in a temporary location. Open the copy in a text editor.
2. Modify the parameters in the file. The following table describes the parameters that you can modify:

Table 28. Parameters for the Level 3 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.

Table 28. Parameters for the Level 3 method entry and exit analysis configuration file (continued)

Tag name	Description
`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 `className` and `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 it is 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. It matches any sequence of characters that starts and ends with the package separator (.).

  For example, `java..String` matches `java.lang.String` and `com.ibm..*` matches any declaration beginning with `com.ibm.`
- If the method name begins with an exclamation point (!), any methods that match the method name are 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 excluded.

For example, an application with a package name of `com.mycompany.myapp` has the following requirements:

- Within the `Customer` class, all methods must be Byte-Code-Instrumented.
- Within the `Supplier` class, all methods must 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 *DC_home*`/runtime/`*app_server_version*`.`*node_name*`.`*server_name*`/custom` directory. Complete the following steps:
     a. In the toolkit custom properties file, set the property `am.camtoolkit.gpe.customxml.L3` to the name (without path) of the file

that you modified in Step 2 on page 233. For more information about toolkit custom properties files, see "The toolkit properties file" on page 221.

b. In the same toolkit custom properties file, set the following property to `true`:

```
com.ibm.tivoli.itcam.toolkit.ai.methodentryexittrace=true
```

- Save the file in any directory on the monitored host. Complete the following steps:

  a. In the toolkit custom properties file, set the property `am.camtoolkit.gpe.customxml.L3` to the path and name for the file that you modified in Step 2 on page 233. For more information about the toolkit custom properties file, see "The toolkit properties file" on page 221.

  b. Set the following property to `true`:

```
com.ibm.tivoli.itcam.toolkit.ai.methodentryexittrace=true
```

Defining custom requests

By default, only certain types of Java classes and methods are monitored as requests by the data collector. Servlets, JSPs, EJB business methods, and certain standard JEE APIs are recognized as requests. You can designate additional classes and methods as *custom requests*.

For example, the data collector does not recognize Struts Action classes as requests by default. However, you can set up custom request definitions and cause the actions to be recognized as Nested Requests.

Complete the following procedure to enable monitoring of custom requests and designate one or more methods as custom requests:

1. Make a copy of the *DC_home*`/itcamdc/etc/custom_requests.xml` file in a temporary location. Then, open the copy in a text editor.
2. Modify the parameters in the file. The following table describes the parameters that you can modify:

Table 29. Parameters for the 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 to the user when the method entry and exit are traced.
`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 in order 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.

Table 29. Parameters for the custom requests configuration file (continued)

Tag name	Description
requestMapper	Optional. If this tag is specified, the data collector uses a request mapper to determine information that identifies the request. You can define nonstandard ways of extracting this information. For more information about enabling and defining request mappers, see "Customizing request information mapping" on page 254.

The Matches and methodName tags can include wildcard characters. The following section describes how the wildcard characters works:

- 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. It matches any sequence of characters that starts and ends with the package separator (.).

  For example, java..String matches java.lang.String and com.ibm..* matches any declaration beginning with com.ibm.

For example, an application with a package name of com.mycompany.myapp has the following requirements:

- Within the Customer class, the creditCheck() method must be treated as a custom request called CreditCheck.
- Within the Supplier class, the inventoryCheck() method must be treated as a custom request called SupplyCheck.

The following example shows the contents of the customized custom_requests.xml file that accomplishes this:

```
<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 in the *DC_home*/runtime/*app_server_version.node_name.server_name*/custom directory. Then, in the toolkit custom properties file, set the property am.camtoolkit.gpe.customxml.custom to the name (without path) of the file that you modified in Step 2 on page 235. For more information about the toolkit custom properties file, see "The toolkit properties file" on page 221.
   - Save the file in any directory on your computer. Then, in the toolkit custom properties file , set the property am.camtoolkit.gpe.customxml.custom to the path and name for the file that you modified in Step 2 on page 235. For more information about the toolkit custom properties file, see "The toolkit properties file" on page 221.

Enabling asynchronous bean request monitoring

If your applications use asynchronous bean requests, and the requests are not displayed in the Tivoli Enterprise Portal or the visualization engine, you must enable asynchronous bean request monitoring using the toolkit custom properties file.

First, check whether custom requests have been defined on the data collector. For more information about defining custom requests, see "Defining custom requests" on page 235. Open the toolkit custom properties file and, if it exists, the global toolkit custom properties file. Check both of these files for the following property (not commented out):

```
am.camtoolkit.gpe.customxml.custom=xml_filename
```

For more information about the toolkit custom properties file, see "The toolkit properties file" on page 221.

If this property exists, custom requests are defined. In this case, edit the XML file that is named in the property. If both the instance-specific toolkit custom properties file and the global toolkit custom properties file have this property, use the file name from the instance-specific file. If the file name does not have a path, the file is located in the *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom directory. Find the tag </customEdgeRequests>, and add the following text immediately before this line:

```
<edgeRequest>
 <requestName>AsyncWorkBean</requestName>
 <Implements>com.ibm.websphere.asynchbeans.Work</Implements>
 <type>application</type>
 <methodName>run</methodName>
</edgeRequest>
<edgeRequest>
 <requestName>AsyncTimerBean</requestName>
 <Implements>commonj.timers.TimerListener</Implements>
 <type>application</type>
 <methodName>timerExpired</methodName>
</edgeRequest>
<edgeRequest>
 <requestName>AsyncAlarmBean</requestName>
 <Implements>com.ibm.websphere.asynchbeans.AlarmListener</Implements>
 <type>application</type>
 <methodName>fired</methodName>
</edgeRequest>
```

If the property does not exist (or is commented out), custom requests have not been defined. In this case, complete the following procedure:

1. Create a file: *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom/custom_requests_async.xml, with the following text:

```
<gpe>
 <bci>
  <customEdgeRequests>
   <edgeRequest>
    <requestName>AsyncWorkBean</requestName>
    <Implements>com.ibm.websphere.asynchbeans.Work</Implements>
    <type>application</type>
    <methodName>run</methodName>
   </edgeRequest>
   <edgeRequest>
    <requestName>AsyncTimerBean</requestName>
    <Implements>commonj.timers.TimerListener</Implements>
    <type>application</type>
    <methodName>timerExpired</methodName>
```

```
    </edgeRequest>
    <edgeRequest>
     <requestName>AsyncAlarmBean</requestName>
     <Implements>com.ibm.websphere.asynchbeans.AlarmListener</Implements>
     <type>application</type>
     <methodName>fired</methodName>
    </edgeRequest>
   </customEdgeRequests>
  </bci>
 </gpe>
```

2. In the toolkit custom properties file, set the following property:

   ```
   am.camtoolkit.gpe.customxml.custom=custom_requests_async.xml
   ```

For more information about the toolkit custom properties file, see "The toolkit properties file" on page 221.

After completing the changes that are described in this section, restart the application server instance that is monitored by the data collector.

Customizing monitoring of custom MBeans

By default, the data collector monitors WebSphere Application Server MBeans. If the environment includes custom MBeans, you can configure the data collector to monitor some of them (according to specific definitions), or all of them.

Configuring data collection for specific custom MBeans

You can define specific MBeans. Data collection is enabled for these MBeans only.

Important: Data collection for the JEE Domain MBean is not available in an IBM WebSphere Application Server environment.

To customize the generic configuration for JMX data collection, complete the following procedure:

1. Make a copy of the *DC_home*/toolkit/etc/was/*app_server_version*/mbeanconfig_*app_server_version*.xml file in a temporary location. Then, open the copy in a text editor.
2. Modify the parameters to fit your custom MBean. The following table describes the parameters that you can modify:

Table 30. Parameters for the JMX MBean configuration file

Element	Nested within	Description
Version	DomainList	Defines the version of the application server
Name	Domain	Defines a domain. If the asterisk (*) is defined, all MBeans that match the query ObjectName are returned; otherwise, only the MBeans that belong to this domain name are returned.
Description	Domain	Describes the domain. This can be any text string.
MBean	Domain	Defines the MBeans that are to be collected.
ObjectName	MBean	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 is replaced with the actual object name internally.
Category	MBean	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.

Table 30. Parameters for the JMX MBean configuration file (continued)

Element	Nested within	Description
RetrieveAllAttrs	MBean	A value of true indicates that all the attributes for the MBean must be collected. If you set this to false, you must define the attributes in the Attr element.
Attr	MBean	Defines the attributes that are to be collected. There can be multiple Attr elements, defining multiple attributes.
Name	Attr	The attribute name.
MappedKey	Attr	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.
MBean	Attr	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.
JavaBean	Attr	Defines the embedded MBean within this attribute. This tag is used when an attribute has an embedded MBean, which refers to another java object. The references java object has the elements of a JavaBean (setter, getter).
TargetType	Attr	Defines the type of the attribute. This is usually specified for the JavaBean type to determine the attribute type.

3. Complete one of the following steps:
   - Save the file in the *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom directory. Then, in the toolkit custom properties file, set the property am.camtoolkit.jmxe.custom to the name (without path) of the file that you modified in Step 2 on page 238. For more information about the toolkit custom properties file, see "The toolkit properties file" on page 221.
   - Save the file in any directory on the monitored host. Then, in the toolkit custom properties file, set the property am.camtoolkit.jmxe.custom to the path and name for the file that you modified in Step 2 on page 238. For more information about this file, see "The toolkit properties file" on page 221.

Enabling and customizing data collection for all custom MBeans

You can enable data collection for all custom MBeans and customize the way that they are identified to the user.

To enable it, in the toolkit properties file, add the following property:

```
am.getallmbeans=y
```

For more information about the toolkit properties file, see "The toolkit properties file" on page 221.

This property is in effect only if the custom MBeans property is commented out in the toolkit properties file, as shown in the following example:

```
#  Uncomment the line  to enable custom mbeans
#am.camtoolkit.jmxe.custom=
   C:/PROGRA~1/IBM/itcam/WEBSPH~1/DC/itcamdc/etc/custom_mbeanconfig.xml
```

Tip: Check that the am.camtoolkit.jmxe.custom property is also not present in the toolkit global properties file. For more information about this file, see "The toolkit properties file" on page 221.

The following properties provide additional options for the display of the MBean data:

```
am.jmxkeyword=type_identifier
am.jmxusecanonical=y
am.jmxtruncate=n
am.jmxlength=30
```

The properties and their definitions are:

am.getallmbeans

To enable data collection for all MBeans, set this property to `y` . If it is set to `n`, data collection for all MBeans is disabled. If the custom MBeans property (`am.camtoolkit.jmxe.custom`) is set, `am.getallmbeans` has no effect.

am.jmxkeyword

The visualization engine presents data on the monitored MBeans by organizing them into categories. The category name is formed from the Domain and type keywords in the MBeans Object Name. If the type keyword does not exist, the name keyword is used to create the category. If the name keyword does not exist, then the object name is used as the category. If this default behavior does not provide enough granularity to distinguish MBean categories, you can use the `am.jmxkeyword` property to define more keywords to be included in the category name.

For example, if you specify `am.jmxkeyword=identifier`, then the value of the identifier keyword from the object name is included in the category name, in addition to value of the type keyword. More than one keyword can be specified in the property. The keywords must be separated by a comma (,).

am.jmxusecanonical

If you want to see all of the keywords from the object name in the category, assign the `am.jmxusecanonical=y` property. This setting results in including all keyword values for the category name, separated by an underscore (_) character.

am.jmxtruncate

In some cases, especially if `am.jmxusecanonical=y`, the category name can be long. By default, the data collector truncates the category name to the length specified by the `am.jmxlength` property, or to 30 characters if the `am.jmxlength` property is not specified. If you do not want the category name to be truncated, you must specify the `am.jmxtruncate=n` property.

am.jmxlength

This property specifies the maximum length of the category name. The default is 30. This property is ignored if the `am.jmxtruncate=n` property is specified.

Modifying performance monitoring infrastructure settings

If the data collector communicates with ITCAM for Application Diagnostics Managing Server, the level of instrumentation for Performance Monitoring Infrastructure (PMI) is determined by the current MOD level that is set in the visualization engine. You can customize the PMI level for each MOD level. The collection level set in Tivoli Enterprise Portal does not affect the PMI level.

Remember: If you use ITCAM for Applications, the managing server (deep-dive) functionality is not available, so you can ignore all references to this function.

By default, the following PMI setting is enabled at each managing server MOD level:

Table 31. Default Performance Monitoring Infrastructure instrumentation settings

Monitoring (MOD) level	PMI setting
1	`Basic`
2	`Extended`
3	`All`

To customize these settings, in the data collector custom properties file (for more information about this file, see "The Data Collector properties file" on page 221), complete the following procedures:

Table 32. Procedures to customize instrumentation of the Performance Monitoring Infrastructure

Type of customization	Procedure

Change the PMI setting that is set for a particular managing server monitoring (MOD) level.	Add or uncomment one or more of the following lines and give it a different setting. The possible values are `none`, `basic`, `extended`, or `all`:
	`am.was6pmi.settings.1=basic`
	`am.was6pmi.settings.2=extended`
	`am.was6pmi.settings.3=all`

Complete fine-grained customization of the instrumentation for a particular PMI module at a particular monitoring level. For a description of the numeric IDs that you need when customizing PMI instrumentation at this detailed level, see the following website: http://www.ibm.com/support/docview.wss?uid=swg21221308	Add a line to set fine-grained customization for a particular module at a particular monitoring level. It has the format `module_type=number1,number2,...`, for example:
	`am.was6custompmi.settings.1=beanmodule=1,2,3,4,5,6,7,8, 9,10,14,15,19,20,21,22,23,24,25,28,29,30,31,32,33,34`
	Use `*` to monitor all IDs in the module, or `none` to monitor none:
	`am.was6custompmi.settings.3=beanModule=*`
	`am.was6custompmi.settings.3=webAppModule=none`

Tip: The `am.was6pmi.*` property names are also valid for monitoring version 7, version 8, and version 8.5 application servers.

If you do not want the level of instrumentation for PMI to change as the managing server MOD level changes, add the following line to the data collector custom properties file (see "The Data Collector properties file" on page 221):

```
am.pmi.settings.nochange=true
```

After making the changes, restart the application server instance.

Enabling Performance Monitoring Infrastructure settings for the Service Integration Bus

You can configure the data collector to collect Service Integration Bus (SIB) Performance Monitoring Infrastructure (PMI) data.

To do this, add the following lines to the data collector custom properties file:

```
am.was6custompmi.settings.1=SIB Service=*
am.was6custompmi.settings.2=SIB Service=*
am.was6custompmi.settings.3=SIB Service=*
```

These lines set custom PMI settings for Level 1, Level 2 and Level 3 monitoring levels respectively.

Tip: The `am.was6custompmi.*` property names are also valid for monitoring version 7, version 8, and version 8.5 application servers.

After you make the changes, restart the application server instance.

For more information about the data collector custom properties file, see "The Data Collector properties file" on page 221.

Enabling and disabling instrumentation of web services as new request types

By default, the data collector monitors all web services. You can disable the monitoring of web services.

To disable instrumentation of web services, set the following property in the data collector custom properties file:

```
ws.instrument=false
```

For more information about the data collector custom properties file, see "The Data Collector properties file" on page 221.

Important: To enable web services composite request monitoring and correlation in the ITCAM for Application Diagnostics Managing Server visualization engine, you must monitor both the web services requester (client) and the web services provider (server) using ITCAM Agent for WebSphere Applications data collectors. The data collectors must be connected to the same Managing Server.

Remember: If you use ITCAM for Applications, the managing server (deep-dive) functionality is not available, so you can ignore all references to this function.

Enabling user ID extraction for servlet and portal requests

By default, the data collector does not monitor the user ID for individual servlet and portal requests. You can enable such monitoring. In this case, the user ID is displayed in the ITCAM for Application Diagnostics Managing Server Visualization Engine.

Enabling user ID extraction for servlet requests

To enable user ID extraction for servlet requests, complete the following procedure:

1. Copy the file *DC_home*/itcamdc/etc/servlet_userid.xml into the directory *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom.
2. Add the following lines to the toolkit custom properties file:

   ```
   com.ibm.tivoli.itcam.toolkit.ai.enable.servletrequestmapper=true
   am.camtoolkit.gpe.customxml.servletUserid=servlet_userid.xml
   ```

   For more information about the toolkit properties file, see "The toolkit properties file" on page 221.

Tip: You can also enable the extraction for all monitored application instances. To do this, place the servlet_userid.xml file into the *DC_home*/runtime/custom directory, and add the lines to the global custom toolkit configuration file. For more information about this file, see "The toolkit properties file" on page 221. By default, the data collector extracts the user ID from the user attribute of the HttpServletRequest object. You can change the algorithm by editing the file servlet_userid.xml:

- To use the HTTP session object instead of the HttpServletRequest, change the lines:

```
<symbol>
            <name>$uidSource</name>
            <eval>$REQUEST</eval>
</symbol>
```

  to:

```
<symbol>
            <name>$uidSource</name>
            <eval>$SESSION</eval>
</symbol>
```

- To use a different attribute name (for example, username) of the session or request object, change the lines:

```
<symbol>
            <name>$uidAttName</name>
            <eval>"user"</eval>
</symbol>
```

  to:

```
<symbol>
            <name>$uidAttName</name>
            <eval>"username"</eval>
</symbol>
```

  Replace username with the correct name of the attribute, do not remove the quotations.

- To use the httpServletRequest.getRemoteUser() method to determine the user ID, change the lines:

```
<symbol>
            <name>$uidSource</name>
            <eval>$REQUEST</eval>
</symbol>
```

  to:

```
<symbol>
            <name>$uidSource</name>
            <eval>REMOTE_USER</eval>
</symbol>
```

You can also customize user ID extraction by editing the request mapper defined in servlet_userid.xml. For a full description and examples of customized request mappers, see "Customizing request information mapping" on page 254.

Enabling user ID extraction for portal requests

To enable user ID extraction for portal requests, complete the following procedure:

- Copy the file *DC_home*/itcamdc/etc/portal_userid.xml into the directory *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom.

- Add the following lines to the toolkit custom properties file (for more information about this file, see "The toolkit properties file" on page 221):

```
com.ibm.tivoli.itcam.toolkit.ai.enable.portalrequestmapper=true
com.ibm.tivoli.itcam.toolkit.ai.enable.portal6requestmapper=true
am.camtoolkit.gpe.customxml.portalUserid=portal_userid.xml
```

Tip: You can also enable the extraction for all monitored application instances. To do this, place the `portal_userid.xml` file into the *DC_home*`/runtime/custom` directory, and add the lines to the global custom toolkit configuration file. For more information about this file, see "The toolkit properties file" on page 221. By default, the data collector extracts user ID by calling the `request.getRemoteUser()` method.

You can also customize user ID extraction by editing the request mapper defined in the `portal_userid.xml` file. For a full description and examples of customized request mappers, see "Customizing request information mapping" on page 254.

Enabling and disabling memory monitoring

The data collector can monitor native memory usage and save results to a log file. This capability is disabled by default.

If you enable data collector memory monitoring, the data collector saves memory usage statistics to the (`trace-dc-native.log`) trace log file. For the location of the data collector trace log file, see the *IBM Tivoli Composite Application Manager: Agents for WebSphere Applications, J2EE, and HTTP Servers Troubleshooting Guide* .

The statistics reflect data collector memory consumption on the native side. The Java side memory consumption is not reflected in the logged numbers.

To enable memory monitoring, set the following property in the data collector custom properties file :

```
log.statistics=true
```

For more information about the data collector custom properties file, see "The Data Collector properties file" on page 221.

By default, the statistics are logged once every 30 seconds. You can set a different period, in milliseconds, in the `log.statistics.frequency` property in the data collector custom properties file. For example, to log memory usage statistics once every 10 seconds, use the following setting:

```
log.statistics.frequency=10000
```

To disable memory monitoring, set the following property in the data collector custom properties file:

```
log.statistics=false
```

Configuring the data collector when changing the application server version

If you upgrade the application server that is being monitored by the data collector from a 7.0 version to a 8.0 or 8.5 version, you must reconfigure the data collector to point to the updated instance of the application server.

Complete the following steps:

1. Unconfigure the data collector from all application server instances before the upgrade. In a Network Deployment environment, the Deployment Manager and the Node Agents must be running, but the application servers instances can be stopped. For more information about unconfiguring the data collector, see “Unconfiguring ITCAM Data Collector for WebSphere” on page 46 on Windows systems or “Unconfiguring ITCAM Data Collector for WebSphere” on page 129 on Linux or UNIX systems.
2. Complete the upgrade of the application server.
3. For a non-Network Development environment, make sure that the application server instance is upgraded and started. For a Network Deployment environment, make sure that the Node Agent and Deployment Manager are upgraded and started; do not start the instances.
4. Use the ITCAM Data Collector for WebSphere Configuration utility to configure the data collector for each application server instance. For more information about data collector configuration, see “Configuring the monitoring agent on Windows systems” on page 32 or “Configuring the monitoring agent on Linux and UNIX systems” on page 111.
5. Start or restart the monitored application server instance. For information about restarting the application server, see “Restarting the application server” on page 313.

Steps to complete if the IP address of the application server host is to be changed

If the IP address of the application server host is to be changed, complete the following procedure:

1. Use the ITCAM Data Collector for WebSphere Unconfiguration utility to unconfigure the data collector for this application server instance. For information about configuration, see “Unconfiguring ITCAM Data Collector for WebSphere” on page 46 on Windows systems or “Unconfiguring ITCAM Data Collector for WebSphere” on page 129 on Linux and UNIX systems.
2. Stop the instance of the application server that is being monitored by the data collector. For information about stopping the application server, see “Stopping the application server” on page 316.
3. Complete the IP address change at the operating system and network level.
4. Start the instance of the application server that is being monitored by the data collector. For information about starting the application server, see “Starting the application server” on page 315.
5. Use the ITCAM Data Collector for WebSphere Configuration utility to configure the data collector again for this application server instance. For information about configuration, see “Configuring the monitoring agent on Windows systems” on page 32 or “Configuring the monitoring agent on Linux and UNIX systems” on page 111.

Moving the data collector to a different host computer

If the data collector communicates to ITCAM for Application Diagnostics Managing Server, you can move it to a different host computer while maintaining the same managing server identity (Probe ID and Controller ID). The managing server sees the new host as the continuation of the old, preserving history, analysis, and so on.

Remember: If you use ITCAM for Applications, the managing server (deep-dive) functionality is not available, so you can ignore all references to this function.

The following section describes some prerequisites for moving the data collector to a different host computer while keeping the same Probe ID and Controller ID:

- Host A and host B 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, complete the following procedure:

1. On host A, stop the instance of the application server that is being monitored by the data collector. For information about stopping the application server, see "Stopping the application server" on page 316.
2. On host B, install the data collector and configure it using the Visualization Engine (Application Monitor) user interface. Configuring the data collector generates the *DC_home*/runtime/*appserver_version*.*node_name*.*server_name*/id file and other data collector runtime property files.
3. Using the Visualization Engine (Application Monitor) user interface, unconfigure the data collector on host B. This step deletes all information about this data collector from the ITCAM for Application Diagnostics database. Do not unconfigure the data collector using the configuration utility.
4. On host B, stop the instance of the application server that is being monitored by the data collector. For more information about stopping the application server, see "Stopping the application server" on page 316.
5. Copy the contents of the *DC_home*/runtime/*appserver_version*.*node_name*.*server_name*/id file on host A to the *DC_home*/runtime/*appserver_version*.*node_name*.*server_name*/id file on host B.
6. On host B, save the *DC_home*/runtime/*appserver_version*.*node_name*.*server_name*/id file.
7. On host B, start the instance of the application server that is being monitored by the data collector. For information about starting the application server, see "Starting the application server" on page 315.

The data collector on host B assumes the identity of the data collector on host A and is configured by the managing server with the runtime configuration of the data collector on host A. This does not affect monitoring in Tivoli Enterprise Portal.

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 must first install IBM Support Assistant (ISA). ISA provides extra help with diagnosing problems and provides extra tools and components for troubleshooting, and provides a place to write problems (PMRs).

Remember: If you use ITCAM for Applications, the managing server (deep-dive) functionality is not available, so you can ignore all references to this function.

MDD for Java analyzes manual or scheduled heap dumps performed by the ITCAM Heap Dump Management feature.

You can use the ITCAM 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 of the Visualization Engine (Application Monitor) user interface using MDD for Java. (The other Memory Diagnosis tools provided by ITCAM, such as Memory Analysis, Heap Analysis and Memory Leak Diagnosis, provide analysis through the Visualization Engine (Application Monitor) user interface.)

MDD for Java only analyzes heap dumps from IBM JDKs. For non-IBM JDKs, use the ITCAM Memory Leak Diagnosis feature.

Searching capabilities for ITCAM Agent for WebSphere Applications are not supported in ISA.

Where to install IBM Support Assistant and Memory Dump Diagnostic for Java

The following section describes two common configurations:

- Install ISA and MDD for Java on a stand-alone server that is not running an application server. After the IBM heap dump is collected on the application server, it must be transferred to the MDD for Java computer for post-processing.

  This configuration is recommended for production environments where you do not want the post-processing of the dump to affect 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 the need to transfer it.

  This configuration might be suitable for a development or test environment where the processor usage of analyzing the heap dump is not a concern.

The decision on where to install might also be influenced by the platforms supported by ISA.

Downloading, installing, configuring, and launching IBM Support Assistant and Memory Dump Diagnostic

For instructions on how to download, install, configure, and launch ISA, including the ISA plug-in for the agent, and Memory Dump Diagnostic for Java, see the online helps in the Visualization Engine (Application Monitor) user interface. Go to **Help > Welcome > Using IBM Support Assistant to diagnose problems**.

Important: ISA can be installed on both the data collector and Managing Server computers, but only the ISA installed on the Managing Server computer can be started from the Visualization Engine (Application Monitor) user interface.

Setting the Heap Dump scan interval

The Heap Dump Management function of ITCAM Agent for WebSphere Applications can create Heap Dumps of the monitored IBM WebSphere Application Server by user request. This function is available only with ITCAM for Application Diagnostics Managing Server.

When in a defined time interval, ITCAM Agent for WebSphere Applications scans the existing Heap Dumps, in order to inform the user of their existence and 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 am.mddmgr.poll.delay property in the toolkit custom properties file to the new interval in seconds. For more information about this file, see "The toolkit properties file" on page 221.

Configuring a data collector for multiple network interfaces

If the application server host has multiple IP addresses at the time of data collector configuration, the ITCAM Data Collector for WebSphere Configuration utility sets the preferred IP address for communication with the managing server. If more than one IP address is added later, set the preferred IP address manually, as described in this section.

Remember: If you use ITCAM for Applications, the managing server (deep-dive) functionality is not available, so you can ignore all references to this function.

If the data collector must expose a specific IP to the Managing Server, complete one of the following steps:

1. In the data collector custom properties file, set the am.socket.exportip and am.socket.bindip properties to the IP address to be exposed. For more information about the data collector custom properties file, see "The Data Collector properties file" on page 221.
2. In the *DC_home*/runtime/*appserver_version.node_name.server_name*/dc.java.properties file, set the appserver.rmi.host property to the IP address to be exposed.
3. Make sure that the managing server can access the required IP address of the data collector (You can verify this by doing a ping).
4. If the data collector is using Port Consolidator:
   a. In the data collector custom properties file, set the proxy.host property to the IP address that is to be exposed. For more information about the data collector custom properties file, see "The Data Collector properties file" on page 221.
   b. In the *DC_home*/itcamdc/etc/proxy.properties file, set the am.socket.exportip and am.socket.bindip properties to the IP address to be exposed.
   c. In the Port Consolidator start script (*DC_home*/itcamdc/bin/proxyserverctrl_ws.bat or *DC_home*/itcamdc/bin/proxyserverctrl_ws.sh), set the property JAVA_RMI_SERVER_HOSTNAME to the IP address to be exposed.

Customizing RMI garbage collection interval

If the data collector communicates with ITCAM for Application Diagnostics Managing Server, it uses RMI over TCP/IP for this communication. One effect of using RMI is that garbage collection occurs every minute. If you do not want this to happen, you can set the garbage collection interval explicitly to a preferred interval.

Remember: If you use ITCAM for Applications, the managing server (deep-dive) functionality is not available, so you can ignore all references to this function.

You can set the garbage collection interval explicitly to a preferred interval by specifying the parameters in the **Generic JVM arguments** field. These parameters must be implemented as a pair.

To do this, complete the following steps:

1. Log in to the IBM WebSphere Application Server administrative console.
2. Click **Servers**.
3. Expand **Server Type** and select **WebSphere application servers**.
4. Click on the name of the server.
5. Expand **Java and Process Management** and select **Process Definition**.
6. Click **Server > Application Servers** and select the *server_name*.
7. Under the **Additional Properties** section, click **Java Virtual Machine**.
8. Scroll down and locate the text box for **Generic JVM argument**s.
9. In the **Generic JVM arguments** field, append the following parameters if such parameters do not exist, or update their values if they exist.

   ```
   -Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000
   ```

   Important: These values require a dash (-) in front of each parameter, and a single space between parameters. You must specify both parameters if you specify them at all. The value is in milliseconds; 3,600,000 represents one hour.

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).

If CICS translation correlation is enabled, the data collector callback code adds composite tracking data, called Global Publish Server (GPS) tokens, 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 for Application Diagnostics Managing Server Visualization Engine.

Remember: If you use ITCAM for Applications, the managing server (deep-dive) functionality is not available, so you can ignore all references to this function.

However, the presence of the GPS token in COMMAREA might not always be desirable. If ITCAM for CICS data collector or ITCAM for CICS Client is not installed on the CICS server, the GPS token might reach the server application, which might not process it correctly. For this reason, transaction correlation is disabled by default.

You can enable GPS tokens for specific transactions based on CTG gateway address or protocol; by CICS system; by CICS program or by the CICS transaction ID. Enable correlation with CICS systems that have the ITCAM for CICS data collector installed, configured, and enabled. To do this, edit the *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom/ctg.filters file. 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 does not have a GPS token inserted into the COMMAREA. "I" denotes an Include filter; any transactions matching an include filter has 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 or port, or both
- Server is the host name of the CICS server (this 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 for Multi Regional Operation (MRO) CICS/CTG environments, this parameter is of little use because 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 *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom/ctg.filters:

```
Type=E,Gateway=local://*
```

To disable addition of GPS tokens to transactions for programs starting'CYN$' to be run on the CICS3101 server, but enable them for transactions for the CYN$ECI2 program on the same server, use the following lines:

```
Type=E,Program=CYN$*,Server=CICS3101
Type=I,Program=CYN$ECI2,Server=CICS3101
```

The default configuration is to disable all correlation through the following line:

```
Type=E,Gateway=*
```

Modifying the garbage collection log path

The data collector configuration set the path for the garbage collection log file (itcam_dc_gclog.log or native_stderr.log) to *AppServer_home*/profiles/*profile_name*/logs/*server_instance_name*. For example, C:\Program~1\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\server1. For version 1.3 JDKs, you cannot modify this. For other JDKs, if you want to change the location or name of this log file, complete the following procedure:

1. In the *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/kwjdc.properties file, make the following modification:

   Change the following parameter to point to the new garbage collection log file location:

   ```
   TEMAGCCollector.gclog.path=gc_logfile_path_and_name
   ```

   Restriction: Do not use variables or templates in this value.

   You can also optionally limit the size of the Garbage Collector logs. To do this, you must set the parameter to the following value:

   ```
   TEMAGCCollector.gclog.path=gc_logfile_path_and_name, x, y
   ```

   Where *x* and *y* are numbers. In this case, the logging is performed to *x* files in rotation. Information for *y* garbage collection cycles is sent to one file before switching to the next file.

2. Log in to the IBM WebSphere Application Server administrative console for the instance of the application server for the data collector installed on the RMI server.
3. Click **Servers**.
4. Expand **Server Type** and select **WebSphere application servers**.
5. Click on the name of the server.
6. Expand **Java and Process Management** and select **Process Definition**.
7. Click **Server > Application Servers** and select the *server_name*.
8. Under the **Additional Properties** section, click **Java Virtual Machine**.
9. In the **Generic JVM arguments** field, change the following parameters to point to the new garbage collection log file location:

Table 33. JVM options for garbage collection logging

JDK type	Parameter
IBM	`-verbosegc -Xverbosegclog:${SERVER_LOG_ROOT}/itcam_gc.log,5,3000`
Sun and HP	`-Xloggc:`*`gc_logfile_path_and_name`* `-XX:+PrintGCTimeStamps`

Make sure that the *gc_logfile_path_and_name* matches the value you specified in Step 1 on page 250.

10. Click **Apply**.
11. In the Messages dialog box, click **Save**.
12. In the Save to Master Configuration dialog box, complete the following steps:
    - If you are under a Network Deployment environment, ensure that **Synchronize changes with Nodes** is selected and then click **Save**.
    - If you are not under a Network Deployment environment, click **Save**.
13. Restart the instance of the application server that is being monitored by the data collector. For more information about restarting the application server, see "Restarting the application server" on page 313.

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 use excessive disk space.

To suppress class loading and unloading events, add the -XX:-TraceClassUnloading -XX:-TraceClassLoading options to the JVM arguments of the application server. Complete the following procedure:

1. Log in to the IBM WebSphere Application Server administrative console for the instance of the application server.
2. Click **Servers**.
3. Expand **Server Type** and select **WebSphere application servers**.
4. Click on the name of the server.
5. Expand **Java and Process Management** and select **Process Definition**.
6. Click **Server > Application Servers** and select the *server_name*.
7. Under the **Additional Properties** section, click **Java Virtual Machine**.
8. In the **Generic JVM arguments** field, add the following string of text:

   ```
   -XX:-TraceClassUnloading -XX:-TraceClassLoading
   ```

9. Click **Apply**.
10. In the Messages dialog box, click **Save**.
11. In the Save to Master Configuration dialog box, complete the following steps:
    - If you are under a Network Deployment environment, ensure that **Synchronize changes with Nodes** is selected and then click **Save**.
    - If you are not under a Network Deployment environment, click **Save**.
12. Restart the instance of the application server that is being monitored by the data collector. For more information about restarting the application server, see "Restarting the application server" on page 313.

What to do when deleting an application server profile

If you do not unconfigure the data collector before you delete an application server profile, data collector installation log and runtime data remains in the system, and running the WebSphere update command fails (typically with a `JACL failed` error message).

Unconfigure the data collector for all monitored application server instances in a profile before deleting it.

Overriding the data collector autoconfiguration

By default, if the data collector communicates with ITCAM for Application Diagnostics Managing Server, it is automatically configured by the managing server with the default configuration profile at the time of first connection. You can disable automatic configuration or select a different profile. These settings only take effect if you complete them before the data collector connects to the managing server for the first time.

Remember: If you use ITCAM for Applications, the managing server deep-dive functionality is not available, so you can ignore all references to this function.

To disable automatic configuration of the data collector in the managing server, in the data collector custom properties file, set the following property:

```
dc.autoconfigure=false
```

For more information about the data collector properties file, see "The Data Collector properties file" on page 221.

To change the profile name for automatic configuration of the data collector in the managing server, in the data collector custom properties file, set the following property:

```
dc.autoconfigure.configname=config_name
```

For more information about the data collector properties file, see "The Data Collector properties file" on page 221:

Important: If the data collector is already configured by the managing servers, changing these settings has no effect.

To configure or unconfigure a data collector from the managing server, or to change the data collector configuration profile, use the visualization engine. Select

Administration > **Server Management** > **Data Collector Configuration**. For more information about data collector configuration by the managing server, see the visualization engine online help.

Properties for communication with a Deployment Manager

The following properties define data collector communication with the deployment manager in a Network Deployment, WebSphere Virtual Enterprise, or WebSphere Compute Grid environment. They are normally set by the configuration utility.

Remember: Beginning with WebSphere Application Server version 8.5, in a Network Deployment environment, WebSphere Virtual Enterprise functions are characterized as intelligent management capabilities and WebSphere Compute Grid functions are characterized as WebSphere batch capabilities.

The properties are in the data collector properties file. For more information about this file, see "The Data Collector properties file" on page 221.

deploymentmgr.rmi.port
Defines the port for RMI communication to the Deployment Manager.

Example:

```
deploymentmgr.rmi.port=Deployment_Manager_RMI_(bootstrap)_port
```

deploymentmgr.rmi.host
Defines the host name or IP address for RMI communication to the Deployment Manager.

Example:

```
deploymentmgr.rmi.host=dmgr.domain.com
```

Settings for the data collector if Java 2 security is enabled

By default, data collector configuration enables Java 2 security on the application server, and sets a permissive policy. This policy ensures that the data collector can run properly, and provides no other security protection. If you need a more restrictive policy, complete the following procedure to ensure that the policy becomes active and the data collector can still work properly.

The data collector sets the Java security policy file location for all monitored application server instances (`java.security.policy` system property) to *DC_home*`/itcamdc/etc/datacollector.policy`. You must edit this file in the following way:

1. Remove all existing content.
2. Copy the sample security policy for the data collector from the *DC_home*`/itcamdc/etc/datacollector.security.policy` file.
3. If ITCAM for Transactions is installed on the server, add a grant statement for the ITCAM for Transactions code base to the security policy file. Follow the model for the grant statements provided in the sample `datacollector.security.policy` file, but use the ITCAM for Transactions installation root directory in the codeBase statement.
4. Add your required security policy settings.
5. Save the file, and create a backup copy.

Important: Each time you configure or reconfigure the data collector for an application server instance, the file *DC_home*`/itcamdc/etc/datacollector.policy`

might be overwritten. To ensure that your security policy remains active, restore this file from the backup copy after configuring or reconfiguring the data collector for any application server instance.

Customizing request information mapping

In some cases, you might have to change the information that identifies the requests monitored by the agent. This information includes the request name, and any data that can be displayed for the request (for example, the query text for an SQL request). To change the information, set up a custom request mapper configuration.

Define a custom request mapper configuration in an XML file. This file determines processing of the request data.

In this file, some built-in *symbols* represent values from the runtime context of the request. You can create additional symbols, which calculate new values. The calculation can include original request values, expressions, calls to Java methods (including methods in the monitored application), conditionals, and iteration over a set of values.

Then, you can *map* the contents of the symbols into the new request data that is provided to Tivoli Monitoring and ITCAM for Application Diagnostics Managing Server. If a particular variable in the request data is not mapped, the original value is retained.

Because different data is collected for request types, a custom request mapper configuration must be specific for a request type. You can configure different request mappers for different request types on the same data collector instance.

To set a custom request mapper configuration for a request type, you must make the following configuration changes:

- Enable custom request mapping for this type in the toolkit custom configuration file.
- Reference the XML file from the same configuration file.

XML file syntax

Create the XML file (for example, `request_custom.xml`). Place it in the *DC_home*`/runtime/custom` directory to use it for all application server instances, or in the *DC_home*`/runtime/`*appserver_version.node_name.server_name*`/custom` directory to use it for one application server instance. Ensure that it contains valid XML. The file must remain available while the configuration is in use.

Top level

The top-level tag is <gpe>. Within this tag, use the tag <runtimeConfiguration>. These tags have no attributes.

Within <runtimeConfiguration>, create a <requestMapperDefinition> tag. This tag must have a `type` attribute. Set it to the request mapper type name for the required request type; see Table 34 on page 265.

Within <requestMapperDefinition>, two tags must be present:

- <symbolDefinitions> contains all definitions of symbols. Symbols represent values that the agent calculates every time a request of this type is detected.

- <selection> contains the mapping of context keys to values. The keys represent the custom data that is passed to the agent. They are predefined for each request type (for more information about request mapper enabling properties and type names, see Table 34 on page 265). The mapping can be conditional.

Also, within the <runtimeConfiguration> tag, you can create a <requestMapperClassPath> tag. Within this tag, you can define JAR files. You can reference Java classes in these JAR files within Request Mapper definitions.

Defining an expression

To define symbols, you must use expressions. The agent evaluates the expressions to assign values to symbols.

Using data in an expression

An expression can use the following data:

- The input data symbols for the request type (for more information, see Table 34 on page 265).
- Other symbols described in the same request mapper definition.
- Numeric constants
- String constants (delimited with `"`, for example, `"string"`)
- Boolean constants (`true`, `TRUE`, `false`, `FALSE`)
- The `null` constant.

If the value of a symbol is an instantiation of a Java class, expressions can contain references to fields and methods that are defined within the class. To refer to a field, use *`symbol.fieldname`*. To refer to a method, use *`symbol.methodname`*`(`*`parameters`*`)`. The method call must return a value. For example, you can use the Java String methods with a symbol that has a String value.

To refer to a static field or method of a class, you can also use *`classname.fieldname`* and *`classname.methodname`*`(`*`parameters`*`)`.

If a symbol refers to an array object, the expression can select an element (*`symbol`*`[`*`selector`*`]`) and determine the length of the array (*`symbol`*`.length`)

Operators

You can use the following operators in an expression:

- Boolean operators: `AND`, `&`, `OR`, `|`, `NOT`, `!`
- Comparison: `==`, `!=`, `GT`, `>`, `LT`, `<`, `GE`, `>=`, `LE`, `<=`
- Numeric operators: `+`, `-`, `*`, `/`
- Parentheses to force order of evaluation: `(`, `)`

Important: You must escape the symbols `<`, `>`, and `&` in XML. Alternatively, you can use the `GT` (greater than), `GE` (greater than or equal), `LT` (less than), `LE` (less than or equal), and `AND` operators.

The expression can evaluate whether a value is an instance of a class, using the `instanceof` operator:

`expression` `instanceof` *`java.class.name`*

This operator, similar to the Java `instanceof` operator, produces a Boolean value. In this example, the value is true if the class to which the *expression* value belongs meets any of the following conditions:

- Is named *java.class.name*
- Is a direct or indirect subclass of the class identified by *java.class.name*.
- Implements, directly or indirectly, the interface identified by *java.class.name*.

The expression can also instantiate a new object of a Java class, using the `new` operator. This operator is similar to the Java `new` operator:

```
new java.class.name(expression1, expression2, ... expressionN)
```

Operator precedence

Operators are evaluated in order of precedence. Operators of the same order of precedence are evaluated from left to right. You can change the order of evaluation by using parentheses `(` and `)`.

The order of precedence is:

1. `.` operator (method call or field reference)
2. `[ ]` (array element selector)
3. `new`
4. `!`, `NOT`
5. `*`, `/`
6. `+`, `-`
7. `GT`, `>`, `LT`, `<`, `GE`, `>=`, `LE`, `<=`, `instanceof`
8. `==`, `!=`
9. `AND`, `&`
10. `OR`, `|`

Example

```
$s1 >= ( 2 * ($s2.sampMethod($s3, true) + 1))
```

The agent evaluates this expression in the following way:

1. The `$s1` symbol is evaluated. It must yield a numeric value.
2. The `$s2` symbol is evaluated. It must yield a Java object.
3. The `$s3` symbol is evaluated.
4. The method `sampMethod` for the object resulting from the evaluation of `$s2` is called. The result of the evaluation of `$s3` is passed as the first parameter, and the Boolean value `true` is passed as the second parameter. The call to `sampMethod` must return a numeric value.
5. 1 is added to the result of step 4.
6. The result of step 5 is multiplied by 2.
7. The result of step 1 is compared with the result of step 6. If the result of step 1 is greater than or equal to the result of step 6, `true` is returned. Otherwise, `false` is returned.

Defining basic symbols

Within the <symbolDefinitions> tag, you can define a basic symbol using the <symbol> tag. For a basic symbol, define an expression that can be evaluated using other symbols.

Within the <symbol> tag, use the following tags:

<name>
The name of the symbol. It is a string and must start with the $ character.

<eval>
The expression that ITCAM must evaluate to produce the value for this symbol. For more information about defining expressions, see "Defining an expression" on page 255.

<type>
The type of the value that the symbol returns. Specify this value as a fully qualified Java class name, or a Java primitive. Specifying the type for the symbol is optional. If it is not defined, the Request Mapper attempts to establish the field type based on the expression. If the Request Mapper is unable to determine the symbol type before evaluating the expression, performance is affected. Therefore, for best performance, it is better to specify the type.

<args>
The arguments for the symbol. This tag is optional; if it is specified, arguments must be supplied for evaluating the symbol. For more information, see "Defining symbol arguments."

Example

```
<symbol>
   <name>$doubles1</name>
   <eval>$s1*2</eval>
   <type>int</type>
</symbol>
```

This symbol returns double the value of another symbol, `$s1`.

Defining symbol arguments

Within the <args> tag of a symbol definition, you can define argument types for the symbol.

In this tag, use the <type> tag to specify the types of arguments. Specify this value as a fully qualified Java class name, or a Java primitive. You can specify any amount of <type> tags; each of these tags defines an argument.

In this case, the symbol must be referenced with arguments in parentheses:
`$symbol(argument1,argument2...)`

The number of arguments must be the same as the number of argument type definitions.

Within the symbol definition, refer to the first argument as `$p0`, the second argument as `$p1`, and so on.

A symbol with arguments works like a Java method. It takes input arguments, and returns a value that depends on the values of the arguments.

Example

```
<symbol>
   <name>$double</name>
   <eval>$p0*2</eval>
   <type>int</type>
```

```
   <args>
       <type>int</type>
   </args>
</symbol>
```

This symbol returns double the value of the argument. To evaluate it, supply a numeric argument: `$double(2)`, `$double($s1)`.

Defining iteration symbols

Within the <symbolDefinitions> tag, you can define an iteration symbol using the <iterationSymbol> tag. An iteration symbol represents a value that is acquired by iterating through a set of objects in a Java array, Enumeration, or Collection. For each of the members, Request Mapper evaluates one or more condition expressions. If an expression returns `true`, Request Mapper uses the member to calculate the return value. Once a member meets the condition expression, Request Mapper does not evaluate the rest of the members.

Within the <iterationSymbol> tag, use the following tags.

<name>
The name of the symbol. It is a string and must start with the $ character.

<type>
The type of the value that the symbol returns. Specify this value as a fully qualified Java class name or a Java primitive. Specifying the type for the symbol is optional. If it is not defined, the Request Mapper attempts to establish the field type based on the expression. If the Request Mapper is unable to determine the symbol type before evaluating the expression, performance is affected. Therefore, for best performance, it is better to specify the type.

<args>
The arguments for the symbol. This tag is optional; if it is specified, arguments must be supplied for evaluating the symbol. For more information, see "Defining symbol arguments" on page 257.

<iterate over="*expression*">
Defines the object (array, Enumeration, or Collection) that contains the members to iterate through. The expression must return such an object. Request Mapper iterates over its members until either one of them causes a condition expression to return `true`, or no more members remain. Define the set of iteration expressions in tags within this tag:

<test>
Define the condition and return expression within this tag. An <iterate> tag can contain several <test> tags. In this case, Request Mapper evaluates all of them. If any condition expression is true, the symbol returns a value using the result expression in the same <test> tag, and no further evaluation is performed.

<castTo>
Optional: If this tag is present, specify the name of a Java type within it, as a fully qualified Java class name or a Java primitive. Request Mapper casts the iterated element to this type before evaluating the condition and return expressions. If this tag is not present, Request Mapper casts a member of an array to the array base type, and a member of an Enumeration or Collection to `java.lang.Object`. For an array member, the array base type is usually the correct choice; therefore, use this tag when iterating over an Enumeration or Collection.

<condition>
An expression that must yield a Boolean value. Use `$iterElement` to refer to the element that is being iterated.

<return>
If the expression in the <condition> tag returns `true`, Request Mapper evaluates the expression in the <return> tag. The iteration symbol returns the value that this expression produces. Use `$iterElement` to refer to the element that is being iterated.

<defaultValue>
Optional. If Request Mapper has iterated over all members of the object, but no condition expression has returned `true`, Request Mapper evaluates the expression in the <defaultValue> tag. The iteration symbol returns the value that the expression produces. If this tag is not present, the default value is `null`.

Examples

```
<iterationSymbol>
  <name>$userNameCookieValue</name>
  <iterate over="$httpServletRequest.getCookies()">
     <test>
        <condition>$iterElement.getName().equals("userName")</condition>
        <return>$iterElement.getValue()</return>
     </test>
   </iterate>
</iterationSymbol>
```

This symbol finds the cookie named "username", and returns its value. `$httpServletRequest.getCookies()` returns an array, so there is no need for the <castTo> element.

```
<iterationSymbol>
  <name>$headerNameStartingWithA</name>
  <iterate over="$httpServletRequest.getHeaderNames()">
    <test>
       <castTo>java.lang.String</castTo>
       <condition>$iterElement.startsWith("A")</condition>
       <return>$iterElement</return>
    </test>
  </iterate>
</iterationSymbol>
```

This symbol finds the header with a name starting with "A", and returns its name. `$httpServletRequest.getHeaderNames()` returns an Enumeration, so the <castTo> element is required.

```
<iterationSymbol>
  <name>$determined_gender</name>
  <iterate over="$children">
    <test>
       <castTo>java.lang.String</castTo>
       <condition>$iterElement.equals("male")</condition>
       <return>"It's a boy"</return>
    </test>
    <test>
       <castTo>java.lang.String</castTo>
       <condition>$iterElement.equals("female")</condition>
       <return>"It's a girl"</return>
    </test>
  </iterate>
  <defaultValue>"unknown"</defaultValue>
</iterationSymbol>
```

This symbol iterates over `$children`, which must be an array, Enumeration, or Collection of strings. If any of the strings equals "male", it returns "it's a boy". If any of the strings equals "female", it returns "it's a girl". Finally, if no string in the `$children` object equals either "male" or "female", the symbol returns "unknown".

Defining conditional symbols

Within the <symbolDefinitions> tag, you can define a conditional symbol using the <conditionalSymbol> tag. A conditional symbol represents a value that is acquired by evaluation a series of condition expressions. If any expression returns `true`, Request Mapper uses the member to calculate the return value. When a member meets the condition expression, Request Mapper evaluates a corresponding return expression, and return the result. After finding a result to return, Request Mapper does not evaluate any further expressions.

Within the <conditionalSymbol> tag, use the following tags.

<name>
The name of the symbol. It is a string and must start with the $ character.

<type>
The type of the value that the symbol returns. Specify this value as a fully qualified Java class name, or a Java primitive. Specifying the type for the symbol is optional. If it is not defined, the Request Mapper attempts to establish the field type based on the expression. If the Request Mapper is unable to determine the symbol type before evaluating the expression, performance is affected. Therefore, for best performance, it is better to specify the type.

<args>
The arguments for the symbol. This tag is optional; if it is specified, arguments must be supplied for evaluating the symbol. For more information, see "Defining symbol arguments" on page 257.

<if condition="*expression*">
The `condition` attribute defines a condition expression to evaluate. The expression must yield a Boolean value. If the value is `true`, Request Mapper uses the contents of the <if> tag to try to determine the return value. The <if> tag must contain either, but not both, of the following contents:

- A <return> tag. This tag contains an expression. If the condition expression is true, Request Mapper evaluates the expression and returns the result.
- Any number of <if> tags, nested within this <if> tag. If the condition expression is true, Request Mapper processes the nested <if> tags in the same way as a top-level <if> tag. That is, it evaluates the expression in the `condition` attribute, and if the expression is true, uses the contents of the tag to try and determine the return value.

Important: If a return value is determined, Request Mapper does not evaluate any further expressions. However, if a condition expression in an <if> tag is true, but it contains nested <if> tags and none of their condition expressions are true, no value is determined. In this case, Request Mapper continues to evaluate subsequent expressions.

<defaultValue>
Optional. If Request Mapper has evaluated all condition expressions, but none of the condition expression has returned `true`, Request Mapper evaluates the expression in the <defaultValue> tag. The conditional symbol returns the value that the expression produces. If this tag is not present, the default value is `null`.

Example

```
<symbol>
  <name>$GET</name>
  <eval>"GET"</eval>
</symbol>
<symbol>
  <name>$PUT</name>
  <eval>"PUT"</eval>
</symbol>
<conditionalSymbol>
  <name>$sessionAttribute</name>
  <if condition="$httpServletRequest.getSession(false) != null>
     <if condition="$httpServletRequest.getSession(false).getAttribute($GET)
!= null">
       <return>$httpServletRequest.getSession(false).getAttribute($GET)</return>
     </if>
     <if condition="true">
       <return>$httpServletRequest.getSession(false).getAttribute($PUT)</return>
      </if>
  </if>
</conditionalSymbol>
```

This symbol is assumed to be a part of the Servlet request mapper. First it checks if an HTTP session exists for the servlet; if not, the symbol returns `null`. If a session is present, the symbol checks if the Servlet has an attribute "GET", it returns the value of that attribute. Otherwise, it returns the value of the "PUT" attribute. The second condition expression is "true"; this value is used as an "else" clause. If the first condition is true, Request Mapper does not evaluate any further expressions; otherwise it continues to the second expression.

Defining external class symbols

Within the <symbolDefinitions> tag, you can define an external class using the <externalClassSymbol> tag. An external class symbol represents an external Java class. External class symbol definition is optional; you can use external Java classes in expressions directly. However, it might enhance the readability of the Request Mapper configuration.

Within the <externalClassSymbol> tag, use the following tags.

<name>
The name of the symbol. It is a string and must start with the $ character.

<className>
The name of the customer defined class.

Important: To refer to any Java class in Request Mapper configuration, whether in an external class symbol definition or in any expression, you must add the full path and name of the JAR file containing the class to the <requestMapperClassPath> tag within the <runtimeConfiguration> tag.

After defining an external symbol, you can refer to the class by the name of the symbol. You can also refer to static methods and fields of the class using the symbol.

Example

```
<externalClassSymbol>
  <name>$rand</name>
  <className>user.class.Random</className>
</externalClassSymbol>
```

This symbol refers to a user-written class, generating a random number. The full path and name of the JAR file containing this class must be present in the <requestMapperClassPath> tag within the <runtimeConfiguration> tag.

To refer to the static method `user.class.Random.generate()` in an expression, you can use the external symbol:

```
$rand.generate()
```

Mapping values to context keys

Within the <requestMapperDefinition> tag, map values to context keys using the <selection> tag. This mapping provides the changes in the monitoring information.

You can map values to the output keys defined for the request type (for more information, see Table 34 on page 265).

If no value is mapped to a key after the evaluation of the request mapper configuration, ITCAM uses the original value extracted from the request.

Within the <selection> tag, use the following tags.

<matchCriteria>
: An expression that must return a Boolean value. The mapping defined within this tag is only used if this expression returns `true`.

<mapTo>
: Defines a key and the value to map to it. Within this tag, a <key> tag contains the key, and a <value> tag contains the value.

<selection>
: You can nest <selection> tags, placing one within another.

If <selection> tags are nested, then the nested mapping is only used if both the outer and the nested <matchCriteria> expressions return `true`.

You can use multiple <selection> tags within a <requestMapperDefinition> tag or within another <selection> tag. If the same key is mapped several times in several <selection> tags on the same nesting level (that is, within the same parent tag), then the first mapping for which the <matchCriteria> expression returned `true` is used.

Do not map the same key both in the outer and nested <selection> tags.

Typically, use the <matchCriteria> value of `true` as an "else" value for the last selection tag on a nesting level. If you want to map different values in different cases, use several <selection> tags within this outer tag; each of them can contain the criteria and values for a particular case. The last tag, with a value of `true`, covers the case when the available data meets none of the criteria.

Examples

```
<selection>
   <matchCriteria>true</matchCriteria>
   <mapTo>
      <key>Result</key>
      <value>$s1</value>
   </mapTo>
</selection>
```

In this mapping configuration, `Result` is set to the value of the symbol `$s1`.

```
<matchCriteria>true</matchCriteria>
   <selection>
      <matchCriteria>$b1</matchCriteria>
      <mapTo>
         <key>Result</key>
         <value>1</value>
      </mapTo>
   </selection>
   <selection>
      <matchCriteria>true</matchCriteria>
      <mapTo>
         <key>Result</key>
         <value>2</value>
      </mapTo>
</selection>
```

In this mapping configuration, the symbol `$b1` must return a Boolean value. `Result` is set to 1 if `$b1` returns `true`, and to 2 if `$b1` returns `false`. If `$b1` returns `true`, Request Mapper uses the mapping for `Result` in the first <selection> tag; the mapping for the same key in the second tag is not used.

Enabling a request mapper

To enable a request mapper for a request type, edit the toolkit custom configuration file or the toolkit global custom configuration file. Follow a different procedure for custom requests.

Add two lines to the `toolkit_custom.properties` or `toolkit_global_custom.properties` file:

- A line setting the enabling property for this request type (for more information, see "Request mapper type names, input, and output data" on page 264) to `true`.
- A line setting the `am.camtoolkit.gpe.customxml.*` property to the name of the mapper XML (for more information, see "XML file syntax" on page 254). This file must be in the same directory as the configuration file referencing it. For example, if you reference the XML file in the *DC_home*`/runtime/toolkit_global_custom.properties` file, place the XML file in the *DC_home*`/runtime` directory. Use any unique value instead of the * symbol.

For more information about the `toolkit_custom.properties` or `toolkit_global_custom.properties` files, see "Properties files for the Data Collector" on page 221.

Example

To enable a request mapper that is defined in `renameDataSource.xml` for the SQL request type, add the following lines to the toolkit custom configuration file or the toolkit global custom configuration file:

```
com.ibm.tivoli.itcam.toolkit.ai.enable.sqlrequestmapper=true
am.camtoolkit.gpe.customxml.renameDataSource=renameDataSource.xml
```

Enabling a request mapper for custom requests

For custom requests, define the request mapper type name in the custom request definition XML file (for more information, see "Defining custom requests" on page 235).

Under the <edgerequest> tag, create a <requestMapper> tag. Place a unique request map type name in this tag. Use this type name in the type attribute of the <requestMapperDefinition> tag of the mapper XML file (for more information, see "XML file syntax" on page 254).

In the toolkit_custom.properties or toolkit_global_custom.properties file, add a line setting the am.camtoolkit.gpe.customxml.* property to the name of the mapper XML file. This file must be in the same directory as the configuration file referencing it. For example, if you reference the XML file in the *DC_home*/runtime/toolkit_global_custom.properties file, place the XML file in the *DC_home*/runtime directory. Use any unique value instead of the * symbol.

For more information about the toolkit_custom.properties or toolkit_global_custom.properties files, see "Properties files for the Data Collector" on page 221.

Example

To enable a request mapper that is defined in customMapper.xml for the SupplyCheck custom request type, use the following definition of the custom request type:

```
<customEdgeRequests>
  <edgeRequest>
    <requestName>SupplyCheck</requestName>
    <Matches>com.mycompany.myapp.Supplier</Matches>
    <type>application</type
    <methodName>inventoryCheck</methodName>
    <requestMapper>customMapper</requestMapper>
  </edgeRequest>
</customEdgeRequests>
```

In the customMapper.xml file, make sure that the type name is set:

```
<requestMapperDefinition type="customMapper">
```

Add the following line to the toolkit custom configuration file or the toolkit global custom configuration file:

```
am.camtoolkit.gpe.customxml.customMapper=customMapper.xml
```

Request mapper type names, input, and output data

The following tables list the information necessary to configure and enable request mappers for different request types.

Request type
The request type.

Enabling property
To enable the request mapper, set this property to true in the toolkit_custom.properties or toolkit_global_custom.properties file.

Important: If you copy this value from the table, remove any spaces and line breaks.

Request mapper type name
Assign this value to the type attribute of the <requestMapperDefinition> tag in the request mapper definition XML file.

Input data symbol names
The symbols representing the request information. You can use these

symbols in expressions within the request mapper definitions (for more information, see "Defining an expression" on page 255).

Output data context keys
To provide changes in the monitoring information, assign values to these keys in the request mapper definition. For more information, see "Mapping values to context keys" on page 262.

Table 34. Request mapper enabling properties and type names

Request type	Enabling property	Request mapper type name
Servlet	com.ibm.tivoli.itcam.toolkit.ai.enable.servletrequestmapper	servlet
JNDI	com.ibm.tivoli.itcam.toolkit.ai.enable.jndirequestmapper	jndiLookup
Custom Request		Defined by user in the edgeRequest definition
EJB	com.ibm.tivoli.itcam.toolkit.ai.enable.ejbrequestmapper	ejb
JCA	com.ibm.tivoli.itcam.toolkit.ai.enable.jcarequestmapper	jca
JDBC Data Source	com.ibm.tivoli.itcam.toolkit.ai.enable.datasourcerequestmapper	dataSource
JDBC SQL Statement	com.ibm.tivoli.itcam.toolkit.ai.enable.sqlrequestmapper	sqlStatement
JMS	com.ibm.tivoli.itcam.toolkit.ai.enable.jmsrequestmapper	jms
JAX-RPC Web Service	com.ibm.tivoli.itcam.toolkit.ai.enable.webservicerequestmapper	webServices
Axis Web Service	com.ibm.tivoli.itcam.toolkit.ai.enable.webservicerequestmapper	webServices
MQI	com.ibm.tivoli.itcam.toolkit.ai.enable.mqrequestmapper	mqi
EJB	com.ibm.tivoli.itcam.toolkit.ai.enable.ejbrequestmapper	ejb
JDBC Connection Factory	com.ibm.tivoli.itcam.toolkit.ai.enable.sqlconnectfactoryrequestmapper	connectionFactory
SCA	com.ibm.tivoli.itcam.toolkit.ai.enable.scarequestmapper	sca
JAX-WS Web Service	com.ibm.tivoli.itcam.toolkit.ai.enable.webservicerequestmapper	webServices
WebSphere Portal Server Portal (extending the org.apache.jetspeed.portlet.Portlet class)	com.ibm.tivoli.itcam.toolkit.ai.enable.portalrequestmapper	portalPortal
WebSphere Portal Server version 6.1, 7, and 8 Portal (implementing the javax.portlet.Portlet interface)	com.ibm.tivoli.itcam.toolkit.ai.enable.portal6requestmapper	Portal6Portal

Important: In ITCAM Agent for WebSphere Applications, there is no meaningful way to configure the custom request mapper for the request types not listed in Table 34.

Table 35. Request mapper input and output data

Request type	Input data symbol names	Output data context keys
Servlet	For more information, see Table 36 on page 269.	**remappedURI** defines a renamed URI **remappedURL** defines a renamed URL **appName** defines a renamed application name **userid** defines the user ID for the request
JNDI	• **$jndiContext** the Context object • **$lookup** the lookup string • **$context** "JNDIlookup"	**renamedLookup** defines a renamed lookup string
Custom Request	• **$this** the 'this' object for the custom request method • **$0** the arguments passed to the custom request method, specified as an array of Objects • **$className** the custom request class name • **$methodName** the custom request method name • **$context** the original request name from the edgeRequest definition	**customRequestName** defines the renamed custom request name
EJB	• **$ejb** the EJB implementation object • **$appName** the name of the application • **$ejbType** the type of the EJB • **$className** the Class name of the EJB implementation object • **$methodName** the EJB business method name • **$context** "EJBBusinessMethod"	**appName** defines the renamed application name **ejbType** defines the renamed EJB type **className** defines the renamed class name **methodName** defines the renamed method name
JCA	• **$interaction** the Interaction object • **$interactionSpec** the InteractionSpec object • **$record** the Record object • **$context** "J2Cexecute"	**lookupName** is the renamed lookupName **productName** is the renamed product name **productVersion** is the renamed product version

Table 35. Request mapper input and output data (continued)

Request type	Input data symbol names	Output data context keys
JDBC Data Source	• **$this** either the DataSource or the Driver object • **$dataSource** the $this object, cast as a DataSource • **$driver** the $this object, cast as a Driver • **$dataSourceName** is the name of the data source, as java.lang.String • **$context** indicates the type of request, either "JDBCgetConnection" or "JDBCgetConnection FromDriver"	**dataSourceName** is the renamed Datasource name, if the $this object is a DataSource **url** is the renamed Driver URL, if the $this object is a Driver
JDBC SQL Statement	• **$this** either the SQL statement, or the SQL Connection • **$sqlText** contains the SQL text as java.lang.String, if the $this object is an SQL statement • **$sqlStatement** the $this object, cast as an SQL Statement • **$sqlConnection** the $this object, cast as an SQL Connection • **$dataSourceName** the data source name • **$context** indicates the type of request: "JDBCexecute", JDBCexecuteQuery", "JDBCexecuteUpdate", "JDBCcreateStatement", "JDBCprepareStatement"	**dataSourceName** is the renamed data source name **sqlText** is the renamed SQL text
JMS	• **$this** the 'this' object for the instrumented method. Can be a QueueBrowser, MessageConsumer, MessageProducer, or MessageListener • **$0** the Queue object, for a Send request, or a Topic object, for a Publish request • **$queueBrowser** the $this object, cast as a QueueBrowser • **$messageConsumer** the $this object, cast as a MessageConsumer • **$messageProducer** the $this object, cast as a MessageProducer • **$messageListener** the $this object, cast as a MessageListener • **$queue** the $0 object, cast as a Queue • **$topic** the $0 object, cast as a Topic • **$context** indicates the type of request: "JMSreceive", "JMSsend", "JMSbrowse", "JMSpublish", "JMSonmessage"	**queueName** the renamed queue name **providerURL** the renamed provider URL **topicName** the renamed topic name

Table 35. Request mapper input and output data (continued)

Request type	Input data symbol names	Output data context keys
JAX-RPC Web Service	• **$messageContext** the IMessageContextWrapper • **$appName** the application name • **$requestName** the default request name • **$url** the URL • **$context** indicates the type of request: "WebServicesJaxRpc ProviderRequest", "WebServicesJaxRpc ClientRequest"	**appName** the renamed application name **requestName** the renamed request name **url** the renamed URL
Axis Web Service	• **$messageContext** the IMessageContextWrapper • **$appName** the application name • **$requestName** the default request name • **$url** the URL • **$context** indicates the type of request: "WebServicesAxisClient Request", "WebServicesAxis ProviderRequest"	**appName** the renamed application name **requestName** the renamed request name **url** the renamed URL
MQI	• **$queue** the MQQueue object, if it is known • **$qmgr** the MQQueueManager object, if it is known • **$message** the MQMessage or MQMsg2 object, if it is known • **$session** the MQSESSION object, if it is known • **$getMsgOptions** the MQGetMessageOptions object, if it is known • **$qmgrName** the name of the queue manager • **$queueName** the name of the queue • **$context** the type of MQ request: "MQCONN", "MQCONNX", "MQDISC", "MQBACK", "MQBEGIN", "MQCLOSE", "MQCMIT", "MQINQ", "MQOPEN", "MQSET", "MQGET", "MQPUT", "MQPUT1", "MQGETBROWSE"	**qmgrName** the rename queue manager name **qname** the renamed queue name
EJB	• **$appName** the name of the application • **$ejbType** the type of the EJB • **$className** the Class name of the EJB implementation object • **$methodName** the EJB business method name • **$context** "EJBBusinessMethod"	**appName** defines the renamed application name **ejbType** defines the renamed EJB type **className** defines the renamed class name **methodName** defines the renamed method name
JDBC Connection Factory	• **$connectionFactory** the ConnectionFactory • **$dataSourceName** the data source name • **$context** "JDBCgetConnection"	**dataSourceName** is the renamed data source name

Table 35. Request mapper input and output data (continued)

Request type	Input data symbol names	Output data context keys
SCA	• **$uri** the URI • **$operationName** the operation name • **$context** indicates the type of request: "SCA_Generic", "SCA_Ref", "SCA_Target"	**uri** is the renamed URI **operationName** is the renamed operation name
JAX-WS Web Service	• **$messageContext** the IMessageContextWrapper • **$appName** the application name • **$requestName** the default request name • **$url** the URL • **$context** indicates the type of request: "WebServicesJAXWS ClientRequest", "WebServicesJAXWS ProviderRequest", "WebServicesJAXWS AsyncRequest"	**appName** the renamed application name **requestName** the renamed request name **url** the renamed URL
WebSphere Portal Server Portal (extending the `org.apache.jetspeed.portlet.Portlet` class)	• **$portletAdapter** PortletAdapter • **$portletRequest** PortletRequest • **$portletResponse** PortletResponse • **$portletName** Portlet name • **$pageTitle** Page title • **$url** URL of the request • **$userid** Request userid • **$context** "Portal.Portlet"	**portletName** the renamed portlet name **title** the renamed page title **url** the renamed URL **userid** the renamed userid
WebSphere Portal Server version 6.1, 7, and 8 Portal (implementing the `javax.portlet.Portlet` interface)	• **$portlet** Portlet • **$renderRequest** RenderRequest • **$renderResponse** RenderResponse • **$portletName** Portlet name • **$pageTitle** Page title • **$url** URL of the request • **$userid** Request userid • **$context** "Portal.Portlet"	**portletName** the renamed portlet name **title** the renamed page title **url** the renamed URL **userid** the renamed userid

For servlet requests, a larger number of input data symbols is provided.

Table 36. Input data symbol names for servlet requests

Symbol Name	Value Type	Symbol Contents
$context	String	"ServletMethod"
$servlet	javax.servlet.http.HttpServlet	The HttpServlet object associated with the servlet request
$httpServletRequest	javax.servlet.http.HttpServletRequest	The HttpServletRequest object associated with the servlet request
$httpServletResponse	javax.servlet.http.HttpServletResponse	The HttpServletResponse object associated with the servlet request
$appName	java.lang.String	The application name associated with the servlet
$URL	java.lang.StringBuffer	The URL that the client used to make the request

Table 36. Input data symbol names for servlet requests (continued)

Symbol Name	Value Type	Symbol Contents
$RemoteUser	java.lang.String	The login name of the user making this request, if authenticated
$URI	java.lang.String	The part of the requestURL from the protocol name up to the query string
$ServletPath	java.lang.String	The part of the request URL that calls the servlet.
$SessionID	javax.servlet.http.HttpSession	The current session associated with this request
$QueryString	java.lang.String	The query string that is contained in the request URL after the path.
$SessionAttribute	java.lang.String	This parameterized symbol returns a session attribute value. It has one parameter, the attribute name (must be a string). For example, $SessionAttribute("attr1") returns the value of the attribute named attr1.
$cookie	javax.servlet.http.Cookie	This parameterized symbol returns a named cookie. It has one parameter, the cookie name (must be a string). For example, $cookie("cookie1") returns the value of the attribute named cookie1.

Example request mapper definitions

The following examples illustrate usage of the request mapper functionality.

Changing the servlet application name

In this example, the application name in a servlet request is replaced by the URI and the query string.

The *DC_home*/runtime/changeAppname.xml file contains the following request mapper definition:

```
<gpe>
   <runtimeConfiguration>
         <requestMapperDefinition type="servlet">
               <selection>
                     <matchCriteria>true</matchCriteria>
                     <mapTo>
                           <key>appName</key>
                           <value>$URI + "." + $QueryString</value>
                     </mapTo>
               </selection>
         </requestMapperDefinition>
   </runtimeConfiguration>
</gpe>
```

Renaming a data source

In this example, the data source name in an SQL request is changed to a version that a user can understand more easily.

The *DC_home*/runtime/renameDataSource.xml file contains the following request mapper definition:

```
<gpe>
 <runtimeConfiguration>
   <requestMapperDefinition type="sqlStatement">
      <selection>
         <matchCriteria>$dataSourceName != null</matchCriteria>
         <selection>
           <matchCriteria>$dataSourceName.equals("jdbc/TradeDataSource")
</matchCriteria>
           <mapTo>
             <key>dataSourceName</key>
             <value>"Daytrader Data Source"</value>
           </mapTo>
         </selection>
         <selection>
           <matchCriteria>$dataSourceName.equals("jdbc/LongDataSource")
</matchCriteria>
           <mapTo>
             <key>dataSourceName</key>
             <value>"Long term trader Data Source"</value>
           </mapTo>
         </selection>
      </selection>
   </requestMapperDefinition>
 </runtimeConfiguration>
<gpe>
```

The first <selection> tag ensures that $dataSourceName is not null. Then the second <selection> tag can safely evaluate $dataSourceName.equals().

If the first <selection> tag was not present, and a null $dataSourceName was passed, the request mapper would generate an exception. Such an exception might result in missing monitoring information.

To enable this request mapper, the file *DC_home*/runtime/toolkit_global_custom.properties contains the following lines:

```
com.ibm.tivoli.itcam.toolkit.ai.enable.sqlrequestmapper=true
am.camtoolkit.gpe.customxml.renameDataSource=renameDataSource.xml
```

Removing sensitive information from an SQL request

In this example, an application includes social security numbers in SQL requests. The request mapper removes the numbers from the version of the request that the user can see.

In the SQL requests, the social security number is listed with the SS column name: SS = *number*. The request mapper looks for the string "SS = " and removes the nine symbols after it.

The *DC_home*/runtime/removeSSN.xml file contains the following request mapper definition:

```
<gpe>
    <runtimeConfiguration>
         <requestMapperDefinition type="sqlStatement">
             <symbolDefinitions>
                 <symbol>
                     <name>$offsetOfSS</name>
                     <eval>$sqlText.indexOf("SS = ")</eval>
                 </symbol>
                 <symbol>
                     <name>$sqlTextContainsSS</name>
```

```
<eval>$sqlText != null AND $offsetOfSS > 0 AND $sqlText.length() GE
$offsetOfSS+16</eval>
                </symbol>
                <conditionalSymbol>
                    <name>$sqlTextPriorToSSKeyword</name>
                    <type>java.lang.String</type>
                    <defaultValue>""</defaultValue>
                    <if condition="$sqlTextContainsSS">
                      <return>$sqlText.substring(0, $offsetOfSS+5)</return>
                    </if>
                </conditionalSymbol>
                <conditionalSymbol>
                    <name>$sqlTextAfterSS</name>
                    <type>java.lang.String</type>
                    <defaultValue>""</defaultValue>
                    <if condition="$sqlTextContainsSS">
                      <return>$sqlText.substring($offsetOfSS+16)</return>
                    </if>
                </conditionalSymbol>
            </symbolDefinitions>
            <selection>
                 <matchCriteria>$sqlText != null AND $sqlText.length() >
0</matchCriteria>
                 <selection>
                      <matchCriteria>$sqlTextContainsSS</matchCriteria>
                      <mapTo>
                           <key>sqlText</key>
                           <value>$sqlTextPriorToSSKeyword + "?" +
$sqlTextAfterSS</value>
                      </mapTo>
                 </selection>
            </selection>
        </requestMapperDefinition>
    </runtimeConfiguration>
</gpe>
```

To enable this request mapper, the file *DC_home*/runtime/toolkit_global_custom.properties contains the following lines:

```
com.ibm.tivoli.itcam.toolkit.ai.enable.sqlrequestmapper=true
am.camtoolkit.gpe.customxml.renameDataSource=removeSSN.xml
```

Part 8. Appendixes

Appendix A. Setting up a secure connection to the Managing Server

If you integrate the data collector with an ITCAM for Application Diagnostics Managing Server, you might want to set up security for this integration by configuring security-related settings in the Managing Server components and in the data collector.

Important: The ITCAM for Application Diagnostics Managing Server is not a component of ITCAM for Applications 7.2. Unless you have ITCAM for Application Diagnostics version 7.1 installed in your environment, ignore this appendix.

For information about configuring the data collector when Java 2 security is enabled, see "Settings for the data collector if Java 2 security is enabled" on page 253.

Complete the procedures in each of the following sections, if they apply.

Node Authentication

Node Authentication is the technique used to ensure that the managing server and data collectors communicate with each other in a secure manner. In Node Authentication-related configuration, the kernel, data collectors, or Port Consolidator operate in secure mode either individually or in combination. 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 `security.enabled` property on that particular component. You can use the following combinations:

- Managing server in secure mode and the data collector in nonsecure mode.
- Data collector in secure mode and the managing server in nonsecure mode.
- Managing server and data collector in secure or nonsecure mode.

Script to run if your SSL certificates have expired

All SSL certificates have an expiration time. For some certificates, the expiration time is four years, after which the product does not function if you have enabled Node Authentication and SSL. If so, to increase the expiration time, complete the procedure at "Script to run if your SSL certificates have expired" on page 283.

Node Authentication on the Managing Server

The following procedures are Node Authentication-related configuration that occurs on the Managing Server component.

kernel-related changes

In the managing server in the `$MSHOME/bin` directory, there is a `setenv.sh` file that is shared by all managing server components. All changes made to the `setenv.sh` file apply to all managing server components. All the managing server components initialize their respective security modules based on the properties in this `setenv.sh` file. The installer configures all of the managing server components with security-enabled configuration by default, except for kernel-related changes, which are enabled by changing the `.kl1` and `.kl2` property files on the managing server.

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 Network Interface Card (NIC) environment or are upgrading the Managing Server from version 6.0 to version 7.1, 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 the kl2.properties file as well.

3. Restart the Managing Server. For more information, see *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

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 (*DC_home*/runtime/*app_server_version.node_name.server_name*/custom/datacollector_custom.properties) complete the following steps:

1. Set security.enabled=true
2. 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. For more information, see "Restarting the application server" on page 313.

For more information, see Appendix H, "Port Consolidator reference and configuration," on page 337 for instructions on configuring the data collector to use the Port Consolidator.

Keystore management and populating certificates

You do not have to use the following commands unless you want to create unique certificates with a new storepass and keypass. You can run keystore management on the managing server and the data collector. These commands populate a new store with those certificates.

For populating all new keystores: Three stores are used by ITCAM for Application Diagnostics: CyaneaMgmtStore to run on the managing server, CyaneaDCStore to run on the data collectors, and CyaneaProxyStore to run on the data collector when you want to enable the data collector port consolidator.

CyaneaMgmtStore contains: mgmttomgmt.cer (cn=cyaneamgmt)dctomgmt.cer (cn=cyaneadc)proxytomgmt.cer (cn=cyaneaproxy)

CyaneaDCStore contains: proxytodc.cer (cn=cyaneaproxy) mgmttodc.cer (cyaneamgmt)

CyaneaProxyStore 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 command 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"

Use the following details to create all the necessary stores and certificates:

Important: Replace "oakland1" with your custom keypass and "oakland2" with your custom storepass. Replace "CyaneaMgmtStore", "CyaneaDCStore", and "CyaneaProxyStore" with your custom store names.

```
keytool -genkey -alias mgmttomgmt -keyalg RSA -keysize 1024 -sigalg MD5withRSA
  -validity 2000 -keypass oakland1 -keystore ./CyaneaMgmtStore
  -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 ./CyaneaMgmtStore -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 ./CyaneaMgmtStore -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 ./CyaneaDCStore -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 ./CyaneaDCStore
  -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 ./CyaneaProxyStore -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 ./CyaneaProxyStore
  -storepass oakland2 -dname "cn=cyaneadc, OU=CyaneaComp, O=Cyanea, L=Oakland,
  ST=CA, C=US"
```

Extracting Certificates

When you created the three Stores, extract the certificates by completing the following steps:

1. Extract all certificates from CyaneaMgmtStore by running the following commands:

   ```
   keytool -export -alias mgmttomgmt -keypass oakland1 -keystore ./CyaneaMgmtStore
     -storepass oakland2 -file mgmttomgmt.cer

   keytool -export -alias dctomgmt -keypass oakland1 -keystore ./CyaneaMgmtStore
     -storepass oakland2 -file dctomgmt.cer
   ```

```
keytool -export -alias proxytomgmt -keypass oakland1 -keystore ./CyaneaMgmtStore
  -storepass oakland2 -file proxytomgmt.cer
```

2. Extract all certificates from CyaneaDCStore by running the following commands:

```
keytool -export -alias proxytodc -keypass oakland1 -keystore ./CyaneaDCStore
  -storepass oakland2 -file proxytodc.cer
```

```
keytool -export -alias mgmttodc -keypass oakland1 -keystore ./CyaneaDCStore
  -storepass oakland2 -file mgmttodc.cer
```

3. Extract all certificates from CyaneaProxyStore by running the following commands:

```
keytool -export -alias mgmttoproxy -keypass oakland1
  -keystore ./CyaneaProxyStore -storepass oakland2 -file mgmttoproxy.cer
```

```
keytool -export -alias dctoproxy -keypass oakland1
  -keystore ./CyaneaProxyStore -storepass oakland2 -file dctoproxy.cer
```

When you have extracted your files, copy the following certificates and Stores to the following locations:

MS_home/etc:CyaneaMgmtStore mgmttoproxy.cer mgmttomgmt.cer mgmttodc.cer

DC_home/itcamdc/etc:CyaneaDCStore CyaneaProxyStore
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 must modify the storepass and keypass lines using the new keystore name:

```
KEYSTR_LOC=MS_home/etc/IBMMSStore
KEYSTR_PASS=oakland2
KEYSTR_KEYPASS=oakland1
```

2. Modify the Visualization Engine (Application Monitor) user interface with the new keystore name, storepass and keypass. Complete the following procedure:
   a. Start the Managing Server.
   b. Log in to the IBM WebSphere Application Server administrative console.
   c. Click **Server > Server Types > WebSphere application servers** and select the *server_name*.
   d. In the **Configuration** tab, go to **Server Infrastructure: Java and Process Management > Process Definition > Additional Properties: Java Virtual Machine > Additional Properties: Custom Properties**.
   e. For the following name and value pairs, click **New**, enter the Name and Value, and click **Apply**:
      1) Set the path of the certificate to use when security is enabled for the Visualization Engine (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/CyaneaMgmtStore`
      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`

f. Restart the application server.

3. Modify *DC_home*/runtime/*app_server_version.node_name.server_name*/custom/datacollector_custom.properties file with the new storename, storepass, and keypass.
   a. Stop the instance of the application server that is being monitored by the data collector.
   b. Go to DC_home/runtime/app_server_version.node_name.server_name/custom/ datacollector_custom.properties.
   c. Set the following property definitions:

      Tip: All the following properties are set during the installation or at configuration time. By default, you do not have to do anything. You must change the following properties only if you changed items that the following properties refer to. All the keywords in angle (< >) brackets must be replaced by the appropriate value.

      - The path of the certificate to use when communicating with the data collector. This is only needed when the data collector is operating in secure mode. The delimiter must be a semicolon (;) on all platforms certificate.path=<AM_HOME>/etc/dctomgmt.cer;AM_HOME/etc/dctoproxy.cer.
      - The keystore location of the data collector keystore.location=@{AM_HOME}/etc/CyaneaDCStore.
      - The keystore password of data collector server keystore.storepass=oakland94612.
      - The keystore key password of data collector server keystore.keypass=oakland94612.

   d. For the property changes to take effect, start the instance of the application server that is monitored by the data collector.
4. Restart the Managing Server to implement the changes made to the managing server and data collector. For more information about managing server processes, see *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*.

Secure Socket Layer communications

On distributed platforms, ITCAM Agent for WebSphere Applications uses the SSL security protocol for integrity and confidentiality. You have the option of configuring all monitoring components to use SSL for communications. The following steps describe 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 servers 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.

Important: If you completed an embedded installation of the IBM WebSphere Application Server with the Managing Server, use the IBM WebSphere Application Server default key. For more information about IBM WebSphere Application Server default keys, refer to the IBM WebSphere Application Server documentation.

This section describes how to customize the default settings for SSL authentication in ITCAM for Applications.

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.
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`. For more information, see *ITCAM Managing Server Installation and Customization Guide* for full instructions for changing the Java Database Connectivity (JDBC) user ID and password for the database schema user.
   - keystore.storepass, keystore.keypass using the same method that is mentioned in the Step 2 on page 278.
   - keystore.storepass and keystore.keypass in *DC_home*`/runtime/`*app_server_version.node_name.server_name*`/custom/datacollector_custom.properties` file.
3. Restart the Managing Server to activate the password encryption changes:
   a. If it is not already stopped, stop the Managing Server.
   b. Start the Managing Server.
4. Restart the VE 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 the following string:

   ```
   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 to activate the changes:
   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 (For more information, see "Node Authentication" on page 275). 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 *DC_home*/runtime/*app_server_version.node_name.server_name*/custom/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.

Important: On the managing server, only the kernel-related changes must be enabled other managing server components are enabled automatically.

Verifying secure communications

To verify SSL is properly configured, look for the message labeled CYND4051I in one of the following files:

Table 37. Location of the CYND4051I message

Platform	Location
Windows systems	*DC_home*\logs\CYN\logs*node_name.server_name**java_msg_log_file*. For example: C:\IBM\ITM\dchome\7.2.0.0.1\logs\CYN\logs\IBMNode01.server1\msg-dc-Ext.log
UNIX and Linux systems	*DC_home*/logs/CYN/logs/*node_name.server_name*/*java_msg_log_file*. For example: opt/IBM/ITM/dchome/7.2.0.0.1/logs/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 38. Classification of the data processed on the CommandAgent channel

Classification	Data
Command and control data	Configuring and unconfiguring the data collector

Table 38. Classification of the data processed on the CommandAgent channel (continued)

Classification	Data
User actions related to threads	• Starting and stopping JVM threads • Changing thread priorities • Getting thread priorities and thread status • Requesting drill-down information to see cookies, etc. ... • Generating thread dumps • Getting thread stack traces
System information	• information • Operating system platform information • JVM information
Application information	• All the applications installed on the monitored • Application binaries and location information • Thread pool information related to JMS, JCA, JTA, Servlet, EJB, etc. ... • Data source information
Performance data	All Performance Monitoring Infrastructure data
Transport data	• ORB data • SOAP ports
Memory Information	• Obtaining JVM Heap Snapshot data • Performing memory leak analysis • Performing heap dump

Privacy filtering

The following procedures describe how to enable and verify privacy filtering.

Enabling privacy filtering

Privacy filtering is used to filter out SQL, cookie, and HTTP request query strings and other private data, for example drivers license numbers. 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 *DC_home*`/runtime/`*app_server_version*`.`*node_name*`.`*server_name*`/custom/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.
```

The log file is `trace-dc.log`.

Script to run if your SSL certificates have expired

All SSL certificates have an expiration time. For some certificates, the expiration time is four years, after which the product does not function if you have enabled Node Authentication and SSL. If so, to increase the expiration time, complete the following procedure:

1. Open the script located at *MS_home*/bin/security_cert.sh with a text editor. This 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
```

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 where 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 B. Configuring the agent for to monitor WebSphere Extreme Scale in security-enabled WebSphere environments

If you want to monitor WebSphere Extreme Scale (WXS) servers in WebSphere Application Server (WAS) security enabled environments, at present it is necessary to perform security configuration manually.

The procedure applies to the following case:

- WXS servers must be deployed inside the WAS application servers (or nodeagent/DMGR processes).
- ITCAM Agent for WebSphere Applications must be deployed on a node where a WXS zone catalog service is running. Configure the Agent for WXS monitoring under this node, and set it to connect to this catalog service instance.
- One Agent instance must be used to monitor only one WXS zone.

Initial Setup

After installing the Agent, but before configuring it, you need to perform several steps. You do not need to repeat them if the Agent or WXS is reconfigured. The steps are different for Windows and for Linux/UNIX systems.

Initial setup procedures on Windows

Perform the following procedures for initial setup on Windows systems.

Set up the Monitoring Agent to use the same JRE as WebSphere Application Server

About this task

Reconfigure the Monitoring Agent to use the same JRE as WebSphere Application Server (WAS). If the JRE used by WAS is not compatible with the Monitoring Agent (because of 64-bit and 32-bit binary platform differences), install a compatible JRE of the same release level, or if that is not available, of a more recent release level.

Procedure

1. Determine the versions and binary platform of the JRE installations used by the Monitoring Agent and the WAS.
   a. Find out the Monitoring Agent JRE location. Open the *ITM_HOME*\TMAITM6\kynenv file and find the JAVA_HOME definition in it, for example:

      ```
      JAVA_HOME=C:\IBM\ITM\java\java50\jre
      ```

   b. Using the resulting *JAVA_HOME*, run the *JAVA_HOME*\bin\java -version command. In its output, check whether the JRE is 32-bit or 64-bit. Example:

      ```
      > java -version
      Java(TM) SE Runtime Environment (build pwi3260sr2-20080818_01(SR2))
      IBM J9 VM (build 2.4, J2RE 1.6.0 IBM J9 2.4 Windows Server 2003 x86-32 jvmwi3260
      -20080816_22093 (JIT enabled, AOT enabled)
      J9VM - 20080816_022093_lHdSMr
      JIT  - r9_20080721_1330ifx2
      GC   - 20080724_AA)
      JCL  - 20080808_02
      ```

In this example, the JRE is 32-bit (x86-32).

c. Find out the home directory, binary platform, and release level of the JRE of the WAS. To do this, write and execute the following batch script.

```
call appserver_home\bin\setupCmdLine.bat
echo JAVA_HOME=%JAVA_HOME%
"%JAVA_HOME%\bin\java" -version
```

The script will display the Java home directory for the WAS JRE and the version information for the JRE (including binary platform).

If the binary platform is the same as that of the WAS installed on the node, use the WAS JRE home directory (*JAVA_HOME*) in the following steps. If the binary platform is different, download and install the JRE of the same binary platform as the Monitoring Agent and of the same version and release number as the WAS JRE. If this version is not available, download and install a newer JRE release from the same vendor. Record the installation home directory (*JAVA_HOME*).

Important: If you use a later JRE release, and the agent is unable to start or to connect with WXS catalog services, contact IBM support.

2. If you downloaded and installed a new JRE, copy the file orb.properties from the Java home directory for the WAS JRE (*appserver_home*\java\jre\lib) to the new Java home directory (*JAVA_HOME*\jre\lib).
3. Edit the *ITM_HOME*\TMAITM6\kynenv file. In the PATH variable, add the *JAVA_HOME*\bin directory.
4. Edit the *ITM_HOME*\TMAITM6\kyncma.ini file. Set the KWJ_JAVA_HOME property to the JRE home directory path (*JAVA_HOME*).

Configure the Monitoring Agent to work with WAS jar files and security properties

About this task

Configure the Monitoring Agent to work with WAS jar files and security properties. To do this, edit the kynwb.properties file.

Procedure

1. Open the *ITM_HOME*\TMAITM6\kynwb.properties file.
2. In the beginning of the file, the agent classpath is listed. Add the following lines before the existing lines.

   Attention: Use the / slash instead of the \ backslash as the directory separator.

   - For WebSphere Application Server 7.0:

     ```
     appserver_home/plugins/com.ibm.ws.runtime.jar;\
     appserver_home/lib/bootstrap.jar;\
     appserver_home/runtimes/com.ibm.ws.admin.client_7.0.0.jar;\
     appserver_home/lib/wsogclient.jar;\
     ```

   - For WebSphere Application Server 6.1:

     ```
     appserver_home/plugins/com.ibm.ws.runtime_6.1.0.jar;\
     appserver_home/lib/bootstrap.jar;\
     appserver_home/runtimes/com.ibm.ws.admin.client_6.1.0.jar;\
     appserver_home/lib/wsogclient.jar;\
     ```

   Example of a modified classpath:

   ```
   C:/IBM/WebSphere/plugins/com.ibm.ws.runtime.jar;\
   C:/IBM/WebSphere/lib/bootstrap.jar;\
   C:/IBM/WebSphere/runtimes/com.ibm.ws.admin.client_7.0.0.jar;\
   ```

```
C:/IBM/WebSphere/lib/wsogclient.jar;\
kynlib/kynwb.jar;\
kynlib/itcam.cg.mbean.jar;\
wasdc/7.1.0.2/installer/lib/itcamfwas.jar;\
```

3. At the end of the *ITM_HOME*\config\kynwb.properties file, add the lines indicating the security property files for use by the Agent. Typically, these files are the ones used by the wsadmin utility:

   ```
   -Dcom.ibm.CORBA.ConfigURL=file:/appserver_profile/properties/sas.client.props
   -Dcom.ibm.SSL.ConfigURL=file:/appserver_profile/properties/ssl.client.props
   ```

   If you require security settings for the agent that are different from those used by the wsadmin utility, create separate copies of the files and provide paths to them instead, for example:

   ```
   -Dcom.ibm.CORBA.ConfigURL=file:C:/IBM/ITM/config/sas.client.props
   -Dcom.ibm.SSL.ConfigURL=file:C:/IBM/ITM/config/ssl.client.props
   ```

Initial setup procedures on Linux and UNIX systems

Perform the following procedures for initial setup on Linux and UNIX systems.

Set up the Monitoring Agent to use the same JRE as WebSphere Application Server

About this task

Reconfigure the Monitoring Agent to use the same JRE as WebSphere Application Server (WAS). If the JRE used by WAS is not compatible with the Monitoring Agent (because of 64-bit and 32-bit binary platform differences), install a compatible JRE of the same release level, or if that is not available, of a more recent release level.

Procedure

1. Determine the versions and binary platform of the JRE installations used by the Monitoring Agent and the WAS.
   a. Find out the Monitoring Agent JRE location. Use the following command:

      ```
      itmcmd execute yn set | grep KWJ_JAVA
      ```

      Example:

      ```
      #bin/itmcmd execute yn set | grep KWJ_JAVA
      KWJ_JAVA_HOME=/AD7102SVT/WAS7ND/java/jre
      ```

   b. Using the resulting *JAVA_HOME* directory, run the *JAVA_HOME*/bin/java -version command. In its output, check whether the JRE is 32-bit or 64-bit. Example:

      ```
      #/AD7102SVT/WAS7ND/java/jre/bin/java -version
      java version "1.6.0"
      Java(TM) SE Runtime Environment (build pap3260sr7ifix-20100220_01(SR7+IZ70326))
      IBM J9 VM (build 2.4, JRE 1.6.0 IBM J9 2.4 AIX ppc-32
         jvmap3260sr7-20100219_54049 (JIT enabled, AOT enabled)
      J9VM - 20100219_054049
      JIT  - r9_20091123_13891
      GC   - 20100216_AA)
      JCL  - 20091202_01
      ```

      In this example, the JRE is 32-bit (ppc-32).

   c. Find out the home directory, binary platform, and release level of the JRE of the WAS. To do this, write and execute the following script.

```
#!/bin/sh
. appserver_home/bin/setupCmdLine.sh
echo JAVA_HOME=$JAVA_HOME
"$JAVA_HOME/bin/java" -version
```

The script will display the Java home directory for the WAS JRE and the version information for the JRE (including binary platform).

If the binary platform is the same as that of the WAS installed on the node, use the WAS JRE home directory (*JAVA_HOME*) in the following steps. If the binary platform is different, download and install the JRE of the same binary platform as the Monitoring Agent and of the same version and release number as the WAS JRE. If this version is not available, download and install a newer JRE release from the same vendor. Record the installation home directory (*JAVA_HOME*).

Important: If you use a later JRE release, and the agent is unable to start or to connect with WXS catalog services, contact IBM support.

2. If you downloaded and installed a new JRE, copy the file `orb.properties` from the Java home directory for the WAS JRE (*appserver_home*`/java/jre/lib`) to the new Java home directory (*JAVA_HOME*`/jre/lib`).
3. Determine the directories of the JRE that will be used.
   a. Change to the *JAVA_HOME* directory.
   b. Find the file `libjvm.so` in the `lib` subdirectory. Use the following command:
      ```
      find lib -name libjvm.so
      ```
      This command might return multiple results, for example:
      ```
      #find lib -name libjvm.so
      lib/ppc/classic/libjvm.so
      lib/ppc/j9vm/libjvm.so
      ```
   c. If multiple results were returned, prefer the following subdirectories:
      - On AIX, `lib/j9vm`
      - On Linux, `lib/j9vm`; if that is not present, `lib/classic`
      - On HP-UX, `lib/PA_RISC2.0/server`
      - On Solaris/SPARC, `lib/sparc/server`
      - On Solaris/x86, `lib/i386/server`

      Record the full pathname of the file (*libjvm*) and the full path to the directory where the file is located (*libjvmdir*)
4. Edit the *ITM_HOME*`/config/yn.ini` file.
   a. Set the KWJ_JAVA_HOME property to *JAVA_HOME*.
   b. Set the KWJ_LIBJVM property to *libjvm*.
   c. Determine the *librarypath* property name for your platform:
      - On AIX, LIBPATH
      - On Linux and Solaris, LD_LIBRARY_PATH
      - On HP-UX, SHLIB_PATH

      Also determine the *librarypath_PREFIX* variable name; it is the *librarypath* property name with _PREFIX appended (for example, LIBPATH_PREFIX on an AIX system, or LD_LIBRARY_PATH_PREFIX on a Linux system).
   d. Edit the *librarypath* property value in *ITM_HOME*`/config/yn.ini`. In the value of the property, replace $*librarypath_PREFIX*$ with the following two directories:

- The immediate parent of *libjvmdir*
- *libjvmdir*

Important: On Solaris, place the directories in a different order:

- *libjvmdir*
- The immediate parent of *libjvmdir*

For example, on an AIX system, the original value was:

```
LIBPATH=$ICCRTE_DIR$/$GSKLIB$:$LIBPATH_PREFIX$$CANDLEHOME$/$ARCHITECTURE$/lib:
 $CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/lib
```

The value after the editing:

```
LIBPATH=$ICCRTE_DIR$/$GSKLIB$:/AD7102SVT/WAS7ND/java/jre/lib/ppc:
  /AD7102SVT/WAS7ND/java/jre/lib/ppc/j9vm: $CANDLEHOME$/$ARCHITECTURE$/lib:
  $CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/lib:
```

On a Solaris system, the original value was:

```
LD_LIBRARY_PATH=$ICCRTE_DIR$/$GSKLIB$:$CANDLEHOME$/$ARCHITECTURE$/lib:
$CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/lib
```

The value after the editing:

```
LD_LIBRARY_PATH=$ICCRTE_DIR$/$GSKLIB$:$CANDLEHOME$/$ARCHITECTURE$/lib:
$CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/lib:
/opt/IBM/WebSphere/AppServer/java/jre/lib/sparc/server:
/opt/IBM/WebSphere/AppServer/java/jre/lib/sparc
```

Configure the Monitoring Agent to work with WAS jar files and security properties

About this task

Configure the Monitoring Agent to work with WAS jar files and security properties. To do this, edit the `kynwb.properties` file.

Procedure

1. Open the *ITM_HOME*/*architecture_code*/yn/config/kynwb.properties file.
2. In the beginning of the file, the classpath is listed. Add the following lines before the existing lines.
   - For WebSphere Application Server 7.0:

     ```
     appserver_home/plugins/com.ibm.ws.runtime.jar:\
     appserver_home/lib/bootstrap.jar:\
     appserver_home/runtimes/com.ibm.ws.admin.client_7.0.0.jar:\
     appserver_home/lib/wsogclient.jar;\
     ```

   - For WebSphere Application Server 6.1:

     ```
     appserver_home/plugins/com.ibm.ws.runtime_6.1.0.jar :\
     appserver_home/lib/bootstrap.jar :\
     appserver_home/runtimes/com.ibm.ws.admin.client_6.1.0.jar :\
     appserver_home/lib/wsogclient.jar;\
     ```

   Example of a modified classpath:

   ```
   /opt/IBM/WebSphere/plugins/com.ibm.ws.runtime.jar:\
   /opt/IBM/WebSphere/lib/bootstrap.jar:\
   /opt/IBM/WebSphere/runtimes/com.ibm.ws.admin.client_7.0.0.jar:\
   /opt/IBM/WebSphere/lib/wsogclient.jar;\
   kynlib/kynwb.jar:\
   kynlib/itcam.cg.mbean.jar:\
   wasdc/7.1.0.2/installer/lib/itcamfwas.jar:\
   ```

3. At the end of the *ITM_HOME*/*architecture_code*/yn/config/kynwb.properties file, add the lines indicating the security property files for use by the Agent. Typically, these files are the ones used by the wsadmin utility:

   ```
   -Dcom.ibm.CORBA.ConfigURL=file:/appserver_profile/properties/sas.client.props
   -Dcom.ibm.SSL.ConfigURL=file:/appserver_profile/properties/ssl.client.props
   ```

   If you require security settings for the agent that are different from those used by the wsadmin utility, create separate copies of the files and provide paths to them instead, for example:

   ```
   -Dcom.ibm.CORBA.ConfigURL=file:/opt/IBM/ITM/config/sas.client.props
   -Dcom.ibm.SSL.ConfigURL=file:/opt/IBM/ITM/config/ssl.client.props
   ```

Set up connection credentials

When a secure Java client is used, it needs to read a properties file that contains a list of CSIv2 settings. These settings determine how the client will authenticate to a server. You must ensure that the authentication is properly configured.

Typically, the file with these settings is specified in the com.ibm.CORBA.ConfigURL JVM property. Additional SSL settings can be found in file specified in the com.ibm.SSL.ConfigURL JVM property.

When ITCAM Agent for WebSphere Applications is configured to monitor eXtreme Scale servers embedded in WebSphere Application Server, it acts as secure Java client. For that reason, -Dcom.ibm.CORBA.ConfigURL and -Dcom.ibm.SSL.ConfigURL must be specified in the kynwb.properties file.

In most cases, these properties point to the sas.client.props and ssl.client.props files in the *appserver_profile*/properties directory. These files are used by tools like wsadmin or xscmd. Therefore, if you can use one of these tools to connect to an Extreme Scale catalog server without the need to enter any credentials, you do not need to customize the settings.

If the connection fails or requires entry of a username or password, you must complete additional configuration.

Modify client properties file

About this task

Edit the sas.client.props file to be used by the Agent. The full path to the file specified in the kynwb.properties file, in the -Dcom.ibm.CORBA.ConfigURL property. Supply the connection and security information for the WebSphere Application Server instance running the Catalog Services instance for which the Agent will be configured.

Procedure

1. Open the *appserver_profile*/properties/sas.client.props file.
2. Change the value of the com.ibm.CORBA.loginSource property to properties:

   ```
   com.ibm.CORBA.loginSource=properties
   ```

3. Set the property com.ibm.CORBA.securityServerHost to the host name of an application server within the WXS zone. The server can be the local server or a different one. The server must be always available when the agent starts up. For example:

   ```
   com.ibm.CORBA.securityServerHost=server.company.com
   ```

4. Set the com.ibm.CORBA.securityServerPort property to the RMI port for the application server profile, for example:

   ```
   com.ibm.CORBA.securityServerPort=2819
   ```

5. Set the property com.ibm.CORBA.loginUserid to the login name for communicating with the application server, and the property com.ibm.CORBA.loginPassword to the password, for example:

   ```
   com.ibm.CORBA.loginUserid=admin
   com.ibm.CORBA.loginPassword=password
   ```

6. Set the following properties to `true` or `false`, corresponding to the **CSIv2 inbound communications** settings in the WebSphere administrative console:

   ```
   com.ibm.CSI.performTLClientAuthenticationRequired
   com.ibm.CSI.performTLClientAuthenticationSupported
   com.ibm.CSI.performTransportAssocSSLTLSRequired
   com.ibm.CSI.performTransportAssocSSLTLSSupported
   ```

   The `com.ibm.CSI.performTLClientAuthentication*` properties are related to **Client certificate authentication** settings. The `com.ibm.CSI.performTransportAssocSSLTLS*` are related to **Transport** settings.

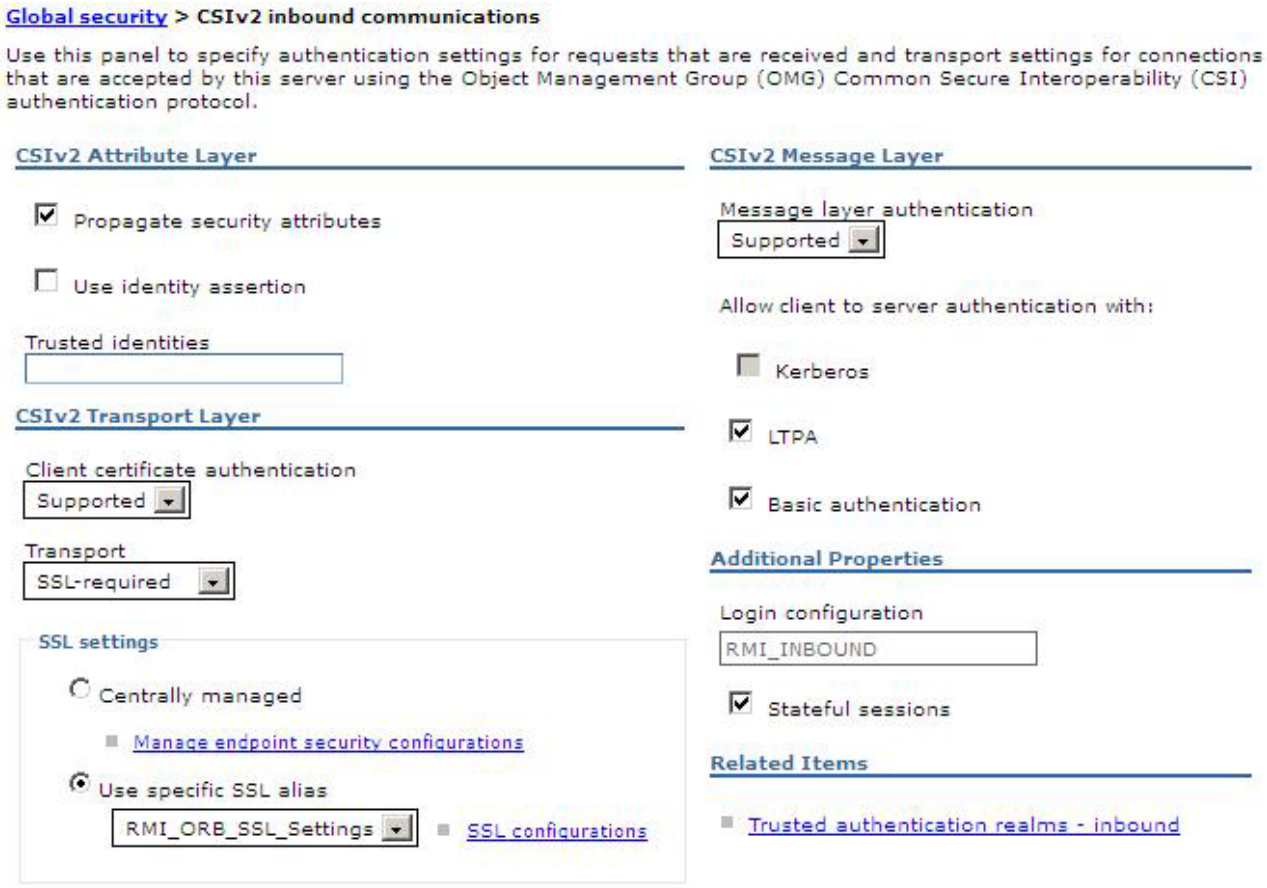

Figure 30. CSIv2 inbound communications settings in the WebSphere administrative console

7. Optional: If the default SSL alias (`DefaultSSLSettings`) is not used, set the SSL configuration alias name in the `com.ibm.ssl.alias` property.
8. Save the file, and then encrypt the password within the `sas.client.props` file. To encrypt the password, run the following command:

- On Windows, *appserver_profile*\bin\PropFilePasswordEncoder.bat sas.client.props com.ibm.CORBA.loginPassword
- On Linux and UNIX systems, *appserver_profile*/bin/PropFilePasswordEncoder.sh sas.client.props com.ibm.CORBA.loginPassword

Important: When client certificate authentication is required and basic authentication is enabled, you might also need to set the property com.ibm.CORBA.validateBasicAuth=false. for more information, see the following page: http://www-01.ibm.com/support/docview.wss?uid=swg21201533.

Modify client SSL properties file

About this task

Edit the ssl.client.props file to be used by the Agent. The full path to the file specified in the kynwb.properties file, in the -Dcom.ibm.SSL.ConfigURL property. Supply the SSL trust store and key store information for the WebSphere Application Server instance running the Catalog Services instance for which the Agent is to be configured.

You can create and manage certificates using the WebSphere administrative console (**Security** > **SSL certificate and key management** > **Key stores and certificates**) or using the iKeyman tool.

Procedure

1. Open the *appserver_profile*/properties/ssl.client.props file.
2. Change the value of the com.ibm.ssl.alias property to to match the value of the same property in the sas.client.props file.

   Tip: The ssl.client.props file can contain several SSL configurations. Each configuration starts with the com.ibm.ssl.alias property.
3. Set the com.ibm.ssl.enableSignerExchangePrompt property to false.
4. Set the following key store properties to enable the client application to access the encryption key:

   com.ibm.ssl.keyStoreName
   The name that identifies this key store

   com.ibm.ssl.keyStore
   The full path and name of the key store file

   com.ibm.ssl.keyStorePassword
   The password for the key store

   com.ibm.ssl.keyStoreType
   The key store type. Use the default PKCS12 type because of its interoperability with other applications.

   Important: If client certificate authentication is not required, the key store can contain any self signed key. Otherwise, the key store must contain a key signed by a certificate that is in the server trust store.
5. Set the following trust store properties to enable the client application to access signer certificates:

com.ibm.ssl.trustStoreName
The name that identifies this trust store

com.ibm.ssl.trustStore
The full path and name of the trust store file

com.ibm.ssl.trustStorePassword
The password for the trust store

com.ibm.ssl.trustStoreType
The trust store type. Use the default `PKCS12` type because of its interoperability with other applications.

Important: If the client is to use an SSL connection, the server signer certificate must be in its trust store.

Tip: For detailed description of properties in ssl.client.props file, search for "ssl.client.props" in the Infocenter for your version of WebSphere Application Server.

Final steps and subsequent maintenance

After completing the steps in this document, use the Zone Configuration workspace to configure the Agent to connect to the WXS catalog service. During this configuration, you do not need to set security parameters, as they are not used.

Important: If, after completing zone configuration, you find the connection to any catalog services does not work (the ERROR status is displayed), restart ITCAM Agent for WebSphere Applications.

If any additional details for your platform are required or you encounter any other difficulties in the security configuration procedure, contact IBM Support.

Attention: When you install a fix pack or interim fix for ITCAM Agent for WebSphere Applications, the changes made in the `yn.ini` and `kynwb.properties` files are overwritten. Therefore, after installing a fix pack or interim fix, you must complete the changes in this document again. For more information, see the technote at: http://www-01.ibm.com/support/docview.wss?uid=swg21575378

Examples of configuration changes

The following examples show configuration changes for different cases.

Using the WebSphere Application Server JVM

The host is a 32-bit Linux system.

ITCAM Agent for WebSphere Applications JRE:

```
$ /opt/IBM/ITM/JRE/li6263/bin/java -version
java version "1.5.0"
Java(TM) 2 Runtime Environment, Standard Edition (build pxi32dev-20081129 (SR9-0 ))
IBM J9 VM (build 2.3, J2RE 1.5.0 IBM J9 2.3 Linux x86-32 j9vmxi3223-20081129 (JIT enabled)
J9VM - 20081126_26240_lHdSMr
JIT  - 20081112_1511ifx1_r8
GC   - 200811_07)
JCL  - 20081128
```

WebSphere Application Server (WAS) version 7 JRE:

```
$ /opt/IBM/WebSphere7ND/AppServer/java/jre/bin/java -version
java version "1.6.0"
Java(TM) SE Runtime Environment (build pxi3260sr9fp1ifix-20110401_01(SR9 FP1+IZ95392+IZ95393+IZ97453))
IBM J9 VM (build 2.4, JRE 1.6.0 IBM J9 2.4 Linux x86-32 jvmxi3260sr9-20110216_75791
 (JIT enabled, AOT enabled)
J9VM - 20110216_075791
JIT  - r9_20101028_17488ifx4
GC   - 20101027_AA)
JCL  - 20110401_02
```

Both the agent and the WAS use a 32-bit JRE. The agent must be configured to use the application server JVM (version 1.6.0).

Agent configuration files before changes:

ITM_home/config/yn.ini:

```
...
LD_LIBRARY_PATH=$ICCRTE_DIR$/$GSKLIB$:$LD_LIBRARY_PATH_PREFIX$$CANDLEHOME$/$ARCHITECTURE$/lib:
$CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/lib
LIBPATH=$ICCRTE_DIR$/$GSKLIB$:$LIBPATH_PREFIX$$CANDLEHOME$/$ARCHITECTURE$/lib:
$CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/lib
PATH=/bin:/usr/bin:$CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/bin:$CANDLEHOME$/$ARCHITECTURE$/bin
...
KWJ_LIBJVM=$KWJ_LIBJVM$
KWJ_JAVA_HOME=$KWJ_JAVA_HOME$
```

ITM_home/li6263/yn/config/kynwb.properties:

```
lib/kynwb.jar:\
lib/itcam.cg.mbean.jar:\
wasdc/7.1.0.2.11/installer/lib/itcamfwas.jar:\
lib/kwjwb.jar:\
lib/kwjmbeans.jar:\
...
-Dkwj.tema.SampleCollectionThreadPool.keepalive=60000

-Xms32m
-Xmx384m
-Xrs
-Xgcpolicy:optavgpause
#-Xnosigcatch
# -Xverify
#-Xcheck:nabounds
#-Xcheck:jni
#-verbose
#-Xdebug
#-Xnoagent
#-Xrunjdwp:transport=dt_socket,server=y,address=8000,suspend=y
#-Djava.compiler=NONE
```

Agent configuration files after changes:

ITM_home/config/yn.ini:

```
...
LD_LIBRARY_PATH=$ICCRTE_DIR$/$GSKLIB$:/opt/IBM/WebSphere7ND/AppServer/java/jre/bin:
/opt/IBM/WebSphere7ND/AppServer/java/jre/bin/j9vm:$CANDLEHOME$/$ARCHITECTURE$/lib:
$CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/lib
LIBPATH=$ICCRTE_DIR$/$GSKLIB$:$LIBPATH_PREFIX$$CANDLEHOME$/$ARCHITECTURE$/lib:
$CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/lib
PATH=/bin:/usr/bin:$CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/bin:$CANDLEHOME$/$ARCHITECTURE$/bin
...
KWJ_LIBJVM=/opt/IBM/WebSphere7ND/AppServer/java/jre/bin/j9vm/libjvm.so
KWJ_JAVA_HOME=/opt/IBM/WebSphere7ND/AppServer/java/jre
```

ITM_home/li6263/yn/config/kynwb.properties:

```
/opt/IBM/WebSphere7ND/AppServer/plugins/com.ibm.ws.runtime.jar:\
/opt/IBM/WebSphere7ND/AppServer/lib/bootstrap.jar:\
/opt/IBM/WebSphere7ND/AppServer/runtimes/com.ibm.ws.admin.client_7.0.0.jar:\
/opt/IBM/WebSphere7ND/AppServer/lib/wsogclient.jar:\
lib/kynwb.jar:\
lib/itcam.cg.mbean.jar:\
wasdc/7.1.0.2.11/installer/lib/itcamfwas.jar:\
lib/kwjwb.jar:\
lib/kwjmbeans.jar:\
...
-Dkwj.tema.SampleCollectionThreadPool.keepalive=60000

-Xms32m
-Xmx384m
-Xrs
-Xgcpolicy:optavgpause
#-Xnosigcatch
# -Xverify
#-Xcheck:nabounds
#-Xcheck:jni
#-verbose
#-Xdebug
#-Xnoagent
#-Xrunjdwp:transport=dt_socket,server=y,address=8000,suspend=y
#-Djava.compiler=NONE
-Dcom.ibm.CORBA.ConfigURL=file:/opt/IBM/WebSphere7ND/profiles/WNDXS2/properties/sas.client.props
-Dcom.ibm.SSL.ConfigURL=file:/opt/IBM/WebSphere7ND/profiles/WNDXS2/properties/ssl.client.props
```

Using a new JVM

The host is a 64-bit AIX system.

ITCAM Agent for WebSphere Applications JRE:

```
$ /opt/IBM/ITM/JRE/aix523/bin/java -version
java version "1.5.0"
Java(TM) 2 Runtime Environment, Standard Edition (build pap32dev-20081129 (SR9-0 ))
IBM J9 VM (build 2.3, J2RE 1.5.0 IBM J9 2.3 AIX ppc-32 j9vmap3223-20081129 (JIT enabled)
J9VM - 20081126_26240_bHdSMr
JIT  - 20081112_1511ifx1_r8
GC   - 200811_07)
JCL  - 20081129
```

WebSphere Application Server (WAS) version 7 JRE:

```
$ /opt/IBM/WebSphere7ND/AppServer/java/jre/bin/java -version
java version "1.6.0"
Java(TM) SE Runtime Environment (build pap6460sr9fp1ifix-20110401_01(SR9 FP1+IZ95392+IZ95393+IZ97453))
IBM J9 VM (build 2.4, JRE 1.6.0 IBM J9 2.4 AIX ppc64-64 jvmap6460sr9-20110216_75791
 (JIT enabled, AOT enabled)
J9VM - 20110216_075791
JIT  - r9_20101028_17488ifx4
GC   - 20101027_AA)
JCL  - 20110401_02
```

On AIX systems, ITCAM Agent for WebSphere Applications runs as 32 bit process and uses the JRE from the /opt/IBM/ITM/JRE/aix523/ directory. If WAS server uses a 64-bit JRE, you must download a separate 32-bit version of JRE 1.6. Download IBM JRE from http://www.ibm.com/developerworks/java/jdk/aix/service.html.

In this example, the JRE was installed to the /usr/java6 directory.

```
$ /usr/java6/jre/bin/java -version
java version "1.6.0"
Java(TM) SE Runtime Environment (build pap3260sr9fp1-20110208_03(SR9 FP1))
IBM J9 VM (build 2.4, JRE 1.6.0 IBM J9 2.4 AIX ppc-32 jvmap3260sr9-20110203_74623 (JIT enabled, AOT enabled)
J9VM - 20110203_074623
JIT  - r9_20101028_17488ifx3
GC   - 20101027_AA)
JCL  - 20110203_01
```

You must copy the ORB properties file from the WAS JRE to the new JRE:

```
$ cp /opt/IBM/WebSphere7ND/AppServer/java/jre/lib/orb.properties /usr/java6/jre/lib/
```

Agent configuration files before changes:

ITM_home/config/yn.ini:

```
...
LD_LIBRARY_PATH=$ICCRTE_DIR$/$GSKLIB$:$LD_LIBRARY_PATH_PREFIX$$CANDLEHOME$/$ARCHITECTURE$/lib:
 $CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/lib
ITM_SAVE_LD_LIBRARY_PATH_64=$LD_LIBRARY_PATH_64$
LIBPATH=$ICCRTE_DIR$/$GSKLIB$:$LIBPATH_PREFIX$$CANDLEHOME$/$ARCHITECTURE$/lib:
 $CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/lib
PATH=/bin:/usr/bin:$CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/bin:$CANDLEHOME$/$ARCHITECTURE$/bin
...
KWJ_LIBJVM=$KWJ_LIBJVM$
KWJ_JAVA_HOME=$KWJ_JAVA_HOME$
```

ITM_home/aix523/yn/config/kynwb.properties:

```
lib/kynwb.jar:\
lib/itcam.cg.mbean.jar:\
wasdc/7.1.0.2.11/installer/lib/itcamfwas.jar:\
lib/kwjwb.jar:\
lib/kwjmbeans.jar:\
...
-Dkwj.tema.SampleCollectionThreadPool.keepalive=60000

-Xms32m
-Xmx384m
-Xrs
-Xgcpolicy:optavgpause
#-Xnosigcatch
# -Xverify
#-Xcheck:nabounds
#-Xcheck:jni
#-verbose
#-Xdebug
#-Xnoagent
#-Xrunjdwp:transport=dt_socket,server=y,address=8000,suspend=y
#-Djava.compiler=NONE
```

Agent configuration files after changes:

ITM_home/config/yn.ini:

```
...
LD_LIBRARY_PATH=$ICCRTE_DIR$/$GSKLIB$:$LD_LIBRARY_PATH_PREFIX$$CANDLEHOME$/$ARCHITECTURE$/lib:
 $CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/lib
ITM_SAVE_LD_LIBRARY_PATH_64=$LD_LIBRARY_PATH_64$
LIBPATH=$ICCRTE_DIR$/$GSKLIB$:/usr/java6/jre/lib/ppc:/usr/java6/jre/lib/ppc/j9vm:
 $CANDLEHOME$/$ARCHITECTURE$/lib:$CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/lib
PATH=/bin:/usr/bin:$CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/bin:$CANDLEHOME$/$ARCHITECTURE$/bin
...
KWJ_LIBJVM=/usr/java6/jre/lib/ppc/j9vm/libjvm.so
KWJ_JAVA_HOME=/usr/java6
```

ITM_home/li6263/yn/config/kynwb.properties:

```
/opt/IBM/WebSphere7ND/AppServer/plugins/com.ibm.ws.runtime.jar:\
/opt/IBM/WebSphere7ND/AppServer/lib/bootstrap.jar:\
/opt/IBM/WebSphere7ND/AppServer/runtimes/com.ibm.ws.admin.client_7.0.0.jar:\
/opt/IBM/WebSphere7ND/AppServer/lib/wsogclient.jar:\
lib/kynwb.jar:\
lib/itcam.cg.mbean.jar:\
wasdc/7.1.0.2.11/installer/lib/itcamfwas.jar:\
lib/kwjwb.jar:\
lib/kwjmbeans.jar:\
...
-Dkwj.tema.SampleCollectionThreadPool.keepalive=60000

-Xms32m
-Xmx384m
-Xrs
-Xgcpolicy:optavgpause
#-Xnosigcatch
# -Xverify
#-Xcheck:nabounds
#-Xcheck:jni
#-verbose
#-Xdebug
#-Xnoagent
#-Xrunjdwp:transport=dt_socket,server=y,address=8000,suspend=y
#-Djava.compiler=NONE
-Dcom.ibm.CORBA.ConfigURL=file:/opt/IBM/WebSphere7ND/profiles/Dmgr01/properties/sas.client.props
-Dcom.ibm.SSL.ConfigURL=file:/opt/IBM/WebSphere7ND/profiles/Dmgr01/properties/ssl.client.props
```

Example custom SSL configuration

In a typical custom setup, ITCAM Agent for WebSphere Applications uses different key stores from the `wsadmin` tool. You can use such a setup in various cases, for example, when the key stores used by the tools do not correspond to the current SSL configuration.

Preparing custom client properties files

As the agent is to use custom settings, you need to create custom copies of the *appserver_profile*`/properties/sas.client.props` and *appserver_profile*`/properties/ssl.client.props` files.

Copy these two files into the *ITM_HOME*`/config` directory,

In the file *ITM_HOME*`\TMAITM6\kynwb.properties` (on Windows systems) or *ITM_HOME*`/`*architecture_code*`/yn/config/kynwb.properties` (on Linux and UNIX systems), set the `-Dcom.ibm.CORBA.ConfigURL` and `-Dcom.ibm.SSL.ConfigURL` properties to point to these files, for example:

```
-Dcom.ibm.CORBA.ConfigURL=file:/opt/IBM/ITM/config/sas.client.props
-Dcom.ibm.SSL.ConfigURL=file:/opt/IBM/ITM/config/ssl.client.props
```

Modifying the client properties file

In the custom `sas.client.props` file, setting the correct credential information and set the com.ibm.CSI.* properties to match application server CSIv2 inbound communications settings. For this example, Figure 31 on page 298 shows the settings.

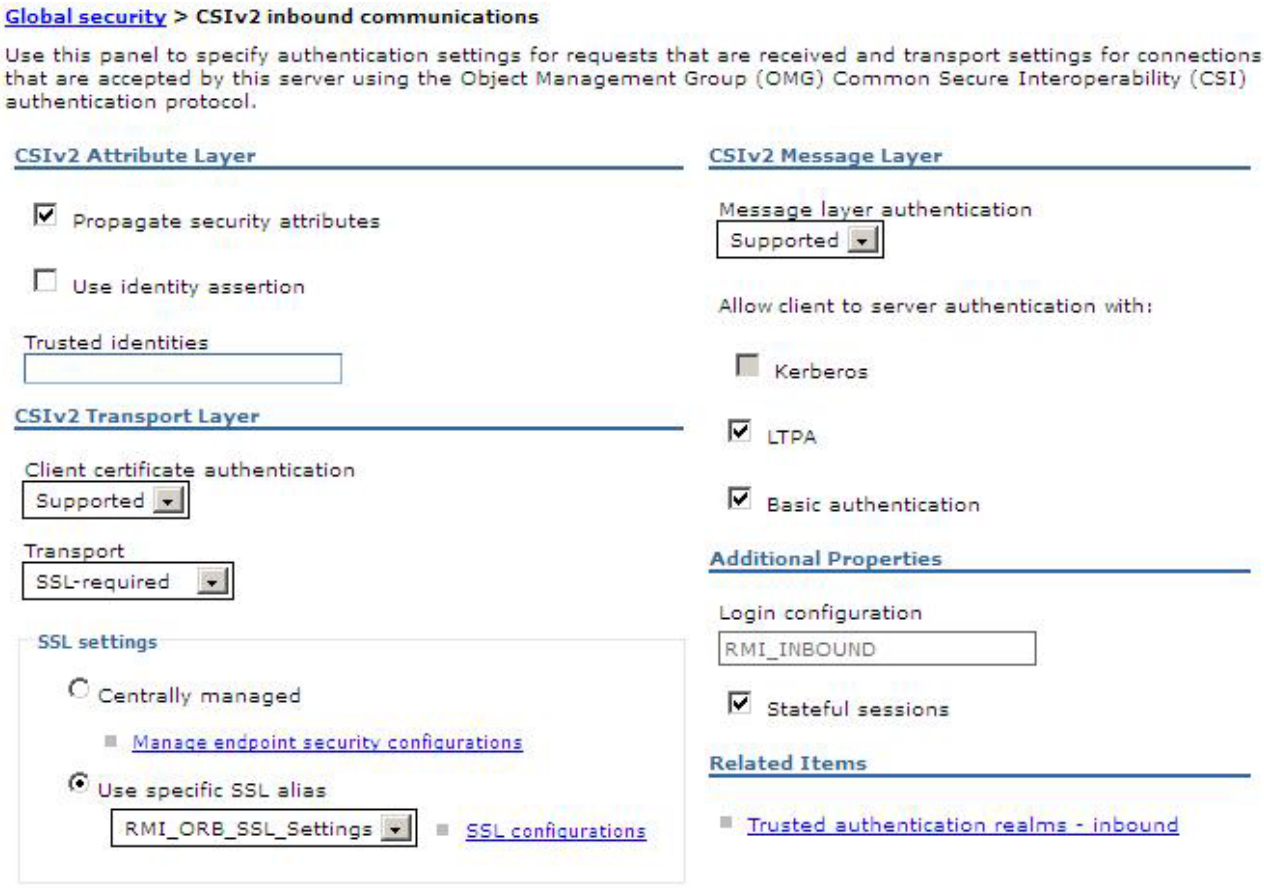

Figure 31. CSIv2 inbound communications settings in the WebSphere administrative console

The following configuration assures that the client is authenticated with the correct user and password and always uses SSL with certificate authentication:

```
#-----------------------------------------------------------------------------
# CSIv2 Configuration (see InfoCenter for more information on these properties).
#
# This is where you enable SSL client certificate authentication.  Must also
# specify a valid SSL keyStore below with a personal certificate in it.
#-----------------------------------------------------------------------------
# Does this client support stateful sessions?
com.ibm.CSI.performStateful=true
# Does this client support/require BasicAuth (userid/password) client authentication?
com.ibm.CSI.performClientAuthenticationRequired=false
com.ibm.CSI.performClientAuthenticationSupported=true
# Does this client support/require SSL client authentication?
com.ibm.CSI.performTLClientAuthenticationRequired=true
com.ibm.CSI.performTLClientAuthenticationSupported=false
# Note: You can perform BasicAuth (uid/pw) and SSL client authentication (certificate)
# simultaneously, however, the BasicAuth identity will always take precedence at the server.
# Does this client support/require SSL connections?
com.ibm.CSI.performTransportAssocSSLTLSRequired=true
com.ibm.CSI.performTransportAssocSSLTLSSupported=false
# Does this client support/require 40-bit cipher suites when using SSL?
com.ibm.CSI.performMessageIntegrityRequired=true
com.ibm.CSI.performMessageIntegritySupported=true
# Note: This property is only valid when SSL connections are supported or required.
# Does this client support/require 128-bit cipher suites when using SSL?
com.ibm.CSI.performMessageConfidentialityRequired=false
com.ibm.CSI.performMessageConfidentialitySupported=true
# Note: This property is only valid when SSL connections are supported or required.
```

```
#--------------------------------------------------------------------------------
# SSL configuration alias referenced in ssl.client.props
#--------------------------------------------------------------------------------
scom.ibm.ssl.alias=ITCAMSSLSettings
```

Creating SSL keys for the agent

On Figure 31 on page 298, the **SSL Alias** is set to `RMI_ORB_SSL_Settings`. Use this alias to review application server SSL settings and create SSL keys for the agent.

In the WebSphere administrative console, navigate to **Security** > **SSL certificate and key management**, and select the alias name (in this example, `RMI_ORB_SSL_Settings`). The trust store and key store names are displayed.

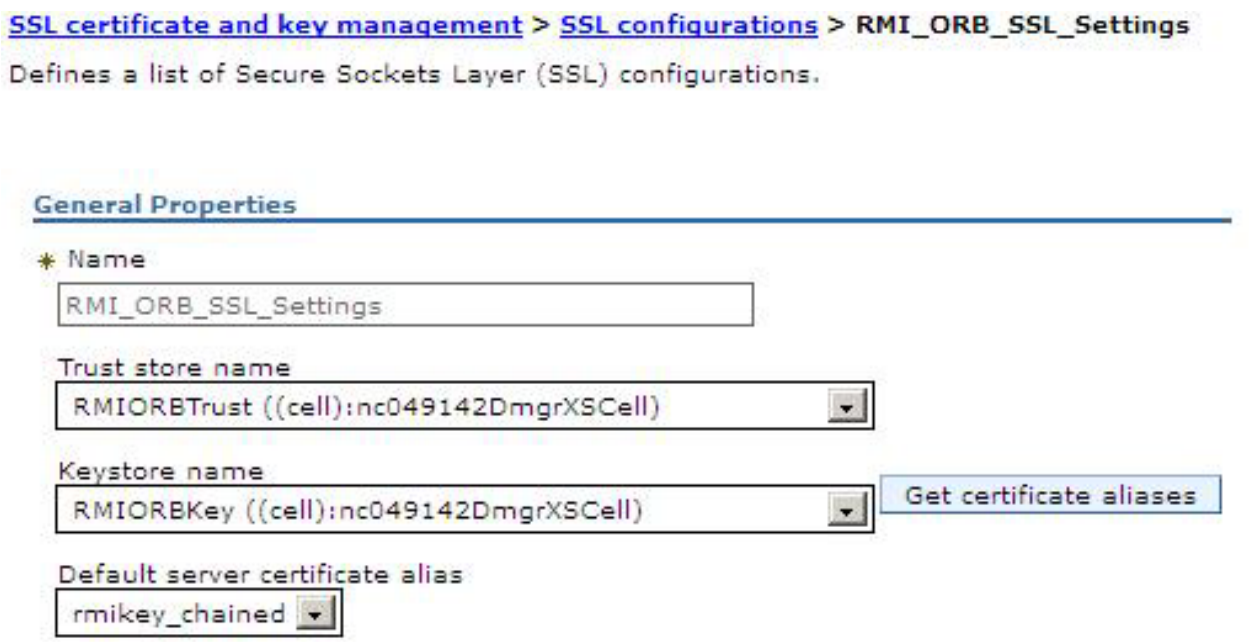

Figure 32. Trust store and key store configuration

The server uses the `rmikey_chained` key, stored in the `RMIORBKey` store. This key is signed by the root certificate of the cell.

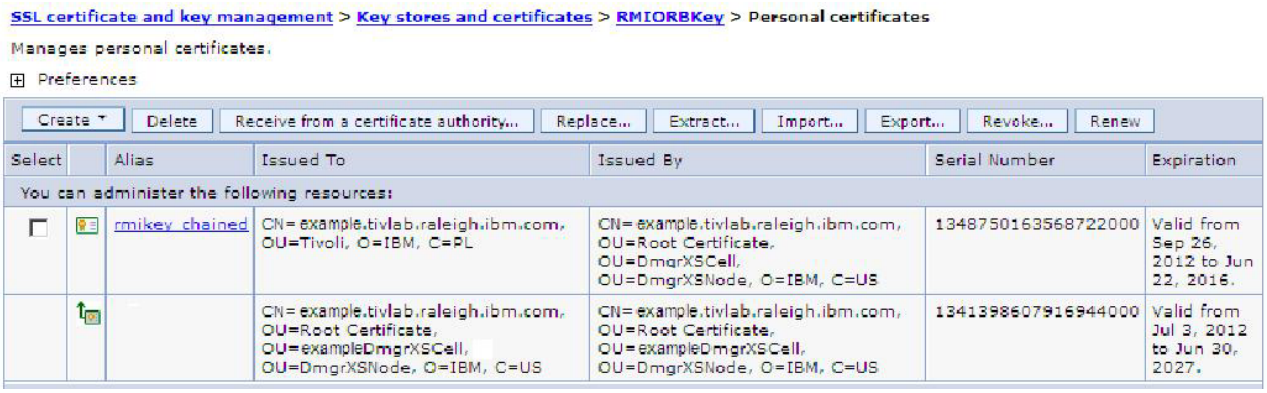

Figure 33. Personal certificates view of the RMIORBKey key store

The server uses the RMIORBTrust key store to check if the connecting client can be trusted. This key store contains only the root signer certificate, so it requires the client to use only keys signed by the root certificate.

Figure 34. Signer certificates view of the RMIORBTrust key store

You must create the key store for ITCAM Agent for WebSphere Applications based on the server SSL keys. In WebSphere Administrative Console, navigate to **Security** > **SSL certificate and key management** and click **New**. Then enter key the store filename with full path (for example, `/opt/IBM/ITM/config/ITCAMkeystore.p12`) and password. Set the management scope to the node that is on the same machine as the agent.

Figure 35. Properties of the key store for the agent

When this key store is created, it contains the server root certificate as a signer certificate. This certificate enables the agent to establish a connection with the server.

Important: If the server uses a self-signed certificate, export the certificate to a file and then import it into the client trust store.
You must also create a chained certificate. Select **Personal certificates** > **Create** > **Chained certificate** and fill in the certificate creation form. Select the same root signing certificate as in the server trust store.

Important: If certificate authentication is disabled in the server `sas.client.props` file, you can create a self-signed certificate instead of chained certificate. In this case, the client self signed certificate is used for SSL connection. It is not validated against server trust store.

Modifying the SSL client properties file

In the custom `ssl.client.props` file that you have created, replace the default section or create a new SSL configuration section at the end of the file. Use the key store that you created as both the key store and the trust store.

```
# ITCAM SSL settings
com.ibm.ssl.alias=ITCAMSSLSettings
com.ibm.ssl.protocol=SSL_TLS
com.ibm.ssl.securityLevel=HIGH
com.ibm.ssl.trustManager=IbmX509
com.ibm.ssl.keyManager=IbmX509
com.ibm.ssl.contextProvider=IBMJSSE2
com.ibm.ssl.enableSignerExchangePrompt=true
# KeyStore information
com.ibm.ssl.keyStoreName=ITCAMKey
com.ibm.ssl.keyStore=/opt/IBM/ITM/config/ITCAMkeystore.p12
com.ibm.ssl.keyStorePassword=password
com.ibm.ssl.keyStoreType=PKCS12
com.ibm.ssl.keyStoreProvider=IBMJCE
com.ibm.ssl.keyStoreFileBased=true
# TrustStore information
com.ibm.ssl.trustStoreName=ITCAMTrust
com.ibm.ssl.trustStore=/opt/IBM/ITM/config/ITCAMkeystore.p12
com.ibm.ssl.trustStorePassword=password
com.ibm.ssl.trustStoreType=PKCS12
com.ibm.ssl.trustStoreProvider=IBMJCE
com.ibm.ssl.trustStoreFileBased=true
com.ibm.ssl.trustStoreReadOnly=false
```

Appendix C. Configuring ITCAM Agent for WebSphere Applications to monitor WebSphere Extended Deployment

IBM Tivoli Composite Application Manager (ITCAM) Agent for WebSphere Applications version 7.2 provides support for WebSphere Extended Deployment (XD).

You must configure the monitoring of the XD cell and then perform additional manual configuration. This procedure is necessary because WebSphere Application Server works with a newer JVM version and the code is not compatible with the JVM version currently used by ITCAM Agent for WebSphere Applications.

Attention: Perform the additional configuration again after installing a new fix pack or interim fix for ITCAM Agent for WebSphere Applications.

WebSphere XD Overview for ITCAM Agent for WebSphere Applications

ITCAM Agent for WebSphere Applications provides enhanced support for monitoring Virtual Enterprise and Compute Grid products, as well as the Intelligent Management and Batch features of WebSphere Application Server 8.5. The cells managed by these products or features are called WebSphere XD (Extended Deployment) cells. For each XD cell, configured for monitoring by the WebSphere agent, the Tivoli Enterprise Portal shows the subnode under the agent node in the navigation tree. The workspaces under the XD cell subnode show the XD monitoring information.

The XD monitoring data is collected through a JMX connection to the deployment manager server and does not require a data collector. However, if a data collector is installed on any WebSphere XD server, it is possible to drill down to more detailed information.

ITCAM provides the following Virtual Enterprise monitoring features:

Monitors the status and metrics of the ODR (On Demand Router) server:

- ODR server status – running, not running, number of running ODR servers in the cell.
- ODR server process JVM and OS metrics.
- Collects requests metrics from ODR servers in the cell and provides summarized statistics over cell, cluster, server, and application.

Monitors the status and metrics of dynamic clusters

- Dynamic clusters topology
- Cluster configuration and state
- Application servers in cluster
- Current number of servers running in cluster
- Max number of servers in cluster
- Dynamic WLM Weight
- ODR server process JVM and OS metrics

Monitors XD application servers JVM information

- Server process JVM and OS metrics

ITCAM provides the following Compute Grid monitoring features:

Monitors Job Scheduler servers

- Job Scheduler server status – running, not running, number of running Job Scheduler servers.
- Job performance metrics reported by job scheduler servers, summarized over cell and per job scheduler.
- Details on queued and executing jobs, including notifications and job steps.
- Job Scheduler server process JVM and OS metrics.

Monitors Grid Endpoint servers

- Grid Endpoint server status – running, not running.
- Job performance metrics reported by grid endpoint servers, summarized over cell, service policy, and application.
- Grid endpoint server process JVM and OS metrics.

There are a number of situations provided to detect problems in the XD environment and to open Tivoli Enterprise Portal events.

WebSphere XD Cell Monitoring Prerequisites

To monitor the WebSphere XD cell, the following prerequisites must be met by the system where the WebSphere Tivoli Enterprise monitoring agent is installed:

- The WebSphere monitoring agent can be installed on any computer which has the WebSphere Virtual Enterprise or WebSphere Compute Grid products or WebSphere Application Server 8.5 (with Batch or Intelligent Management enabled). You do not have to install the WebSphere monitoring agent on the same system as the deployment manager, it can be on the same or a different system.
- The WebSphere XD products installed on the monitoring agent system must be the same version and release as the WebSphere XD products installed on the deployment manager system.
- The WebSphere monitoring agent user must have read and execute access to the installed files for the WebSphere product.
- It must be possible to establish WebSphere administrative client connection to the deployment manager. A network connection must be available and not be blocked by a firewall. This connection is typically available if any of the servers assigned to the cell are running on the system.
- If security is enabled for the WebSphere XD cell then there must be an existing WebSphere user or new WebSphere user created which has rights to complete the following tasks:
  - Establish administrative client connection
  - Access ConfigService
  - Query Perf MBean for Performance Monitoring Infrastructure (PMI) information
  - Query other WebSphere MBeans

  This user is specified directly or indirectly within the deployment manager connection properties during monitoring agent configuration.

Configure WebSphere XD Cell monitoring

You can configure a WebSphere agent to monitor WebSphere XD cells. To add an XD cell to the Tivoli Enterprise Portal, you must run the **Add_XD_Cell** take action option from Tivoli Enterprise Portal. Then the XD cell subnode displays in Tivoli Enterprise Portal and you can configure all connection settings using configuration workspace.

Complete the following steps to configure the agent to monitor the XD cell:

- This step is optional, but if you want to see any data in the jobs workspace you must install ITCAM CG Monitor enterprise application using `itcam.cg.py wsadmin` script described in the next section.
- From the Tivoli Enterprise Portal, run the **ADD_XD_Cell** take action command from the WebSphere agent node.
- Refresh the navigation tree, the XD Cell subnode displays under WebSphere agent node.
- Click the XD Cell subnode and follow the link, to open the configuration workspace.
- In the configuration workspace, specify connection settings and optionally update monitoring settings.

Convert WebSphere keystores to JKS format

To connect the WebSphere XD cell with enabled security you must specify the SSL truststore and keystore files in the configuration workspace on the Connection configuration tab. If you use JKS stores in your WebSphere configuration, you can specify them directly in the connection settings. If you use PKCS12 stores, you must create JKS stores and import keys from PKCS12 stores into JKS stores. Use the following steps to complete the import.

1. In a Windows environment, start `<WebSphere Location>\bin\ikeyman.bat`. In a UNIX environment, start `<WebSphere Location>/bin/ikeyman.sh`.
2. In the IBM Key Manager main menu, select **Key Database File>Open**.
3. From the **Key Database Type**, select **PKCS12**.
4. Click **Browse** next to the **File Name** field, and select the `<WebSphere Location>\profiles\<Deployment Manager Name>\etc\key.p12` file. Click **OK**.
5. In the Password Prompt dialog box that displays, type `WebAS` then click **OK**.
6. In the **Key Database Content** drop-down menu, select **Personal Certificates**.
7. Select the **default** key and click **Extract Certificate**.
8. From the **Data Type** drop-down menu, select **Binary DER data**.

   Important: Pay attention to the **Certificate file name** and **Location** fields. You can change the values or leave the default values.

   Click **OK**.
9. From the IBM Key Manager main menu, click **Key Database File >Open**.
10. From the **Key Database Type** drop-down menu, select **JKS**.
11. Click **Browse** next to the **File Name** field and select the `<WebSphere Location>\profiles\<Deployment Manager Name>\etc\DummyClientTrustFile.jks` file. Click **OK**.
12. In the Password Prompt dialog box, type `WebAS` then click **OK**.
13. In the **Key Database Content** drop-down menu, select **Signer Certificates**.

14. Click **Add** and specify the certificate file name extracted in steps 7 and 8. Click **OK**.
15. In the Enter a Label dialog box, type `imported` label and click **OK**.
16. Select **Key Database File > Exit** in the **IBM Key Manager** main menu to exit.

Install "ITCAM CG Monitor" enterprise application

To see details on the executing jobs (Jobs workspace), an optional ITCAM CG Monitor enterprise application can be deployed to the Job Scheduler deployment target (server or cluster). This application can be deployed using the supplied wsadmin script or through the admin console. `/opt/IBM/WebSphere_6.1_ND_XD/AppServer/bin/wsadmin.sh --lang jython -f ./itcam.cg.py deploy ./itcam.cg.ear`.

Note: The ITCAM CG Monitor enterprise application can be deployed and started on the Job Scheduler without any interruption to the Job Scheduler.

In order to deploy the ITCAM CG Monitor application using wsadmin, run the following command:

On Windows: From `<ITM root>/TMAITM6/kynlib run: wsadmin -lang jython [connection settings] -f itcam.cg.py deploy`

On UNIX or Linux: From `<ITM root>/<platform>/yn/lib run: wsadmin.sh -lang jython [connection settings] -f itcam.cg.py deploy`

`Where [connection settings] depends on environment and typically are: -user wasuser -password waspassword.`

Run Add XD Cell

1. In the Tivoli Enterprise Portal, click **WebSphere Agent - WebSphere**.
2. Right-click, select **Take Action > Select**.
3. In the **Select Action** dialog box, click **Add_XD_Cell**.
4. Type the cell name, click **OK**.
5. Wait for the refresh icon to appear in the navigation tree toolbar.
6. When the XD Cell node displays in the navigation tree. Click the XD Cell node, then click the link to open the configuration workspace.

Configure the Deployment Manager Connection

The configuration workspace specifies connection settings and monitoring settings.

1. Click **WebSphere XD Cell**
2. Click the link to open the configuration workspace. The configuration workspace displays the following tabs:
   - Connection Settings
   - Connection Security Settings
   - Collection Settings
   - Job Filter Settings
3. Complete the fields in the tabs using the hover help as a guide. You can also use the configuration options following these steps as a guide.
4. When the connection settings are saved, refresh the workspace and check the cell connection status. If all settings are correct then status changes to

Connected . If settings are incorrect, the status changes to **Error**. For details on the connection error, see the WebSphere Agent event log in the WebSphere Agent status workspace.

SOAP Connection to WebSphere XD cell with enabled security

- **Connector Host**: The address or host name that the deployment manager is listening on.
- **Connector port**: The SOAP port that the deployment manager is listening on.
- **Connector type**: The connector type can be SOAP or RMI. In this case use SOAP.
- Connector Security Enabled: Set to **True** to enable security
- **User name**: Add the WebSphere user name.
- **User password** Add the WebSphere user password.

  Tip: The monitoring agent saves the password to a file in encrypted form. The encryption key is available with the WebSphere monitoring agent files. To have a more secure password it is recommended to use the SSL keys instead of password.
- **SSL Trust Store File:** This is a store of keys trusted by SOAP client. It stores deployment manager public SSL key. After installation, WebSphere creates such file in the following path `-- <WAS home>/etc/DummyClientTrustFile.jks.` a WebSphere administrator can customize this file.
- **SSL Trust Store Password:** This is the password for the SSL Trust Store file. The default WebSphere password is “WebAS”.
- **SSL Key Store File:** This is a store of SOAP client public and private keys. After installation WebSphere creates this file in the following path `-- <WAS home>/etc/DummyClientKeyFile.jks`. A WebSphere administrator can customize this file.
- **SSL Key Store Password:** This is the password for the SSL Key Store file. The default WebSphere password is “WebAS".

Simple configuration with SOAP connection and no security configured

- **Connector Host** The address or host name that the deployment manager is listening on.
- **Connector Port** The SOAP port that the deployment manager is listening on.
- **Connector Type** This can be SOAP or RMI. In this case use SOAP.
- **Connector Security Enabled** Set to **False** to disable security.

See also “WebSphere XD Overview for ITCAM Agent for WebSphere Applications” on page 303.

Additional configuration procedure on Windows systems

Complete the following procedure for configuration on Windows systems.

Set up the Monitoring Agent to use the same JRE as WebSphere Application Server

About this task

Reconfigure the Monitoring Agent to use the same JRE as WebSphere Application Server (WAS). If the JRE used by WAS is not compatible with the Monitoring Agent (because of 64-bit and 32-bit binary platform differences), install a

compatible JRE of the same release level, or if that is not available, of a more recent release level.

Procedure

1. Determine the versions and binary platform of the JRE installations used by the Monitoring Agent and the WAS.
   a. Find out the Monitoring Agent JRE location. Open the *ITM_HOME*\TMAITM6\kynenv file and find the JAVA_HOME definition in it, for example:

      ```
      JAVA_HOME=C:\IBM\ITM\java\java50\jre
      ```

   b. Using the resulting *JAVA_HOME*, run the *JAVA_HOME*\bin\java -version command. In its output, check whether the JRE is 32-bit or 64-bit. Example:

      ```
      > java -version
      Java(TM) SE Runtime Environment (build pwi3260sr2-20080818_01(SR2))
      IBM J9 VM (build 2.4, J2RE 1.6.0 IBM J9 2.4 Windows Server 2003 x86-32 jvmwi3260
      -20080816_22093 (JIT enabled, AOT enabled)
      J9VM - 20080816_022093_lHdSMr
      JIT  - r9_20080721_1330ifx2
      GC   - 20080724_AA)
      JCL  - 20080808_02
      ```

      In this example, the JRE is 32-bit (x86-32).

   c. Find out the home directory, binary platform, and release level of the JRE of the WAS. To do this, write and execute the following batch script.

      ```
      call appserver_home\bin\setupCmdLine.bat
      echo JAVA_HOME=%JAVA_HOME%
      "%JAVA_HOME%\bin\java" -version
      ```

      The script will display the Java home directory for the WAS JRE and the version information for the JRE (including binary platform).

   If the binary platform is the same as that of the WAS installed on the node, use the WAS JRE home directory (*JAVA_HOME*) in the following steps. If the binary platform is different, download and install the JRE of the same binary platform as the Monitoring Agent and of the same version and release number as the WAS JRE. If this version is not available, download and install a newer JRE release from the same vendor. Record the installation home directory (*JAVA_HOME*).

   Important: If you use a later JRE release, and the agent is unable to start or to connect with the XD deployment manager, contact IBM support.
2. If you downloaded and installed a new JRE, copy the file orb.properties from the Java home directory for the WAS JRE (*appserver_home*\java\jre\lib) to the new Java home directory (*JAVA_HOME*\jre\lib).
3. Edit the *ITM_HOME*\TMAITM6\kynenv file.
   a. Set the KWJ_JAVA_HOME property to the JRE home directory path (*JAVA_HOME*).
   b. In the PATH variable, add the *JAVA_HOME*\bin directory.

Additional configuration procedure on Linux and UNIX systems

Complete the following procedure for configuration on Linux and UNIX systems.

Set up the Monitoring Agent to use the same JRE as WebSphere Application Server

About this task

Reconfigure the Monitoring Agent to use the same JRE as WebSphere Application Server (WAS). If the JRE used by WAS is not compatible with the Monitoring Agent (because of 64-bit and 32-bit binary platform differences), install a compatible JRE of the same release level, or if that is not available, of a more recent release level.

Procedure

1. Determine the versions and binary platform of the JRE installations used by the Monitoring Agent and the WAS.
   a. Find out the Monitoring Agent JRE location. Use the following command:

      ```
      itmcmd execute yn set | grep KWJ_JAVA
      ```

      Example:

      ```
      #bin/itmcmd execute yn set | grep KWJ_JAVA
      KWJ_JAVA_HOME=/AD7102SVT/WAS7ND/java/jre
      ```

   b. Using the resulting *JAVA_HOME* directory, run the *JAVA_HOME*/bin/java -version command. In its output, check whether the JRE is 32-bit or 64-bit. Example:

      ```
      #/AD7102SVT/WAS7ND/java/jre/bin/java -version
      java version "1.6.0"
      Java(TM) SE Runtime Environment (build pap3260sr7ifix-20100220_01(SR7+IZ70326))
      IBM J9 VM (build 2.4, JRE 1.6.0 IBM J9 2.4 AIX ppc-32
         jvmap3260sr7-20100219_54049 (JIT enabled, AOT enabled)
      J9VM - 20100219_054049
      JIT  - r9_20091123_13891
      GC   - 20100216_AA)
      JCL  - 20091202_01
      ```

      In this example, the JRE is 32-bit (ppc-32).

   c. Find out the home directory, binary platform, and release level of the JRE of the WAS. To do this, write and execute the following script.

      ```
      #!/bin/sh
      . appserver_home/bin/setupCmdLine.sh
      echo JAVA_HOME=$JAVA_HOME
      "$JAVA_HOME/bin/java" -version
      ```

      The script will display the Java home directory for the WAS JRE and the version information for the JRE (including binary platform).

   If the binary platform is the same as that of the WAS installed on the node, use the WAS JRE home directory (*JAVA_HOME*) in the following steps. If the binary platform is different, download and install the JRE of the same binary platform as the Monitoring Agent and of the same version and release number as the WAS JRE. If this version is not available, download and install a newer JRE release from the same vendor. Record the installation home directory (*JAVA_HOME*).

   Important: If you use a later JRE release, and the agent is unable to start or to connect with the XD deployment manager, contact IBM support.
2. If you downloaded and installed a new JRE, copy the file orb.properties from the Java home directory for the WAS JRE (*appserver_home*/java/jre/lib) to the new Java home directory (*JAVA_HOME*/jre/lib).

3. Determine the directories of the JRE that will be used.
   a. Change to the *JAVA_HOME* directory.
   b. Find the file `libjvm.so` in the `lib` subdirectory. Use the following command:
      ```
      find lib -name libjvm.so
      ```
      This command might return multiple results, for example:
      ```
      #find lib -name libjvm.so
      lib/ppc/classic/libjvm.so
      lib/ppc/j9vm/libjvm.so
      ```
   c. If multiple results were returned, prefer the following subdirectories:
      - On AIX, `lib/j9vm`
      - On Linux, `lib/j9vm`; if that is not present, `lib/classic`
      - On HP-UX, `lib/PA_RISC2.0/server`
      - On Solaris/SPARC, `lib/sparc/server`
      - On Solaris/x86, `lib/i386/server`

      Record the full pathname of the file (*libjvm*) and the full path to the directory where the file is located (*libjvmdir*)
4. Edit the *ITM_HOME*`/config/yn.ini` file.
   a. Set the KWJ_JAVA_HOME property to *JAVA_HOME*.
   b. Set the KWJ_LIBJVM property to *libjvm*.
   c. Determine the *librarypath* property name for your platform:
      - On AIX, LIBPATH
      - On Linux and Solaris, LD_LIBRARY_PATH
      - On HP-UX, SHLIB_PATH

      Also determine the *librarypath_PREFIX* variable name; it is the *librarypath* property name with _PREFIX appended (for example, LIBPATH_PREFIX on an AIX system, or LD_LIBRARY_PATH_PREFIX on a Linux system).
   d. Edit the *librarypath* property value in *ITM_HOME*`/config/yn.ini`. In the value of the property, replace $*librarypath_PREFIX*$ with the following two directories:
      - The immediate parent of *libjvmdir*
      - *libjvmdir*

      For example, the original value was:
      ```
      LIBPATH=$ICCRTE_DIR$/$GSKLIB$:$LIBPATH_PREFIX$$CANDLEHOME$/$ARCHITECTURE$/lib:
       $CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/lib
      ```
      the value after the editing:
      ```
      LIBPATH=$ICCRTE_DIR$/$GSKLIB$:/AD7102SVT/WAS7ND/java/jre/lib/ppc:
        /AD7102SVT/WAS7ND/java/jre/lib/ppc/j9vm:$CANDLEHOME$/$ARCHITECTURE$/lib:
        $CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/lib:
      ```

Examples of configuration changes

The following examples show configuration changes for different cases.

Using the WebSphere Application Server JVM

The host is a 32-bit Linux system.

ITCAM Agent for WebSphere Applications JRE:

```
$ /opt/IBM/ITM/JRE/li6263/bin/java -version
java version "1.5.0"
Java(TM) 2 Runtime Environment, Standard Edition (build pxi32dev-20081129 (SR9-0 ))
IBM J9 VM (build 2.3, J2RE 1.5.0 IBM J9 2.3 Linux x86-32 j9vmxi3223-20081129 (JIT enabled)
J9VM - 20081126_26240_lHdSMr
JIT  - 20081112_1511ifx1_r8
GC   - 200811_07)
JCL  - 20081128
```

WebSphere Application Server (WAS) version 8 JRE:

```
$ /opt/IBM/WebSphere8ND/AppServer/java/jre/bin/java -version
Java(TM) SE Runtime Environment (build pxi3260_26fp2-20110801_01)
IBM J9 VM (build 2.6, JRE 1.6.0 Linux x86-32 20110729_87983 (JIT enabled, AOT enabled)
J9VM - R26_Java626_GA_FP2_20110729_1129_B87983
JIT  - r11_20110215_18645ifx11
GC   - R26_Java626_GA_FP2_20110729_1129_B87983
J9CL - 20110729_87983)
JCL  - 20110712_01
```

Both the agent and the WAS use a 32-bit JRE. The agent must be configured to use the application server JVM (version 1.6.0).

Agent configuration file before changes:

ITM_home/config/yn.ini:

```
...
LD_LIBRARY_PATH=$ICCRTE_DIR$/$GSKLIB$:$LD_LIBRARY_PATH_PREFIX$$CANDLEHOME$/$ARCHITECTURE$/lib:
 $CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/lib
LIBPATH=$ICCRTE_DIR$/$GSKLIB$:$LIBPATH_PREFIX$$CANDLEHOME$/$ARCHITECTURE$/lib:
 $CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/lib
PATH=/bin:/usr/bin:$CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/bin:$CANDLEHOME$/$ARCHITECTURE$/bin
...
KWJ_LIBJVM=$KWJ_LIBJVM$
KWJ_JAVA_HOME=$KWJ_JAVA_HOME$
```

Agent configuration file after changes:

ITM_home/config/yn.ini:

```
...
LD_LIBRARY_PATH=$ICCRTE_DIR$/$GSKLIB$:/opt/IBM/WebSphere8ND/AppServer/java/jre/bin:
 /opt/IBM/WebSphere8ND/AppServer/java/jre/bin/j9vm:$CANDLEHOME$/$ARCHITECTURE$/lib:
 $CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/lib
LIBPATH=$ICCRTE_DIR$/$GSKLIB$:$LIBPATH_PREFIX$$CANDLEHOME$/$ARCHITECTURE$/lib:
 $CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/lib
PATH=/bin:/usr/bin:$CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/bin:$CANDLEHOME$/$ARCHITECTURE$/bin
...
KWJ_LIBJVM=/opt/IBM/WebSphere8ND/AppServer/java/jre/bin/j9vm/libjvm.so
KWJ_JAVA_HOME=/opt/IBM/WebSphere8ND/AppServer/java/jre
```

Using a new JVM

The host is a 64-bit AIX 6.1 system.

ITCAM Agent for WebSphere Applications JRE:

```
$ /opt/IBM/ITM/JRE/aix523/bin/java -version
java version "1.5.0"
Java(TM) 2 Runtime Environment, Standard Edition (build pap32dev-20081129 (SR9-0 ))
IBM J9 VM (build 2.3, J2RE 1.5.0 IBM J9 2.3 AIX ppc-32 j9vmap3223-20081129 (JIT enabled)
J9VM - 20081126_26240_bHdSMr
JIT  - 20081112_1511ifx1_r8
GC   - 200811_07)
JCL  - 20081129
```

WebSphere Application Server (WAS) version 8 JRE:

```
$ /opt/IBM/WebSphere8ND/AppServer/java/jre/bin/java -version
java version "1.6.0"
Java(TM) SE Runtime Environment (build pap6460_26fp2-20110801_01)
IBM J9 VM (build 2.6, JRE 1.6.0 AIX ppc64-64 20110729_87983 (JIT enabled, AOT enabled)
J9VM - R26_Java626_GA_FP2_20110729_1129_B87983
JIT  - r11_20110215_18645ifx11
GC   - R26_Java626_GA_FP2_20110729_1129_B87983
J9CL - 20110729_87983)
JCL  - 20110712_01
```

On AIX systems, ITCAM Agent for WebSphere Applications version 7.1 runs as 32 bit process and uses the JRE from the `/opt/IBM/ITM/JRE/aix523/` directory. If WebSphere Application Server uses a 64-bit JRE, you must download a separate 32-bit version of JRE 1.6. Download IBM JRE from http://www.ibm.com/developerworks/java/jdk/aix/service.html.

In this example, the JRE was installed to the `/usr/java6` directory.

```
$ /usr/java6/jre/bin/java -version
java version "1.6.0"
Java(TM) SE Runtime Environment (build pap3260sr9fp2-20110627_03(SR9 FP2))
IBM J9 VM (build 2.4, JRE 1.6.0 IBM J9 2.4 AIX ppc-32 jvmap3260sr9-20110624_85526 (JIT enabled, AOT enabled)
J9VM - 20110624_085526
JIT  - r9_20101028_17488ifx17
GC   - 20101027_AA)
JCL  - 20110530_01
```

You must copy the ORB properties file from the WAS JRE to the new JRE:

```
$ cp /opt/IBM/WebSphere8ND/AppServer/java/jre/lib/orb.properties /usr/java6/jre/lib/
```

Agent configuration file before changes:

ITM_home`/config/yn.ini`:

```
...
LD_LIBRARY_PATH=$ICCRTE_DIR$/$GSKLIB$:$LD_LIBRARY_PATH_PREFIX$$CANDLEHOME$/$ARCHITECTURE$/lib:
 $CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/lib
ITM_SAVE_LD_LIBRARY_PATH_64=$LD_LIBRARY_PATH_64$
LIBPATH=$ICCRTE_DIR$/$GSKLIB$:$LIBPATH_PREFIX$$CANDLEHOME$/$ARCHITECTURE$/lib:
 $CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/lib
PATH=/bin:/usr/bin:$CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/bin:$CANDLEHOME$/$ARCHITECTURE$/bin
...
KWJ_LIBJVM=$KWJ_LIBJVM$
KWJ_JAVA_HOME=$KWJ_JAVA_HOME$
```

Agent configuration file after changes:

ITM_home`/config/yn.ini`:

```
...
LD_LIBRARY_PATH=$ICCRTE_DIR$/$GSKLIB$:$LD_LIBRARY_PATH_PREFIX$$CANDLEHOME$/$ARCHITECTURE$/lib:
 $CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/lib
ITM_SAVE_LD_LIBRARY_PATH_64=$LD_LIBRARY_PATH_64$
LIBPATH=$ICCRTE_DIR$/$GSKLIB$:/usr/java6/jre/lib/ppc:/usr/java6/jre/lib/ppc/j9vm:
 $CANDLEHOME$/$ARCHITECTURE$/lib:$CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/lib
PATH=/bin:/usr/bin:$CANDLEHOME$/$BINARCH$/$PRODUCTCODE$/bin:$CANDLEHOME$/$ARCHITECTURE$/bin
...
KWJ_LIBJVM=/usr/java6/jre/lib/ppc/j9vm/libjvm.so
KWJ_JAVA_HOME=/usr/java6
```

Appendix D. Starting and stopping the monitoring environment

Procedures are provided for starting and stopping various components, databases, and application servers associated with ITCAM Data Collector for WebSphere.

Disabling and re-enabling a data collector

If you want to disable a data collector without unconfiguring or uninstalling it, complete the following procedure:

1. Log in to the IBM WebSphere Application Server administrative console.
2. Expand **Servers > Server Type** and click **WebSphere application servers**.
3. Choose the *server_name*.
4. On the Configuration tab, under the **Server Infrastructure** section, expand **Java and Process Management** and select **Process Definition**.
5. Under the **Additional Properties** section, go to **Java Virtual Machine > Custom Properties**.
6. Find a property with the name `ITCAM_DC_ENABLE`. If this property is not present, add it.
7. Set the value of this property to `false`.
8. Click **OK** or **Apply**. Click **Save**.
9. Restart the application server (for more information, see "Restarting the application server")

To re-enable a data collector that was disabled in this way, complete the following procedure:

1. Log in to the IBM WebSphere Application Server administrative console.
2. Expand **Servers > Server Type** and click **WebSphere application servers**
3. Choose the *server_name*.
4. On the Configuration tab, under the **Server Infrastructure** section, expand **Java and Process Management** and select **Process Definition**.
5. Under the **Additional Properties** section, go to **Java Virtual Machine > Custom Properties**.
6. Find the property with the name `ITCAM_DC_ENABLE`.
7. Set the value of this property to `true`.
8. Click **OK** or **Apply**. Click **Save**.
9. Restart the application server (for more information, see "Restarting the application server")

Restarting the application server

There are separate procedures for restarting the application server in a Network Deployment and non-Network Deployment environments.

Restarting the application server in a non-Network Deployment

To restart the application server, complete the following steps:

Table 39. Restarting the application server

Platform	Steps

Windows	Complete one of the following steps:
	• (recommended) From the Windows Start menu:
	1. From the Windows Start menu, click **(All) Programs > IBM WebSphere > *application_server_and_version*> Profiles > *profile_name* > First steps**.
	2. Click **Stop the server**.
	Wait for the First steps output window to display a message similar to the following message:
	`Server server_name stop completed`
	3. Click **Start the server**.
	The First steps output window displays a message that is similar to the following message:
	`Server server_name open for e-business`
	• From a command line:
	`cd AppServer_home\profiles\profile_name\bin`
	`stopServer server_name [options]`
	`startServer server_name`

Linux or UNIX systems	`cd AppServer_home/profiles/profile_name/bin`
	`./stopServer server_name [options]`
	`./startServer server_name`

The *server_name* is the name of the configuration directory of the server that you want to restart. The default is `server1`.

The *profile_name* specifies the profile name. The default is `default`.

If WebSphere Global Security is enabled, add the following options to every command:

- The `-username` *name* or `-user` *name* option specifies the user name for authentication if security is enabled in the server.
- The `-password` *password* option specifies the password for authentication if security is enabled in the server.

Important: If you are running in a secure environment but have not provided a user ID and password, you receive an error message.

Restarting the application server in a Network Deployment environment

To restart the application server, complete the following steps:

1. Change to the *AppServer_home*`/bin` directory.
2. Stop all servers that are on the node, and the node itself. Run the `stopNode -stopservers` command
3. Stop the deployment manager process. Run the `stopManager` command.

4. Start the deployment manager process. Run the `startManager` command.
5. Start the node. Run the `startNode` command.
6. For each application server on the node, start the application server using the procedure in "Starting the application server in a non-Network Deployment environment."

On Linux or UNIX systems, add `./` before every command to run it.

If WebSphere Global Security is enabled, add the following options to every command:

- The `-username` *name* or `-user` *name* option specifies the user name for authentication if security is enabled in the server.
- The `-password` *password* option specifies the password for authentication if security is enabled in the server.

Important: If you are running in a secure environment but have not provided a user ID and password, you receive an error message.

Starting the application server

There are separate procedures for starting the application server in a Network Deployment and non-Network Deployment environments.

Starting the application server in a non-Network Deployment environment

To start the application server, complete the following steps:

Table 40. Starting the application server.

Platform	Steps

Windows systems	Complete one of the following steps:
	• (recommended) From the Windows Start menu:
	1. From the Windows Start menu, click **(All) Programs > IBM WebSphere > *application_server_and_version*> Profiles > *profile_name* > First steps**.
	2. Click **Start the server**.
	The First steps output window displays a message that is similar to the following message:
	`Server server_name open for e-business`
	• From a command line:
	`cd AppServer_home\profiles\profile_name\bin`
	`startServer server_name`

Linux or UNIX systems	`cd AppServer_home/profiles/profile_name/bin` `./startServer server_name`

The *server_name* is the name of the configuration directory of the server that you want to start. The default is `server1`.

The *profile_name* specifies the profile name for the application servers. The default is `default`.

If WebSphere Global Security is enabled, add the following options to every command:

- The `-username` *name* or `-user` *name* option specifies the user name for authentication if security is enabled in the server.
- The `-password` *password* option specifies the password for authentication if security is enabled in the server.

Important: If you are running in a secure environment but have not provided a user ID and password, you receive an error message.

Starting the application server in a Network Deployment environment

To start the application server, complete the following steps:

1. Change to the *AppServer_home*`/bin` directory.
2. Start the deployment manager process. Run the `startManager` command.
3. Start the node. Run the `startNode` command.
4. For each application server on the node, start the application server using the procedure in "Starting the application server in a non-Network Deployment environment" on page 315.

On Linux or UNIX systems, add `./` before every command to run it.

If WebSphere Global Security is enabled, add the following options to every command:

- The `-username` *name* or `-user` *name* option specifies the user name for authentication if security is enabled in the server.
- The `-password` *password* option specifies the password for authentication if security is enabled in the server.

Important: If you are running in a secure environment but have not provided a user ID and password, you receive an error message.

Stopping the application server

There are separate procedures for stopping the application server in Network Deployment and non-Network Deployment environments.

Stopping the application server in a non-Network Deployment environment

Complete the following steps to stop the application server:

Table 41. Stopping the application server.

Platform	Steps

Windows	Complete one of the following steps:
	• (recommended) From the Windows Start menu:
	1. From the Windows Start menu, click **(All) Programs > IBM WebSphere > *application_server_and_version*> Profiles > *profile_name* > First steps**.
	2. Click **Stop the server**.
	Wait for the First steps output window to display a message that is similar to the following message:
	`Server server_name stop completed`
	• From a command line:
	`cd AppServer_home\profiles\profile_name\bin`
	`stopServer server_name [options]`

Linux or UNIX systems	`cd AppServer_home/profiles/profile_name/bin` `./stopServer server_name [options]`

The *server_name* is the name of the configuration directory of the server that you want to stop. The default is `server1`.

The *profile_name* specifies the profile name for the application servers. The default is `default`.

If WebSphere Global Security is enabled, add the following options to every command:

- The `-username` *name* or `-user` *name* option specifies the user name for authentication if security is enabled in the server.
- The `-password` *password* option specifies the password for authentication if security is enabled in the server.

Important: If you are running in a secure environment but have not provided a user ID and password, you receive an error message.

Stopping the application server in a Network Deployment environment

Complete following steps to stop the application server:

1. Change to the *AppServer_home*`/bin` directory.
2. Stop all servers that are on the node, and the node itself. Run the `stopNode -stopservers` command
3. Stop the deployment manager process. Run the `stopManager` command.

On Linux or UNIX systems, add `./` before every command to run it.

If WebSphere Global Security is enabled, add the following options to every command:

- The `-username` *name* or `-user` *name* option specifies the user name for authentication if security is enabled in the server.
- The `-password` *password* option specifies the password for authentication if security is enabled in the server.

Important: If you are running in a secure environment but have not provided a user ID and password, you receive an error message.

Appendix E. Using regular expressions

Regular expressions are sets of symbols and characters that are used to match patterns of text. You can use regular expressions to search specific IP addresses across your web environment. You can use regular expressions 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.

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. 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 URLs: `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)

Important: 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 are not to 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 are valid:

!*.24.45.46
!12.*.45.56
!12.24.*.56
!12.24.45.*
!12.24.45.56

You can replace any "octet" (there are four in an IP address: octet . octet . octet . octet) with a wildcard (*). Note that this is not the regular expression wildcard (.*) from the positive filters.

Appendix F. Manual changes to application server configuration for the data collector

You might want to configure and unconfigure data collector monitoring for an application server instance manually. Also, the data collector configuration might fail because of unexpected circumstances. You can restore the application server configuration manually if you created a backup of the configuration.

Important: You must make manual changes to the WebSphere Application Server configuration for data collectors as the WebSphere administrative user.

Restoring the application server configuration from a backup

If you configured a stand-alone application server instance for data collection either manually or with the configuration or migration utility and the application server fails to start, you must restore the application server configuration from a backup. If you did not create a backup, contact IBM Support.

In a Network Deployment environment, if you configured an application server instance for data collection manually or with the configuration or migration utility and the application server fails to start, you have the following options:

- You can restore the application server configuration from a backup configuration. If you did not create a backup, contact IBM Support.
- You can manually unconfigure the data collector. The Deployment Manager and the Node Agent on the application server must be running. For more information, see "Manually removing data collector configuration from an application server instance" on page 329.

This section applies only to the Windows, UNIX, and Linux platforms.

To apply the backup configuration using the **restoreConfig** command, complete one of the following procedures:

- In a non-Network Deployment environment:
  1. Locate your backup configuration file. The default directory is *DC_home*/data. If several backup files are present, check the modification date and time of the file. It must be the date and time of the failed configuration. If you did not complete any other data collector configurations on the same host after the failed one, use the most recent file in the directory.
  2. Stop all instances of the application server. Complete the steps in "Stopping the application server" on page 316.
  3. Run the **restoreConfig** command from the *Appserver_home*/profiles/*profile_name*/bin directory. The syntax is:

Table 42. Syntax of the restoreConfig command in a non-Network Deployment environment

Operating system	Syntax	Example
Windows	restoreConfig.bat *full_path_to_backup_file*	restoreConfig.bat "C:\Program Files\IBM\ITM\dchome\7.2.0.0.1 \data\ WebSphereConfig_2006-04-22.zip"

Table 42. Syntax of the restoreConfig command in a non-Network Deployment environment (continued)

Operating system	Syntax	Example
UNIX or **Linux**	`./restoreConfig.sh` *full_path_to_backup_file*	`./restoreConfig.sh /opt/IBM/ITM /dchome/7.2.0.0.1/data/ WebSphereConfig_2006-04-22.zip`

For more information about the arguments of the **restoreConfig** command, from the WebSphere Application Server v8.0 information center search for "restoreConfig command".

4. Start the instances of the application server. For more information, see "Starting the application server" on page 315.

- In a Network Deployment environment:
  1. Locate your backup configuration file. The default directory is *DC_home*`/data`. If several backup files are present, check the modification date and time of the file; it must be the date and time of the failed configuration. If you did not complete any other data collector configurations on the same host after the failed one, use the most recent file in the directory.
  2. Stop all instances of the application servers. Complete the steps in "Stopping the application server" on page 316.
  3. Create a temporary directory in any convenient path (*temp_directory*). On a UNIX or Linux host, create it under `/tmp`.
  4. Run the `restoreConfig` command from the *Appserver_home*`/profiles/`*profile_name*`/bin` directory. The syntax is:

Table 43. Syntax of restoreConfig command, Network Deployment environment

Operating system	Syntax	Example
Windows	`restoreConfig.bat` *full_path_to_backup_file*	`restoreConfig.bat "C:\Program Files\IBM\itcam\WebSphere \DC\config_dc\backup\ WebSphereConfig_2006-04-22.zip" -location` *temp_directory*
UNIX or **Linux**	`./restoreConfig.sh` *full_path_to_backup_file*	`./restoreConfig.sh /opt/IBM/itcam/WebSphere/DC/config_dc /backup/WebSphereConfig_2006-04-22.zip -location` *temp_directory*

Running the `restoreConfig` command restores the original application server configuration to the temporary directory.

5. Copy the `server.xml`, `variables.xml`, and `pmi-config.xml` files from the following path:

   temp_directory`/`*restored_configuration_home*`/cells/`*cell_name*`/nodes/`*node_name*`/servers/`*server_name*

   to the following path on the Deployment Manager host:

   Appserver_home`/profiles/`*profile_name*`/config/cells/`*cell_name*`/nodes/`*node_name*`/servers/`*server_name*
6. Complete a node sync from the Deployment Manager administrative console for the node.
7. In the Deployment Manager administrative console, save changes to the master configuration.
8. Start the instances of the application server. For more information about starting application server instances, see "Starting the application server" on page 315.

Manually configuring the data collector to monitor an application server instance

You can configure the data collector to monitor an application server instance without using the configuration utility. You must create two settings files, and then manually add settings in the WebSphere Administrative Console. The runtime directory is created automatically when the data collector is started for the application server instance.

Important:

- You must make manual changes to the WebSphere Application Server configuration for data collectors as the WebSphere administrative user.
- You must be an experienced WebSphere administrator to make manual changes to the WebSphere Application Server for data collection. Any error in the manual configuration change can result in the application server not starting.
- If you manually configure the data collector to monitor application server instances, you cannot use the ITCAM Data Collector for WebSphere Unconfiguration utility to unconfigure the data collector.

Step 1. Create the `dcManualInput.txt` file

The `dcManualInput.txt` file contains some of the values needed for initial configuration of the data collector.

To create the `dcManualInput.txt` file, complete the following steps:

1. On Windows systems, copy the contents of the file *DC_home*`\itcamdc\etc\was\dcInput_manual.properties` into *DC_home*`\runtime\`*profile_name*`.`*cell_name*`.`*node_name*`.`*server_name*`.DCManualInput.txt`.

   On Linux or UNIX systems, copy the contents of the file *DC_home*`/itcamdc/etc/was/dcInput_manual.properties` into *DC_home*`/runtime/`*profile_name*`.`*cell_name*`.`*node_name*`.`*server_name*`.DCManualInput.txt`.
2. Edit the contents of the file.

   You must set the parameters in section 1 of the file according to the descriptions provided in Table 44. Do not change the parameters in section 2.

Table 44. Configuration Parameters for Section 1

Parameter	Value
local.hostname	The IP address or fully qualified domain name of the local system.
was.version	A short version number. Valid values are `70`, `80`, and `85`. Use `70` for WebSphere Application Server 7.0 and all products based on it, `80` for WebSphere Application Server version 8.0 and all products based on it, and `85` for WebSphere Application Server version 8.5 and all products based on it.
itcam.home	ITCAM home directory.
was.nodename	Node name.
was.servername	Server name.
was.profilename	WebSphere profile name.

Table 44. Configuration Parameters for Section 1 (continued)

Parameter	Value
am.camtoolkit.gpe.dc.operation.mode	Operation mode of the data collector. Valid values are any combination of `WR`, `MS`, `TT`, `SOA`, `ECAM`, and `DE`, where: **WR** Integrates the data collector with the ITCAM Agent for WebSphere Applications monitoring agent. **MS** Integrates the data collector with the ITCAM for Application Diagnostics Managing Server. **TT** Integrates the data collector with ITCAM for Transactions. **SOA** Integrates the data collector with ITCAM for SOA monitoring agent. **ECAM** Integrates ITCAM for WebSphere Application Server data collector with Tivoli Performance Viewer (TPV). **DE** Integrates the data collector with the ITCAM Diagnostics Tool. The tool is previewed in the ITCAM for Application Diagnostics beta. You must specify only the operation modes required. For example, if you are connecting the data collector to the ITCAM Agent for WebSphere Applications monitoring agent only, specify `WR`. Separate multiple operation modes with a comma.
interp	Platform code. For a complete list of platform codes, see Appendix D of the *IBM Tivoli Monitoring: Installation and Setup Guide*.
kwj.serveralias	(Optional) WebSphere Application Server alias name.
temagclog.path	(Optional) Garbage Collection log file path name. Enter a unique file name with full path. The path name must not include spaces.
tema.host	Host name or IP address of the ITCAM Agent for WebSphere Applications monitoring agent. Mandatory if the operation mode includes ITCAM Agent for WebSphere Applications (WR).
tema.port	Port to use for communicating with the ITCAM Agent for WebSphere Applications monitoring agent. Mandatory if the operation mode includes ITCAM Agent for WebSphere Applications (WR).
ms.hostname	Host name or IP address of the ITCAM for Application Diagnostics Managing Server. Mandatory if the operation mode includes ITCAM for Application Diagnostics Managing Server (MS).
kernel.codebase.port	Codebase port number of the Managing Server. The default is 9122. Mandatory if the operation mode includes ITCAM for Application Diagnostics Managing Server (MS).

Table 44. Configuration Parameters for Section 1 (continued)

Parameter	Value
kernel.rfs.port	Managing Server kernel port number. The default is 9120. Mandatory if the operation mode includes ITCAM for Application Diagnostics Managing Server (MS).
probe.controller.rmi.port	Range of Controller RMI port numbers. The default is 8300 - 8399. Mandatory if the operation mode includes ITCAM for Application Diagnostics Managing Server (MS).
probe.rmi.port	Range of RMI port numbers. The default is 8200 is 8299. Mandatory if the operation mode includes ITCAM for Application Diagnostics Managing Server (MS).
ms.home	Managing Server home directory. Mandatory if the operation mode includes ITCAM for Application Diagnostics Managing Server (MS).
tt.connection.string	Host name or IP address and the port number of the Transaction Collector component of ITCAM for Transactions in the format of `tcp:`*`host_name`*`(IP):`*`port`*. Mandatory if the operation mode includes ITCAM for Transactions (TT).

Step 2. Create the `itcam_wsBundleMetaData.xml` file

The file `itcam_wsBundleMetaData.xml` contains some of the values needed for initial configuration of the data collector.

To create this file, complete the following steps:

1. Create a directory `wsBundleMetaData` under the *`DC_home`*`\runtime` directory on Windows system or under the *`DC_home`*`/runtime` directory on Linux or UNIX systems.
2. On Windows systems, copy the contents of the file *`DC_home`*`\itcamdc\etc\was\itcam_wsBundleMetaData_template.xml` into `itcam_wsBundleMetaData.xml`.

   On Linux and UNIX systems, copy the contents of the file *`DC_home`*`/itcamdc/etc/was/itcam_wsBundleMetaData_template.xml` into `itcam_wsBundleMetaData.xml`.
3. In the `itcam_wsBundleMetaData.xml` file, replace the variable `@{CONFIGHOME}` with the full path to your data collector home directory.
4. On Windows systems, place the file `itcam_wsBundleMetaData.xml` in the directory *`DC_home`*`\runtime\wsBundleMetaData`.

   On Linux and UNIX systems, place the file `itcam_wsBundleMetaData.xml` in the directory *`DC_home`*`/runtime/wsBundleMetaData`.

Step 3. Add settings with the WebSphere Administrative Console

Tip: The application server instance you are configuring for data collection must be running.

Complete the following steps:

1. Log in to the WebSphere administrative console.

2. Click **Servers**.
3. Expand **Server Type** and select **WebSphere application servers**.
4. Click the name of the server.
5. Expand **Java and Process Management** and select **Process Definition**.
6. Under the **Additional Properties** section, click **Java Virtual Machine**.
7. In the **Generic JVM arguments** field, add the following entries.

```
-agentlib:am_ibm_16=${WAS_SERVER_NAME} -Xbootclasspath/p:$
{ITCAMDCHOME}/toolkit/
lib/bcm-bootstrap.jar -Djava.security.policy=
${ITCAMDCHOME}/itcamdc/etc/datacollector.policy -verbosegc -
Dcom.ibm.tivoli.itcam.ai.runtimebuilder.
inputs=${ITCAMDCHOME}/runtime/$name_of_the_file_created_DCManualInput.txt
-Dsun.rmi.dgc.client.gcInterval=3600000
-Dsun.rmi.dgc.server.gcInterval=3600000 -
Dsun.rmi.transport.connectionTimeout=300000
-Dws.bundle.metadata=${ITCAMDCHOME}/runtime/wsBundleMetaData -
Dam.wascell=$replace_with_was_cell_name
-Dam.wasprofile=$replace_with_was_profile_name -
Dam.wasnode=$replace_with_was_node_name
-Dam.wasserver=$replace_with_was_server_name
```

   When adding the entries, take note of the following:
   - All entries must be on a single line.
   - Separate different arguments by spaces before the - sign, do not use spaces anywhere else.
   - Replace the following variables with the actual names:
     - *$name_of_the_file_created_DCManualInput.txt*
     - *$replace_with_was_cell_name*
     - *$replace_with_was_profile_name*
     - *$replace_with_was_node_name*
     - *$replace_with_was_server_name*
8. Click **Apply**.
9. In the Messages dialog box, click **Save**.
10. In the Save to Master Configuration dialog box, complete the following steps:
    - If you are under a Network Deployment environment, ensure that **Synchronize changes with Nodes** is selected and then click **Save**.
    - If you are not under a Network Deployment environment, click **Save**.
11. Click **Server** > **Application Servers** and select the *server_name*.
12. In the **Configuration** tab, go to **Server Infrastructure** > **Java and Process Management** > **Process Definition** > **Environment Entries**.
13. Depending on the operating system, the hardware platform, and the application server JVM, set the following environment entry:

Table 45. Environment Entry

Platform	Environment Entry name	Environment Entry value
AIX R6.1 (32 bit JVM)	LIBPATH	/lib:${*ITCAMDCHOME*}/toolkit/lib/aix533:${*ITCAMDCHOME*}/toolkit/lib/aix533/ttapi
AIX R6.1 (64 bit JVM)	LIBPATH	/lib:${*ITCAMDCHOME*}/toolkit/lib/aix536:${*ITCAMDCHOME*}/toolkit/lib/aix536/ttapi

Table 45. Environment Entry (continued)

Platform	Environment Entry name	Environment Entry value
AIX R7.1 (32 bit JVM)	LIBPATH	/lib:${*ITCAMDCHOME*}/toolkit/lib/aix533:${*ITCAMDCHOME*}/toolkit/lib/aix533/ttapi
AIX R7.1 (64 bit JVM)	LIBPATH	/lib:${*ITCAMDCHOME*}/toolkit/lib/aix536:${*ITCAMDCHOME*}/toolkit/lib/aix536/ttapi
HP-UX R11 (32 bit JVM)	SHLIB_PATH	/lib:${*ITCAMDCHOME*}/toolkit/lib/hp11:${*ITCAMDCHOME*}/toolkit/lib/hp11/ttapi
HP-UX R11 (64 bit JVM)	SHLIB_PATH	/lib:${*ITCAMDCHOME*}/toolkit/lib/hp116:${*ITCAMDCHOME*}/toolkit/lib/hp116/ttapi
HP-UX R11 Integrity (64 bit JVM)	SHLIB_PATH	/lib:${*ITCAMDCHOME*}/toolkit/lib/hpi116:${*ITCAMDCHOME*}/toolkit/lib/hpi116/ttapi
Linux x86_64 R2.6 (64 bit JVM)	LD_LIBRARY_PATH	/lib:${*ITCAMDCHOME*}/toolkit/lib/lx8266:${*ITCAMDCHOME*}/toolkit/lib/lx8266/ttapi
Linux Intel R2.6 (32 bit JVM)	LD_LIBRARY_PATH	/lib:${*ITCAMDCHOME*}/toolkit/lib/lx6263:${*ITCAMDCHOME*}/toolkit/lib/lx6263/ttapi
Linux ppc R2.6 (32 bit JVM)	LD_LIBRARY_PATH	/lib:${*ITCAMDCHOME*}/toolkit/lib/lpp263:${*ITCAMDCHOME*}/toolkit/lib/lpp263/ttapi
Linux ppc R2.6 (64 bit JVM)	LD_LIBRARY_PATH	/lib:${*ITCAMDCHOME*}/toolkit/lib/lpp266:${*ITCAMDCHOME*}/toolkit/lib/lpp266/ttapi
Linux S390 R2.6 (32 bit JVM)	LD_LIBRARY_PATH	/lib:${*ITCAMDCHOME*}/toolkit/lib/ls3263:${*ITCAMDCHOME*}/toolkit/lib/ls3263/ttapi
Linux S390 R2.6 (64 bit JVM)	LD_LIBRARY_PATH	/lib:${*ITCAMDCHOME*}/toolkit/lib/ls3266:${*ITCAMDCHOME*}/toolkit/lib/ls3266/ttapi
Solaris R10 (32 bit JVM)	LD_LIBRARY_PATH	/lib:${*ITCAMDCHOME*}/toolkit/lib/sol293:${*ITCAMDCHOME*}/toolkit/lib/sol293/ttapi
Solaris R10 (64 bit JVM)	LD_LIBRARY_PATH	/lib:${*ITCAMDCHOME*}/toolkit/lib/sol296:${*ITCAMDCHOME*}/toolkit/lib/sol296/ttapi

Table 45. Environment Entry (continued)

Platform	Environment Entry name	Environment Entry value
Solaris R10 Opteron (64 bit JVM)	LD_LIBRARY_PATH	/lib:${*ITCAMDCHOME*}/toolkit/lib/sol606:${*ITCAMDCHOME*}/toolkit/lib/sol606/ttapi
Windows (32 bit JVM)	PATH	/lib;${*ITCAMDCHOME*}/toolkit/lib/win32;${*ITCAMDCHOME*}/toolkit/lib/win32/ttapi
Windows (64 bit JVM)	PATH	/lib;${*ITCAMDCHOME*}/toolkit/lib/win64;${*ITCAMDCHOME*}/toolkit/lib/win64/ttapi

14. Set the environment entry name NLSPATH to the following value:
    ${ITCAMDCHOME}/toolkit/msg/%L/%N.cat
15. Click **Apply** and click **Save**.
16. In the Save to Master Configuration dialog box, complete the following steps:
    - If you are under a Network Deployment environment, ensure that **Synchronize changes with Nodes** is selected and then click **Save**.
    - If you are not under a Network Deployment environment, click **Save**.
17. Click **Server > Application Servers** and select the *server_name*.
18. In the **Configuration** tab, go to **Server Infrastructure** > **Java and Process Management** > **Process Definition** > **Java Virtual Machine** > **Additional Properties: Custom Properties**.
19. For the following name and value pairs, click **New**, enter the name and value, and click **Apply**:
    - Create an am.home property and set its value to the *dchome*/itcamdc directory path. For example:am.home=/opt/IBM/ITM/dchome/7.2.0.0.1/itcamdc
    - Create a com.ibm.tivoli.itcam.toolkit.ai.runtimebuilder.enable.rebuild property and set its value to true. For example: com.ibm.tivoli.itcam.toolkit.ai.runtimebuilder.enable.rebuild=true
    - Create a ITCAM_DC_ENABLED property and set its value to true, if the operation mode parameter in the dcManualInput.txt file includes ECAM.
    - Create a TEMAGCCollector.gclog.path property. If the generic Java Virtual Machine verlogsegclog argument is set, set the value of the TEMAGCCollector.gclog.path property to the same value. Otherwise, set the TEMAGCCollector.gclog.path property to None.

      To identify the value of the verlogsegclog property, complete the steps:
      a. In the **Configuration** tab, go to **Server Infrastructure** > **Java and Process Management** > **Process Definition** > **Java Virtual Machine**.
      b. Locate the verlogsegclog property in the **Generic JVM arguments** field and note its value.
20. In the Messages dialog box, click **Save**.
21. In the Save to Master Configuration dialog box, complete the following steps:
    - If you are under a Network Deployment environment, ensure that **Synchronize changes with Nodes** is selected. Click **Save**.
    - If you are not under a Network Deployment environment, click **Save**.

22. In the Navigation Pane, click **Environment** > **WebSphere Variables**.
23. Set the following variables. For each variable, choose the server name as the scope.
    - Set `ITCAMDCHOME` to `DC_home`.
    - Set `ITCAMDCVERSION` to the *version.release.maintenance_level* of the data collector. For example, `7.2.0.0.1`
24. Click **Apply** and click **Save**.
25. In the Save to Master Configuration dialog box, complete the following steps:
    - If you are under a Network Deployment environment, ensure that **Synchronize changes with Nodes** is selected and then click **Save**.
    - If you are not under a Network Deployment environment, click **Save**.
26. Restart the application server instance. The data collector reads the settings files and creates the runtime directory.

Manually removing data collector configuration from an application server instance

You can manually remove the data collector configuration from an application server instance, if any of the following conditions apply:

- In a non-Network Deployment environment, you manually added the data collector configuration to the application server instance and you want to unconfigure data collection. The application server instance must be running.
- In a Network Deployment environment, you manually added the data collector configuration to the application server instance and you want to unconfigure data collection. The Node Agent and Deployment Manager on the application server must be running.
- In a Network Deployment environment, you configured the application server instance for data collection manually and the application server fails to start. The Node Agent and Deployment Manager on the application server must be running.

If you configured a stand-alone application server instance for data collection either manually or with the configuration or migration utility and the application server fails to start, you must restore your WebSphere Application Server configuration with your backup configuration. For more information, see "Restoring the application server configuration from a backup" on page 321. If you did not create a backup, contact IBM Support.

Remember:

- You must make manual changes to the WebSphere Application Server configuration for data collectors as the WebSphere administrative user.
- Making manual changes to the WebSphere Application Server for data collection must be performed by an experienced WebSphere administrator only. Any error in the manual configuration change can result in the application server not starting.
- If you manually configure the data collector to monitor application server instances, you cannot use the ITCAM Data Collector for WebSphere Unconfiguration utility to unconfigure the data collector.

To manually remove the data collector configuration, complete the following procedure:

1. Log in to the WebSphere Administration Server Console.

2. Click **Servers**.
3. Expand **Server Type** and select **WebSphere application servers**.
4. Click the name of the server.
5. On the Configuration tab, under Server Infrastructure, expand **Java and Process Management** and select **Process Definition**.
6. Under the **Additional Properties** section, click **Java Virtual Machine**.
7. Under the **Additional Properties** section, click **Custom Properties**.
8. Remove any of the following JVM Custom Properties, if they are present:
   - `am.home`
   - `ITCAM.DC.ENABLED`
   - `TEMAGCCollector.gclog.path`
   - `com.ibm.tivoli.itcam.toolkit.ai.runtimebuilder.enable.rebuild`
   - `com.ibm.tivoli.jiti.injector.ProbeInjectorManagerChain.primaryInjectorFile` (if it is present)
9. Identify the JVM arguments added for ITCAM Data Collector for WebSphere:
   a. In the Navigation Pane, click **Environment** > **WebSphere Variables**.
   b. If you configured the application server for data collection manually, locate the JVM arguments you added manually.

      If you configured the application server for data collection with the configuration utilities, compare the value of the arguments `AM_OLD_ARGS` and `AM_CONFGI_JVM_ARGS` to determine which arguments were added by the configuration utility.
10. Click **Server** > **Application Server** and select the *server_name*.
11. On the Configuration tab, navigate to **Server Infrastructure** > **Java and Process Management** > **Process Definition** > **Java Virtual Machine**.
12. In **Generic JVM Arguments**, remove the JVM arguments you identified in step 9 for ITCAM Data Collector for WebSphere.
13. Click **Apply** or **OK**.
14. In the **Messages** dialog box, click **Save**.
15. In the **Save to Master Configuration** dialog box, complete one of the following steps:
    - If you are under a Network Deployment environment, make sure the check box **Synchronize changes with Nodes** is selected, then click **Save**.
    - If you are not under a Network Deployment environment, click **Save**.
16. Remove environment entries added for ITCAM Data Collector for WebSphere.
    a. In the Configuration tab, go to **Server Infrastructure** > **Java and Process Management** > **Process Definition** > **Environment Entries**.
    b. Depending on the hardware platform, delete the `LIBPATH` (on AIX systems), `SHLIB_PATH` (on HP-UX systems), `LD_LIBRARY_PATH` (on Linux systems), or `PATH` (on Windows systems) environment entry.
    c. Remove the `NLSPATH` environment entry.
17. Click **Apply** or **OK**.
18. In the **Messages** dialog box, click **Save**.
19. In the **Save to Master Configuration** dialog box, complete one of the following steps:
    - If you are under a Network Deployment environment, make sure the check box **Synchronize changes with Nodes** is selected, then click **Save**.
    - If you are not under a Network Deployment environment, click **Save**.

20. In the Navigation Pane, click **Environment** > **WebSphere Variables**.
21. Delete the following variables:
    - AM_CONFIG_JVM_ARGS
    - AM_OLD_JVM_ARGS
    - ITCAMDCHOME
    - ITCAMDCVERSION
22. In the **Messages** dialog box, click **Save**.
23. In the **Save to Master Configuration** dialog box, complete one of the following steps:
    - If you are under a Network Deployment environment, make sure the check box **Synchronize changes with Nodes** is selected, then click **Save**.
    - If you are not under a Network Deployment environment, click **Save**.
24. If you configured the server instance for data collection with the data collector configuration tool, rather than manually, complete the following steps:
    a. Navigate to the *DC_home*/runtime directory.
    b. Rename the file $profile.$cell.$node.$server.input.properties to $profile.$cell.$node.$server.input.properties.bak
25. If you are manually removing the data collector configuration from all application server instances in a profile, perform the following steps:
    a. Navigate to the $appserverhome/bin directory.
    b. Run the command osgiCfgInit.sh/bat -all on Windows systems or osgiCfgInit.sh -all on UNIX and Linux systems.
26. Restart the application server instance that was monitored by the data collector.

Appendix G. Attribute groups and sizing information for historical warehousing

You can find the record size and recording frequency information for ITCAM Agent for WebSphere Applications in Table 46. This information helps you size the amount of disk space needed for any historical logging.

Table 46. Information for historical warehousing

Table Name	Object Name	Record size	Recording Frequency
KYNPREV	WebSphere Agent Events	616	1 record for each product event. These records are written when problems occur. It is impossible to say how often this might occur.
KYNAPSST	Application Server Status	1680	1 record per interval per server instance.
KYNLOGANAL	Log Analysis	1072	1 record per interval for each entry written into the application server log stream or file.
KYNAPSRV	Application Server	1616	1 record per interval per application server.
KYNCONTNR	EJB Containers	892	1 record per interval per application server, plus 1 record per interval per EJB container.
KYNEJB	Enterprise Java Beans	1056	1 record per interval for each EJB method.
KYNCNTROP	Container Object Pools	816	1 record per interval per application server, plus 1 record per interval per EJB container.
KYNAPP	Web Applications	1064	1 record per interval per web application.
KYNSERVLT	Servlets JSPs	1352	1 record per interval per servlet.
KYNTRANS	Container Transactions	840	1 record per interval per application server plus 1 record per interval per EJB container.
KYNCACHE	Dynamic Cache	852	1 record per cache per cycle.
KYNCACHT	Dynamic Cache Templates	1212	1 record per cache template per cycle.
KYNJ2C	J2C Connection Pools	1012	1 record per JEE connection pool per cycle.
KYNSERVS	Servlet Sessions	1072	1 record per servlet session per interval.
KYNTHRDP	Thread Pools	880	1 record per thread pool per interval.
KYNWLMCL	Workload Management Client	596	1 record per WLM client per interval.
KYNWLMSR	Workload Management Server	636	1 record per WLM server per interval.

Table 46. Information for historical warehousing (continued)

Table Name	Object Name	Record size	Recording Frequency
KYNGCACT	Garbage Collection Analysis	748	1 record per interval per application server.
KYNGCAF	Allocation Failure	620	1 record per interval for each allocation failure block.
KYNGCCYC	Garbage Collection Cycle	688	1 record per garbage-collection cycle per interval.
KYNREQUEST	Request Analysis	1516	1 record per interval for each workload in each application server.
KYNREQSEL	Selected Request	1252	1 record per interval for each workload degradation in each application server.
KYNDATAS	Datasources	1168	1 record per interval per data source in each application server.
KYNJMSSUM	JMS Summary	864	1 record per interval per WebSphere MQ queue in each application server.
KYNREQHIS	Request Times and Rates	992	1 record per interval per WebSphere Application Server.
KYNDBCONP	DB Connection Pools	1124	1 record per data source per interval plus 1 record per application server per interval.
KYNDCMSG	DC Messages – WebSphere	1412	1 record per each entry written into DC log message file.
KYNDCSSTK	DCS Stack	1056	1 record per DCS stack per interval plus 1 record per application server per interval.
KYNHAMGMT	High Availability Manager	736	1 record per application server per interval.
KYNWEBSGW	Web Services Gate Way	968	1 record per Web Services Gateway per interval plus 1 record per application server per interval.
KYNWEBSVC	Web Services	1032	1 record per Web Service per interval plus 1 record per application server per interval.
KYNALARMM	Alarm Manager	980	1 record per WorkManager per interval plus 1 record per application server per interval.
KYNSCHED	Scheduler	1000	1 record per Scheduler per interval plus 1 record per application server per interval.
KYNCLICOM	Client Communications	1220	1 record per application server per interval.
KYNDURSUB	Durable Subscriptions	1516	1 record per Durable Subscription per interval.
KYNMECOM	Messaging Engine Communications	1004	1 record per application server per interval.
KYNMSGENG	Messaging Engines	976	1 record per Message Engine per interval plus 1 record per application server per interval.
KYNMSGQUE	Queue	1304	1 record per Queue per interval.

Table 46. Information for historical warehousing (continued)

Table Name	Object Name	Record size	Recording Frequency
KYNSVCOMEL	Service Component Elements	1752	1 record per Service Component Element per interval plus 1 record per application server per interval.
KYNSVCCOMP	Service Components	704	1 record per Service Component plus 1 record per application server.
KYNTOPICSP	Topic Spaces	1288	1 record per Topic Space per interval.
KYNWMQCL	WMQ Client Link Communications	988	1 record per application server per interval.
KYNWMQLINK	WMQ Link Communications	1004	1 record per application server per interval.
KYNWPMSV	Workplace Mail Service	648	1 record per application server per interval.
KYNWPMQM	Workplace Mail Queues	584	1 record per Mail Queue per interval.
KYNWPMIP	Workplace Mail IMAP/POP	600	1 record per protocol (IMAP/POP) per interval.
KYNWPTALS	Portal Summary	772	1 record per application server per interval.
KYNWPPAGE	Portal Page Summary	844	1 record per Portal Page per interval plus 1 record per application server.
KYNWPLETS	Portlet Summary	848	1 record per Portlet per interval plus 1 record per application server.
KYNAPHLTH	Application Health Status	1152	1 record per interval per application for each application server.
KYNAPMONCF	Application Monitoring Configuration	n/a	Not a historical table.
KYNRQMONCF	Requests Monitoring Configuration	n/a	Not a historical table.
KYNBASELN	Baseline	n/a	Not a historical table.
KYNLPORT	Listener Port	1472	1 record per interval per JMS listener port.
KYNGZCAT	WebSphere XS Catalog	388	1 record per interval per catalog server.
KYNGZRID	WebSphere XS Grid	364	1 record per interval per grid's partition plus summarization records for mapset, grid, domain, mapset server, grid server, and domain server.
KYNGZMAP	WebSphere XS Map	344	1 record per interval per map's partition plus summarization records for map, grid, domain, map server, grid server, and domain server.
KYNGZSERV	WebSphere XS Server	820	1 record per container plus summarization records for zone and core group.
KYNGZCONT	WebSphere XS Container	304	1 record per container server plus summarization records for every server, core group, and zone.

Table 46. Information for historical warehousing (continued)

Table Name	Object Name	Record size	Recording Frequency
KYNGZGRPLC	WebSphere XS Grid Placement	172	1 record per placement status of map in grid.
KYNXDCG	WebSphere XD Compute Grid	888	1 record per cell and job scheduler server.
KYNXDCLL	WebSphere XD Cell	664	1 record per XD cell.
KYNXDDCL	WebSphere XD Dynamic Clusters	456	1 record per dynamic cluster.
KYNXDGE	WebSphere XD Grid Endpoints	1368	1 record per cell, every grid endpoint, application, service policy, and any combinations of the aforementioned.
KYNXDJBN	WebSphere XD Job Notifications	612	1 record per job notification.
KYNXDJOB	WebSphere XD Jobs	1372	1 record per job.
KYNXDODR	WebSphere XD ODR	1860	1 record per every ODR and statistics (deployment targets, server, application, service policy, cell, and combinations of the aforementioned.)
KYNXDSPV	WebSphere XD Policy Violations	624	1 record per every service policy violation.
KYNXDSRV	WebSphere XD Servers	584	1 record per every server or ODR.
KYNXDSTP	WebSphere XD Steps	660	1 record per every step in job.

Appendix H. 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 an ITCAM for Application Diagnostics Managing Server.

Important: The ITCAM for Application Diagnostics Managing Server is not a component of ITCAM for Applications 7.2. Unless you have ITCAM for Application Diagnostics version 7.1 installed in your environment, ignore this appendix.

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 is routed through the Port Consolidator. However, the traffic from the data collector to the Managing Server is direct.

Important: Typically, all data collectors and Port Consolidators are installed on the same physical computer. However, it is possible to run the Port Consolidator on a different computer. Contact IBM Software Support for setup assistance in this case.

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.

To configure a data collector to use the Port Consolidator, complete the following procedure:

1. Edit the *DC_home*/runtime/*app_server_version*.*node_name*.*server_name*/custom/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 computer, but it can 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_*.

   Important:

   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 338.

2. Restart the instance of the application server that is being monitored by the data collector. For more information, see "Restarting the application server" on page 313.
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 47. Command for starting the Port Consolidator

Platform	Command
Windows	`proxyserverctrl_ws.bat start`
UNIX and **Linux**	`./proxyserverctrl_ws.sh start`

Do not close the command prompt window.

Important: 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 337.

5. Open the Self-Diagnosis page of the Visualization Engine (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 48. Location of the CYND4051I message

Platform	Command
Windows systems	*DC_home*`\logs\CYN\logs\`*node_name.server_name*`\`*java_msg_log_file*. For example: `C:\IBM\ITM\dchome\7.2.0.0.1\logs\CYN\logs\IBMNode01.server1\msg-dc-Ext.log`
UNIX and Linux systems	*DC_home*`/logs/CYN/logs/`*node_name.server_name*`/`*java_msg_log_file*. For example: `opt/IBM/ITM/dchome/7.2.0.0.1/logs/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 49. Entering the proxyserverctrl_ws command

Platform	Command
Windows	`proxyserverctrl_ws.bat list`
UNIX and **Linux**	`./proxyserverctrl_ws.sh list`

You see that the data collector is listed as one Service type, `PPECONTROLLER`. Keep this command prompt window open for future use.

7. Verify the data collector connection to the Port Consolidator (again) by entering one of the following commands:

Table 50. Entering the proxyserverctrl_ws command

Platform	Command
Windows	`proxyserverctrl_ws.bat list`

Table 50. Entering the proxyserverctrl_ws command (continued)

Platform	Command
UNIX and **Linux**	`./proxyserverctrl_ws.sh list`

You see that the data collector is 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, complete the following procedure:

1. Unconfigure the data collector in the Visualization Engine (Application Monitor) user interface:
   a. Start the Managing Server.
   b. Click **Administration > Server Management > data collector Configuration**.

      The data collector Management page opens.
   c. Select the data collector you want to unconfigure, and click **Apply**.

   The unconfigured data collector is added to the Unconfigured data collectors page.

   Important:
   - If the data collection has reports associated with it, you are prompted to delete those reports before unconfiguring the data collector.
   - For further information about unconfiguring a data collector in the IBM WebSphere Application Server administrative console, see the section on unconfiguring a data collector in the *IBM Tivoli Composite Application Manager for Application Diagnostics: User's Guide*.
2. Stop the Port Consolidator. From a command prompt, enter one of the following values:

Table 51. Entering the proxyserverctrl_ws command

Platform	Command
Windows	`proxyserverctrl_ws.bat stop`
UNIX and **Linux**	`./proxyserverctrl_ws.sh stop`

3. Verify that the Port Consolidator is stopped by entering one of the following commands:

Table 52. Entering the proxyserverctrl_ws command

Platform	Command
Windows	`proxyserverctrl_ws.bat list`
UNIX and **Linux**	`./proxyserverctrl_ws.sh list`

   You see the message `KERNELPROXY is down`.
4. Reconfigure the data collector to bypass the Port Consolidator:
   a. Stop the application server. For more information, see "Stopping the application server" on page 316.

b. Edit the *DC_home*/runtime/*app_server_version.node_name.server_name*/custom/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 *DC_home*/runtime/*appserver_version.node_name.server_name*/*appserver_version.node_name.server_name*.datacollector.properties file; if they are present, remove them.

d. Restart the instance of the application server that is being monitored by the data collector. For more information, see "Restarting the application server" on page 313.

5. In the Self-Diagnosis page of the Visualization Engine (Application Monitor) user interface, check to see that the data collector is listed. The data collector shows up as unconfigured.
6. Check the configuration of your data collector. In the Visualization Engine (Application Monitor) user interface, click **Administration > Server Management > data collector Configuration**.

   The data collector is listed. However, it shows as unavailable.
7. View **Unconfigured data collectors**.

   Your data collector is listed.

Appendix I. Support information

You can obtain support for IBM products in a number of ways.

Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

You can find useful information by searching the information center for ITCAM for Applications. However, sometimes you need to look beyond the information center to answer your questions or resolve problems.

To search knowledge bases for information that you need, use one or more of the following approaches:

- Find the content that you need by using the IBM Support Portal.

  The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. The IBM Support Portal lets you access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the demo videos (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos) about this tool. These videos introduce you to the IBM Support Portal, explore troubleshooting and other resources, and demonstrate how you can tailor the page by moving, adding, and deleting portlets.
- Search for content by using the IBM masthead search.

  You can use the IBM masthead search by typing your search string into the Search field at the top of any ibm.com® page.
- Search for content by using any external search engine, such as Google, Yahoo, or Bing.

  If you use an external search engine, your results are more likely to include information that is outside the ibm.com domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

  Tip: Include "IBM" and the name of the product in your search if you are looking for information about an IBM product.

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, and known limitations and workarounds. Technotes are continuously updated to provide current product information.

The following two procedures describe how to view Technotes and how to subscribe to support updates. Alternatively, you can watch demos of these procedures at the following website:

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

Viewing Technotes

Complete the following actions to access Technotes for this product:

1. Launch the IBM Software Support website: http://www.ibm.com/software/support.
2. Click the **Troubleshoot** tab.
3. Specify the product name in the **Quick find** field and press Enter.
4. Select the product name from the list and add the product to **My products list**.
5. Click **Finish** to confirm your selection.
6. Click **View all troubleshooting links**.
7. In the **Filter by document type** list, select Technotes (FAQs) and Technotes (troubleshoohting) to filter your view to display all of the Technotes for the product.

Subscribing to new support updates

To stay informed of important information about the IBM products that you use, you can subscribe to updates.

By subscribing to receive updates about ITCAM Agent for WebSphere Applications, you can receive important technical information and updates for specific IBM Support tools and resources.

With My Notifications, you can subscribe to Support updates for any IBM product. (My Notifications replaces My Support, which is a similar tool that you might have used in the past.) With My Notifications, you can specify that you want to receive daily or weekly e-mail announcements. You can specify what type of information you want to receive (such as publications, hints and tips, product flashes (also known as alerts), downloads, and drivers). My Notifications enables you to customize and categorize the products about which you want to be informed and the delivery methods that best suit your needs.

To subscribe to my Notifications, complete these steps:

1. Go to the IBM Support Portal and click **My Notifications** in the **Notifications** portlet.
2. Sign in using your IBM ID and password, and click **Submit**.
3. Identify what and how you want to receive updates.
   a. Click the **Subscribe** tab.
   b. Select **Tivoli**.
   c. Select one or more products by name and click **Continue**.
   d. Select your preferences for how to receive updates, whether by e-mail, online in a designated folder, or as an RSS or Atom feed.
   e. Select the types of documentation updates that you want to receive, for example, Technotes, new information about product downloads, and discussion group comments.
   f. Click **Submit**.

Until you modify your My Notifications preferences, you receive notifications of updates that you have requested. You can modify your preferences when needed (for example, if you stop using one product and begin using another product).

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. Launch the IBM Software Support website: http://www.ibm.com/software/support.
2. Click the **Downloads** tab.
3. Specify the product name in the **Quick find** field and press Enter.
4. Select the product name from the list and add the product to **My products list**.
5. Click **Finish** to confirm your selection.
6. Click **View all download links**.
7. In the **Filter by version** list, select the version of the product for which you want to display fixes.

Contacting IBM Software Support

IBM Support provides assistance with product defects, answers FAQs, and helps users resolve problems with the product.

After trying to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before contacting IBM Support, your company or organization must have an active IBM software maintenance contract, and you must be authorized to submit problems to IBM. For information about the types of available support, see the Support portfolio topic in the "*Software Support Handbook*".

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem.

   For more information, see the Getting IBM support topic in the *Software Support Handbook*.
2. Gather diagnostic information. See the Troubleshooting guide for more information.
3. Submit the problem to IBM Support in one of the following ways:
   - Online through the IBM Support Portal: You can open, update, and view all of your service requests from the Service Request portlet on the Service Request page.
   - By phone: For the phone number to call in your region, see the Directory of worldwide contacts web page.

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

For more information about exchanging information with IBM Support, see http://www.ibm.com/software/support/probsub.html

Exchanging information with IBM

To diagnose or identify a problem, you might need to provide IBM Support with data and information from your system. In other cases, IBM Support might provide you with tools or utilities to use for problem determination.

Sending information to IBM Support

To reduce the time that is required to resolve your problem, you can send trace and diagnostic information to IBM Support.

Procedure

To submit diagnostic information to IBM Support:

1. Open a problem management record (PMR).
2. Collect the diagnostic data that you need. Diagnostic data helps reduce the time that it takes to resolve your PMR. You can collect the diagnostic data manually or automatically:
3. Compress the files by using the `.zip` or `.tar` file format.
4. Transfer the files to IBM. You can use one of the following methods to transfer the files to IBM:
   - The Service Request tool
   - Standard data upload methods: FTP, HTTP
   - Secure data upload methods: FTPS, SFTP, HTTPS
   - Email

   All of these data exchange methods are explained on the IBM Support website.

Receiving information from IBM Support

Occasionally an IBM technical-support representative might ask you to download diagnostic tools or other files. You can use FTP to download these files.

Before you begin

Ensure that your IBM technical-support representative provided you with the preferred server to use for downloading the files and the exact directory and file names to access.

Procedure

To download files from IBM Support:

1. Use FTP to connect to the site that your IBM technical-support representative provided and log in as `anonymous`. Use your email address as the password.
2. Change to the appropriate directory:
   a. Change to the `/fromibm` directory.
      ```
      cd fromibm
      ```
   b. Change to the directory that your IBM technical-support representative provided.
      ```
      cd nameofdirectory
      ```
3. Enable binary mode for your session.
   ```
   binary
   ```
4. Use the **get** command to download the file that your IBM technical-support representative specified.
   ```
   get filename.extension
   ```

5. End your FTP session.

```
quit
```

Tivoli Support Technical Exchange

You can become a participant in the new Tivoli Support Technical Exchange, where 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 will be invited to attend a 1-hour to 2-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 website: http://www.ibm.com/software/sysmgmt/products/support/supp_tech_exch.html

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

W

Trademarks

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

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

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

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

ITIL is a registered trademark, and a registered community trademark of The Minister for the Cabinet Office, and is registered in the U.S. Patent and Trademark Office.

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

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

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

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, or service names may be trademarks or service marks of others.

Notices

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

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

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

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

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements or changes in the product(s) or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM 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 want to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information might be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments might vary significantly. Some measurements might have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement might have been estimated through extrapolation. Actual results might vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

COPYRIGHT LICENSE:

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

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

SC27-2818-02