

IBM Tivoli Composite Application Manager
Version 7.1.0.2

*Agent for WebSphere Applications
Installation and Configuration Guide for
z/OS*



IBM Tivoli Composite Application Manager
Version 7.1.0.2

*Agent for WebSphere Applications
Installation and Configuration Guide for
z/OS*



Note

Before using this information and the product it supports, read the information in “Notices” on page 199.

2010

This 2010 edition applies to ITCAM for Application Diagnostics 7.1.0.2 and all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2006, 2010.**

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

Contents

Figures	vii
--------------------------	------------

Tables	ix
-------------------------	-----------

About this publication xi

Intended audience	xi
Publications	xi
ITCAM for Application Diagnostics library	xi
Related publications	xii
Accessing terminology online	xiii
Accessing publications online	xiii
Ordering publications.	xiii
Accessibility	xiv
Tivoli technical training	xiv
Support information	xiv
Conventions used in this publication	xv
Typeface conventions	xv
Variables for directories	xv

Part 1. Introduction to ITCAM Agent for WebSphere Applications on z/OS. 1

Chapter 1. IBM Tivoli Composite Application Manager Agent for WebSphere Applications on z/OS. . . . 3

Overview of the monitoring and diagnostic capabilities	3
Components of the Agent on z/OS	5

Chapter 2. Worksheets for installing, configuring and upgrading ITCAM Agent for WebSphere Applications on z/OS . . 7

Worksheet for installing and configuring the Data Collector.	7
Roles for installing and configuring the Data Collector.	8
Worksheet for installing and configuring the monitoring agent	9
Roles for installing and configuring the monitoring agent	9
Worksheet for upgrading from ITCAM for WebSphere, ITCAM for Web Resources, and ITCAM for WebSphere Application Server	10

Part 2. Installing and Configuring the Data Collector on z/OS 11

Chapter 3. Installing and configuring the Data Collector on IBM z/OS 13

Step 1: Installing the Data Collector	13
Step 2: Creating a new configuration directory.	13
Step 3: configuring the CYN1 subsystem	15

Step 3a: updating the PARMLIB	15
Step 3b: defining the dynamic subsystem	15
Step 3c: updating RACF	16
Step 3d: updating PROCLIB	16
Step 3e: verifying or configuring the connection to the Managing Server	16
Step 3f: authorizing data sets and updating the link list.	16
What to do next	17
Step 4: verifying the installation	17
What to do next	17
Step 5: executing the runtime setup script	17
Step 5a: overview of the runtime setup script	18
Step 5b: tasks to perform before running the script	19
Step 5c: upgrading monitoring of an application server instance monitored by a previous version of the Data Collector	32
Step 5d: executing the runtime setup script in prompt mode.	36
Step 5e: executing the runtime setup script in batch	41
Step 6: additional configuration tasks.	43
Step 6a: verifying the configuration for data collection for the Visualization Engine (Application Monitor) user interface	44
What to do next	44

Chapter 4. Customization and advanced configuration for the Data Collector 45

Properties files for the Data Collector.	45
Tuning Data Collector performance and monitoring scope	46
Data Collector internal buffering and turbo mode settings.	47
Enabling instrumentation and monitoring of RMI/IIOP requests between application servers	48
Disabling various types of Byte Code Instrumentation for J2EE APIs	50
Controlling instrumentation of application classes for lock analysis, memory leak analysis, and method profiling and tracing	52
Disabling Heap Analysis on IBM WebSphere Application Server 6.1.x	59
Defining custom requests.	60
Enabling Asynchronous Bean request monitoring	61
Customizing monitoring of custom MBeans	63
Modifying Performance Monitoring Infrastructure settings	65
Enabling Performance Monitoring Infrastructure settings for the Service Integration Bus	66
Enabling and customizing SMF monitoring.	66
Installing the IEFU83 exit.	67
Initializing IBM z/OS	67

Customizing the CYN1 Subsystem for optional SMF Collection	67
Verifying the IBM z/OS components	70
Enabling and disabling instrumentation of Web Services as new request types	71
Enabling and disabling memory monitoring	72
Setting the server alias.	73
Changing Managing Server communication configuration	73
Configuring the Data Collector after changing the application server version	73
Steps to perform after changing the IP address of the Data Collector	74
Steps to support changing application server addressing mode	74
Moving the Data Collector to a different host computer	75
Configuring a Data Collector for multiple network interfaces	76
Customizing CICS transaction correlation	76
Overriding the Data Collector autoconfiguration	78
Properties for communication with a Deployment Manager	78
Enabling integration with ITCAM for Transactions	78
Verify setup prerequisites.	79
Verify the Transactions directory	80
Modify LIBPATH and CLASSPATH	80
Modify toolkit custom properties file	81
Steps to reduce background CPU utilization	82
Customizing RMI garbage collection interval	82
Disabling WebSphere SMF or increasing the recording interval	83
Changes to the Data Collector properties file	83
Changes in the Visualization Engine of the Managing Server	84
Disabling Data Collector communication with the Monitoring Agent	84
Turning off writing of SMF records in the CYN1 subsystem.	85
Disabling the LogCmd feature	86

Chapter 5. Unconfiguring the Data Collector on IBM z/OS 87

How to enter values for configuration options.	87
Unconfiguring the Data Collector in prompt mode	91
Unconfiguring the Data Collector in batch (auto-run) mode.	94
Editing the cynzucfg.cntl batch job and submitting it as a z/OS JCL job that uses BPXBATCH	94
Executing the unconfig.sh script through a command line	95
Unconfiguring the Data Collector manually.	95

Part 3. Installing and Configuring the monitoring agent on z/OS 97

Chapter 6. Installing and configuring the monitoring agent on IBM z/OS 99

Configuring the monitoring agent on z/OS.	99
Steps for configuring the monitoring agent on z/OS	99
Optional postconfiguration steps	144

Part 4. Appendixes 155

Appendix A. Applying the latest maintenance. 157

Appendix B. Environment Checking Utility for z/OS 159

Overview.	159
Installation	159
Running the Environment Checking Utility	159
Special considerations	162
Execution environment requirements	162
Javacores	162

Appendix C. Setting up security 165

Setting up the user ID and password for the Data Collector with IBM WebSphere Application Server Global Security enabled	165
Setting up RACF access to FACILITY profile ERBSDS.MON2DATA	167
Node Authentication	168
Script to run if your SSL certificates have expired	168
Node Authentication on the Managing Server	168
Data Collector custom properties file changes	169
Keystore management and populating certificates	169
Secure Socket Layer communications	172
Password encryption and Kernel property file encryption	172
Enabling Secure Socket Layer at the Data Collector level	173
Verifying secure communications.	173
Privacy filtering	174
Enabling privacy filtering	175
Script to run if your SSL certificates have expired	175
Settings for the Data Collector if Java 2 security is used	177

Appendix D. Common Services Address Space command reference . 179

Starting the Common Services Address Space	179
Stopping the Common Services Address Space	180
Modifying the Common Services Address Space	180
The ACT command	180
The CPU command	181
The INACT command	181
The DUMP command	181
The SMFWRITE command	182
The TRACE command	182
The SPINLOG command	183
The ZAP command	183
The STAMP command	183
The VER command	184

The STATS command.	184
----------------------------	-----

Appendix E. Using regular expressions 185

Regular expression library	185
Frequently used regular expressions.	185
Specifying exclusions with the bang (!) operator (Quality of Service listening policies only).	186

Appendix F. Support information . . . 187

Searching knowledge bases.	187
Finding Release Notes	187
Searching the information center on your local system or network.	188
Searching the Internet	188
Obtaining fixes	188
Receiving Weekly support updates	189

Contacting IBM Software Support	189
Determining the business impact of your problem	190
Describing your problem and gathering background information.	190
Submitting your problem to IBM Software Support	190
Tivoli Support Technical Exchange	191

Appendix G. Accessibility 193

Index 195

Trademarks 197

Notices 199

Figures

1. Agent interaction with IBM Tivoli Monitoring	4	27. Specify Agent IP.UDP Configuration Values screen	126
2. Agent interaction with ITCAM for Application Diagnostics Managing Server	5	28. JCL for allocating the agent's runtime members	127
3. How the setupwas.sh script invokes wsadmin.sh in a Network Deployment environment	19	29. Specify Persistent Datastore Values menu	128
4. TSO Screen	100	30. Allocate Persistent Datastore Menu	129
5. ICAT welcome screen	101	31. Persistent Datastore Specifications screen	130
6. Primary ICAT screen	102	32. Create or Edit PDS Maintenance Jobcard screen	131
7. Set Up Work Environment screen	103	33. PDS information panel	132
8. Setting up work options	104	34. JCL for creating PDS maintenance members	133
9. Set Up Configuration Environment screen	105	35. JCL for allocating Persistent Datastore files	134
10. JCL for allocating ICAT work libraries	106	36. Complete Persistent Datastore Configuration screen (1 of 2)	135
11. Configure Products screen	107	37. Complete Persistent Datastore Configuration screen (2 of 2)	136
12. Product Selection Menu	108	38. Complete the Configuration screen (1 of 7)	137
13. Runtime Environments screen	109	39. Complete the Configuration screen (2 of 7)	138
14. Add Runtime Environment screen (1 of 2)	110	40. Complete the Configuration screen (3 of 7)	139
15. Add Runtime Environment screen (2 of 2)	111	41. Complete the Configuration screen (4 of 7)	140
16. JCL for allocating a new RTE's libraries	113	42. Complete the Configuration screen (5 of 7)	141
17. Product Component Selection menu	114	43. Complete the Configuration screen (6 of 7)	142
18. Product RTE configuration screen	115	44. Complete the Configuration screen (7 of 7)	142
19. Specify Java SubAgent Parameters screen	116	45. JCL for copying postconfiguration agent libraries	144
20. Update Agent Collection menu.	117	46. README PDS output (1 of 8)	146
21. JCL for creating agent runtime members	120	47. README PDS output (2 of 8)	147
22. Specify Agent Address Space Parameters screen	121	48. README PDS output (3 of 8)	148
23. Specify Advanced Agent Configuration Values screen	122	49. README PDS output (4 of 8)	149
24. Tivoli Enterprise Monitoring Server selection screen	123	50. README PDS output (5 of 8)	150
25. Panel for the monitoring server information	124	51. README PDS output (6 of 8)	151
26. Specify Agent IP.PIPE Configuration Values screen	125	52. README PDS output (7 of 8)	152
		53. README PDS output (8 of 8)	153

Tables

1. List of options for the createcfg.sh script	14	15. Procedures to customize instrumentation of the Performance Monitoring Infrastructure	66
2. Default ports	20	16. Navigation to modifying LIBPATH in the IBM WebSphere Application Server administrative console	80
3. List of options for the setupwas.sh script	24	17. Navigation to JVM custom properties in the IBM WebSphere Application Server administrative console	83
4. List of options for the migratecfg.sh script	33	18. List of options for the unconfig.sh script	88
5. List of options for the migratecfg.sh script that override default settings for setupwas.sh	34	19. Navigation to JVM custom properties in the IBM WebSphere Application Server administrative console	171
6. Specifying the location of <i>MS_home</i>	40	20. Location of the CYND4051I message	174
7. Adding lines to toolkit_custom.properties	50	21. Classification of the data processed on the CommandAgent channel	174
8. Modifying lines in toolkit_custom.properties	51	22. Example of Dump command output	182
9. Byte Code Instrumentation configuration files	52	23. Examples of Zap command	183
10. Parameters for the memory leak diagnosis configuration file	56	24. Criteria for assessing the business impact of your problem	190
11. Parameters for the Level 3 method entry and exit analysis configuration file	58		
12. Parameters for the custom requests configuration file	60		
13. Parameters for the JMX MBean configuration file	63		
14. Default Performance Monitoring Infrastructure instrumentation settings	65		

About this publication

This publication provides information about installing, customizing, starting, and maintaining IBM® Tivoli® Composite Application Manager Agent for WebSphere® Applications on IBM z/OS®.

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 Application Diagnostics library

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

- *IBM Tivoli Composite Application Manager for Application Diagnostics: Prerequisites*
Provides the hardware and software requirements for installing ITCAM for Application Diagnostics components.
- *IBM Tivoli Composite Application Manager for Application Diagnostics: User's Guide*
Provides the user overview, user scenarios, and Helps for every ITCAM for Application Diagnostics component.
- *IBM Tivoli Composite Application Manager for Application Diagnostics: Planning an Installation*
Provides the user with a first reference point for a new ITCAM for Application Diagnostics installation or upgrade.
- ITCAM Agent for WebSphere Applications Installation and Configuration Guides:
 - *IBM Tivoli Composite Application Manager: Agent for WebSphere Applications Installation and Configuration Guide*
 - *IBM Tivoli Composite Application Manager: Agent for WebSphere Applications Installation and Configuration Guide for z/OS*

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

Provide installation instructions for setting up and configuring ITCAM Agent for WebSphere Applications on distributed, z/OS, and IBM i systems.

- ITCAM Agent for J2EE Applications Installation and Configuration Guides:

- *IBM Tivoli Composite Application Manager: Agent for J2EE Data Collector Installation and Configuration Guide*
- *IBM Tivoli Composite Application Manager: Agent for J2EE Monitoring Agent Installation and Configuration Guide*

Provide installation instructions for setting up and configuring ITCAM Agent for J2EE.

- *IBM Tivoli Composite Application Manager: Agent for HTTP Servers Installation and Configuration Guide*

Provides installation instructions for setting up and configuring ITCAM Agent for HTTP Servers.

- *IBM Tivoli Composite Application Manager for Application Diagnostics Managing Server Installation Guide*

Provides installation instructions for setting up and configuring ITCAM for Application Diagnostics Managing Server.

- *IBM Tivoli Composite Application Manager for Application Diagnostics: Troubleshooting Guide*

Provides instructions on problem determination and troubleshooting for ITCAM for Application Diagnostics.

- *IBM Tivoli Composite Application Manager for Application Diagnostics: Messaging Guide*

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

Related publications

The following documentation also provides useful information:

- IBM Tivoli Documentation Central:

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

<http://www.ibm.com/tivoli/documentation.html>

- IBM WebSphere Application Server:

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

<http://www.ibm.com/software/webservers/appserv/was/library>

- IBM DB2®:

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

<http://www.ibm.com/software/data/sw-library/>

- IBM Tivoli Enterprise Console®:

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

<http://submit.boulder.ibm.com/tividd/td/EnterpriseConsole3.9.html>

- IBM Tivoli Data Warehouse:

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

<http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?toc=/com.ibm.tivoli.tdwi.doc/toc.xml>

- IBM Tivoli Change and Configuration Management Database:

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

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

- IBM Support Assistant:

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

<http://www.ibm.com/software/support/isa/index.html?rcss=rtlrrr>

Accessing terminology online

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

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

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

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

Accessing publications online

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

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

<https://www.ibm.com/developerworks/wikis/display/tivolidoccentral/Home>

Access the Tivoli Information Center for ITCAM for Application Diagnostics at the following Web address:

http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/topic/com.ibm.itcamfad.doc_7101/ic-homepage.html

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

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

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

Ordering publications

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

<http://www.elink.ibm.link.ibm.com/public/applications/publications/cgibin/pbi.cgi>

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, contact your software account representative to order Tivoli publications. To locate the telephone number of your local representative, perform the following steps:

1. Go to the following Web site:
<http://www.elink.ibm.link.ibm.com/public/applications/publications/cgibin/pbi.cgi>
2. Select your country from the list and click **Go**.
3. Click **About this site** in the main panel to see an information page that includes the telephone number of your local representative.

Accessibility

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

For additional information, see Appendix G, “Accessibility,” on page 193.

Tivoli technical training

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

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

Support information

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

Online

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

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

Follow the instructions.

IBM Support Assistant

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

Troubleshooting Guide

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

Conventions used in this publication

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

Typeface conventions

This publication uses the following typeface conventions:

Bold

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

Italic

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

Monospace

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

Variables for directories

This guide refers to the following variables:

- *install_home*: the directory where the Data Collector is installed. The default location is `/usr/lpp/itcam/WebSphere/DC`.

Note: This directory can be mounted as read only in daily use.

- *config_home*: a read-write directory that is linked by a symbolic link to the *install_home* for the IBM z/OS Data Collector. This is the directory in which you can modify the configuration of the Data Collector and where the runtime setup script registers its values. The location of this directory is specified during the SMP/E installation, and its default is `/u/itcam71`.

Note: /u/itcam71 is also the default location for the monitoring agent Runtime Environment configuration files. However, the Data Collector *config_home* and the monitoring agent file location are not linked, and can be changed independently.

- *AppServer_home*: the directory where the application server core product files are installed.

Part 1. Introduction to ITCAM Agent for WebSphere Applications on z/OS

Chapter 1. IBM Tivoli Composite Application Manager Agent for WebSphere Applications on z/OS

This chapter introduces the ITCAM Agent for WebSphere Applications on z/OS and explains how it can help you monitor, administer, and diagnose your z/OS systems that run IBM WebSphere Application Server.

Overview of the monitoring and diagnostic capabilities

IBM Tivoli Composite Application Manager Agent for WebSphere Applications is a component of ITCAM for Application Diagnostics, Version 7.1.0.2. It is also a component of ITCAM for Applications Version 6.2.3. If you are using ITCAM for Applications, the Managing Server (deep dive) functionality is not available; please ignore all references to this functionality in this document.

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, the user can:

- 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 IBM Tivoli Monitoring automatically monitors
- 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 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, the user 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 capabilities of IBM Tivoli Monitoring, and information on 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.

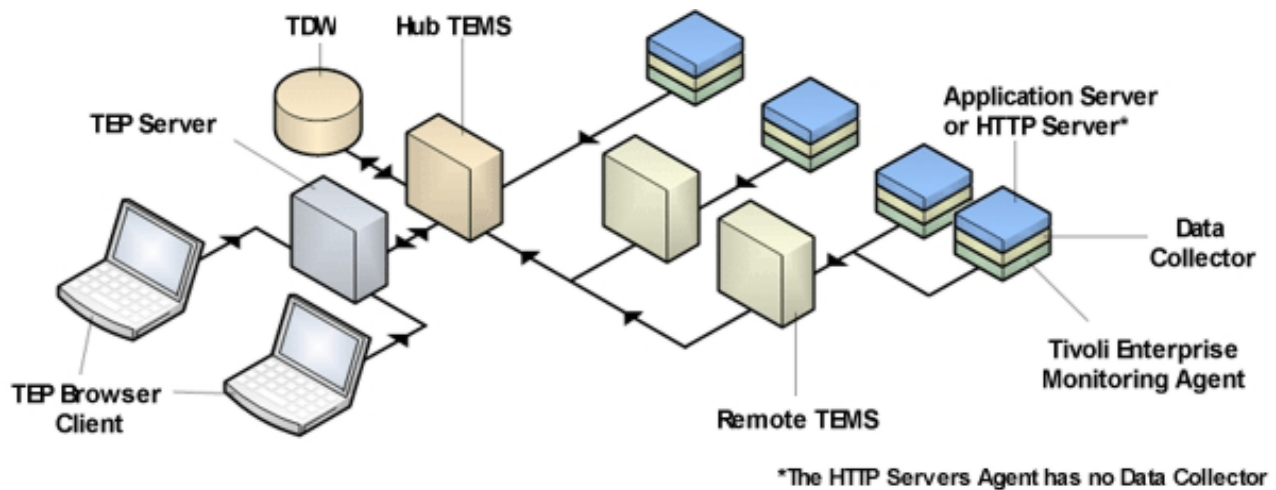


Figure 1. Agent interaction with IBM Tivoli Monitoring

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.

Most information provided by ITCAM Agent for WebSphere Applications and available through the Tivoli Enterprise Portal can also be viewed through the Visualization Engine. The Visualization Engine also provides additional diagnostic information, including:

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

The diagram on 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).

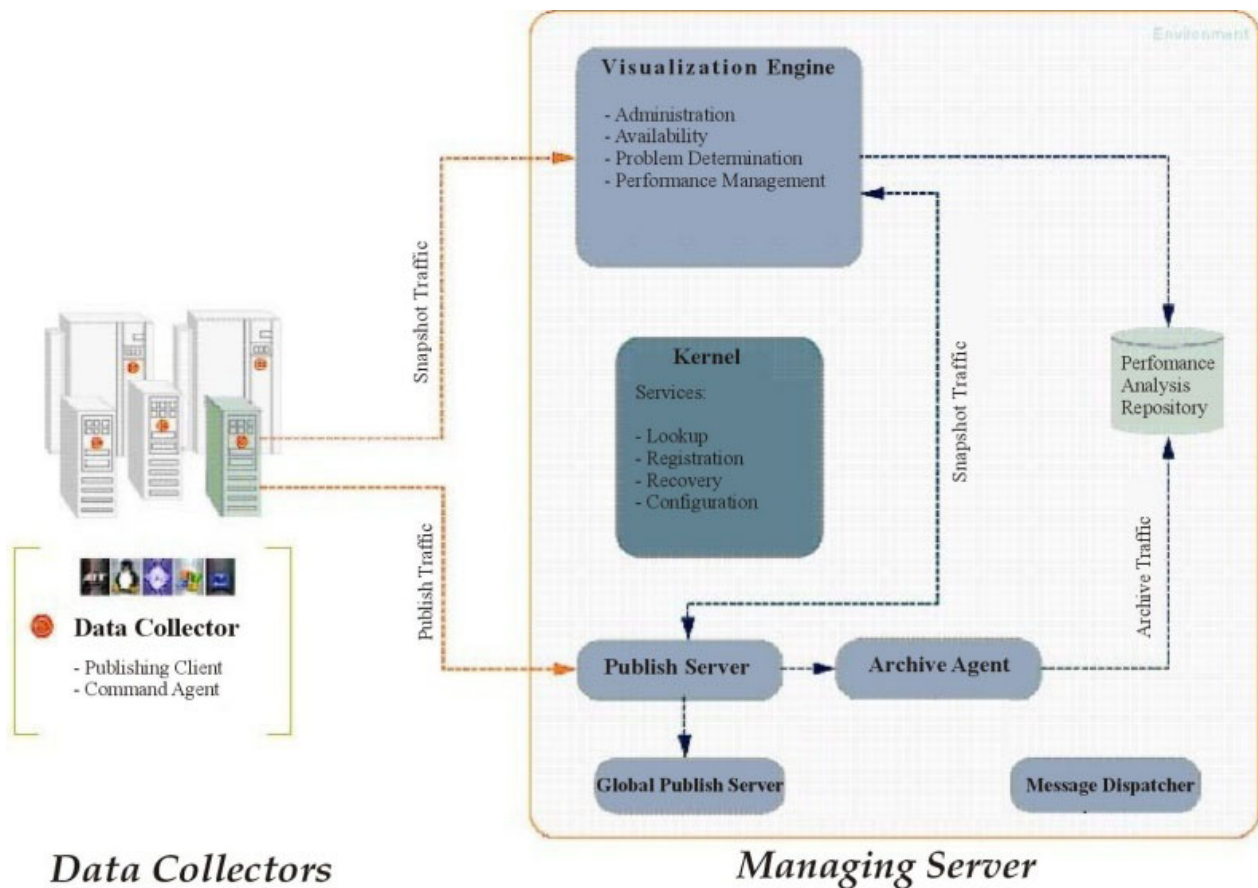


Figure 2. Agent interaction with ITCAM for Application Diagnostics Managing Server

Components of the Agent on z/OS

ITCAM Agent for WebSphere Applications consists of two components: the *Data Collector* and the *Monitoring Agent*. On z/OS, these components are deployed by separate SMP/E installs. You may deploy them in any order.

Data Collector

The Data Collector collects monitoring and diagnostics information from the application server using the following methods:

- In *Byte Code Instrumentation (BCI)*, the Data Collector injects monitoring calls into the Java code that processes application requests. Data is collected on request processing time and on different types of J2EE API calls within each request. These are sometimes referred to as *nested requests*. BCI monitoring requirements may be different; while on a production system request level monitoring may be sufficient, on a test or development system, or when a problem is being investigated, it 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 overhead, is determined by the *monitoring level*, which can be set for every monitored application server. With IBM Tivoli Monitoring, levels L1 and L2 are supported; with ITCAM for Application Diagnostics Managing

Server, the additional level L3 is available. The monitoring level can be set independently for IBM Tivoli Monitoring and the Managing Server, and for every application server instance.

- *Performance Monitoring Interface (PMI)* is an API provided by IBM WebSphere Application Server, supplying a number of performance metrics.
- *Garbage Collection logs* are written by IBM WebSphere Application Server, and contain detailed information about the garbage collection process. Such information can be useful for application server monitoring and tuning.
- *SMF* supplies performance and statistical information that IBM WebSphere Application Server can be configured to write.

The Data Collector sends the information to the monitoring agent. It also communicates directly with the Managing Server (if the Managing Server infrastructure is used).

You must configure the Data Collector for every instance of the application server that you need to monitor.

After the Data Collector has been installed using SMP/E, you can remount the HFS or zFS filesystem containing your target files (*install_home*, by default `/usr/lpp/itcam/WebSphere/DC`) as read-only. This directory can be shared by any number of Data Collector configurations in different LPARs and environments.

You need to create a directory on a read-write file system for configuration data (*config_home*, by default `/u/itcam71`). The configuration is specific to each application server instance. One *config_home* can hold configuration data for any number of IBM WebSphere Application Server instances within the same LPAR. Typically, you will create a unique *config_home* on each LPAR. You can also create separate configuration home directories for different environments within an LPAR (for example, production and testing, different Network Deployment cells, or different application server versions).

Monitoring Agent

The Monitoring Agent collects information from the Data Collector, and processes and aggregates it for presentation to the user. It also parses the IBM WebSphere Application Server System Logger logstream.

In WebSphere Extended Deployment, if cell monitoring is configured, the monitoring agent communicates to the Deployment Manager over the network to retrieve configuration and performance information for the cell.

The Monitoring Agent sends monitoring information to the Tivoli Enterprise Monitoring Server. It also receives Take Action commands from the Tivoli Enterprise Monitoring Server.

The Monitoring Agent requires the IBM Tivoli Monitoring framework. After installing the monitoring agent using SMP/E, you must configure one or several Runtime Environments of the monitoring agent using ICAT. A Runtime Environment will communicate to Data Collector instances on the same z/OS system image; they may use several *config_home* directories. Typically, one Runtime Environment per system image is used.

Chapter 2. Worksheets for installing, configuring and upgrading ITCAM Agent for WebSphere Applications on z/OS

A typical installation of ITCAM Agent for WebSphere Applications on z/OS uses the IBM Tivoli Monitoring infrastructure for monitoring application server performance. It can also communicate with ITCAM for Application Diagnostics Managing Server for deep dive diagnostics. The Managing Server must be installed on a Windows, Linux, or UNIX system.

For such an installation, you need to install and configure both components of the Agent - the monitoring agent and the Data Collector. You must install both of them on the same z/OS system, and configure them in every LPAR where application servers are to be monitored.

You can also opt for a deep dive diagnostics only installation, where Tivoli Monitoring is not used, and diagnostics is provided by the Managing Server. In this case, you do not need to install the monitoring agent. Install the Data Collector, and configure it in every LPAR where application servers are to be monitored.

Worksheet for installing and configuring the Data Collector

Perform the tasks for configuring and customizing the Data Collector in the following order:

1. If you will be using ITCAM for Application Diagnostics Managing Server, install the Managing Server. See *IBM Tivoli Composite Application Manager: Managing Server Installation Guide*.
2. Install the Data Collector (FMID HAAD710) and the ITCAM Common Services (FMID HAAD71C), and apply the latest maintenance, that is, all applicable Program Temporary Fixes (PTFs), for them. See each of the following documents:
 - *IBM Tivoli Composite Application Manager for Application Diagnostics Program Directory*
 - *IBM Tivoli Composite Application Manager for Application Diagnostics Common Services Program Directory*
3. Create a configuration directory (*config_home*) for the Data Collector. You need to create a configuration directory for every LPAR where application servers are to be monitored. You can also create several configuration directories in the same LPAR, in order to separate different environments. See "Step 2: Creating a new configuration directory" on page 13.
4. Configure the CYN1 subsystem. You must configure this subsystem for every LPAR where application servers are to be monitored. See "Step 3: configuring the CYN1 subsystem" on page 15.
5. Verify the installation and configure the Data Collector. You must configure it for every application server instance that is to be monitored. See Chapter 3, "Installing and configuring the Data Collector on IBM z/OS," on page 13.
6. Perform customizations of the Data Collector, as required.
See Chapter 4, "Customization and advanced configuration for the Data Collector," on page 45.

7. (optional) Set up secure communication between the Data Collector and the Managing Server.

See Appendix C, “Setting up security,” on page 165.

Important: if you are installing the Data Collector on a SYSPLEX:

- You can share target HFS and MVS™ datasets between LPARs on a shared DASD.
- Do not use shared configuration directories (*config_home*) between LPARs.
- Configure the Data Collector on each LPAR individually.

Roles for installing and configuring the Data Collector

The following roles are required to complete the installation and configuration:

- IBM z/OS SMP/E system programmer
- IBM z/OS UNIX System Services (USS) administrator
- IBM WebSphere Application Server administrator
- Security administrator
- Network administrator
- Storage administrator

Note: This worksheet specifies the people who might perform each of the tasks. This serves as an approximate guide. However, follow the links to each of the sections to verify the person in your organization who will actually perform the task.

- “Step 1: Installing the Data Collector” on page 13 (all of the above roles)
- “Step 2: Creating a new configuration directory” on page 13 (IBM z/OS SMP/E system programmer)
- “Step 3: configuring the CYN1 subsystem” on page 15
 - “Step 3a: updating the PARMLIB” on page 15 (IBM z/OS SMP/E system programmer)
 - “Step 3b: defining the dynamic subsystem” on page 15 (IBM z/OS SMP/E system programmer)
 - “Step 3c: updating RACF” on page 16 (Security administrator)
 - “Step 3d: updating PROCLIB” on page 16 (IBM z/OS SMP/E system programmer)
 - “Step 3e: verifying or configuring the connection to the Managing Server” on page 16 (Network administrator)
 - “Step 3f: authorizing data sets and updating the link list” on page 16 (IBM z/OS SMP/E system programmer)
- “Step 4: verifying the installation” on page 17 (IBM z/OS SMP/E system programmer)
- “Step 5: executing the runtime setup script” on page 17
 - “Step 5a: overview of the runtime setup script” on page 18 (IBM WebSphere Application Server administrator, IBM z/OS SMP/E system programmer)
 - “Step 5b: tasks to perform before running the script” on page 19 (IBM WebSphere Application Server administrator, IBM z/OS SMP/E system programmer, Security administrator, Storage administrator)
 - “Step 5c: upgrading monitoring of an application server instance monitored by a previous version of the Data Collector” on page 32 (IBM WebSphere Application Server administrator)

- “Step 5d: executing the runtime setup script in prompt mode” on page 36 (IBM WebSphere Application Server administrator)
- “Step 5e: executing the runtime setup script in batch” on page 41 (IBM WebSphere Application Server administrator)
- “Step 6: additional configuration tasks” on page 43
 - “Step 6a: verifying the configuration for data collection for the Visualization Engine (Application Monitor) user interface” on page 44 (IBM z/OS SMP/E system programmer)
- Chapter 4, “Customization and advanced configuration for the Data Collector,” on page 45: perform the tasks in this chapter as required (IBM z/OS SMP/E system programmer, IBM WebSphere Application Server administrator, Network administrator).

Worksheet for installing and configuring the monitoring agent

Perform the tasks for configuring and customizing the Monitoring Agent in the following order:

1. Make sure a Tivoli Enterprise Monitoring Server is installed and configured either on z/OS, Windows, or a Linux or UNIX system. See either the *IBM Tivoli Monitoring: Installation and Setup Guide* (for Windows and UNIX) or the *Configuring IBM Tivoli Enterprise Monitoring Server on z/OS*.
2. Make sure IBM Tivoli Management Services version 6.2.2 fix pack 1 or later are installed, configured, and operating on the LPARs where you plan to configure the monitoring agent runtime environment. (You will need to configure the environment on every LPAR where an application server is to be monitored by the Data Collector). See *Program Directory for IBM Tivoli Management Services on z/OS*.
3. Install the monitoring agent (FMID HKYN710), and apply the latest maintenance, that is, all applicable Program Temporary Fixes (PTFs), for it. See *Program Directory for IBM Tivoli Composite Application Monitor (ITCAM) for Application Diagnostics on z/OS, Tivoli Enterprise Monitoring Agent V7.1.0*.
4. Create a Runtime Environment (RTE) for the monitoring agent on every system image where an application server is to be monitored by the Data Collector, using ICAT. See “Steps for configuring the monitoring agent on z/OS” on page 99.
5. After creating each RTE, perform optional post-configuration steps as required. See “Optional postconfiguration steps” on page 144.

Roles for installing and configuring the monitoring agent

The following roles are required to complete the installation and configuration:

- IBM z/OS SMP/E system programmer
- IBM WebSphere Application Server administrator

Note: This worksheet specifies the people who might perform each of the tasks. This serves as an approximate guide. However, you need to verify the person in your organization who will actually perform the task.

- Installing IBM Tivoli Management Services and the Monitoring Agent (IBM z/OS SMP/E system programmer)
- Configuring a Runtime Environment and performing optional post-configuration steps, see Chapter 6, “Installing and configuring the monitoring agent on IBM z/OS,” on page 99 (IBM WebSphere Application Server administrator)

Worksheet for upgrading from ITCAM for WebSphere, ITCAM for Web Resources, and ITCAM for WebSphere Application Server

If you are upgrading an installation of ITCAM for WebSphere Data Collector version 6.0, ITCAM for WebSphere Data Collector 6.1 (also shipped with ITCAM for Web Resources 6.2), or ITCAM for WebSphere Application Server 7.0 or 7.1 (shipped with WebSphere Application Server), follow the worksheets for installation, with the following caveats:

- When installing the Data Collector (FMID HAAD710), specify an installation home directory different from the one used for the previous version of the Data Collector.
- When installing ITCAM Common Services (FMID HAAD71C), use a different SMP/E Consolidated Software Inventory (CSI) from the one used for the previous version of the Data Collector.
- When configuring Monitoring Agent Runtime Environments, specify a different product home directory from the one used for the previous version of the monitoring agent. (The default, `/u/itcam71/tema`, is likely to satisfy this requirement).
- When creating Data Collector configuration directories, specify different directories from the ones used for the previous version of the Data Collector. (The default, `/u/itcam71`, is likely to satisfy this requirement).
- To upgrade monitoring of application server instances monitored by ITCAM for WebSphere 6.0 Data Collector, unconfigure the old Data Collector before configuring the new one. See “Upgrading monitoring from Data Collector version 6.0” on page 32.
- To upgrade monitoring of application server instances monitored by ITCAM for WebSphere Data Collector 6.1 (also shipped with ITCAM for Web Resources 6.2), use the `migratecfg.sh` script to preserve configuration. See “Upgrading monitoring from Data Collector version 6.1 or ITCAM for WebSphere Application Server 7.0 or 7.1” on page 32.
- To upgrade monitoring of application server instances monitored by ITCAM for WebSphere Application Server Data Collector 7.0 or 7.1 (shipped with WebSphere Application Server), simply configure monitoring of these instances using the `setupwas.sh` script. See “Upgrading monitoring from Data Collector version 6.1 or ITCAM for WebSphere Application Server 7.0 or 7.1” on page 32.

Attention: As soon as you shut down an old Monitoring Agent Runtime Environment and start the new one, monitoring of any Data Collectors versions below 6.1 fix pack 4 will stop. To restore it, upgrade monitoring of the application server instances to the new version of the Data Collector. This does not affect monitoring with the Managing Server.

Part 2. Installing and Configuring the Data Collector on z/OS

Chapter 3. Installing and configuring the Data Collector on IBM z/OS

In a new installation, you need to install the Data Collector and configure it to monitor application server instances. If a previous version of the Data Collector is installed, you need to install the new version of the Data Collector, and then upgrade monitoring of application server instances.

Step 1: Installing the Data Collector

In order to install the Data Collector, perform the following actions:

1. If it was not installed before, or a previous version was installed, install ITCAM Common Services version 7.1, FMID HAAD71C. See *Program Directory for IBM Tivoli Composite Application Monitor (ITCAM) for Application Diagnostics on z/OS, Agent for WebSphere Applications (Common Services) V7.1.0*.
2. Install the Data Collector version 7.1, FMID HAAD710. See *Program Directory for IBM Tivoli Composite Application Monitor (ITCAM) for Application Diagnostics on z/OS, Agent for WebSphere Applications (Data Collector) V7.1.0*.

Attention: if a previous version of the Data Collector is installed on the same file system, make sure to specify a different installation home directory.

3. Install all Program Temporary Fixes (PTFs) shipped with the Data Collector and with ITCAM Common Services.
4. Install any new PTFs available for the Data Collector and ITCAM Common Services; . To see a list of recent PTFs and to acquire them, you can visit the IBM Tivoli Composite Application Manager for Application Diagnostics support site.

Select **Download**, then **Fixes by version**. Click the "PSP buckets": *z/OS Data Collectors V7.1 PSP (WAS DC)* and *z/OS Data Collectors V7.1 PSP (Common Services)*. Read the *Service Recommendation Summary* in each of these documents.

Step 2: Creating a new configuration directory

After installing the Data Collector, you must create a configuration directory (*config_home*). The default path for this directory is */u/itcam71*.

This configuration directory is required before you can configure the Data Collector to monitor application server instances or upgrade monitoring from a previous version of the Data Collector.

Attention: Do not use configuration directories created for a previous version of the Data Collector.

You can also create an additional configuration directory for a different environment or LPAR.

In order to create a new configuration directory (*config_home*) on a read-write HFS or zFS file system, perform the following actions:

1. Make sure all the latest maintenance is applied (see Appendix A, "Applying the latest maintenance," on page 157).

2. Change to the *install_home* directory (by default, /usr/lpp/itcam/WebSphere/DC) and run the createcfg.sh script from that directory. The parameters for the script are set out in Table 1.

Table 1. List of options for the createcfg.sh script

Command-line option	Description	Equivalent environment variable and value
-batch	Turns off prompting so that the script will run to completion with no user interaction. This parameter is required when running the background, as in the CYNZISRT job. The default is to prompt for all optional values.	ITCAM_BATCH=y
-debug	Adds diagnostic trace information to the standard output. Use this parameter if you encounter problems and need IBM technical support. The default is to refrain from putting out the extra diagnostic information.	ITCAM_DEBUG=y
-cleanup	If you use this parameter, any existing <i>config_home</i> will be removed and re-created by the script. Do not use this parameter if you wish to retain continuity with a previous configuration of the Data Collector. The default is to reuse any existing <i>config_home</i> directory structure.	ITCAM_CLEANUP=y
-config <i>config_home</i>	Specify the full path of the configuration home directory that will be created by the createcfg.sh script. The default is /u/itcam71 .	ITCAM_CONFIG=config_home
-install <i>install_home</i>	Specify the full path of the install_home directory, which must have been previously created by the SMP/E install process. You may wish to specify a path containing a symbolic link for flexibility. The default is derived from the full path to the createcfg.sh script.	ITCAM_INSTALL=install_home
-owner <i>user[:group]</i>	Sets the owner of the files and directories in <i>config_home</i> as createcfg.sh completes its processing. A user and optionally a group may be specified in the same format as specified for chown. If the current effective user does not have superuser privilege, this parameter is ignored. The default is to leave the ownership of the files and directories in <i>config_home</i> unchanged.	ITCAM_OWNER=user[:group]

Table 1. List of options for the createcfg.sh script (continued)

Command-line option	Description	Equivalent environment variable and value
-access permissions	Sets the access permissions for the files and directories in the config_home created by createcfg.sh. The permissions are specified in the same format as for chmod, and may be either numeric like 664 or symbolic format like a+Xr,u+w,g+w,o-w . The default is to leave the access permissions of the files and directories in config_home unchanged.	ITCAM_ACCESS=permissions

Alternatively, you can run the CYN5ZIRT job, which will execute the createcfg.sh script. Refer to the *Program Directory for IBM Tivoli Composite Application Monitor (ITCAM) for Application Diagnostics on z/OS, Agent for WebSphere Applications (Data Collector) V7.1.0* for instructions and sample source code for this job.

Important: If you are creating a new configuration directory on an LPAR where the Data Collector was not configured before, you must also create the CYN1 subsystem on this LPAR. Refer to the *Program Directory for IBM Tivoli Composite Application Monitor (ITCAM) for Application Diagnostics on z/OS, Agent for WebSphere Applications (Common Services) V7.1.0* for instructions.

Step 3: configuring the CYN1 subsystem

Perform the instructions in each of the following sections to configure the CYN1 subsystem.

Perform this step on every LPAR where the Data Collector is configured for the first time. Before configuring the CYN1 subsystem; you need to create it; see *IBM Tivoli Composite Application Manager for Application Diagnostics Common Services Program Directory*.

If you are upgrading from a previous version of the Data Collector, some of the procedures may have already been performed.

If you are creating an additional configuration directory on an LPAR where the current version of the Data Collector is already configured, do not perform this step.

Step 3a: updating the PARMLIB

Update the SYS1.PARMLIB(IEFSSNxx) used in your installation to include the statement:

```
SUBSYS SUBNAME(CYN1)
```

Step 3b: defining the dynamic subsystem

The Parmlib update will take effect with the next IPL of the system and is permanent. An IPL of the system is not required to dynamically add a subsystem. The following command will define the CYN1 subsystem without an IPL and will remain in place until the next IPL:

```
SETSSI ADD,SUBNAME=CYN1
```

Step 3c: updating RACF

Installations have a significant number of options they can choose to enable started tasks and authorize them with RACF®. Usually a started task must have a RACF association with a STARTED class table that specifies either a user or a group for the started task. This must be done in accordance with your installation's specifications to permit functioning of the CYN1 subsystem and CYN1PROC started task. A possible solution to this would be to issue the following RACF commands:

```
RDEF STARTED (CYN1*) OWNER(STCRACF) STDATA(USER(STCRACF))  
SETROPTS REFRESH RACLIST(STARTED)
```

The Userid associated with the started tasks must have RACF access to the IBM z/OS libraries installed in the subsequent steps.

Step 3d: updating PROCLIB

Locate the CYN.SCYNPROC data set. Either concatenate this data set to the JES2 procedure PROC00 DD statement or copy member CYN1PROC from CYN.SCYNPROC into a procedure library that is already part of the JES2 procedure PROC00 DD statement.

Note: Do not rename the CYN1PROC member to CYN1. This would cause errors.

Step 3e: verifying or configuring the connection to the Managing Server

If you will be using ITCAM for Application Diagnostics Managing Server, make sure that Data Collector can resolve the Manager Server domain name or IP address. If the Managing Server is using the partially qualified domain name (for example, demo instead of demo.ibm.com), make sure that Data Collector can ping the Managing Server successfully, or edit the USS /etc/hosts file (using root permission) to add the partially qualified or fully qualified name. Examples:

```
9.22.33.44      XYZ4141  
9.11.222.333   TESTMACH-AIX-S01.ABCD.IBM.COM  
9.12.888.99    DEV-LNX-W01.ABCD.IBM.COM
```

Also try to verify the setting in *MS_home/bin/setenv.sh* for the KERNEL_HOST01 setup. If the host name cannot be resolved or pinged, use the IP address for troubleshooting.

Step 3f: authorizing data sets and updating the link list

Update the link list as defined in SYS1.PARMLIB to include the CYN.SCYNAUTH data set name using either a LNKLISTxx or a PROGxx member of PARMLIB. Also include CYN.SCYNAUTH in the authorized library list using either IEAAPFxx or PROGxx in PARMLIB as appropriate.

Note: If you use the IEAAPFxx option, simply add a line that contains CYN.SCYNAUTH *volser* where *volser* is the volume name the library was installed on. If you use PROGxx, simply add lines that contain

```
APF ADD DSNAME(CYN.SCYNAUTH) VOLUME(volser) LNKLIST ADD NAME(LNKLIST00)  
DSN(CYN.SCYNAUTH) VOLUME(volser)
```

where *volser* is the volume name the library was installed on.

What to do next

See “Step 4: verifying the installation.”

Step 4: verifying the installation

After installing the Data Collector on IBM z/OS, verify that the installed directories and files match those listed in this section. To verify the installation, perform the following procedure:

1. Change to the *install_home* directory (by default, /usr/lpp/itcam/WebSphere/DC).
2. Enter the following command:

```
ls -laF
```

A list of files and directories displays.

3. Verify that the following directories are shown in the list:

- bin
- itcamdc
- toolkit

4. Change to the *config_home* directory (by default, /u/itcam71).

5. Enter the following command:

```
ls -laF
```

A list of files and directories displays.

6. Verify that the following directories are shown in the list:

- bin
- runtime

Also, verify that the following symlinks are shown in the list

- itcamdc
- toolkit

Finally, verify that the following file is shown in the list:

- itcam.properties

7. If these files are not present, run the createcfg.sh script in *install_home/bin* (by default, /usr/lpp/itcam/WebSphere/DC/bin).

What to do next

See “Step 5: executing the runtime setup script.”

Step 5: executing the runtime setup script

View the contents of this section in the following order:

1. “Step 5a: overview of the runtime setup script” on page 18
2. “Step 5b: tasks to perform before running the script” on page 19
3. See one of the following options:
 - If you are upgrading monitoring of an application server instance from a previous version of the Data Collector: “Step 5c: upgrading monitoring of an application server instance monitored by a previous version of the Data Collector” on page 32

- You can execute the runtime setup script in prompt mode, in which you invoke the script and then get prompted for configuration values: “Step 5d: executing the runtime setup script in prompt mode” on page 36.
- You can execute the runtime setup script in batch (auto-run) mode, in which you set the configuration values in a batch-mode invocation script then invoke the script without further interaction: “Step 5e: executing the runtime setup script in batch” on page 41.

Step 5a: overview of the runtime setup script

The runtime setup script for the IBM z/OS Data Collector provides a simple, command line interface to configure an ITCAM for Application Diagnostics runtime environment for a specified application server. A runtime environment consists of a user-specified runtime directory tree for each monitored application server on the host.

You run the script from the *config_home/bin* directory. The script will also invoke the IBM WebSphere admin scripting engine (*wsadmin.sh*) to configure the application server instance to be monitored.

Overview of the runtime environment

After the Data Collector target files have been installed with SMP/E, you can remount the HFS or zFS filesystem containing your target files (*install_home*, by default */usr/lpp/itcam/WebSphere/DC*) as read-only. This directory can be shared by any number of Data Collector configurations in different LPARs and environments.

The runtime environment to be configured has been created on a read-write file system (*config_home*, by default */u/itcam71*). Typically, you will create a unique *config_home* on each LPAR, and possibly for different environments within an LPAR (i.e. production and testing).

When you run the Data Collector runtime setup script (*setupwas.sh*) in prompt mode, you will be prompted for the WebSphere Application Server config-root directory of the server to be configured. The script will discover the application server instances in that directory and prompt you to select one of those instances.

If, for example, you are using the default *config_home* (*/u/itcam71*) and configuring an instance of IBM WebSphere Application Server 7.0 on a node called *node1* and a server called *server1*, the runtime setup script will create a directory called */u/itcam71/runtime/was70.node1.server1/*.

This directory will contain subdirectories with all the configuration files for the server, plus symbolic links for all the executable files to the SMP/E target library files in */usr/lpp/itcam*. When you apply maintenance through Program Temporary Fixes (PTFs) or Authorized Program Analysis Report fixes (APAR SYSMODs), you do not need to take any further action to distribute the updated code because all of the executable files are symbolically linked. The only situations that might require additional intervention is if instrumentation and configuration files (usually in that directory's */etc* subdirectory) are updated. The SYSMOD hold data will inform you of any required actions.

If you need to monitor several application server instances, configure the Data Collector for each of them using the *setupwas.sh* script. As long as the instances are on the same LPAR, you can use the same configuration directory for all of the

instances. However, you may choose to use different configuration directories as well (for example, to separate the test and production environments).

Configuration in a Network Deployment environment

If you are installing and configuring the Data Collector in a Network Deployment environment, it is important to note that you must perform Data Collector setup for a server on the server's host. The runtime setup script invokes the `wsadmin.sh` scripting engine for the necessary application server configuration, but you must supply the host name of the Deployment Manager in the `setupwas.sh` script if the Deployment Manager is not running on the same node as the server you are configuring.

If you change an instance of IBM WebSphere Application Server from 31-bit to 64-bit mode or vice versa, re-run the `setupwas.sh` runtime setup script. This will re-create symbolic links from the `config_home` to the correct (64-bit or 31-bit, as applicable) versions of the native libraries in the `install_home`.

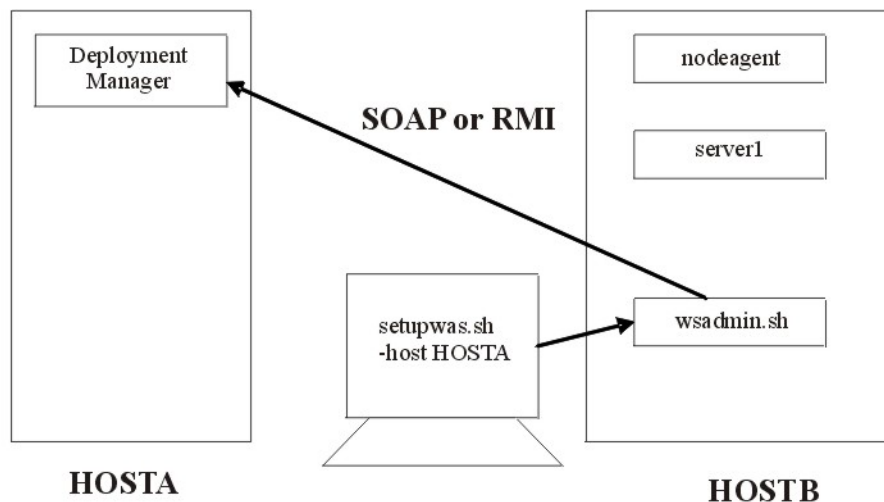


Figure 3. How the `setupwas.sh` script invokes `wsadmin.sh` in a Network Deployment environment

In the diagram, the user is configuring `server1` on host `HOSTB`, which is a node in the cell controlled by the Deployment Manager on `HOSTA`. The ITCAM `setupwas.sh` task is performed on `HOSTB`, but the `-host` parameter specifies the hostname (or IP address) of the Deployment Manager host. The cell configuration repository is on `HOSTA`. The `setupwas.sh` script issues an application server node synchronization when it is completed and pushes the configuration out to the managed node. The server named "server1" on `HOSTB` does not need to be running during the configuration, but if the node agent is not running the configuration will fail.

Step 5b: tasks to perform before running the script

Before you run the script, read the following information, and perform tasks as necessary:

Setting up the user ID and password for the Data Collector with IBM WebSphere Application Server Global Security enabled

Installing, configuring, and running the Data Collector on z/OS with Global Security turned on may require additional steps, depending on your security configuration. See “Setting up the user ID and password for the Data Collector with IBM WebSphere Application Server Global Security enabled” on page 165.

512 MB of virtual storage

You will need at least 512 MB on the ASSIZEMAX parameter in the RACF OMVS segment for the user to run the setup script. It is recommended that you run the script using a USS telnet session, but if you use OMVS under TSO, make sure that the TSO procedure you use has a large enough REGION size to support this.

Performance Monitoring Infrastructure enabled by the script

If the Performance Monitoring Infrastructure (PMI) is not already enabled when you run the runtime setup script, the script will enable it with default settings. This is a requirement for Data Collector configuration. In addition, by default, the Data Collector configuration modifies the PMI collection levels based on the Application Monitor's Monitoring Level (MOD) at WebSphere startup. Thus it overrides whatever PMI settings you have already set.

If you do not want the Data Collector configuration to modify the PMI collection levels based on the MOD level, perform Step 1 of “Step 6: additional configuration tasks” on page 43 after you execute the runtime configuration script or batch job.

Adjusting for ports being blocked by your firewall or being used by other applications

Note: this step does not apply if the Data Collector will not communicate with ITCAM for Application Diagnostics Managing Server.

At various times during the configuration you will need to specify or accept the defaults for port numbers used by ITCAM for Application Diagnostics, application servers, or databases. Perform the following procedure:

1. Use the netstat command from the Data Collector host to determine whether any of the following default ports are being used by other applications:

Table 2. Default ports

Usage	Port number
Data Collector connections (from the Managing Server) Note: this does not apply to ITCAM for Web Resources 6.2.	For each Data Collector that connects to the Managing Server, one port from each of the following ranges: • For the Data Collector Remote Method Invocation (RMI) port: 8200-8299 • For the Data Collector RMI Controller: 8300-8399

2. Run the following commands from the Data Collector host to determine whether the default Kernel Codebase, Kernel RMI, Kernel Remote File Sharing (RFS), and Publish Server 1 ports on the Managing Server host are being blocked by a firewall:

```
telnet MS_hostname 9122
telnet MS_hostname 9118
telnet MS_hostname 9120
telnet MS_hostname 9103
```

If these ports are not blocked then you usually get a blank screen. If any of these ports are blocked by a firewall, you get a message similar to the following text:

Unable to connect to remote host

3. Run the following commands from the Managing Server host to determine whether the Managing Server can connect to the Data Collector host at the default ports:

```
telnet DC_hostname port_number
```

port_number is, for each Data Collector that connects to the Managing Server, one port from each of the following ranges:

- For the Data Collector RMI port: 8200-8299
- For the Data Collector RMI Controller: 8300-8399
- If you will also have IBM CICS® or IBM IMS™ Data Collectors connecting to the Managing Server: 8700-8799
- If you will also have IBM CICS or IBM IMS Data Collectors connecting to the Managing Server: 8800-8899

If these ports are not blocked then you usually get a blank screen. If any of these ports are blocked by a firewall, you get a message similar to the following text:

Unable to connect to remote host

4. If you discovered in the previous steps that the default ports are being used by other applications or are being blocked by a firewall, take one of the following actions:
 - Before the Data Collector installation, change your environment so that these become available.
 - During the Data Collector installation and configuration, specify a port or range of ports that is different from the defaults.

Verifying the connection to wsadmin.sh

The runtime setup script needs to be able to connect to IBM WebSphere Application Server wsadmin.sh utility. Perform the following procedure to verify the connection to wsadmin.sh:

1. Make sure the region size is sufficient, particularly if you are running under TSO using OMVS. The wsadmin.sh utility starts up a JVM, and that can take a lot of memory.
2. If you are in a Network Deployment (ND) environment, make sure the Deployment Manager is running. If it is not, start the Deployment Manager.
3. If you are in a non-ND environment, make sure the instance of the application server that is being monitored by the Data Collector is running.
4. Run wsadmin.sh from the directory in which it is located:

```
./wsadmin.sh -conntype SOAP|RMI -port port -host hostname -user  
          user_ID -password password
```

See Table 3 on page 24 for a description of the options. (These particular options for running wsadmin.sh. are equivalent to the corresponding options for running the runtime setup script.)

Note: In general, you may use any application server wsadmin.sh script, but the one under *AppServer_home*/profiles/default/bin for the application server instance you are configuring is usually the most appropriate. The wsadmin.sh script will use the wsadmin.properties file associated with it.

If you successfully connect to the Deployment Manager, you will get a message similar to the following text:

```
WASX7209I: Connected to process "dmgr" on node SOMENODE using SOAP connector;  
The type of process is: DeploymentManager  
WASX7029I: For help, enter: "$Help help"
```

If you cannot connect successfully to `wsadmin.sh`, you will get a message similar to the following text:

```
WASX7246E: Cannot establish "SOAP" connection to host "SOMEHOST"...
```

In this case, verify that the SOAP port as set on the application server (stand-alone mode) or on the Deployment Manager (Network Deployment) is not used on the Data Collector host or blocked by a firewall. Check the WebSphere Application Server or Deployment Manager logs for the SOAP or RMI port number.

Otherwise, there might be a problem with your installation or configuration of IBM WebSphere Application Server. Contact IBM Software Support.

Securely setting the user ID and password for RMI or SOAP

When WebSphere Global Security is enabled, the Data Collector needs a user ID and password for RMI or SOAP communication with IBM WebSphere Application Server.

You can set them using the `-user` and `-password` options of the runtime setup script, or the `ITCAM_USER` and `ITCAM_PASSWORD` environment variables. However, in this case the password may be visible on the console for an extended period, and will be included in the job output as plain text. This may cause security issues.

To provide maximum security, you can set the user and password in client properties files and encrypt them prior to running the runtime setup script. The script will use the data from these files.

Setting the user ID and password in `sas.client.props` for RMI connector types:

To set the RMI user ID and password using the `sas.client.props` file, perform the following procedure:

1. Set the following properties in `AppServer_home/profiles/default/properties/sas.client.props`:

```
com.ibm.CORBA.loginSource=properties  
com.ibm.CORBA.loginUserId=user_ID  
com.ibm.CORBA.loginPassword=password
```

2. Run the following command to encrypt the password:

```
PropFilePasswordEncoder.sh  
AppServer_home/profiles/default/properties/sas.client.props  
com.ibm.CORBA.loginPassword
```

Run it from the `AppServer_home/profiles/default/bin` directory.

Setting the user ID and password in `soap.client.props` for SOAP connector types:

To set the SOAP user ID and password using the `soap.client.props` file, perform the following procedure:

1. Set the following properties in `AppServer_home/profiles/default/properties/soap.client.props`:

```
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/default/properties/soap.client.props  
com.ibm.SOAP.loginPassword
```

Run it from the *AppServer_home/profiles/default/bin* directory.

Selecting an IP address for the Data Collector

If the z/OS system has more than one IP address, you must select the right IP address for binding the Data Collector:

- The address must be a local IP address, not a VIPA address.
- If the Data Collector will communicate with ITCAM for Application Diagnostics Managing Server, the address must be on the same network as the Managing Server.

Use this address for the `-bindip` parameter for the `setupwas.sh` script, or select this address when running `setupwas.sh` in prompt mode.

Values for configuration options

The runtime setup script comes with a set of product-provided defaults for the configuration options.

If running the configuration script in prompt mode, you can change the product-provided default values in the following ways:

- You can specify options in the command line when initiating the script.
- You can export the equivalent environment variables before running the script.

Then when answering the prompts, you can override the existing defaults, if you choose. Some options are not prompted for. For those options, if you want to specify values that differ from the product-provided defaults, you must specify the options before the script starts up.

If running the script in batch mode, you set the values (without ever being prompted) by one of the following means:

- Specifying the equivalent environment variables in the `cynzsetu.cntl` batch job file
- Specifying options at a command line that runs `setupwas.sh` in batch mode
- Exporting the equivalent environment variable prior to running `setupwas.sh` in batch mode

Table 3 on page 24 lists the options used to run the runtime setup script.

Note: The `-user` and `-password` options may be required if Global Security is enabled.

Table 3. List of options for the *setupwas.sh* script

Command-line option	Description	Equivalent environment variable and value
-server <i>servername</i>	The application server instance name. (This is the name for the server displayed in the IBM WebSphere Application Server administrative console, not the short name used to construct the z/OS started task names. This is sometimes referred to as the long name.) For example, <i>server1</i> . This option is required if running in batch mode.	ITCAM_SERVER= <i>servername</i>
-log <i>logfile_name</i> -nolog	Indicate either -log or -nolog for whether you want the runtime configuration script to create a log of all the configuration operations that it performs. If you indicate -log, you can indicate a different location than the default. By default the log file is called <i>setupwas.log</i> and is located under the <i>config_home</i> . For example, <i>/u/itcam71/runtime/setupwas.log</i> . The default is to create this log file.	N/A. Available as an option on the command line only.
-help	Usage help	N/A. Available as an option on the command line only.
-batch	If specified, no prompting will be done. The script will terminate if necessary parameters are not specified or not valid in the batch job. Required to run the script in batch mode.	ITCAM_BATCH=y
-debug	Specifies whether to produce messages for debugging. Use this option if you have been having problems configuring the Data Collector using the script and need to provide details to IBM Software Support.	ITCAM_DEBUG=y
-config <i>config_home</i>	The Data Collector configuration home directory. For example: <i>/u/itcam71</i> The configuration home directory contains all the configuration information which can be changed. The default is derived from the <i>itcam.properties</i> file, which is created by the installation process. Several paths may resolve to this directory; you can use this option to specify the path that <i>setupwas.sh</i> will use in configuring the Data Collector. Note: This directory is different from the <i>install_home</i> directory. The <i>install_home</i> directory contains the program modules and template configuration files, which are not modified in the configuration process; it can be mounted as read only in daily use. Both of these directories are created during the installation process.	ITCAM_CONFIG= <i>config_home</i>
-owner <i>user[:group]</i>	Ownership of the directories and files created during configuration. For example: <i>wsadmin:wscfg</i> Default is none. Root access will be required if this parameter is used.	ITCAM_OWNER= <i>user[:group]</i>

Table 3. List of options for the `setupwas.sh` script (continued)

Command-line option	Description	Equivalent environment variable and value
<code>-access permission</code>	Permission to set for the directories and files created during configuration. For example: <code>u=rwX,g=rwX,o=rX</code> Default is none. Root access will be required if this parameter is used.	<code>ITCAM_ACCESS=permission</code>
<code>-cleanup</code>	In the case when a runtime directory with the configuration files for this server already exists, this option indicates that you want to remove it. A new runtime directory with a configuration for the application server instance will be created. If this option is not specified, an existing runtime directory being retained but overwritten. Whether you specify this option or not, the customized property files are always completely re-created. However, when you choose to specify this option, the <code>.id</code> and <code>.mod</code> files from the previous configuration are removed. If you choose to specify this option: - You will have to re-apply a configuration to the Data Collector in the Visualization Engine (Application Monitor) user interface. In other words you will have to use the Unconfigured Data Collector Overview page to configure the Data Collector, as described in the Visualization Engine (Application Monitor) user interface online helps. - The Data Collector history is no longer available under the original Data Collector server name in the Visualization Engine (Application Monitor) user interface. It is not necessary to specify this option, so if the consequences of specifying it are undesirable, do not specify it.	<code>ITCAM_CLEANUP=y</code>
<code>-conntype SOAP RMI</code>	The connection type for communications used by <code>wsadmin.sh</code>. The default is to use the connection type specified in the <code>wsadmin.properties</code> file associated with the <code>wsadmin.sh</code> script you have chosen. (The IBM WebSphere Application Server default for this parameter is SOAP.)	<code>ITCAM_CONNTYPE=connect_type</code>

Table 3. List of options for the *setupwas.sh* script (continued)

Command-line option	Description	Equivalent environment variable and value
-port <i>port</i>	The port number used by <i>wsadmin.sh</i>. In a Network Deployment (ND) environment, specify the Deployment Manager's SOAP or RMI port (not the application server instance SOAP or RMI port). To find the SOAP port number in the control region job log, look for the following string: BB000222I: ADMC0013I: The SOAP connector is available at port <i>port</i> To find the RMI port number in the control region job log, look for the following string: BB000222I: ADMC0026I: The RMI connector is available at port <i>port</i> The default is to use the port specified in the <i>wsadmin.properties</i> file associated with the <i>wsadmin.sh</i> script you have chosen.	ITCAM_PORT= <i>port</i>
-host <i>host</i>	The fully-qualified host name or IP address used by <i>wsadmin.sh</i>. If you are in an ND environment, enter the value for the host for the Deployment Manager. You can use <i>localhost</i> in a stand-alone environment, or in an ND environment when the Deployment Manager is located on the local host. The default is the value specified in the <i>wsadmin.properties</i> file associated with the <i>wsadmin.sh</i> script you have chosen.	ITCAM_HOST= <i>host_name</i>
-probermiport <i>range</i>	Set probe RMI port range. The default value is 8200–8299. The Managing Server host will initiate RMI connections to the Data Collector host on these ports.	ITCAM_PROBERMIPORT= <i>range</i>
-probecontrollermiport <i>range</i>	Set probe controller RMI port ranges. The default value is 8300–8399. The Managing Server host will initiate RMI connections to the Data Collector host on these ports.	ITCAM_PROBECONTROLLERMIPORT= <i>range</i>
-profile <i>profile_script</i>	Specifies a profile script for running <i>wsadmin.sh</i>. The Web site for IBM WebSphere Application Server provides the following description of a profile script: "The profile script runs before other commands, or scripts. If you specify -c, the profile script runs before it invokes this command. If you specify -f, the profile script runs before it runs the script. In interactive mode, you can use the profile script to perform any standard initialization that you want. You can specify multiple -profile options on the command line, and they invoke in the order that you supply them."	ITCAM_PROFILE= <i>script</i>
-user <i>user_id</i>	The user ID to use for connection to <i>wsadmin.sh</i> . This is required if Global Security is enabled and it is not set in the <i>sas.client.props</i> (RMI) or <i>soap.client.props</i> (SOAP) files.	ITCAM_USER= <i>user_id</i>

Table 3. List of options for the *setupwas.sh* script (continued)

Command-line option	Description	Equivalent environment variable and value
<code>-password password</code>	The password to use for connection to <code>wsadmin.sh</code> . This is required if Global Security is enabled and it is not set in the <code>sas.client.props</code> (RMI) or <code>soap.client.props</code> (SOAP) files.	<code>ITCAM_PASSWORD=password</code>
<code>-wasroot path</code>	The configuration directory for IBM WebSphere Application Server (<i>AppServer_home</i>). It is the partial path to the <code>wsadmin.sh</code> file. For example: <code>/u/WAS600/Servers/AppServer</code> If you specify a value for <code>-wsadmin</code> , this option will be ignored. Note: Specifying more of the path to the <code>wsadmin.sh</code> script results in a quicker location of the <code>wsadmin.sh</code> script.	<code>ITCAM_WASROOT=AppServer_home</code>
<code>-wsadmin path_and_file</code>	Specifies the full path to the <code>wsadmin.sh</code> file. For example: <code>/u/WAS600/Servers/AppServer/profiles/default/bin/wsadmin.sh</code> This option is required if running in batch mode and the default <code>wsadmin.sh</code> script that <code>setupwas.sh</code> selects is not acceptable.	<code>ITCAM_WSADMIN=path_and_file</code>
<code>-temahost IP_or_host</code>	The fully-qualified host name or IP address for the host where the Monitoring Agent is located. The monitoring agent must run on the same host as the application server. For that reason, <code>127.0.0.1</code> or <code>localhost</code> is always a correct choice. For instructions on configuring the monitoring agent, see “Configuring the monitoring agent on z/OS” on page 99.	<code>ITCAM_TEMAHOST=IP_or_host</code>
<code>-temaport port</code>	The port number used for the Monitoring Agent. The product-provided default is 63335.	<code>ITCAM_TEMAPORT=port</code>
<code>-temagc</code>	Enable monitoring agent garbage collection monitoring. The default is not to enable.	<code>ITCAM_TEMAGC=y</code>
<code>-gcoutput</code>	If monitoring garbage collection, sets ITCAM to output the records to the IBM WebSphere Application Server SYSOUT log. The default is to set ITCAM to suppress the records.	<code>ITCAM_GCOUTPUT=y</code>
<code>-itcam -noitcam</code>	If <code>-itcam</code> is specified, Data Collector support for ITCAM for Application Diagnostics Managing Server will be configured. If running in prompt mode, this option sets the default, which you can override when answering the prompt. If running in batch mode, setting the value for the option or environmental variable specifies the value for the parameter.	<code>ITCAM_ITCAM=y</code>

Table 3. List of options for the *setupwas.sh* script (continued)

Command-line option	Description	Equivalent environment variable and value
-smf -nosmf -leavesmf	If -smf is specified and Data Collector support for the Visualization Engine (Application Monitor) user interface will be configured, IBM WebSphere Application Server will be set to write SMF performance records. If -nosmf is specified, IBM WebSphere Application Server will be set to not write SMF performance records. If -leavesmf is specified, no changes will be made to WebSphere SMF data collection. If running in prompt mode, this option sets the default, which you can override when answering the prompt. If running in batch mode, setting the value for the option or environmental variable specifies the value for the parameter.	ITCAM_SMF=y n leave
-kernelip <i>IP_or_host</i>	The IP address or host name for the Managing Server's Kernel. The default is 127.0.0.1 (which is not an acceptable value since the Managing Server is not supported on z/OS). If you are configuring support for the Managing Server, you must specify the address either by using this option or environment variable, or by entering a value at the prompt. The IP address or host name must be reachable from the Data Collector host.	ITCAM_KERNELIP= <i>IP_or_host</i>
-rfsport01 <i>port</i>	The port number of the Managing Server Remote File Sharing (RFS) server. The default is 9120.	ITCAM_RFSPORT01= <i>port</i>
-rfsport02 <i>port</i>	The port number of the RFS server for the secondary Kernel. This only applies if an additional Kernel was created for the Managing Server. See customization chapters in the <i>IBM Tivoli Composite Application Manager: Managing Server Installation and Customization Guide</i> . The default is 9121.	ITCAM_RFSPORT02= <i>port</i>
-kernelport01 <i>port</i>	The port number of the Managing Server codebase server. The default is 9122.	ITCAM_KERNELPORT01= <i>port</i>
-kernelport02 <i>port</i>	The port number of the Managing Server codebase server. This only applies if an additional Kernel was created for the Managing Server. See the one of the customization chapters in the <i>IBM Tivoli Composite Application Manager: Managing Server Installation and Customization Guide</i> . The default is 9123.	ITCAM_KERNELPORT02= <i>port</i>

Table 3. List of options for the `setupwas.sh` script (continued)

Command-line option	Description	Equivalent environment variable and value
<code>-mshome MS_home</code>	The Managing Server installation directory. If the runtime configuration script is able to connect to the Managing Server and retrieve the value of <code>MS_home</code>, this option will be ignored. But if you are configuring support for the Managing Server and the runtime configuration script is not able to connect to the Managing Server and retrieve the value of <code>MS_home</code>, the value specified for this option will be used. The following examples of the format you must use when entering the path are the defaults: - Managing Server on Windows: C:\\IBM\\itcam\\WebSphere\\MS Note: - When you are specifying a Windows directory path as a command-line option (<code>-mshome</code>) or as an environment variable (<code>ITCAM_MSHOME</code>), you must use double backslashes (<code>\\</code>). This is different from when you enter the value for <code>MS_home</code> at the prompt, where you would use single backslashes (<code>\\</code>). - When using the <code>-mshome</code> command-line option, if the full name contains any blank characters, you must use the short name without blanks. When using the <code>ITCAM_MSHOME</code> environment variable, embedded blanks present in the name are acceptable. - Managing Server on UNIX: /opt/IBM/itcam/WebSphere/MS - Managing Server on Linux: /opt/ibm/itcam/WebSphere/MS	<code>ITCAM_MSHOME=MS_home</code>
<code>-nomshomeconnect</code>	Do not contact the running Managing Server to get the Managing Server home path. The default, if you are configuring support for the Managing Server, is to contact it. Only use this option for abnormal situations when the Managing Server returns an incorrect home path.	<code>ITCAM_MSHOMECONNECT=n</code>

Table 3. List of options for the *setupwas.sh* script (continued)

Command-line option	Description	Equivalent environment variable and value
<code>-cleanupplugins</code>	For IBM WebSphere Application Server 6.1, attempt to remove any ITCAM IBM WebSphere Application Server plugin files and directories created for Data Collector versions before 6.1 Fix Pack 4. Default is to retain the existing files and directories. Versions of the Data Collector since 6.1 Fix Pack 4, including the current version, no longer need IBM WebSphere Application Server plugins. These plugins, therefore, may be safely removed unless a version of the ITCAM Data Collector older than 6.1 Fix Pack 4 monitors any Application Server in the node. If Data Collector versions before 6.1 Fix Pack 4 were never configured for this application server instance, the plugins were not created. In this case, the option will have no effect.	<code>ITCAM_CLEANUPPLUGINS=y</code>
<code>-defaulthostname</code> <i>IP_or_host</i>	Using the value returned by running the <code>hostname</code> command as the host name is usually acceptable in most environments, but in some environments, that value will not work. If running the <code>hostname</code> command returns a value that is not usable for configuring the Data Collector, you can use the <code>-defaulthostname</code> option. The <code>-defaulthostname</code> option specifies the fully-qualified host name or IP address that will replace the value of the local host name for all purposes in configuring the Data Collector, such as for the bind IP or export IP.	<code>ITCAM_DEFAULTHOSTNAME=IP_or_host</code>
<code>-defaulthostip</code> <i>IP</i>	The <code>-defaulthostip</code> option overrides the IP address derived from <code>-defaulthostname</code> . This option is normally not needed.	<code>ITCAM_DEFAULTHOSTIP=IP</code>
<code>-dmgrhost</code> <i>IP_or_host</i>	For an ND environment, the Deployment Manager's RMI fully-qualified host name or IP address. The default is the deployment manager hostname as known to WebSphere.	<code>ITCAM_DMGRHOST=IP_or_host</code>
<code>-localhost</code> <i>hostname</i>	Used for a <code>findServers</code> node match if there is a problem identifying nodes. This is only meaningful if the <code>WAS_NODE</code> associated with <code>wsadmin.sh</code> is not usable. The default is the value entered for the <code>-defaulthostname</code> option.	<code>ITCAM_LOCALHOST=hostname</code>
<code>-localip</code> <i>IP_address</i>	Used for a <code>findServers</code> node match if there is a problem identifying nodes. This is only meaningful if the <code>WAS_NODE</code> associated with <code>wsadmin.sh</code> is not usable. The default is the value entered for the <code>-bindip</code> option.	<code>ITCAM_LOCALIP=IP_address</code>
<code>-bindip</code> <i>IP_or_host</i>	The listening IP address or fully-qualified host name to be used for the TCP/IP connection. The default is the first (or only) IP address on the host system. Make sure a local IP address, and not a VIPA IP address, is specified.	<code>ITCAM_BINDIP=IP_or_host</code>

Table 3. List of options for the `setupwas.sh` script (continued)

Command-line option	Description	Equivalent environment variable and value
<code>-exportip IP_or_host</code>	Indicates the IP address or fully qualified host name that will be used by the Data Collector to communicate with the Managing Server. If there is more than one Network Interface Card (NIC) or multiple IP addresses configured on the Data Collector host, choose one of them. The default is the value entered for <code>-bindip</code> .	<code>ITCAM_EXPORTIP=IP_or_host</code>
<code>-nottransform</code>	Do not run the <code>wsc2n.sh</code> script after configuring the Data Collector. The default is to run the <code>wsc2n.sh</code> script, which transforms the changed IBM WebSphere Application server configuration files into the formats that the application server uses. This script is started for diagnostic purposes; it checks for any configuration errors. However, you can use the <code>-nottransform</code> option to avoid running it. The configuration files will be transformed when you restart the application server; any configuration error will be logged, and may cause the restart to fail. Only use <code>-nottransform</code> if you are reasonably confident there are no configuration errors.	<code>ITCAM_TRANSFORM=n</code>

Specifying values for directory paths, user names, or passwords when running the runtime setup script

The rules for which characters are allowed for particular operands are different. Characters that are allowed in a directory path might not be allowed in a user ID.

Also, some rules might be dictated by the security system being used. If the security system is RACF, then the user ID must start with an alphabetic character, #, \$ or @. (These are the characters in a US English code page. In other international code pages, the actual character might be different. For example, \$ is usually the national currency symbol.)

The following rules apply to user IDs in TSO/RACF:

- 1-8 alphanumeric characters
- The user ID can consist entirely of numbers and need not begin with any particular character.
- For RACF users that are TSO users,, the user ID cannot exceed seven characters and must begin with an alphabetic, X'7B' (#), X'5B' (\$), or X'7C' (@) character.

The following rules apply to passwords in TSO/RACF:

- 1-8 alphanumeric characters
- Each installation can define its own password syntax rules.
- Lowercase alphanumeric characters are valid and maintained in the case entered if `SETR PASSWORD(MIXEDCASE)` is in effect.

The rules for characters allowed in filename and directory paths are dictated by UNIX System Services:

- A file name can be up to 255 characters long.
- To be portable, the file name must use only the characters in the POSIX portable file name character set:
 - Uppercase or lowercase, A to Z

- Numbers, 0 to 9
- Period (.)
- Underscore (_)
- Hyphen (-)
- A file path consists of a series of file names representing directories, separated with the forward-slash (/) character.

The ITCAM scripts do not attempt to filter or validate operands provided that might be used as user IDs, groups, files, servers, and so on. The underlying operating system and subsystems will provide return codes and error messages if the names provided do not meet their specific criteria.

Step 5c: upgrading monitoring of an application server instance monitored by a previous version of the Data Collector

If an application server instance was monitored by ITCAM for WebSphere Data Collector version 6.0, ITCAM for WebSphere Data Collector 6.1 (also shipped with ITCAM for Web Resources 6.2), or ITCAM for WebSphere Application Server 7.0 or 7.1 (shipped with WebSphere Application Server), you can upgrade monitoring for it to ITCAM Agent for WebSphere Applications Data Collector version 7.1. To do this, follow the instructions in this step.

Upgrading monitoring from Data Collector version 6.0

If the application server instance is monitored by ITCAM for WebSphere Data Collector version 6.0, you must unconfigure the old Data Collector from this instance before configuring the new Data Collector.

Perform one of the following procedures, depending on how you configured the version 6.0 Data Collector:

- If you configured the version 6.0 Data Collector using the `setupwas.sh` configuration script, follow the instructions in Chapter 5, “Unconfiguring the Data Collector on IBM z/OS,” on page 87. You must log in as the root user before executing the unconfiguration script. If the Data Collector is configured to monitor several instances of the application server, you must unconfigure it for each of the instances.
- If you did not configure the version 6.0 Data Collector using the `setupwas.sh` configuration script, uninstall the version 6.0 Data Collector using the instructions in the ITCAM for WebSphere 6.0 installation and customization guide at the following Web site:

http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?topic=/com.ibm.itcamwas.doc_6.0/updates/cynmst_60_full451.htm

The unconfiguration script will not work if you did not use the `setupwas.sh` configuration script when configuring the version 6.0 Data Collector.

Then, run the setup script in prompt mode (see “Step 5d: executing the runtime setup script in prompt mode” on page 36) or in batch mode (see “Step 5e: executing the runtime setup script in batch” on page 41). You will need to set up all setup parameters, as in a new configuration.

Upgrading monitoring from Data Collector version 6.1 or ITCAM for WebSphere Application Server 7.0 or 7.1

If the application server instance is monitored by ITCAM for WebSphere Data Collector 6.1 (also shipped with ITCAM for Web Resources 6.2) or ITCAM for

WebSphere Application Server 7.0 or 7.1 (shipped with WebSphere Application Server), you can simply run the `setupwas.sh` script to configure monitoring with the new version of the Data Collector.

If you are upgrading from ITCAM for WebSphere Data Collector 6.1, you can preserve the setup parameters used for installation of the previous version. To do this, use the `migratecfg.sh` script before running the setup script. The `migratecfg.sh` script can also run the setup script itself.

Important: Do not run `migratecfg.sh` to upgrade from ITCAM for WebSphere Application Server 7.0 or 7.1. In this case, proceed to “Step 5d: executing the runtime setup script in prompt mode” on page 36 or “Step 5e: executing the runtime setup script in batch” on page 41.

Change to the `config_home/bin` directory (by default, `/u/itcam71/bin`) and run the `migratecfg.sh` script from that directory. The parameters for the script are set out in Table 4.

If you do not specify the `-runsetup` parameter, the script will save the monitoring configuration. You will need to run `setupwas.sh` to upgrade monitoring of the instance; the existing configuration will be picked up automatically.

If you specify the `-runsetup` parameter, the script will save the monitoring configuration and run `setupwas.sh` to upgrade monitoring of the instance. You may need to specify several parameters to override defaults settings for `setupwas.sh`. These parameters are set out in Table 5 on page 34; if you do not specify any of them, the existing settings are used.

Table 4. List of options for the `migratecfg.sh` script

Command-line option	Description	Equivalent environment variable and value
<code>-source old_runtime_dir</code>	The full path to the old Data Collector runtime directory for the application server instance. It is <code>old_config_home/runtime/appserver_version.node_name.server_name</code> , where <code>old_config_home</code> is the configuration home directory of the old Data Collector. You must specify this value, either in the parameter or environment variable or in a script prompt.	<code>ITCAM_SOURCE=old_runtime_dir</code>
<code>-runsetup</code>	If specified, runs the <code>setupwas.sh</code> script after saving the existing configuration. In this way, the entire upgrade process is completed in one script run. The default is only to save the existing configuration. They are used when the <code>setupwas.sh</code> script is run later.	<code>ITCAM_RUNSETUP=y</code>
<code>-batch</code>	If specified, no prompting will be done. The script will terminate if necessary parameters are not specified or not valid. Required to run the script in batch mode. If <code>-runsetup</code> is specified, the <code>setupwas.sh</code> script will be run in batch mode as well.	<code>ITCAM_BATCH=y</code>

Table 4. List of options for the *migratecfg.sh* script (continued)

Command-line option	Description	Equivalent environment variable and value
-debug	Adds diagnostic trace information to the standard output. Use this parameter if you encounter problems and need IBM technical support. The default is to refrain from putting out the extra diagnostic information.	ITCAM_DEBUG=y
-help	Usage help	N/A. Available as an option on the command line only.

Table 5. List of options for the *migratecfg.sh* script that override default settings for *setupwas.sh*

Command-line option	Description	Equivalent environment variable and value
-host <i>host</i>	The fully-qualified host name or IP address used by <i>wsadmin.sh</i>. If you are in an ND environment, enter the value for the host for the Deployment Manager. You can use <i>localhost</i> in a stand-alone environment, or in an ND environment when the Deployment Manager is located on the local host. The host name is read from the old Data Collector configuration. You can override it using this parameter.	ITCAM_HOST= <i>host_name</i>
-conntype SOAP RMI	The connection type for communications used by <i>wsadmin.sh</i>. The default is to use the connection type specified in the <i>wsadmin.properties</i> file associated with the <i>wsadmin.sh</i> script you have chosen. (The IBM WebSphere Application Server default for this parameter is SOAP.)	ITCAM_CONNTYPE= <i>connect_type</i>
-port <i>port</i>	The port number used by <i>wsadmin.sh</i>. In a Network Deployment (ND) environment, specify the Deployment Manager's SOAP or RMI port (not the application server instance SOAP or RMI port). To find the SOAP port number in the control region job log, look for the following string: BB000222I: ADMC0013I: The SOAP connector is available at port <i>port</i> To find the RMI port number in the control region job log, look for the following string: BB000222I: ADMC0026I: The RMI connector is available at port <i>port</i> The default is to use the port specified in the <i>wsadmin.properties</i> file associated with the <i>wsadmin.sh</i> script for the application server instance.	ITCAM_PORT= <i>port</i>

Table 5. List of options for the *migratecfg.sh* script that override default settings for *setupwas.sh* (continued)

Command-line option	Description	Equivalent environment variable and value
<code>-user <i>user_id</i></code>	The user ID to use for connection to <i>wsadmin.sh</i> . This is required if Global Security is enabled and it is not set in the <i>sas.client.props</i> (RMI) or <i>soap.client.props</i> (SOAP) files.	<code>ITCAM_USER=<i>user_id</i></code>
<code>-password <i>password</i></code>	The password to use for connection to <i>wsadmin.sh</i> . This is required if Global Security is enabled and it is not set in the <i>sas.client.props</i> (RMI) or <i>soap.client.props</i> (SOAP) files.	<code>ITCAM_PASSWORD=<i>password</i></code>
<code>-profile <i>profile_script</i></code>	Specifies a profile script for running <i>wsadmin.sh</i> . The Web site for IBM WebSphere Application Server provides the following description of a profile script: "The profile script runs before other commands, or scripts. If you specify <code>-c</code> , the profile script runs before it invokes this command. If you specify <code>-f</code> , the profile script runs before it runs the script. In interactive mode, you can use the profile script to perform any standard initialization that you want. You can specify multiple <code>-profile</code> options on the command line, and they invoke in the order that you supply them."	<code>ITCAM_PROFILE=<i>script</i></code>
<code>-owner <i>user[:group]</i></code>	Ownership of the directories and files created during installation. For example: <code>wsadmin:wscfg</code> Default is none. Root access will be required if this parameter is used.	<code>ITCAM_OWNER=<i>user[:group]</i></code>
<code>-access <i>permission</i></code>	Permission to set for the directories and files created during installation. For example: <code>u=rwX,g=rwX,o=rX</code> Default is none. Root access will be required if this parameter is used.	<code>ITCAM_ACCESS=<i>permission</i></code>
<code>-defaulthostname <i>IP_or_host</i></code>	Using the value returned by running the <i>hostname</i> command as the host name is usually acceptable in most environments, but in some environments, that value will not work. If running the <i>hostname</i> command returns a value that is not usable for configuring the Data Collector, you can use the <code>-defaulthostname</code> option. The <code>-defaulthostname</code> option specifies the fully-qualified host name or IP address that will replace the value of the local host name for all purposes in configuring the Data Collector, such as for the bind IP or export IP.	<code>ITCAM_DEFAULTHOSTNAME=<i>IP_or_host</i></code>
<code>-defaulthostip <i>IP</i></code>	The <code>-defaulthostip</code> option overrides the IP address derived from <code>-defaulthostname</code> . This option is normally not needed.	<code>ITCAM_DEFAULTHOSTIP=<i>IP</i></code>
<code>-localip <i>IP_address</i></code>	Used for a <i>findServers</i> node match if there is a problem identifying nodes. This is only meaningful if the <i>WAS_NODE</i> associated with <i>wsadmin.sh</i> is not usable. The default is the value entered for the <code>-bindip</code> option.	<code>ITCAM_LOCALIP=<i>IP_address</i></code>

If you have successfully run `migratecfg.sh` with the `-runsetup` parameter, the configuration script for upgrading monitoring of the application server instance is complete. Proceed to “Step 6: additional configuration tasks” on page 43.

If you have successfully run `migratecfg.sh` without the `-runsetup` parameter, you must run the `setupwas.sh` script to upgrade monitoring of the application server instance. The existing configuration settings will be used, but you can override them using `setupwas.sh` parameters. Run the setup script in prompt mode (see “Step 5d: executing the runtime setup script in prompt mode”) or in batch mode (see “Step 5e: executing the runtime setup script in batch” on page 41).

Attention: The `migratecfg.sh` and `setupwas.sh` scripts do not remove the runtime directory for the old version of the Data Collector. After upgrading monitoring to the new version, you can remove the old runtime directory manually.

Step 5d: executing the runtime setup script in prompt mode

Perform the following procedure to execute the runtime setup script in prompt mode:

Note: In the prompts that occur when executing the runtime setup script in prompt mode, if a default value is applicable, it will be shown in brackets at the end of the prompt. If no value is entered, the default value will be used. The default value also serves as an example of the format of the value that is required.

1. If WebSphere Global Security is enabled, log in as a WebSphere administrator, which will be able to administer the application server configuration.
2. If you are running the application server in a Network Deployment environment, make sure the Deployment Manager and the node agent are running. If you need to restart the node agent, instructions are at the following Web site:
http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.zseries.doc/info/zseries/ae/txml_restartnodeagent.html
3. If you are running the application server in a non-ND environment, make sure the instance of the application server that is being monitored by the Data Collector is running. If it is not, start the instance of the application server that is being monitored by the Data Collector.
4. If you will be configuring the Data Collector to be used with the Managing Server and Visualization Engine (Application Monitor) user interface, if it is not already running, start the Managing Server and the Visualization Engine (Application Monitor) user interface.
5. If you want to set any of the configuration options as environment variables before running the runtime setup script, export the environment variables. See the right-hand column of Table 3 on page 24 for a list of the environment variables. Here are examples of how to export an environment variable from a command line:

```
export ITCAM_CONNTYPE=RMI
export ITCAM_MSHOME=/opt/IBM/itcam/WebSphere/MS
```

By exporting these variables, the `setupwas.sh` script will use them as the new default values. You will not need to enter a value (simply press **Enter**) when you are prompted for them.

6. Run the following command from the `config_home/bin` directory:

```
./setupwas.sh [options]
```

The default path for the location of the script is `/u/itcam71/bin`.

See Table 3 on page 24 for a list of the options for running the script command.

If you set any options in the command line, the `setupwas.sh` script will use them as the new default values. You will not need to enter the values again; simply press **Enter** when you are prompted for them.

Some prompts may be skipped if `setupwas.sh` has only found one option (for example, only one IP address or `wsadmin.sh` file).

If there are multiple IP addresses for the host where the Data Collector is being configured, you will be prompted to select an IP address:

Select host IP address:

- 1) 9.42.6.136
- 2) 199.999.44.99
- 3) 192.111.22.44

Enter selection: 1

7. Enter the number that corresponds to the correct IP address. Make sure a local IP address, and not a VIPA address, is selected.

You will be prompted for the path of *AppServer_home*:

Enter the path of the WAS user install root [/u/WAS70]:

8. Enter the path name of *AppServer_home* and press **Enter**.

You must respond with a valid path name, for example, `/u/WAS600/DeployMgr/DeploymentManager`.

The ITCAM for Application Diagnostics configuration script uses this path to search for the `wsadmin.sh` script that will be used to configure the target application server for ITCAM monitoring.

You will be prompted to select one of the discovered occurrences of the `wsadmin.sh` script:

Searching for `wsadmin.sh`. Please wait...

Found `wsadmin.sh` in the following locations:

- 1) `/u/WAS600/DeployMgr/DeploymentManager/bin/wsadmin.sh`
WAS home is `/u/WAS600/DeployMgr/DeploymentManager`
Node PLEX1Manager in cell PLEX1Network is type DMGR
- 2) `/u/WAS600/DeployMgr/DeploymentManager/profiles/default/bin/wsadmin.sh`
WAS home is `/u/WAS600/DeployMgr/DeploymentManager`
Node PLEX1Manager in cell PLEX1Network is type DMGR

Enter the number of the `wsadmin.sh` to use [2]:

9. Enter the number that corresponds to the path for the appropriate `wsadmin.sh` script and press **Enter**.

Note: You may use any one of the listed `wsadmin.sh` scripts. In general any application server `wsadmin.sh` script will work, but the one under *AppServer_home/profiles/default/bin* for the application server instance you are configuring is usually the most appropriate. The `wsadmin.sh` script will use the `wsadmin.properties` file associated with it.

The script will check for the application server version and use the `wsadmin.sh` that you selected to find all server instances that are configured on this node. Then you will be prompted to select one of the discovered instances of the application server:

Node: TVT6007

- 1) BBOS001
- 2) BBOS003

- 3) BBOSBVT
- 4) BBOSFP5
- 5) BBOSNVW
- 6) bbose1j

Enter the number of the server to select:

Note:

- a. The list normally does not include Deployment Manager or Node Manager servers.
 - b. If the server was specified using the `-server` command line option or the `ITCAM_SERVER` environment variable, `setupwas.sh` will not show this prompt.
10. Enter the number that corresponds to the name of the server for the appropriate instance of the application server that you want to monitor and press **Enter**.

If there are already subdirectories with the configuration files for that application server instance in the runtime directory (for example if the instance of the application server has already been configured for ITCAM for Application Diagnostics and you are now updating the configuration), the script will ask you whether you want to overwrite (instead of removing and recreating) the runtime directory for the application server instance that is being configured:

The ITCAM configuration already exists:
 /u/ibm1/abc610/usr/lpp/itcam/WebSphere/DC/runtime/was61.ABC01.IBM123
 You may retain this directory and replace the configuration and connection files within, or you may remove it and start over fresh.
 Do you wish to remove the was61.ABC01.IBM123 directory? (y|n):

11. If that prompt displays, enter y or n and press **Enter**.

In the case when there are already subdirectories with the configuration files for that server in the runtime directory, entering y indicates that you want to remove the existing runtime directory. A new runtime directory with a configuration for the application server instance will be created instead of the existing runtime directory being retained but overwritten.

Whether you enter y or enter n, the customized property files are always completely re-created. However, when you enter n, the `.id` and `.mod` files from the previous configuration are kept. If you enter n:

- You will not have to re-apply a configuration to the Data Collector in the Visualization Engine (Application Monitor) user interface. In other words you will not have to use the Unconfigured Data Collector Overview page to configure the Data Collector, as described in the Visualization Engine (Application Monitor) user interface online helps.
- The Data Collector history remains available under the original Data Collector server name in the Visualization Engine (Application Monitor) user interface.

You will be prompted for the listening port of the Monitoring Agent:

Enter the port number of the TEMA agent or "none" [63335]:

Note: The Monitoring Agent is installed separately. Check the Monitoring Agent installation and configuration options for the port number of the Monitoring Agent, which must be installed on the same IBM z/OS host as the Data Collector.

12. Enter the port number and press **Enter**. The default for the port number is 63335. If you do not want the Data Collector to communicate with the monitoring agent (in a deep dive diagnostics only installation), enter none. You will be prompted whether you want the Monitoring Agent to monitor Garbage Collection:

Do you want TEMA to monitor Garbage Collection? (y|n):

Enter y only if Garbage Collection in the Tivoli Enterprise Portal is needed; otherwise, enter n. Then press **Enter**.

You will be prompted whether you want the Data Collector to communicate with the Managing Server:

Do you wish to configure the Data Collector to use the ITCAM Managing Server? (y|n):

13. Enter y or n and press **Enter**.

If you entered n, go to Step 18 on page 41.

You will be prompted for the IP address (or fully qualified host name) of the Managing Server:

Enter the IP address or host name of the ITCAM Managing Server [127.0.0.1]:

14. Enter the IP address (or fully qualified host name) of the Managing Server and press **Enter**.

Note: The prompt default is the IP loopback address (127.0.0.1). You can never use this address as the host name of the Managing Server for an IBM z/OS Data Collector, because the Managing Server is not supported on this platform. It is used as an example of the format of the response required, for example, 9.52.106.25.

You will be prompted for the Managing Server codebase port:

Enter the MS Codebase Port [9122]:

15. Enter the Managing Server codebase port. The default is 9122.

The configuration script then attempts to connect to the Managing Server and retrieve the value for *MS_home*. If successful, it produces a message similar to the following text:

```
URL being tested: http://tio-lnx-s01.usca.ibm.com:
9122/../../ITCAM61_MS_CONTEXT.properties
Successfully acquired MSHOME value of D:\IBM\itcam\WebSphere\MS2
```

If connection to the Managing Server is not successful, you will be prompted to enter the value for *MS_home*:

Enter ITCAM Managing Server install directory [/opt/IBM/itcam/WebSphere/MS]:

In this case, enter the installation directory of the Managing Server (*MS_home*) on the host where the Managing Server is located, and press **Enter**. Specify the directory name as you normally would for the platform on which the Managing Server is installed:

Table 6. Specifying the location of *MS_home*

Platform for Managing Server	Default value
Windows	C:\IBM\itcam\WebSphere\MS Note: In this situation where you are being prompted for the value of <i>MS_home</i> use single backslashes (\). This is different from when you enter the value for <i>MS_home</i> at the command line with the <i>-mshome</i> option or with the ITCAM_MSHOME parameter, where you would use double backslashes (\\).
UNIX	/opt/IBM/itcam/WebSphere/MS
Linux	/opt/ibm/itcam/WebSphere/MS

After *MS_home* has been retrieved (or entered), you will be prompted for whether you want to collect SMF data:

Do you wish to collect WebSphere SMF data? (y|n|leave):

Attention: The use of virtual memory and CPU time by IBM WebSphere Application Server can be substantially increased by activating the SMF option.

16. Enter y or n and press **Enter**. If the Data Collector communicates with the Managing Server, or if garbage collection (GC) analysis is enabled for the Monitoring Agent, verbose garbage collection logging is enabled for the servant JVMs (using the JVM argument *-verbose:gc*). The Data Collector analyzes GC activity by intercepting the verbose GC log data as it is being written to SYSOUT. The Data Collector can be configured to suppress writing the data to SYSOUT (after it has been analyzed), or allow the data to be written. Allowing the verbose GC data to be written will consume JES spool space.

JVM Garbage Collection information will be gathered.
You may eliminate the output of the GC log from
SYSOUT in order to conserve SP00L space.

Do you wish GC log data included in output? (y|n) [n]:

17. Enter y or n. Select n unless GC information is needed in the SYSOUT file. You will then be provided with a summary of all the parameters provided followed by a prompt asking you if you want to proceed with the configuration:

Setup will create an ITCAM runtime with the following parameters:

- 1) wsadmin location :

/u/WAS600/DeployMgr/DeploymentManager/profiles/default/bin/wsadmin.sh
- 2) WAS server name : bboselj

WAS version : 6.0.2.18 ND
Deployment : Network Deployment
- 3) ITCAM for Tivoli Enterprise Portal Interface

TEMA Host : 127.0.0.1
TEMA Port : 63335
Monitor GC : Yes
GC Log Output : Delete
- 4) ITCAM for Tivoli Application Monitor Interface : Yes

```
ITCAM MS host      : tio-lnx-s01.usca.ibm.com
Codebase port      : 9122
ITCAM MS home      : D:\IBM\itcam\WebSphere\MS2
Collect SMF data   : Yes
```

Enter item number to modify, 'y' to accept, or 'n' to cancel:

18. Take one of the following actions:

- Enter y to accept the configuration. Then press **Enter**.

Note: The `setupwas.sh` script can be safely re-run over an already configured application server.

- Enter n to exit the runtime setup script. Then press **Enter**.

Up to this point, no configuration changes have been made, it is safe to exit at this point and nothing will have been done to your IBM WebSphere Application Server configuration.

- If the parameters for one of the numbered items are not correct, modify the configuration information by entering the item number and pressing **Enter**. The script will prompt you for that information again.

The script displays summary information (unless you entered n to exit the runtime setup script). Then it begins configuration.

19. If you have a Network Deployment environment, run the script for each server you wish to monitor. The script must be run on the host associated with the node that owns the server.

20. The runtime setup script creates a log of all the configuration operations that it performs. You can review the log for any error conditions, and you might be requested to provide the log contents to IBM software support. The log file is called `setupwas.log` and is located under the `config_home`. For example, `/u/itcam71/runtime/setupwas.log`.

For successful configuration look for messages similar to the following text:

```
ITCAM 7.1 setupwas.sh configuration completed for
/u/ejack/Runtimes/HAAD710/runtime/was60.TVT6007.bboslj
```

The runtime configuration script provides basic Data Collector configuration, but it does not cover all of the advanced options that the Data Collector is capable of delivering. Refer to the sections that describe configuration of advanced options. See Chapter 4, “Customization and advanced configuration for the Data Collector,” on page 45.

What to do next

See “Step 6: additional configuration tasks” on page 43.

Step 5e: executing the runtime setup script in batch

Executing the runtime setup script in batch eliminates the need for command-line-execution prompting. You can either enter values for environmental variables in the CYNZSETU batch job and submit it as a z/OS JCL job that uses BPXBATCH, or you can execute the `setupwas.sh` script through a command line.

Perform one of the following procedures to execute the runtime setup script in batch (auto-run) mode:

- “Editing the CYNZSETU batch job and submitting it as a z/OS JCL job that uses BPXBATCH” on page 42
- “Executing the `setupwas.sh` script through a command line” on page 42

Editing the CYNZSETU batch job and submitting it as a z/OS JCL job that uses BPXBATCH

A sample batch job is provided in the SMP/E install dataset, CYN.SCYNINST member CYNZSETU. This job runs the `setupwas.sh` script using the UNIX System Services batch processor, BPXBATCH. To run the script using this job, perform the following procedure:

1. If WebSphere Global Security is enabled, log in as a WebSphere administrator, which will be able to administer the application server configuration.
2. If you are running the application server in a Network Deployment environment, make sure the Deployment Manager and the node agent are running. If you need to restart the node agent, instructions are at the following Web site:

`http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.zseries.doc/info/zseries/ae/txml_restartnodeagent.html`
3. If you are running the application server in a non-ND environment, make sure the instance of the application server that is being monitored by the Data Collector is running. If it is not, start the instance of the application server that is being monitored by the Data Collector.
4. Copy the sample batch job CYNZSETU to a dataset with similar attributes (changes made to the target library may be overwritten by future maintenance).
5. Using TSO/ISPF Edit, modify the environment variables appropriately.
See Table 3 on page 24 for the list of environment variables.
6. Save the batch job file you modified in Step 5.
7. In TSO, submit a z/OS JCL job using the contents of the file you modified in Step 5, which uses BPXBATCH.

Using a z/OS JCL submitted job with BPXBATCH is advantageous if you want to produce a record or do not want to tie up your terminal.

Resolve any security issues you encounter when running the job.
8. The runtime setup script creates a log of all the configuration operations that it performs. You can review the log for any error conditions, and you might be requested to provide the log contents to IBM software support. The log file is called `setupwas.log` and is located under the `config_home`. For example, `/u/itcam71/runtime/setupwas.log`.

For successful configuration look for messages similar to the following text:

Successfully configured data collector for server ibm001

The runtime configuration script provides basic ITCAM for Application Diagnostics configuration, but it does not cover all of the advanced options that ITCAM for Application Diagnostics is capable of delivering. See Chapter 4, “Customization and advanced configuration for the Data Collector,” on page 45 for instructions for customization and configuration of advanced options.

What to do next: See “Step 6: additional configuration tasks” on page 43.

Executing the `setupwas.sh` script through a command line

Perform the following procedure to execute the runtime setup script in batch (auto-run) mode by executing the `setupwas.sh` script through a command line:

1. If WebSphere Global Security is enabled, log in as a WebSphere administrator, which will be able to administer the application server configuration.

2. If you are running the application server in a Network Deployment environment, make sure the Deployment Manager and the node agent are running. If you need to restart the node agent, instructions are at the following Web site:

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.zseries.doc/info/zseries/ae/txml_restartnodeagent.html

3. If you are running the application server in a non-ND environment, make sure the instance of the application server that is being monitored by the Data Collector is running. If it is not, start the instance of the application server that is being monitored by the Data Collector.
4. Run `setupwas.sh` from a command line.

Perform the same procedure as you would for running `setupwas.sh` in prompt mode (see “Step 5d: executing the runtime setup script in prompt mode” on page 36), but indicate all the options you want to specify at the command line (or by exporting the corresponding environment variable prior to running `setupwas.sh`). Make sure to indicate options that are required for running in batch mode (see Table 3 on page 24 for the list of options, especially those that are required for running in batch mode).

5. The runtime setup script creates a log of all the configuration operations that it performs. You can review the log for any error conditions, and you might be requested to provide the log contents to IBM software support. The log file is called `setupwas.log` and is located under the `config_home`. For example, `/u/itcam71/runtime/setupwas.log`.

For successful configuration look for messages similar to the following text:

Successfully configured data collector for server ibm001

The runtime configuration script provides basic ITCAM for Application Diagnostics configuration, but it does not cover all of the advanced options that ITCAM for Application Diagnostics is capable of delivering. See Chapter 4, “Customization and advanced configuration for the Data Collector,” on page 45 for instructions for customization and configuration of advanced options.

What to do next: See “Step 6: additional configuration tasks.”

Step 6: additional configuration tasks

Perform the following steps:

1. Performance Monitoring Infrastructure (PMI) has been enabled (if it was not already enabled) to default settings when you ran the runtime setup script. This is a requirement for Data Collector configuration. In addition, by default, the Data Collector configuration modifies the PMI collection levels based on the Application Monitor's Monitoring Level (MOD) at WebSphere startup. Thus it overrides whatever PMI settings you have already set. For the procedure to modify PMI settings, or to prevent the Data Collector from modifying PMI collection levels, see “Modifying Performance Monitoring Infrastructure settings” on page 65.
2. Restart the instance of the application server that will be monitored by the Data Collector.
3. Perform the tasks described in each of the following sections, if applicable.

Step 6a: verifying the configuration for data collection for the Visualization Engine (Application Monitor) user interface

This section describes how to verify the configuration of Data Collectors that will be used with the Managing Server (Visualization Engine (Application Monitor) user interface). Perform this procedure if you are using ITCAM for Application Diagnostics Managing Server.

Note: During the configuration, you must have:

1. Restarted the instance of the application server that will be monitored by the Data Collector.
2. If it was not already running, started the Managing Server and the Visualization Engine (Application Monitor) user interface.

Perform the following procedure:

1. Verify that the Data Collector components are enabled and running in the Self-Diagnosis page of the Visualization Engine (Application Monitor) user interface. See the topic on viewing the Self-Diagnosis for the Data Collector Controller in the online helps.
2. Verify that the Data Collector is communicating with the Managing Server: see the topic on viewing a stack trace in the online helps.

What to do next

Perform configuration for optional features of the Data Collector. See Chapter 4, "Customization and advanced configuration for the Data Collector," on page 45.

Chapter 4. Customization and advanced configuration for the Data Collector

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

Perform the procedures in each of the following sections, if they apply.

Properties files for the Data Collector

Several properties files control Data Collector configuration and behavior.

For most common changes to this configuration, you will need to edit the Data Collector properties file and the Toolkit properties file. Several other properties files also exist.

The Data Collector properties file

The Data Collector properties file is automatically created by the installer, and is unique for every application server instance monitored by the Data Collector. Its name is `config_home/runtime/appserver_version.node_name.server_name/datacollector.properties`.

However, to facilitate future upgrades, **do not change** this file.

Instead, add the settings you want to modify to the Data Collector custom properties file. This file is named `config_home/runtime/app_server_version.node_name.server_name/custom/datacollector_custom.properties`; this will override the values in the Data Collector properties file.

Note: If the `config_home/runtime/app_server_version.node_name.server_name/custom/datacollector_custom.properties` file does not exist, create it when you need to make changes. You may also need 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 `config_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 as they will be overwritten.

Instead, add the settings you want to modify to the Data Collector custom properties file. This file is named `config_home/runtime/app_server_version.node_name.server_name/custom/toolkit_custom.properties`; this will override the values in the Toolkit properties file.

You may also set toolkit properties for all the application server instances monitored by this installation of the Data Collector. To do this, add the settings to

the global toolkit custom properties file: *config_home/runtime/custom/toolkit_global_custom.properties* . However, if a property is set in the instance specific *toolkit_custom.properties* file, it will override the value in the global file for this instance.

Note: If the *config_home/runtime/app_server_version.node_name.server_name/custom/toolkit_custom.properties* or *config_home/runtime/custom/toolkit_custom.properties* file does not exist, create it when you need to make changes. You may also need to create the custom directory.

Other properties files

The following properties files are unique for every application server instance monitored by the Data Collector:

- *config_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.
- *config_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.
- *config_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.

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 Visualization Engine, monitoring levels (known as Monitoring On Demand, or MOD, levels) are L1, L2, and L3.

This level is set independently for IBM Tivoli Monitoring and the Managing Server. For example, the user may set monitoring level L1 for IBM Tivoli Monitoring from the Tivoli Enterprise Portal, and at the same time set MOD L2 in the Managing Server Visualization Engine. In this case, only L1 data will be available in the Tivoli Enterprise Portal, but L2 information will be displayed in the Visualization Engine.

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.

Note: 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 impacts the performance overhead, as well as the scope and accuracy of the monitoring. While 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 and turbo mode 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.

Internal Buffering settings

The following parameters in the Data Collector properties file (see “The Data Collector properties file” on page 45) control internal buffering in the Data Collector.

internal.memory.limit

The default value is 100 (MB). This property limits the amount of memory the Data Collector may use for all its buffering needs. Reducing this setting can lower the memory overhead introduced by the Data Collector; however, it can also increase the probability of buffer overflow at MOD L2 or L3 during periods of very 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 52.

internal.memory.accept.threshold

The default value is 2 (MB). Once the amount of memory specified in `internal.memory.limit` is reached, a buffer overflow state happens, and data will not be 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 accepted by the Data Collector. If your URL length typically exceeds this value, it should be increased to avoid display truncation.

internal.sql.limit

The default value is 5000. This property controls the maximum SQL length accepted by the Data Collector. If your SQL statement length is typically greater than this value, the value should be increased 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, as the default send buffer size is more than adequate.

Turbo Mode

If the Data Collector cannot send data to the Managing server fast enough, Data collector buffer space may be exhausted. The Data Collector may react in two ways, depending on whether *turbo mode* is enabled or disabled.

Turbo mode is controlled by the **dc.turbomode.enabled** setting in the Data Collector properties file (see “The Data Collector properties file” on page 45). Set it to true to enable turbo mode, or to false to disable it. By default, turbo mode is disabled.

If turbo mode is enabled, the Data Collector will enter turbo mode when three quarters of the maximum memory size (set in `internal.memory.limit`) is used. In turbo mode, the Data Collector raises the priority of the threads that send data to the Managing Server and the Monitoring Agent. Application threads remain at a lower priority, and may freeze until the buffer shortage is relieved. This ensures maximum reporting accuracy but can have a significant impact on application performance.

In turbo mode, the Data Collector also continues to monitor any existing requests, but any new incoming requests will not be monitored until the buffer shortage is relieved. The application will process them, and the Data Collector will notify the Managing Server of a "dropped" request.

If turbo mode is disabled, the Data Collector will drop any monitoring data in the event of a buffer shortage. Therefore, information in the Tivoli Enterprise Portal and Visualization Engine may be incomplete, but application performance will not be impacted.

Disable turbo mode on "mission critical" production systems, where any application thread freeze is not acceptable in any situation. However, a danger of buffer shortage (and, therefore, engagement of turbo mode) usually happens only in MOD L2 or L3; on production systems, users need to enable these levels only when investigating an issue. Turbo mode may be of use in such an investigation. So, if a significant performance impact in the event of an investigation is acceptable, you can enable turbo mode.

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

If the Data Collector will communicate with ITCAM for Application Diagnostics Managing Server, and two or more application servers are using Remote Method Invocation over Internet InterORB Protocol (RMI/IIOP), you need to enable instrumentation and monitoring of RMI/IIOP requests in order to view composite requests (via correlation icons) in the Visualization Engine.

All the servers must be instrumented by Data Collectors connected to the same Managing Server.

For version 6.1 and 7 application servers, in the Toolkit custom properties file (see “The Toolkit properties file” on page 45), add or uncomment the following property:

```
org.omg.PortableInterceptor.ORBInitializerClass.com.ibm.tivoli.itcam.toolkit.  
ai.orbinterceptor.Initializer=true
```

If a previous version of the Data Collector was used to monitor this application server instance, check settings that may have been added in the past to enable RMI/IIOP instrumentation, and remove them if found. Perform the following procedure:

1. Log into the IBM WebSphere Application Server administrative console for the instance of the application server for the Data Collector.
2. Click **Server > Application Servers** and select the *server_name*.
3. Navigate to **Additional Properties: Process Definition > Servant > Additional Properties: Custom Properties**.
4. Remove the following JVM custom properties, if any of them exist:
`am.ejb.rmilistener.enable`
`amprotocol_iiop_propagate_unknown_service_ctxs`
5. Click **Apply** or **OK**.
6. In the Messages window, click **Save**.
7. In the Save to Master Configuration window, take the following actions:
 - If you are under a Network Deployment environment, be sure the check box **Synchronize changes with Nodes** is selected and then click **Save**.
 - If you are not under a Network Deployment environment, click **Save**.
8. In the *AppServer_home/profiles/default/config/cells/cell_name/nodes/node_name/servers/server_name/was.env* file, remove the property `protocol_iiop_propagate_unknown_service_ctxs` if it is present.
9. For the Data Collector installed on the RMI client, check both the toolkit properties file and the toolkit custom properties file (see “The Toolkit properties file” on page 45), and remove property `am.ejb.rmilistener.enable` if it is present.

For version 6.0.x application servers, perform the following procedure to enable RMI/IIOP instrumentation:

1. Log into the IBM WebSphere Application Server administrative console for the instance of the application server for the Data Collector.
2. Click **Environment > WebSphere Variables** and change the scope to the server level.
3. Change the value of `protocol_iiop_propagate_unknown_service_ctxs` variable to 1. If the environment variable `protocol_iiop_propagate_unknown_service_ctxs` does not exist, add it and set its value to 1.
4. Click **Apply** or **OK**.
5. In the Messages window, click **Save**.
6. In the Save to Master Configuration window, take the following actions:
 - If you are under a Network Deployment environment, be sure the check box **Synchronize changes with Nodes** is selected and then click **Save**.
 - If you are not under a Network Deployment environment, click **Save**.

7. Check both the toolkit properties file and the toolkit custom properties file (see “The Toolkit properties file” on page 45), and remove or comment out the property `am.ejb.rmilistener.enable` if it is present.
8. Restart the application server instance.

Disabling various types of Byte Code Instrumentation for J2EE 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 J2EE APIs, set (or uncomment) the following properties in the toolkit custom properties file (see “The Toolkit properties file” on page 45). These properties are set to true by default. After changing the file, restart the application server instance.

Table 7. Adding lines to `toolkit_custom.properties`

Type of J2EE API	Line to add to <code>toolkit_custom.properties</code> file
Enterprise JavaBeans (EJB)	<code>com.ibm.tivoli.itcam.toolkit.ai.enableejb=false</code>
Java Connector Architecture (JCA)	<code>com.ibm.tivoli.itcam.toolkit.ai.enablejca=false</code>
Java Database Connectivity (JDBC)	<code>com.ibm.tivoli.itcam.toolkit.ai.enablejdbc=false</code>
Java Naming and Directory Interface (JNDI)	<code>com.ibm.tivoli.itcam.toolkit.ai.enablejndi=false</code>
Java Message Service (JMS)	<code>com.ibm.tivoli.itcam.toolkit.ai.enablejms=false</code>
Web containers for Servlets/JavaServer Pages (JSP)	<code>com.ibm.tivoli.itcam.dc.was.webcontainer=false</code>
HTTP session count tracking	<code>com.ibm.tivoli.itcam.toolkit.ai.enablesessioncount=false</code>
CICS Transaction Gateway (CTG)	<code>com.ibm.tivoli.itcam.dc.ctg.enablectg=false</code>
IMS	<code>com.ibm.tivoli.itcam.dc.mqi.enableims=false</code>
Java Data Objects (JDO)	<code>com.ibm.tivoli.itcam.dc.mqi.enablejdo=false</code>
Message Queue Interface (MQI)	<code>com.ibm.tivoli.itcam.dc.mqi.enablemqi=false</code>
Axis web service	<code>com.ibm.tivoli.itcam.toolkit.ai.axis.enablewebservice=false</code>
Remote Method Invocation (RMI)	<code>am.ejb.rmilistener.enable=false</code>

Table 7. Adding lines to toolkit_custom.properties (continued)

Type of J2EE API	Line to add to toolkit_custom.properties file
IBM WebSphere Application Server EJB container	com.ibm.tivoli.itcam.dc.was.enableEJBContainer=false
WebSphere Portal Server 5.1	com.ibm.tivoli.itcam.dc.was.wps51.enable.CaptureWPServlet=false com.ibm.tivoli.itcam.dc.was.wps51.enable.CaptureAuthorization=false com.ibm.tivoli.itcam.dc.was.wps51.enable.WPSDistributedMapCache=false com.ibm.tivoli.itcam.dc.was.wps51.enable.CaptureGatewayServlet=false com.ibm.tivoli.itcam.dc.was.wps51.enable.CaptureLogin=false com.ibm.tivoli.itcam.dc.was.wps51.enable.CaptureModelBuilding=false com.ibm.tivoli.itcam.dc.was.wps51.enable.CapturePageLoading=false com.ibm.tivoli.itcam.dc.was.wps51.enable.CapturePageRendering=false com.ibm.tivoli.itcam.dc.was.wps51.enable.CapturePortal=false com.ibm.tivoli.itcam.dc.was.wps51.enable.CapturePortalActionLegacy=false com.ibm.tivoli.itcam.dc.was.wps51.enable.CapturePortalActionStd=false
WebSphere Portal Server 6	com.ibm.tivoli.itcam.dc.was.wps6.enable.CaptureWPServlet=false com.ibm.tivoli.itcam.dc.was.wps6.enable.CaptureAuthorization=false com.ibm.tivoli.itcam.dc.was.wps6.enable.WPSDistributedMapCache=false com.ibm.tivoli.itcam.dc.was.wps6.enable.CaptureGatewayServlet=false com.ibm.tivoli.itcam.dc.was.wps6.enable.CaptureLogin=false com.ibm.tivoli.itcam.dc.was.wps6.enable.CaptureModelBuilding=false com.ibm.tivoli.itcam.dc.was.wps6.enable.CapturePageLoading=false com.ibm.tivoli.itcam.dc.was.wps6.enable.CapturePageRendering=false com.ibm.tivoli.itcam.dc.was.wps6.enable.CapturePortal=false com.ibm.tivoli.itcam.dc.was.wps6.enable.CapturePortalActionLegacy=false com.ibm.tivoli.itcam.dc.was.wps6.enable.CapturePortalActionStd=false com.ibm.tivoli.itcam.dc.was.wps6.enable.CaptureStandardPortal=false

For most API types, BCI information is only collected for MOD levels L2 and L3. If the MOD Level is set to L1, BCI data is not sent to IBM Tivoli Monitoring or the Managing Server, although the method entry and exit is still intercepted. (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, as shown above) is also collected at MOD L1. For performance reasons, you can also 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 (see “The Toolkit properties file” on page 45):

Table 8. Modifying lines in toolkit_custom.properties

Type of J2EE API	Line to add to toolkit_custom.properties file
JCA	com.ibm.tivoli.itcam.toolkit.ai.jca.callback.unconditional=false
JDBC	com.ibm.tivoli.itcam.toolkit.ai.jdbc.callback.unconditional=false
JNDI	com.ibm.tivoli.itcam.toolkit.ai.jndi.callback.unconditional=false
JMS	com.ibm.tivoli.itcam.toolkit.ai.jms.callback.unconditional=false

Attention: Setting any of these properties to false may result in some missing data when MOD Level is switched from L1 to L2. For example, the Data Collector may not be able to determine the Data Source names for JDBC requests.

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.

To enable BCI for lock analysis, Level 3 memory leak analysis, and Level 3 method entry and exit tracing, you must make adjustments to the toolkit custom properties file (see “The Toolkit properties file” on page 45).

Making these adjustments will activate the use of one or more configuration files in the *DC_home/itcamdc/etc* directory, which contain the default settings to control BCI. The configuration files and default settings are described in the following table:

Table 9. Byte Code Instrumentation configuration files

File name	Purpose	Default behavior
lock_analysis.xml	Defines application lock analysis BCI. Note: Specific behavior in each MOD level is determined by settings in the Data Collector properties file.	Lock acquire 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 53).
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.
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, see “Enabling Byte Code Instrumentation features with default settings” on page 53.

If you want to customize the default settings and make more granular choices for what classes and methods to modify, see the following sections:

- “Customizing lock analysis” on page 53
- “Customizing memory leak diagnosis” on page 55
- “Customizing method profiling and method entry and exit tracing” on page 57

Attention: Enabling Byte Code Instrumentation for any of these features will slightly increase resource usage even on monitoring levels where no data is collected for them.

Enabling Byte Code Instrumentation features with default settings

Perform the following procedure 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. 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 (see “The Toolkit properties file” on page 45), 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
```

See Table 9 on page 52 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 acquire 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 (see “Properties files for the Data Collector” on page 45) control the lock analysis information provided by the Data Collector.

internal.lockanalysis.collect.Ln.lock.event

This property whether lock acquisition/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 as there is little benefit in displaying lock acquisition events if they do not involve contention; lock contention events are collected separately. However, you may wish to enable lock event collection for some development tasks.

Example:

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

internal.lockanalysis.collect.Ln.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 prior to 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 enables 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, and the user should only enable L3 for a limited time to reduce performance impact.

Example:

```
internal.lockanalysis.collect.L2.contend.events = justone
```

internal.lockanalysis.collect.Ln.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, perform the following procedure:

1. Make a copy of the *install_home/itcamdc/etc/lock_analysis.xml* 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 will be Byte-Code-Instrumented. By default, all lock requests in all application classes are selected. By modifying this tag, you can implement a more granular selection, although within a class all lock requests are Byte-Code-Instrumented. Multiple `lockingClasses` tags can be specified.

The `lockingClasses` 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 sub-packages. 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 identified in the tag are specifically excluded from BCI for lock analysis. This is useful for indicating that all classes are to be Byte-Code-Instrumented except for those classes that are specifically excluded.

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` should be Byte-Code-Instrumented for lock analysis.
- The `Supplier` class should 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 `config_home/runtime/app_server_version.node_name.server_name/custom` directory, then complete the following steps:
 - a. In the toolkit custom properties file (see “The Toolkit properties file” on page 45), set the property `am.camtoolkit.gpe.customxml.lock` to the name (without path) of the file you modified in Step 2 on page 54.
 - 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, then complete the following steps:
 - a. In the toolkit custom properties file (see “The Toolkit properties file” on page 45), set the property `am.camtoolkit.gpe.customxml.lock` to the path and name for the file you modified in Step 2 on page 54.
 - 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 may configure the Data Collector to exclude some classes from BCI for memory leak analysis.

Perform the following procedure to set classes for Memory Leak Diagnosis:

1. Make a copy of the `install_home/itcamdc/etc/memory_leak_diagnosis.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 tags you can modify:

Table 10. Parameters for the memory leak diagnosis configuration file

Tag name	Description
heapAllocationTarget	Defines the allocating and allocated classes for which heap allocations will be Byte-Code-Instrumented. By default, all allocating and allocated classes are selected. By modifying the allocatingClassName and allocatedClassName tags within the heapAllocationTarget tag, you can implement a more granular selection. Each heapAllocationTarget tag must contain exactly one allocatingClassName tag, and one or more allocatedClassName tags. Multiple heapAllocationTarget tags can be specified.
allocatingClassName	Identifies the name of a class or classes to be modified. Each heapAllocationTarget tag must contain exactly one allocatingClassName tag.
allocatedClassName	Identifies the specific heap allocation requests within the class or classes identified by the allocatingClassName tag that are to be Byte-Code-Instrumented. Each heapAllocationTarget tag must contain one or more allocatedClassName tags.

Both allocatingClassName and allocatedClassName tags can include wildcard characters. The following 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 sub-packages. 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 specifically excluded.

For example, an application with a package name of com.mycompany.myapp has the following requirements:

- Within the Customer class, all heap allocations should be Byte-Code-Instrumented.
- Within the Supplier class, all heap allocations should be Byte-Code-Instrumented except for allocations for classes beginning with java.lang.String.

The following example 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.appttrace.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 *config_home/runtime/app_server_version.node_name.server_name/custom* directory, then complete the following steps:
 - a. In the toolkit custom properties file (see “The Toolkit properties file” on page 45), set the property `am.camtoolkit.gpe.customxml.leak` to the name (without path) of the file you modified in Step 2 on page 55.
 - 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, then complete the following steps:
 - a. In the toolkit custom properties file (see “The Toolkit properties file” on page 45), set the property `am.camtoolkit.gpe.customxml.leak` to the path and name for the file you modified in Step 2 on page 55.
 - b. In the same toolkit custom properties file, sets 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 may 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 will only instrument method profiling data when the method exceeds certain thresholds of CPU time and real (“wall clock”) time usage. There are also limits on the total number of methods, stack size, and running thread size. You can customize the thresholds and limits.

The following properties in the Data Collector properties file (see “The Data Collector properties file” on page 45) control the thresholds and limits for method profiling.

am.mp.cpuThreshold

The default is 30 milliseconds. Only the methods which take at least the minimum amount of CPU time specified in this property are captured for method profiling data. This avoids unnecessary clutter. Generally, methods with greater than the value specified in this property are considered useful. Customers can reduce or increase this value if needed.

am.mp.clockThreshold

The default is 30 milliseconds. Only the methods which take at least the minimum amount of wall clock time specified in this property are captured for method profiling data. This avoids unnecessary clutter. Generally, methods with greater than the value specified in this property are considered useful. Customers can reduce or increase this value if needed.

am.mp.leagueTableSize

The default is 1000. This is the maximum number of methods that are monitored for method profiling data. Customers can reduce or increase this value if needed. Decreasing it will help in reducing 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, perform the following procedure:

1. Make a copy of the *install_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 you can modify:

Table 11. 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 <code>className</code> and <code>methodName</code> tags within the <code>methodSelection</code> tag, you can implement a more granular selection. Each <code>methodSelection</code> tag must contain exactly one <code>className</code> tag, and one or more <code>methodName</code> tags. Multiple <code>methodSelection</code> tags can be specified.
className	Identifies the name of a class or classes to be modified. Each <code>methodSelection</code> tag must contain exactly one <code>className</code> tag.
methodName	Identifies a method or method within the class or classes identified by the <code>className</code> tag to be modified for entry/exit tracing. Each <code>methodSelection</code> tag must contain one or more <code>methodName</code> tags.

Both `className` 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 sub-packages. 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 specifically excluded from BCI for entry and exit tracing. This is useful for indicating that all methods within a class or group of classes are to be Byte-Code-Instrumented except for those methods that are specifically excluded.

For example, an application with a package name of `com.mycompany.myapp` has the following requirements:

- Within the `Customer` class, all methods should be Byte-Code-Instrumented.
- Within the `Supplier` class, all methods should be Byte-Code-Instrumented except for those methods beginning with the `get` or `set`.

The following example shows the contents of the customized `method_entry_exit.xml` file that accomplishes this:

```
<aspect>
  <type>application</type>
  <name>com.ibm.tivoli.itcam.toolkit.ai.aspectj.apprace.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 `config_home/runtime/app_server_version.node_name.server_name/custom` directory, then complete the following steps:
 - a. In the toolkit custom properties file (see “The Toolkit properties file” on page 45), set the property `am.camtoolkit.gpe.customxml.L3` to the name (without path) of the file you modified in Step 2 on page 58.
 - 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, and then complete the following steps:
 - a. In the toolkit custom properties file (see “The Toolkit properties file” on page 45), set the property `am.camtoolkit.gpe.customxml.L3` to the path and name for the file you modified in Step 2 on page 58.
 - b. Set the following property to true:
`com.ibm.tivoli.itcam.toolkit.ai.methodentryexittrace=true`

Disabling Heap Analysis on IBM WebSphere Application Server 6.1.x

If you are monitoring IBM WebSphere Application Server 6.1.x, you may want to reduce overhead when running the Data Collector. If you do not need the faster heap analysis provided through the Heap Analysis feature of the Visualization Engine, or are not using ITCAM for Application Diagnostics Managing Server, you can reduce the overhead involved with running the Data Collector by disabling Heap Analysis.

For IBM WebSphere Application Server 6.1.x, disable Heap Analysis by performing the procedure in this section. The benefit is that you can reduce the overhead involved with running the Data Collector significantly. After disabling Heap Analysis, you still can get memory diagnosis data by using the Heap Dump Management function of ITCAM for Application Diagnostics, although Heap Dump Management might be slower than Heap Analysis. See the Memory Diagnosis section of the online helps for instructions on performing Heap Dump Management. Disabling Heap Analysis limits the data collected for the Heap Analysis and Memory Leak Candidates pages displayed in the Application

Monitor user interface. See the Memory Diagnosis section of the online helps for details on Heap Analysis and Memory Leak Candidates reports.

Perform the following procedure to disable Heap Analysis on IBM WebSphere Application Server 6.1.x by setting AM_HEAPDUMP=false as an environment variable in the IBM WebSphere Application Server administrative console:

1. Log into the IBM WebSphere Application Server administrative console.
2. Click **Server > Application Servers** and select the *server_name*.
3. In the **Configuration** tab, navigate to **Server Infrastructure > Java and Process Management > Process Definition > Servant > Environment Entries**.
4. Add the AM_HEAPDUMP environment entry with a value of false.
5. Click **Apply** or **OK**.
6. In the Messages window, click **Save**.
7. In the Save to Master Configuration window, take one of the following actions:
 - If you are under a Network Deployment environment, be sure the check box **Synchronize changes with Nodes** is selected and then click **Save**.
 - If you are not under a Network Deployment environment, click **Save**.
8. Restart the instance of the application server that is being monitored by the Data Collector.

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 J2EE APIs are recognized as requests. You can designate additional classes and methods as *custom requests*.

For example, ITCAM will not recognize Struts Action classes as requests by default, however you may set up custom request definitions and cause the Actions to be recognized as Nested Requests.

Perform the following procedure to enable monitoring of custom requests and designate one or more methods as custom requests:

1. Make a copy of the *install_home/itcamdc/etc/custom_requests.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 you can modify:

Table 12. 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 is 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 or not a class must be a system or application class in order to match the edgeRequest tag.

Table 12. Parameters for the custom requests configuration file (continued)

Tag name	Description
methodName	Identifies the names of the methods within one of the classes identified by the Matches tag that are to be Byte-Code-Instrumented for custom request processing. Exactly one methodName tag can be specified in each edgeRequest tag.

The Matches and 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 sub-packages. 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 should be treated as a custom request called CreditCheck.
- Within the Supplier class, the inventoryCheck() method should 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 *config_home/runtime/app_server_version.node_name.server_name/custom* directory. Then, in the toolkit custom properties file (see “The Toolkit properties file” on page 45), set the property *am.camtoolkit.gpe.customxml.custom* to the name (without path) of the file you modified in Step 2 on page 60.
- Save the file in any directory on your computer. Then, in the toolkit custom properties file (see “The Toolkit properties file” on page 45), set the property *am.camtoolkit.gpe.customxml.custom* to the path and name for the file you modified in Step 2 on page 60.

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 will need to enable Asynchronous Bean request monitoring using the Toolkit custom properties file..

First, check whether custom requests have been defined on the Data Collector (see “Defining custom requests” on page 60). Open the toolkit custom properties file and, if it exists, the global toolkit custom properties file (see “The Toolkit properties file” on page 45). Check both of these files for the following property (not commented out):

```
am.camtoolkit.gpe.customxml.custom=xml_filename
```

If this property exists, custom requests have been defined. In this case, edit the XML file 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 filename from the instance specific file. If the filename does not have a path, the file is located in the the *config_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, perform the following procedure:

1. create a new file: *config_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 (see “The Toolkit properties file” on page 45), set the property:

```
am.camtoolkit.gpe.customxml.custom=custom_requests_async.xml
```

After performing the changes described in this section, restart the application server instance monitored by the Data Collector.

Customizing monitoring of custom MBeans

By default, the Data Collector will monitor WebSphere Application Server MBeans. If the environment includes custom MBeans, you may 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 may define specific MBeans. Data collection will be enabled for these MBeans only.

Note: Data collection for the J2EE Domain MBean is not available in an IBM WebSphere Application Server environment.

Perform the following procedure to customize the generic configuration for JMX data collection:

1. Make a copy of the `install_home/itcamdc/etc/was/app_server_version/mbeanconfig_app_server_version.xml` file in a temporary location. Open the copy in a text editor.
2. Modify the parameters to fit your custom MBean. The following table describes the parameters you can modify:

Table 13. 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 <code>ObjectName</code> will be returned; otherwise, only the MBeans that belong to this domain name will be returned.
Description	Domain	Describes the domain. This can be any text string.
MBean	Domain	Defines the MBeans to be collected.
ObjectName	MBean	Defines the MBean object name for collection. If the MBean element is used within an <code>Attr</code> element (which indicates the embedded MBean), then the object name is any symbolic name, such as <code>\$ATTRIBUTE_VALUE</code> . This symbolic name will be 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 <code>JMXAcquireAttribute</code> to get the MBean attributes.
RetrieveAllAttrs	MBean	A value of <code>true</code> indicates that all the attributes for the MBean must be collected. If you set this to <code>false</code> , you must define the attributes in the <code>Attr</code> element.
Attr	MBean	Defines the attributes to be collected. There may be multiple <code>Attr</code> 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 <code>JMXAcquireAttribute</code> to get the specific attribute.

Table 13. Parameters for the JMX MBean configuration file (continued)

Element	Nested within	Description
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 *config_home/runtime/app_server_version.node_name.server_name/custom* directory. Then, in the toolkit custom properties file (see “The Toolkit properties file” on page 45), set the property `am.camtoolkit.jmxe.custom` to the name (without path) of the file you modified in Step 2 on page 63.
- Save the file in any directory on the monitored host. Then, in the toolkit custom properties file (see “The Toolkit properties file” on page 45), set the property `am.camtoolkit.jmxe.custom` to the path and name for the file you modified in Step 2 on page 63.

Enabling and customizing data collection for all custom MBeans

You may enable data collection for all custom MBeans and customize the way they are identified to the user.

To enable it, set the following property in the Toolkit properties file (see “The Toolkit properties file” on page 45):

```
am.getAllMbeans=y
```

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 (see “The Toolkit properties file” on page 45).

The following properties provide additional options for 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

Set this property to `y` to enable data collection for all MBeans. 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 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 need to see all of the keywords from the object name in the category, assign the `am.jmxusecanonical=y` property. This setting will result 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 quite long. By default, the Data Collector will truncate 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, 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 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.

By default, the following PMI setting will be enabled at each Managing Server MOD level:

Table 14. Default Performance Monitoring Infrastructure instrumentation settings

Monitoring (MOD) level	PMI setting
1	Basic
2	Extended
3	All

To customize these settings, perform the following procedures in the Data Collector custom properties file (see “The Data Collector properties file” on page 45):

Table 15. Procedures to customize instrumentation of the Performance Monitoring Infrastructure

Type of customization	Procedure
Change the PMI setting that will be 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: <pre>am.was6pmi.settings.1=basic am.was6pmi.settings.2=extended am.was6pmi.settings.3=all</pre>
Perform fine-grained customization of the instrumentation for a particular PMI module at a particular monitoring level. See the following Web site for a description of the numeric IDs that you will need when customizing PMI instrumentation at this detailed level: 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 <code>module_type=number1,number2,...</code>, for example: <pre>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</pre> Use * to monitor all IDs in the module, or none to monitor none: <pre>am.was6custompmi.settings.3=beanModule=* am.was6custompmi.settings.3=webAppModule=none</pre>

Attention: The `am.was6pmi.*` property names are also valid for monitoring Version 7 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 45):

```
am.pmi.settings.nochange=true
```

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, perform the following procedure:

1. Add the following lines to the Data Collector custom properties file (see “The Data Collector properties file” on page 45):

```
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.

2. Restart the instance of the application server that is being monitored by the Data Collector.

Enabling and customizing SMF monitoring

IBM WebSphere Application Server can be configured to write performance and statistical information to SMF. The Data Collector can use this information. To enable the Data Collector to gather data from SMF, you need to perform configuration on the CYN1 subsystem.

Installing the IEFU83 exit

Update SYS1.PARMLIB(SMFPRMxx) to enable the SMF exit IEFU83 and recording of SMF type 120 records. An example of an entry to enable an IEFU83 exit and recording of SMF type 120s is:

```
SYS(TYPE(4,5,28,30,37,38,39,70,71,72,73,74,75,76,77,78,120))
SYS(NODETAIL)
SYS(NOINTERVAL)
SYS(EXITS(IEFACTRT,IEFUJI,IEFU83,IEFU84,IEFU85,IEFUTL,IEFU29,IEFUJV))
SUBSYS(STC,EXIT(IEFACTRT,IEFUJI,IEFU29,IEFU83,IEFU84,IEFU85))
```

If you currently do not have a SYS or SUBSYS statement, you must include at a minimum:

```
SYS(TYPE(120),EXIT(IEFU83))
SUBSYS(STC,EXIT(IEFU83))
```

If your installation already has an IEFU83 exit, the IBM z/OS command SETPPROG may be used to create a cascade effect of calls to multiple yet distinct modules that will receive control, sequentially, to view or process the SMF records.

If your installation uses dynamic exits, update SYS1.PARMLIB(PROGxx) with the following commands:

```
EXIT ADD EXITNAME(SYS.IEFU83) MODNAME(CYN1FU83) DSN(CYN.SCYNAUTH) FIRST
EXIT ADD EXITNAME(SYSSTC.IEFU83) MODNAME(CYN1FU83) DSN(CYN.SCYNAUTH) FIRST
```

If your installation does not use dynamic exits, update SYS1.PARMLIB(COMMNDxx) with the following commands:

```
SETPROG EXIT,ADD,EX=SYS.IEFU83,MOD=CYN1FU83,DSN=CYN.SCYNAUTH,FIRST
SETPROG EXIT,ADD,EX=SYSSTC.IEFU83,MOD=CYN1FU83,DSN=CYN.SCYNAUTH,FIRST
```

Initializing IBM z/OS

Depending upon the options you selected when installing the CYN1 subsystem, installing the IEFU83 exit, authorizing the CYN.SCYNAUTH library and adding CYN.SCYNAUTH to the active Linklist, an IPL might be required.

Customizing the CYN1 Subsystem for optional SMF Collection

In order to collect SMF information for all the IBM WebSphere Application Server server instances on an LPAR, it might be necessary to customize parameters that control the building of in-core repository tables in CYN1PROC's address space. These parameters indicate the maximum number of IBM WebSphere Application Server instances, the sizes of the bean section, the bean method section, the web application section, and the servlet section pools. So, for example, if you're running more IBM WebSphere Application Server instances than the maximum allowed, then CYN1PROC's maximum IBM WebSphere Application Server instances allowed parameter must be changed, and the other CYN1PROC parameters might require tuning too.

The CYN1 subsystem uses address space storage to store SMF information collected from the various IBM WebSphere Application Server for IBM z/OS instances running in the same LPAR. SMF statistics comprise server and container data, bean data, bean method data, web application data, and servlet data. This data is collected from SMF type 120 records and reside in the CYN1PROC address space according to a hierarchical structure with the server instance as the top level. Memory for such a structure is pre-allocated by the CYN1PROC address space when it comes up according to a predefined parameter template, which specifies

the maximum number of server instances, the sizes of the bean section, bean method section, web application section, and servlet section pools.

The parameter template is assembled and linked in the SCYNAUTH library and its name is of the form CYNPxxxx. By default, CYN1 will load the CYNPTEST parameter template which is provided with the SCYNAUTH library. CYNPTEST is specified as a default parameter in the CYN1 cataloged procedure (PARMS=), as follows:

```
//CYN1PROC PROC SMFWRITE='ON',PARMS='TEST'
//STEP1 EXEC PGM=CYN1DRVR,REGION=0K,TIME=NOLIMIT,
// PARM='&PARMS,&SMFWRITE'
//*****
//*
//* PROPRIETARY-STATEMENT:
//* LICENSED MATERIAL - PROPERTY OF IBM
//*
//* 5655-L42
//*
//* (C) COPYRIGHT IBM CORP. 2006 ALL RIGHTS RESERVED
//* (C) COPYRIGHT CYANEA SYSTEMS CORP. 2002-2004 ALL RIGHTS RESERVED
//*
//* US GOVERNMENT USERS RESTRICTED RIGHTS - USE, DUPLICATION
//* DISCLOSURE RESTRICTED BY GSA ADP SCHEDULE CONTRACT WITH IBM CORP.
//*
//* -----
//*
//* THIS WILL START THE SUBSYSTEM CYN1
//* 'TEST' WILL BE APPENDED TO 'CYNP' THUS FORMING 'CYNPTEST'
//* WHICH IS THE NAME OF THE PARAMETER LOAD MODULE
//* 'ON' WILL BE THE DEFAULT VALUE ASSUMED FOR THE SMFWRITE
//* VARIABLE STATING THAT SMF RECORDS TYPE 120 WILL BE
//* ALLOWED TO BE WRITTEN
//*
//*****
//STEPLIB DD DISP=SHR,DSN=CYN.SCYNAUTH
//SYSLOG DD SYSOUT=*,FREE=CLOSE,SPIN=UNALLOC
//*SYSUDUMP DD SYSOUT=*,FREE=CLOSE,SPIN=UNALLOC
//*SYSABEND DD SYSOUT=*,FREE=CLOSE,SPIN=UNALLOC
//*SYSMDUMP DD SYSOUT=*,FREE=CLOSE,SPIN=UNALLOC
//*
```

For example, START CYN1PROC will start CYN1PROC using the default specification in the PARMS value of the cataloged procedure (either explicit values, or a parameter member, for example,, CYNPTEST).

START CYN1PROC,PARMS='PROD' will start CYN1PROC using the values defined in the parameter member CYNPPROD.

START CYN1PROC,PARMS='/ 10, 30, 30, 10, 10/' will start CYN1PROC using the specified values instead of the values specified in a parameter member.

Configuring the parameters statically

The source code for a generic CYNPxxxx parameter template can be found in the CYNPXXXX member of the distribution library CYN.SCYNPROC, encapsulated by sample JCL to assemble and link it into the CYN.SCYNAUTH library. You can customize the values in that member and rename it with any arbitrary suffix of at most 4 characters. Then you can either edit the CYN1 catalog procedure to reference that member as the default parameter template, or override the default when you start the CYN1PROC address space. For example the JES command:

START CYN1PROC,PARMS=ABCD specifies that the CYN1PROC address space will load the member CYNPABCD from the library CYN.SCYNAUTH when coming up and it will use the values specified in that member to allocate its in memory SMF structures.

You can only modify the following lines in that member:

```
... PEQUSENN EQU 10 # OF SERVER ENTRIES
... PEQUBSNN EQU PEQUSENN*2*10 NUMBER OF BEAN SECTION ENTRIES
... PEQUBMNN EQU PEQUBSNN*10 # OF BEAN METHOD ENTRIES
... PEQUWSNN EQU PEQUSENN*2*10 # OF WEBAPP SECTION ENTRIES
... PEQUSVNN EQU PEQUWSNN*10 # OF SERVLET SECTION ENTRIES ...
```

Furthermore, only the number 10 can be changed. Do not change the 2. For each server entry there are two sets of pools, a current pool containing the currently accumulated SMF statistics and an in-progress pool containing the latest SMF statistics. The SMF statistics in the two pools are then aggregated into the currently accumulated SMF statistics. Thus the factor of 2 which is specified in the PEQUBSNN and PEQUWSNN constants, and which normally must not be changed.

The constant PEQUSENN specifies the maximum number of server instances running in the LPAR for which CYN1 will keep SMF statistics for. Once a server entry is allocated, it remains so until the CYN1 region is brought down. Specify a number big enough to accommodate your needs, but keep in mind that the size of the bean section, bean method, web application, and servlet section pools will be multiplied by that number.

The constant PEQUBSNN specifies the average number of bean section entries per pool and per server instance. Some server instances might have more, some other less. That number is the size of the common pool. Specify the appropriate number here.

The constant PEQUBMNN specifies the average number of bean method entries per bean section. Some beans might have more, some other less. That number is the size of the common pool. Again specify the appropriate number.

The constant PEQUWSNN specifies the average number of web application section entries per pool and per server instance. Some server instances might have more, some other less. That number is the size of the common pool. Specify the appropriate number here.

The constant PEQUSVNN specifies the average number of servlet entries per web application section. Some web applications might have more, some other less. That number is the size of the common pool. Again specify the appropriate number.

Keep in mind that because of the multiplication factors, the number that you specify at the higher levels (server, bean sections, web application sections) are propagated at the lower levels. Be aware of that rather than specifying the biggest numbers just to be safe. The parameter template might not assemble correctly if the size of the SMF structure is too big.

Configuring the parameters dynamically

Another way to specify the size of the parameter values is to override the PARMS parameter in the start command with those values explicitly. The values are included between two slashes (/), separated with spaces or commas, and they must all be present. For example, specifying: START CYN1PROC,PARMS=' / 10,20,5,7,8/' will cause CYN1PROC to dynamically compute its memory

requirements with: Number of server instances: 10 (PEQUSENN) Average number of bean sections per server instance: 20 (PEQUBSNN) Average number of bean methods per bean section: 5 (PEQUBMNN) Average number of web applications per server instance: 7 (PEQUWSNN) Average number of servlets per web application: 8 (PEQUSVNN) All 5 values must be specified. CYN1PROC will not create a parameter member.

Verifying the IBM z/OS components

The following IBM z/OS commands may be used to help ensure the installation was successful.

To verify the definition of the CYN1FU83 exit, use the command:

```
D PROG,EXIT,MODNAME=CYN1FU83
```

This will normally produce messages similar to the following text:

```
CSV462I 16.46.00 PROG,EXIT DISPLAY 978
MODULE CYN1FU83
EXIT(S) SYS.IEFU83 SYSSTC.IEFU83
```

To verify the installation of the SYSSTC.IEFU83 exit, use the command:

```
D PROG,EXIT,EX=SYSSTC.IEFU83,DIAG
```

This will normally produce messages similar to the following text:

```
CSV464I 10.09.39 PROG,EXIT DISPLAY 136
EXIT SYSSTC.IEFU83
MODULE STATE EPADDR LOADPT LENGTH JOBNAME
CYN1FU83 A 8A0241A0 0A0241A0 000001E0 *
(verify the Loadpoint and Length are not zero)
```

To verify the installation of the SYS.IEFU83 exit, use the command:

```
D PROG,EXIT,EX=SYS.IEFU83,DIAG
```

This will normally produce messages similar to the following text:

```
CSV464I 10.12.26 PROG,EXIT DISPLAY 291
EXIT SYS.IEFU83
MODULE STATE EPADDR LOADPT LENGTH JOBNAME
CYN1FU83 A 932FB5C8 132FB5C8 000001E0 *
(verify the Loadpoint and Length are not zero)
```

To verify that CYN.SCYNAUTH is APF authorized, use the command:

```
D PROG,APF,DSNAME=CYN.SCYNAUTH
```

This will normally produce a message similar to the following text:

```
CSV450I 17.04.49 PROG,APF DISPLAY 386
FORMAT=DYNAMIC
ENTRY VOLUME DSNAME
1 STCE03 CYN.SCYNAUTH
```

To verify that CYN.SCYNAUTH is in the active Linklist, use the command:

```
D PROG,LNKLST
```

This will normally produce a message similar to the following:

```
RESPONSE=STLABCE
CSV470I 14.28.30 LNKLST DISPLAY 539
LNKLST SET LINK00 LNKAUTH=LNKLST
```

ENTRY	APF	VOLUME	DSNAME
1	A	IPL12B	SYS1.LINKLIB
2	A	RES20F	CYN.SCYNAUTH
3			

To verify that CYN1 Subsystem is defined, use the command:

```
D SSI,SUB=CYN1
```

This will normally produce a message similar to the following text:

```
IEFJ100I 10.32.59 SSI DISPLAY 349
SUBSYS=CYN1
DYNAMIC=YES STATUS=INACTIVE COMMANDS=REJECT
```

Verify that the system is recording SMF type 120 records and the CYN1 subsystem is capturing data in conjunction with the IEFU83 exits. This test must be done after all previous tests and when the application server changes (see the following section) have been implemented, the conversation activated and the application server is up and running. At that point, use the following commands:

```
S CYN1PROC
```

Wait for a number of minutes equal to the SMF interval length to run the following command.

```
F CYN1PROC,DUMP,AS,$CYNSETB,192
```

This will normally produce output similar to the following text:

CYN0004I: DUMP,AS,\$CYNSETB,192						
CYN0013I:	13803000	00000000	00000000	00000000	00000000	
CYN0013I:	13803010	00000000	00000000	00000000	00000000	
CYN0013I:	13803020	00000000	00000000	00000000	00000000	
CYN0013I:	13803030	00000000	00000000	00000000	00000000	
CYN0013I:	13803040	00000000	00000000	00000000	00000000	
CYN0013I:	13803050	00000000	00000000	00000000	00000000	
CYN0013I:	13803060	13803514	00000037	C1C4C3C4	D7D30000	ADCDPL
CYN0013I:	13803070	00000000	00000000	00000000	00000000	
CYN0013I:	13803080	00000000	00000000	00000000	00000000	
CYN0013I:	13803090	00000000	00000000	00000000	00000000	
CYN0013I:	138030A0	00000000	00000000	C2C2D6C1	E2D9F200	BBOASR2
CYN0013I:	138030B0	C2C2D6C1	E2D9F2C3	13803444	13803478	BBOASR2C

ADCDPL is the cell name for the application server instance.

BBOASR2 is the node name for the application server instance.

BBOASR2C is the application server instance name.

To find out the version of the CYN1PROC, use the following command:

```
F CYN1PROC,VER
```

```
CYN0004I: VER
```

```
CYN00045I: CYN1 ID: CYN1DRVR 03.01.00 09/14/04 18.09
```

Enabling and disabling instrumentation of Web Services as new request types

By default, the Data Collector monitors JAX-RPC 1.1 and Axis 1.x Web Services. To enable monitoring of JAX-WS Web Services, you need to perform additional steps. You can also disable monitoring of all Web Services.

To enable instrumentation of JAX-WS Web Services, you need to deploy the JAX-WS handler for the Data Collector. To do this, perform the following procedure on every application server that is a requester (client) or provider (server) of JAX-WS Web Services, and is monitored by the Data Collector:

1. Copy the file `DC_home/itcamdc/lib/com.ibm.tivoli.itcam.dc.jaxws-handlers.jar` into the `AppServer_home/plugins` directory.
2. Change to the `AppServer_home` directory, and run the following command:
 - on Windows, `osgiCfgInit.bat`
 - on Linux or UNIX systems, `./osgiCfgInit.sh`
3. Restart the application server instances monitored by the Data Collector.

To disable instrumentation of Web Services, set the following property in the Data Collector custom properties file (see “The Data Collector properties file” on page 45):

```
ws.instrument=false
```

Important: To enable Web Services composite request monitoring and correlation in the Visualization Engine and in ITCAM for Transactions, you need to monitor both the Web services requester (client) and the Web services provider (server) using ITCAM Agent for WebSphere Applications Data Collectors, and the Data Collectors must be connected to the same Managing Server.

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 will save memory usage statistics to the trace log file (`trace-dc-native.log`). For the location of the Data Collector trace log file, see *IBM Tivoli Composite Application Manager for Application Diagnostics 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 (see “The Data Collector properties file” on page 45):

```
log.statistics=true
```

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
```

Setting the server alias

You can set up the server alias for a monitored application server instance. The server alias is the name for the Tivoli Enterprise Portal node that represents the instance. This is only required if the first 18 characters in the server names are not unique for this Monitoring Agent runtime environment.

To set the server alias, in the file *config_home/runtime/appserver_version.node_name.server_name/kwjdc.properties*, uncomment and set the `com.ibm.tivoli.kwj.serveralias` property to the required alias.

Attention: A server alias must be unique for the Monitoring Agent runtime environment. Otherwise, the information for the instance might not be displayed in the Tivoli Enterprise Portal.

Note: If you need to define or change a server alias when information for the application server instance is already displayed in Tivoli Enterprise Portal, perform the following steps:

1. Stop the monitored application server instance.
2. In the Tivoli Enterprise Portal, issue the `Remove_Subnode Take Action` command for the affected node (old alias). The node will be grayed out in the Tivoli Enterprise Portal. You can use the **Clear Offline Entries...** action in the portal to remove it.
3. On the application server host, edit the *config_home/runtime/appserver_version.node_name.server_name/kwjdc.properties* file and set the `com.ibm.tivoli.kwj.serveralias` property.
4. Restart the monitoring agent.
5. Start the monitored application server instance.

Changing Managing Server communication configuration

If you want to enable or disable communication with the Managing Server, or to change the Managing Server for your Data Collector, run the runtime setup script. See “Step 5: executing the runtime setup script” on page 17.

Configuring the Data Collector after changing the application server version

If you upgrade the application server being monitored by the Data Collector from a 6.x version to a 7.x version, you must reconfigure the Data Collector to point to the updated instance of the application server.

Complete the following steps:

1. For a non-Network Development environment, unconfigure the Data Collector from all application server instances before the upgrade. See Chapter 5, “Unconfiguring the Data Collector on IBM z/OS,” on page 87.
2. Perform the upgrade of the application server.
3. For a non-Network Development environment, make sure the application server instance is upgraded and started. For a Network Deployment environment, make sure the Deployment Manager and Node Agent are upgraded and started; do not start the instances.
4. Use `setupwas.sh` to configure the Data Collector for each application server instance. See “Step 5: executing the runtime setup script” on page 17.

5. Start or restart the monitored application server instance.

Steps to perform after changing the IP address of the Data Collector

If after configuring the Data Collector you have changed the IP address of the host where the Data Collector is located, you need to update the Data Collector properties. Otherwise, the Data Collector cannot connect to the Managing Server.

The reason for this problem is that Data Collector configuration will remember the previous IP address in some of the runtime files. After you change the IP address, the Data Collector still references the previous IP address.

To avoid a failed connection when you restart the application server after changing the Data Collector's IP address, perform the following procedure:

1. To test basic connectivity, on the Managing Server host, for the new Data Collector IP address, issue the following command:
`ping ip_address`
2. On the Data Collector host, in the Data Collector properties file (see “The Data Collector properties file” on page 45), set the following properties to the new IP address of the Data Collector:

- `am.socket.bindip`
- `am.socket.exportip`

For example:

```
am.socket.bindip=9.12.20.220
am.socket.exportip=9.12.20.220
```

3. Using the IBM WebSphere Application Server Administrative Console, check if the `java.rmi.server.hostname` JVM custom property is set. If it is, change its value to the new IP address.

Steps to support changing application server addressing mode

WebSphere Application Server versions 6.1 and 7.0 offer the capability to run in either 31-bit or 64-bit addressing modes (AMODE). When the Data Collector is configured for an application server instance, it detects the AMODE and sets its internal configuration accordingly. If you change the application server AMODE later, you need to adjust Data Collector configuration. If you expect to change the AMODE more than once, you can configure automatic Data Collector AMODE configuration at every application server startup.

If you change the AMODE of the application server (for example, using the admin console) and do not configure the Data Collector for it, the application server will fail to start, with an ABEND message.

To configure the Data Collector after changing the application server AMODE, perform one of the following procedures:

- Run the Data Collector AMODE reconfiguration script from a shell prompt:

```
cd DC_home/bin/
./setmode.sh AppServer_home
```

where *AppServer_home* is the WebSphere Application Server home directory.

- Alternatively, reconfigure the Data Collector for the Application Server instance using the runtime setup script. See “Step 5: executing the runtime setup script” on page 17

You can make the Data Collector AMODE configuration automatic; this is especially useful if you expect to change AMODE for the same application server more than once. To do this, modify the started task JCL procedure for WebSphere Application Server. This procedure typically resembles the following JCL code:

```
//W7ASRA PROC ENV=,AMODE=00
// SET ROOT='/u/WAS70/w7cell/w7nodea'
// SET WSDIR='AppServer'
//BBOPASR EXEC PGM=BPXBATSL,REGION=0M,TIME=NOLIMIT,MEMLIMIT=NOLIMIT,
// PARM='PGM &ROOT./&WSDIR./lib/bboosrmr &AMODE.'
//STDENV DD PATH='&ROOT/&ENV/was.env'
//*
/* Output DDs
/*
//DEFAULTDD DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//HRDCPYDD DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//SYSOUT DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//CEEDUMP DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//SYSPRINT DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
```

Paste the sample JCL code from *config_home/bin/setmode.cntl* immediately before the first step of the procedure. The result will be similar to the following JCL code:

```
//W7ASRA PROC ENV=,AMODE=00
// SET ROOT='/u/WAS70/w7cell/w7nodea'
// SET WSDIR='AppServer'
//SETMODE EXEC PGM=BPXBATCH,REGION=0M,
// PARM='SH /u/itcam71/bin/setmode.sh &ROOT/&ENV'
//STDIN DD DUMMY
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
//BBOPASR EXEC PGM=BPXBATSL,REGION=0M,TIME=NOLIMIT,MEMLIMIT=NOLIMIT,
// PARM='PGM &ROOT./&WSDIR./lib/bboosrmr &AMODE.'
//STDENV DD PATH='&ROOT/&ENV/was.env'
//*
/* Output DDs
/*
//DEFAULTDD DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//HRDCPYDD DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//SYSOUT DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//CEEDUMP DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//SYSPRINT DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
```

This code invokes the Data Collector AMODE configuration script. Therefore, at every startup of the application server, the Data Collector will be configured for the current application server AMODE.

Moving the Data Collector to a different host computer

If the Data Collector communicates to ITCAM for Application Diagnostics Managing Server, you may move it to a different host computer while maintaining the same Managing Server identity (Probe ID and Controller ID). The Managing Server will see the new host as the continuation of the old, preserving history, analysis, etc.

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, perform the following procedure:

1. On host A, stop the instance of the application server that is being monitored by the Data Collector.
2. On host B, install the Data Collector and configure it using the Visualization Engine (Application Monitor) user interface. Configuring the Data Collector will generate 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 tool.
4. On host B, stop the instance of the application server that is being monitored by the Data Collector.
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.

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.

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 Configuration tool will set 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.

If the Data Collector needs to expose a specific IP to the Managing Server, complete one of the following steps:

1. In the Data Collector custom properties file (see “The Data Collector properties file” on page 45), set the *am.socket.exportip* and *am.socket.bindip* properties to the IP address to be exposed.
2. In the file *config_home/runtime/appserver_version.node_name.server_name/dc.java.properties*, 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).

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 will add 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 will correlate every CICS

transaction with the corresponding CTG call using the GPS token. The user can then view a detailed breakdown of transaction response time in the ITCAM Visualization Engine.

However, the presence of the GPS token in COMMAREA may 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 may (in some cases) 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 file *DC_home/runtime/app_server_version.node_name.server_name/custom/ctg.filters* . This file can contain any number of lines with the following syntax:

```
Type=E|I[,Gateway=<CTG URL>][,Server=<CICS Server>][,Program=<CICS Program>]
[,Transid=<Mirror tran ID>]
```

Each line defines a filter, which disables or enables GPS tokens for some transactions.

The Type parameter is mandatory for each line. A value of "E" sets up an Exclude filter; transactions matching it will not have a GPS token inserted into the COMMAREA. "I" denotes an Include filter; any transactions matching an include filter will have a GPS token, overriding any Exclude filter applying to them.

All other parameters are optional, but at least one of them must be present on every line. To match a filter, a transaction must match all of the parameters set on the line:

- Gateway is any part of the CTG URL, including the protocol, host name and/or port
- Server is the host name of the CICS server (this may be different from the CTG host name)
- Program is the CICS program name (a field in a CICS transaction request)
- Transid is the CICS Mirror Transaction ID. Except Multi Regional Operation (MRO) CICS/CTG environments, this parameter is of little use as all CTG transactions will 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=*
```

Overriding the Data Collector autoconfiguration

By default, if the Data Collector communicates with ITCAM for Application Diagnostics Managing Server, it will be automatically configured by the Managing Server with the default configuration profile at the time of first connection. You may disable automatic configuration or select a different profile. These settings only take effect if you perform them before the Data Collector connects to the Managing Server for the first time.

To disable automatic configuration of the Data Collector in the Managing Server, set the following property in the Data Collector custom properties file (see “The Data Collector properties file” on page 45):

```
dc.autoconfigure=false
```

To change the profile name for automatic configuration of the Data Collector in the Managing Server, set the following property in the Data Collector custom properties file (see “The Data Collector properties file” on page 45):

```
dc.autoconfigure.configname=config_name
```

Note: If the Data Collector has already been configured by the Managing Servers, changing these settings will not have any effect.

To configure or unconfigure a Data Collector from the Managing Server, or to change the Data Collector configuration profile, use the Visualization Engine. From the top navigation, select **Administration > Server Management > Data Collector Configuration**. For more information on 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 or Extended Deployment. They are normally set by the configuration utility.

The properties are in the Data Collector properties file (see “The Data Collector properties file” on page 45).

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
```

Enabling integration with ITCAM for Transactions

If you are using the ITCAM for Transactions product, you can enable integration between ITCAM Agent for WebSphere Applications and ITCAM for Transactions using Transaction Tracking Application Programming Interface (TTAPI). ITCAM for Transactions will use information from ITCAM Agent for WebSphere Applications

to correlate every transaction with the application calls that control it. The user can then view a detailed breakdown of transaction response time in the IBM Tivoli Enterprise Portal.

Transaction Tracking Application Programming Interface (TTAPI) enables the integration of ITCAM Agent for WebSphere Applications and ITCAM for Transactions. ITCAM for Application Diagnostics Managing Server is required for this.

The Data Collector can generate TTAPI events for the following requests:

- All composite requests that generate events to Global Publishing Server (GPS), including:
 - RMI/IIOP
 - Web Services
 - MQI
 - CICS
 - IMS
- Top level EJB requests (including Message-Driven Beans)
- Top level Servlet and JSP requests
- Custom edge requests
- JDBC nested requests

Verify setup prerequisites

Verify that:

- ITCAM for Transactions on z/OS must be installed and correctly configured. (You can access documentation for ITCAM for Transactions at http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/index.jsp?topic=/com.ibm.itcamt.doc_7.1/welcome.htm).
- ITCAM for Transactions SCYTLOAD library must be added to your z/OS linklist or WebSphere Servant region (STEPLIB).
- Computer time clock must be accurate and synchronized with the other participating servers (UTC time synchronized within 2 minutes).
- If both sides of a Web Service based transaction interface use IBM WebSphere Application Server, and the ITCAM for Application Diagnostics Data Collector is installed on both sides, Web Service instrumentation must be enabled on both the requester and provider sides. See “Enabling and disabling instrumentation of Web Services as new request types” on page 71
- If both sides of a Remote Method Invocation over Internet InterORB Protocol (RMI-IIOP) based transaction interface use IBM WebSphere Application Server, and the ITCAM for Application Diagnostics Data Collector is installed on both sides, RMI-IIOP instrumentation (see “Enabling instrumentation and monitoring of RMI/IIOP requests between application servers” on page 48) must be enabled on both client and server sides. Also, the WebSphere Application Server environment variable `protocol_iiop_propagate_unknown_service_ctxs` must be set to 1 on both sides. For WebSphere Application Server version 6.1, APAR PK33874 must be installed (it is planned for inclusion in WebSphere Application Server 6.1.0.6)
- To correlate CICS transactions, CTG instrumentation must be enabled on the ITCAM for Application Diagnostics Data Collector (it is enabled by default). GPS

tokens are required for correlating transactions; they are enabled by default when CTG instrumentation is enabled. See “Customizing CICS transaction correlation” on page 76.

- To integrate transactions tracking with ITCAM for CICS Transactions and ITCAM for IMS Transactions Data Collectors, those data collectors must be enabled for Transactions Tracking. Additional software installation may be required to enable Transaction Tracking in the ITCAM for CICS and ITCAM for IMS Data Collectors.
- For the WebSphere Application Server instances that GET and PUT messages through the MQI interface, use the ITCAM for Application Diagnostics Managing Server Visualization Engine to enable MQ monitoring in the Data Collector. Select **Administration > Server Management > Data Collector Profiles**, and select the Data Collector Profile used for this Data Collector. In the **DC Profiles Menu**, click **Custom L2**, and enable the MQI event.

Verify the Transactions directory

Verify that your ITCAM for Transactions contains a directory with the following files:

- A JAR file: `cytapi4j.jar`
- Two external links to the Transaction Tracking JNI modules: `libcytapi64.so`, `libcytapi.so`

To display the directory contents, you can issue the UNIX System Services command `ls -la` in the Transactions Tracking directory. Check that the JAR file and the two links are shown, as in the following example:

```
41200 Aug 11 15:00 cytapi4j.jar
      8 Aug 25 23:06 libcytapi64.so -> CYTATJ64
      8 Aug 25 23:06 libcytapi.so  -> CYTATJAV
```

Modify LIBPATH and CLASSPATH

Modify the LIBPATH and CLASSPATH definitions in the WebSphere servant region.

LIBPATH is an environment property that contains an existing value (used by ITCAM). Add the path of the Transactions directory described above, separated by a colon (:).

To modify LIBPATH perform the following steps:

1. Log into the IBM WebSphere Application Server administrative console.
2. Depending on your application server version, perform one of the following procedures:

Table 16. Navigation to modifying LIBPATH in the IBM WebSphere Application Server administrative console

Version 6.1 or 7 application server	1. Click Server > Application Servers and select the <i>server_name</i>. 2. In the Configuration tab, navigate to Server Infrastructure > Java and Process Management > Process Definition > Servant > Environment Entries > Custom Properties.
-------------------------------------	---

Table 16. Navigation to modifying LIBPATH in the IBM WebSphere Application Server administrative console (continued)

Version 6.0 application server	1. Click Server > Application Servers and select the <i>server_name</i>. 2. In the Configuration tab, navigate to Server Infrastructure > Java and Process Management > Process Definition > Servant > Custom Properties.
--------------------------------	--

3. Edit the field **LIBPATH**. Add a colon (:) and then the path of the Transactions directory. Example: `:/usr/lpp/itcam/ittsvt/FOR_ITCAM`

CLASSPATH is a general property of the servant region JVM, often containing no entries. If there is an entry, add the new entry as a new line with no separators. Add the full path and name of the `cytapi4j.jar` file.

To modify CLASSPATH perform the following steps:

1. Log into the IBM WebSphere Application Server administrative console.
2. Click **Server > Application Servers** and select the *server_name*.
3. In the **Configuration** tab, navigate to **Server Infrastructure > Java and Process Management > Process Definition > Servant > Java Virtual Machine**.
4. Edit the field **Classpath**. Add a new line with the full path and name of the `cytapi4j.jar` file. Example: `/usr/lpp/itcam/ittsvt/FOR_ITCAM/cytapi4j.jar`

Modify toolkit custom properties file

To enable integration with ITCAM for Transactions, you need to modify the toolkit custom properties file.

Add the following properties to the toolkit custom properties file (see “The Toolkit properties file” on page 45):

```
com.ibm.tivoli.itcam.dc.ttapi.enable=true
com.ibm.tivoli.itcam.dc.ttapi.ttas.transport=ssn:CYTZ
```

Note: Usually, "CYTZ" is the Transactions Tracking Container Subsystem name. If the MVS subsystem name is different in your installation, modify the `com.ibm.tivoli.itcam.dc.ttapi.ttas.transport` property accordingly.

To display Transactions Tracking Application Programming Interface (TTAPI) status when the Data Collector initializes, add the following property:

```
com.ibm.tivoli.itcam.dc.ttapi.status.display=true
```

To integrate the Data Collector with ITCAM for Transactions Web Response Time (T5) agent, add the following property:

```
com.ibm.tivoli.itcam.dc.ttapi.wrm.servlet.enabled=true
```

By default, this amount is limited to 10.

To enable Optim[™] Performance Manager integration, set the following property in the toolkit custom properties file (see “The Toolkit properties file” on page 45 file:

```
com.ibm.tivoli.itcam.dc.ttapi.jdbc.opm.enabled=true
```

If any monitored J2EE application changes the JDBC connection client attributes during an active session, also set the following property:

```
com.ibm.tivoli.itcam.dc.ttapi.jdbc.opm.clientinfo.reset=true
```

If exceptions (failed requests) for JNDI and JDBC nested requests happen within a reporting period, they are reported via TTAPI, and the status of the transaction is set to Fail. The user is able to inspect individual exceptions. To limit the amount of JDBC and JNDI exceptions displayed for a top level transaction, set the following property in the toolkit custom properties file (see “The Toolkit properties file” on page 45):

```
com.ibm.tivoli.itcam.dc.ttapi.maxExceptions=number
```

To disable collecting JNDI information, set the following property in the toolkit custom properties file (see “The Toolkit properties file” on page 45):

```
com.ibm.tivoli.itcam.dc.ttapi.jndi.enabled=false
```

Steps to reduce background CPU utilization

The Data Collector consumes CPU cycles in the background regardless of the level of WebSphere request activity. This no-load or load-independent CPU utilization may be higher than desired.

Load-independent CPU utilization can be reduced by a combination of the following actions:

- Adjusting JVM-defined Garbage Collection (GC) intervals
- Being less aggressive in the frequency of some performance data collection
- Choosing not to gather some types of performance data

Note: High CPU utilization can also be caused by ongoing instrumentation; in this case, it is not strictly load-independent. CPU utilization on instrumentation can be reduced by disabling some types of BCI (Byte Code Instrumentation), or by limiting them to Level 2 and 3 monitoring only, thus freeing up the CPU while Level 1 is used. See “Disabling various types of Byte Code Instrumentation for J2EE APIs” on page 50.

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. you don't want this to happen, you can specify the garbage collection interval explicitly to a preferred interval.

The Data Collector communicates with the Managing Server using TCP/IP sockets and RMI. One effect of using RMI is that garbage collection occurs every minute. If you don't want this to happen, you can specify 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 into the IBM WebSphere Application Server administrative console.
2. Click **Server > Application Servers** and select the *server_name*.
3. In the **Configuration** tab, navigate to **Server Infrastructure > Java and Process Management > Process Definition > Additional Properties: Java Virtual Machine**.
4. In the **Generic JVM arguments** field, append the following parameters if such parameters don't exist, or update their values if they already exist.

```
-Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000
```

Note: 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.

Disabling WebSphere SMF or increasing the recording interval

When the ITCAM for Application Diagnostics setup executes, if the SMF option (y) is chosen, ITCAM for Application Diagnostics adds WebSphere-defined SMF recording properties to the control region with a recording interval of 2 minutes. Disabling the recording of SMF or increasing the interval to 6 minutes may reduce garbage collection CPU utilization. The related properties are stored and must be changed in the Control region.

Perform the following procedure:

1. Log into the IBM WebSphere Application Server administrative console for the instance of the application server for the Data Collector.
2. Depending on your application server version, perform one of the following procedures:

Table 17. Navigation to JVM custom properties in the IBM WebSphere Application Server administrative console

Version 6.0 application server	1. Click Server > Application Servers and select the <i>server_name</i>. 2. In the Configuration tab, navigate to Server Infrastructure > Java and Process Management > Process Definition > Control [for Process Type] > Custom Properties.
Version 6.1 or 7 application server	1. Click Server > Application Servers and select the <i>server_name</i>. 2. In the Configuration tab, navigate to Server Infrastructure > Java and Process Management > Process Definition > Control [for Process Type] > Environment Entries.

3. Take one of the following actions:
 - If you want to turn off SMF recording, delete the properties.
 - If you want to increase the recording interval, change the following property to a value of 360:


```
server_SMF_interval_length
```
4. Click **Apply**.
5. In the Messages window, click **Save**.
6. In the Save to Master Configuration window, take one of the following actions:
 - If you are under a Network Deployment environment, be sure the check box **Synchronize changes with Nodes** is selected and then click **Save**.
 - If you are not under a Network Deployment environment, click **Save**.

Changes to the Data Collector properties file

The following changes are to be done in Data Collector properties file (see “The Data Collector properties file” on page 45). You can choose any number of the following actions to take:

- If you do not need PMI supplied metrics, you may want to disable their collection by the Data Collector. Set the following property:


```
internal.pspmiinfo.disable=yes
```

- Reduce the thread event agent priority.
Set the following property for thread priority when in NORMAL mode:
`ea.thread.priority=5`

Set the following property for thread priority when in TURBO mode (see “Turbo Mode” on page 48). This must normally be the same or higher than Normal mode:
`ea.turbo.priority=5`
- Reduce the network agent thread priority.
Set the following property for thread priority when in NORMAL mode:
`na.thread.priority=5`

Set the following property for thread priority when in TURBO mode:
`na.turbo.priority=5`
- Increase the Publishing Server interval to 2 seconds. In light or no-load regions, this can be effective. Set the following property:
`internal.probe.publishing.frequency=2000`
- Increase the time the Network Agent sleeps in NORMAL mode. Set the following property:
`networkagent.publish.frequency=2000`

Changes in the Visualization Engine of the Managing Server

If you use ITCAM for Application Diagnostics Managing Server, you may Increase the interval in which the Managing Server polls each Data Collector for system resources.

Perform the following procedure:

1. In the Visualization Engine (Application Monitor) user interface, go to **Administration -> Managing Server System Properties**.
2. Change the System Resource Polling Frequency to a value in seconds. For example, 120 for 2 minutes, or 180 for 3 minutes.

Disabling Data Collector communication with the Monitoring Agent

If you do use IBM Tivoli Monitoring, you may disable Data Collector communication with the monitoring agent. This communication is always enabled after initial Data Collector configuration, but you can disable it manually.

After disabling communication to the monitoring agent, in order to minimize CPU use, disable the Toolkit Request Aggregator and Monitoring Agent garbage collection monitoring.

Only perform the following steps if you do not use, and do not plan to use, the IBM Tivoli Monitoring infrastructure.

Step 1. Disabling communication in the kwjdc.properties file

To disable Data Collector communication with the Monitoring Agent, perform the following procedure: edit the `config_home/runtime/app_server_version.node_name.server_name/kwjdc.properties` file.

In this file, comment out the following properties:

```
com.ibm.tivoli.kwj.agentport  
com.ibm.tivoli.kwj.agenthostname
```

Step 2. Disabling the Toolkit Request Aggregator

To disable the Toolkit Request Aggregator, set the following property in the toolkit custom properties file (see “The Toolkit properties file” on page 45):

```
com.ibm.tivoli.itcam.toolkit.ra.enablerequestaggregator=false
```

Step 3. Disabling garbage collection logging

If communication to the monitoring agent is disabled, the Data Collector does not need to monitor garbage collection (GC). GC is monitored based on JVM logging output. You can disable this output.

To disable garbage collection logging, perform the following procedure:

1. Log into the IBM WebSphere Application Server administrative console for the instance of the application server for the Data Collector.
2. Click **Server > Application Servers** and select the *server_name*.
3. In the **Configuration** tab, navigate to **Server Infrastructure > Java and Process Management > Process Definition > Servant > Additional Properties: Java Virtual Machine**.
4. In the **Generic JVM Arguments** field, if the parameter `-verbose:gc` is present, remove it.
5. Click **Apply**.
6. In the Messages window, click **Save**.
7. In the Save to Master Configuration window, take one of the following actions:
 - If you are under a Network Deployment environment, be sure the check box **Synchronize changes with Nodes** is selected and then click **Save**.
 - If you are not under a Network Deployment environment, click **Save**.

Step 4. Restarting the application server instance

After making the changes, restart the application server instance that is monitored by the Data Collector.

Turning off writing of SMF records in the CYN1 subsystem

You may want to turn off writing of application generated SMF records (type 120, subtypes 3, 6, and 8) to the SMF data sets during time frames when this data is not needed. Perform the following procedure:

1. Issue the following command to the CYN1 subsystem:

```
F [ xxxx | yyyy ],SMFWRITE OFF
```

xxxx is the name of the proc. For example, CYN1PROC.

Use *yyyy* if an ID was assigned. *yyyy* is the ID assigned to the CYN1 started task.

2. To verify, issue the following command:

```
F [ xxxx | yyyy ], SMFWRITE SHOW
```

See “The SMFWRITE command” on page 182 as a reference.

Disabling the LogCmd feature

If the LogCmd feature is enabled, disable it, because it is not used by ITCAM for Application Diagnostics. If the feature is disabled, as it is by default, a logger thread is created that opens a socket used for processing remote commands for setting logging and debug levels. ITCAM for Application Diagnostics supplies its own feature in CommandAgent.

LogCmd is disabled by default when the Data Collector version 6.1.0.4 or later is installed. However, you must perform the following procedure if the Response Time Tracking product coexists.

In the *config_home/runtime/appserver_version.node_name.server_name/cynlogging.properties* file, change the text:

```
# control whether logcmd enabled  
jlog.noLogCmd=true
```

to the following text:

```
# control whether logcmd enabled  
jlog.noLogCmd=false
```

Chapter 5. Unconfiguring the Data Collector on IBM z/OS

This chapter describes how to unconfigure the Data Collector either using the unconfiguration script or manually.

Take one of the following actions:

- If you will be using the unconfiguration script:
 1. Read the description of how to enter values for configuration options: “How to enter values for configuration options.”
 2. Depending on how you want to execute the unconfiguration script, see one of the following sections:
 - You can execute the unconfiguration script in prompt mode, in which you invoke the script and then get prompted for configuration values: “Unconfiguring the Data Collector in prompt mode” on page 91.
 - You can execute the unconfiguration script in batch (auto-run) mode, in which you set the configuration values in a batch-mode invocation script then invoke the script without further interaction: “Unconfiguring the Data Collector in batch (auto-run) mode” on page 94.

Note: Unconfiguring the Data Collector will not undo any manual changes of the IBM WebSphere Application Server servant JVM options.

- If tried to run the `unconfig.sh` script to unconfigure it and it failed, you need to unconfigure the Data Collector manually. See “Unconfiguring the Data Collector manually” on page 95.

If the Data Collector has been configured to monitor several instances of the application server, you need to unconfigure it separately for each instance.

How to enter values for configuration options

The runtime setup script comes with a set of product-provided defaults for the configuration options.

If you will be unconfiguring the Data Collector in prompt mode, you can change the product-provided default values in the following ways:

- You can specify options in the command line when initiating the script.
- You can export the equivalent environment variables before running the script.

Then when answering the prompts, you can override the existing defaults, if you choose. Some options are not prompted for. For those options, if you want to specify values that differ from the product-provided defaults, you must specify the options before the script starts up.

If running the script in batch mode, you set the values (without ever being prompted) by one of the following means:

- Specifying the equivalent environment variables in `cynzucfg.cntl` batch job file
- Specifying options at a command line that runs `unconfig.sh` in batch mode
- Exporting the equivalent environment variable prior to running `unconfig.sh` in batch mode

See Table 18 on page 88 for a list of the options:

Note: Some options are required if Global Security is enabled.

Table 18. List of options for the *unconfig.sh* script

Command-line option	Description	Equivalent environment variable and value
<code>-log logfile_name</code> <code>-nolog</code>	Indicate either <code>-log</code> or <code>-nolog</code> for whether you want the runtime unconfiguration script to create a log of all the unconfiguration operations that it performs. If you indicate <code>-log</code> , you can indicate a different location than the default. By default the log file is called <code>unconfig.log</code> and is located under the <code>config_home</code> . For example, <code>/u/itcam71/runtime/unconfig.log</code> . The default is to create this log file.	N/A. Available as on option on the command line only.
<code>-?</code>	Usage help	N/A. Available as on option on the command line only.
<code>-batch</code>	If specified, no prompting will be done. The script will terminate if necessary parameters are not specified or not valid in the batch job. Required to run the script in batch mode.	<code>ITCAM_BATCH=y</code>
<code>-debug</code>	Specifies whether to produce messages in the log file for debugging. Use this option if you have been having problems unconfiguring the Data Collector using the script and need to provide details to IBM Software Support.	<code>ITCAM_DEBUG=y</code>
<code>-config config_home</code>	The Data Collector configuration directory. For example: <code>/u/itcam71</code>	<code>ITCAM_CONFIG=config_home</code>
<code>-cleanup</code>	This option indicates that you want to remove the existing runtime directory for the application server instance. Whether you specify this option or not, the IBM WebSphere Application Server customization done for ITCAM for Application Diagnostics is removed. However, when you choose to specify this option, the <code>.id</code> and <code>.mod</code> files from the Data Collector configuration are removed. If you choose to specify this option: • If you perform a subsequent configuration for the same application server instance, you will have to re-apply a configuration to the Data Collector in the Visualization Engine (Application Monitor) user interface. In other words you will have to use the Unconfigured Data Collector Overview page to configure the Data Collector, as described in the Visualization Engine (Application Monitor) user interface online helps. • The Data Collector history is no longer available under the original Data Collector server name in the Visualization Engine (Application Monitor) user interface. It is not necessary to specify this option, so if the consequences of specifying it are undesirable, do not specify it.	<code>ITCAM_CLEANUP=y</code>
<code>-cleanuppolicy</code>	Specifies that any ITCAM changes to the server security policy file should be undone. Since the security policy file is shared by all servers on the node, the ITCAM modifications should only be cleaned up if there are no other servers on the same WebSphere node with a DC configured.	<code>ITCAM_CLEANUPPOLICY=y</code>

Table 18. List of options for the *unconfig.sh* script (continued)

Command-line option	Description	Equivalent environment variable and value
-cleanupplugins	For IBM WebSphere Application Server 6.1, attempt to remove any ITCAM IBM WebSphere Application Server plugin files and directories created for Data Collection versions before 6.1 Fix Pack 4. Default is to retain the existing files and directories. Versions of the Data Collector since 6.1 Fix Pack 4, including the current version, no longer need IBM WebSphere Application Server plugins. These plugins, therefore, may be safely removed unless a version of the ITCAM Data Collector older than 6.1 Fix Pack 4 monitors any Application Server in the node.	ITCAM_CLEANUPPLUGINS=y
-conntype SOAP RMI	The connection type for communications used by wsadmin.sh. The default is to use the connection type specified in the wsadmin.properties file associated with the wsadmin.sh script you have chosen. (The IBM WebSphere Application Server default for this parameter is SOAP.)	ITCAM_CONNTYPE=connect_type
-port port	The port number used by wsadmin.sh. In a Network Deployment (ND) environment, specify the Deployment Manager's SOAP or Remote Method Invocation (RMI) port (not the application server instance SOAP or RMI port). To find the SOAP port number in the control region job log, look for the following string: BB000222I: ADMC0013I: The SOAP connector is available at port port To find the RMI port number in the control region job log, look for the following string: BB000222I: ADMC0026I: The RMI connector is available at port port The default is to use the port specified in the wsadmin.properties file associated with the wsadmin.sh script you have chosen.	ITCAM_PORT=port
-host host	The fully-qualified host name or IP address used by wsadmin.sh. If you are in an ND environment, enter the value for the host for the Deployment Manager. Unless you are in an ND environment and the Deployment Manager is located on the local host, do not enter localhost. The default is the value specified in the wsadmin.properties file associated with the wsadmin.sh script you have chosen.	ITCAM_HOST=host_name

Table 18. List of options for the *unconfig.sh* script (continued)

Command-line option	Description	Equivalent environment variable and value
<code>-profile <i>profile_script</i></code>	Specifies a profile script for running <i>wsadmin.sh</i> . The Web site for IBM WebSphere Application Server provides the following description of a profile script: "The profile script runs before other commands, or scripts. If you specify <code>-c</code> , the profile script runs before it invokes this command. If you specify <code>-f</code> , the profile script runs before it runs the script. In interactive mode, you can use the profile script to perform any standard initialization that you want. You can specify multiple <code>-profile</code> options on the command line, and they invoke in the order that you supply them."	<code>ITCAM_PROFILE=script</code>
<code>-user <i>user_id</i></code>	The user ID to use for connection to <i>wsadmin.sh</i> . This is required if Global Security is enabled and it is not set in the <i>sas.client.props</i> (RMI) or <i>soap.client.props</i> (SOAP) files.	<code>ITCAM_USER=user_id</code>
<code>-password <i>password</i></code>	The password to use for connection to <i>wsadmin.sh</i> . This is required if Global Security is enabled and it is not set in the <i>sas.client.props</i> (RMI) or <i>soap.client.props</i> (SOAP) files.	<code>ITCAM_PASSWORD=password</code>
<code>-server <i>servername</i></code>	The application server's name. (This is the name for the server displayed in the IBM WebSphere Application Server administrative console, not the short name used to construct the z/OS started task names. This is sometimes referred to as the long name.) For example, <i>server1</i> . This option is required if running in batch mode.	<code>ITCAM_SERVER=servername</code>
<code>-wasroot <i>path</i></code>	The installation directory for IBM WebSphere Application Server (<i>AppServer_home</i>). It is the partial path to the <i>wsadmin.sh</i> file. For example: <i>/u/WAS600/Servers/AppServer</i> If you specify a value for <code>-wsadmin</code> , this option will be ignored. Note: Specifying more of the path to the <i>wsadmin.sh</i> script results in a quicker location of the <i>wsadmin.sh</i> script.	<code>ITCAM_WASROOT=AppServer_home</code>
<code>-wsadmin <i>path_and_file</i></code>	Specifies the full path to the <i>wsadmin.sh</i> file. For example: <i>/u/WAS600/Servers/AppServer/profiles/default/bin/wsadmin.sh</i> This option is required if running in batch mode and the default <i>wsadmin.sh</i> script that <i>setupwas.sh</i> selects is not acceptable.	<code>ITCAM_WSADMIN=path_and_file</code>
<code>-defaulthostname <i>IP_or_host</i></code>	Using the value returned by running the <i>hostname</i> command as the host name is usually acceptable in most environments, but in some environments, that value will not work. If running the <i>hostname</i> command returns a value that is not usable for configuring the Data Collector, you can use the <code>-defaulthostname</code> option. The <code>-defaulthostname</code> option specifies the fully-qualified host name or IP address that will replace the value of the local host name for all purposes in configuring the Data Collector, such as for the bind IP or export IP.	<code>ITCAM_DEFAULTHOSTNAME=IP_or_host</code>
<code>-localhost <i>hostname</i></code>	Used for a <i>findServers</i> node match if there is a problem identifying nodes. This is only meaningful if the <i>WAS_NODE</i> associated with <i>wsadmin.sh</i> is not usable. The default is the value entered for the <code>-defaulthostname</code> option.	<code>ITCAM_LOCALHOST=hostname</code>

Table 18. List of options for the *unconfig.sh* script (continued)

Command-line option	Description	Equivalent environment variable and value
<code>-localip</code> <i>IP_address</i>	Used for a findServers node match if there is a problem identifying nodes. This is only meaningful if the WAS_NODE associated with wsadmin.sh is not usable. The default is the value entered for the <code>-bindip</code> option.	<code>ITCAM_LOCALIP=IP_address</code>
<code>-nottransform</code>	Do not run the wsc2n.sh script after configuring the Data Collector. The default is to run the wsc2n.sh script, which transforms the changed IBM WebSphere Application server configuration files into the formats that the application server uses. This script is started for diagnostic purposes; it checks for any configuration errors. However, you can use the <code>-nottransform</code> option to avoid running it. The configuration files will be transformed when you restart the application server; any configuration error will be logged, and may cause the restart to fail. Only use <code>-nottransform</code> if you are reasonably confident there are no configuration errors. Note: Do not use this option if you are running IBM WebSphere Application server version 5.1.	<code>ITCAM_TRANSFORM=n</code>

Unconfiguring the Data Collector in prompt mode

Perform the following procedure to unconfigure the Data Collector using the unconfiguration script in prompt mode:

Note: In the prompts that occur when executing the unconfiguration script in prompt mode, if a default value is applicable, it will be shown in brackets at the end of the prompt. If no value is entered, the default value will be used. The default value also serves as an example of the format of the value that is required.

1. If WebSphere Global Security is enabled, log in as a WebSphere administrator, which will be able to administer the application server configuration.
2. If you are running the application server in a Network Deployment (ND) environment, make sure the Deployment Manager and the node agent are running. If you need to restart the node agent, instructions are at the following Web site:
http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.zseries.doc/info/zseries/ae/xml_restartnodeagent.html
3. If you are running the application server in a non-ND environment, make sure the instance of the application server that is being monitored by the Data Collector is running. If it is not, start the instance of the application server that is being monitored by the Data Collector.
4. If you want to set any of the configuration options as environment variables before running the unconfiguration script, export the environment variables. See the right-hand column of Table 18 on page 88 for a list of the environment variables. Here are examples of how to export an environment variable from a command line:

```
export ITCAM_CONNTYPE=RMI
export ITCAM_CLEANUP=y
```

By exporting these variables, the `unconfig.sh` script will use them as the new default values. You will not need to enter a value (simply press **Enter**) when you are prompted for them.

5. Run the following command from the `config_home/bin` directory:

```
./unconfig.sh [options]
```

The default path for the location of the script is `/u/itcam71/bin`.

See Table 18 on page 88 for a list of the options for running the script command.

By setting options in the command line, the `unconfig.sh` script will use them as the new default values. You will not need to enter a value (simply press **Enter**) when you are prompted for them.

If there are multiple IP addresses for the host where the Data Collector is being configured, you will be prompted to select an IP address:

Select host IP address:

- 1) 9.11.22.111
- 2) 199.999.44.99
- 3) 192.111.22.44

Enter selection: 1

6. Enter the number that corresponds to the correct IP address.

You will be prompted for the path of `AppServer_home`:

Enter the path of the WAS user install root `[/u/WAS610]`:

7. Enter the HFS or zFS path name of `AppServer_home` and press **Enter**.

The ITCAM for Application Diagnostics configuration script uses this path to search for the `wsadmin.sh` script that was used to configure the target application server for ITCAM monitoring during the configuration.

You must respond with a valid HFS or zFS path name, for example, `/u/WAS600`.

You will be prompted to select one of the discovered occurrences of the `wsadmin.sh` script:

Found `wsadmin.sh` in the following locations:

- 1) `/u/WAS610/DeployMgr/AppServer/bin/wsadmin.sh`
- 2) `/u/WAS610/DeployMgr/AppServer/profiles/default/bin/wsadmin.sh`
- 3) `/u/WAS610/DeployMgr/DeploymentManager/bin/wsadmin.sh`

Enter the number of the `wsadmin` to use for unconfiguration:

8. Enter the number that corresponds to the path for the appropriate `wsadmin.sh` script and press **Enter**.

The script will use the `wsadmin.sh` that you selected to find all server instances that are running on this node. Then you will be prompted to select one of the discovered instances of the application server:

- 1) IBM123
- 2) IBM124
- 3) IBM125
- 4) IBMabc

Enter the number of the server to select:

9. Enter the number that corresponds to the appropriate instance of the application server that you want to unconfigure and press **Enter**.

You will be prompted whether you want to remove the runtime directory for the application server instance that is being unconfigured:

Do you wish to remove the `was61.TIVOLI.IBM123` directory? (y|n) [n]:

10. Enter y or n and press **Enter**.

Entering y indicates that you want to remove the existing runtime directory for the application server instance.

Whether you enter y or enter n, the IBM WebSphere Application Server customization done for ITCAM for Application Diagnostics is removed. However, when you enter y, the .id and .mod files from the Data Collector configuration are removed. If you enter y:

- If you perform a subsequent configuration for the same application server instance, you will have to re-apply a configuration to the Data Collector in the Visualization Engine (Application Monitor) user interface. In other words you will have to use the Unconfigured Data Collector Overview page to configure the Data Collector, as described in the Visualization Engine (Application Monitor) user interface online helps.
- The Data Collector history is no longer available under the original Data Collector server name in the Visualization Engine (Application Monitor) user interface.

It is not necessary to enter y, so if the consequences of specifying it are undesirable, enter n.

After this, you will be prompted whether the ITCAM changes to the security Java 2 security policy file should be reversed:

ITCAM configuration adds statements to the Java 2 security file server.policy. Since this policy file is shared by all servers on this node, you should only remove these statements when the last server configured for ITCAM is unconfigured.

Do you wish to remove ITCAM changes to the server.policy file? (y|n) [n]:

11. Choose y or n. Do not enter y if any other IBM WebSphere Application Server instance in the same node will still be monitored by the Data Collector.

The script will prompt you whether the ITCAM plugins directory is to be removed from IBM WebSphere Application Server.

If you are running this script you have installed FP4 (Fix Pack #4) or some subsequent PTF. After FP4 is installed, ITCAM plugins are no longer required by ITCAM. If all WAS servers in this node monitored by ITCAM are at the ITCAM FP4 level or later, the ITCAM plugins in the WAS directories may be safely removed.

However, the plugins should not be removed if any ITCAM/DC monitors in the node are pre-FP4.

12. Enter y or n. Do not enter y if any other IBM WebSphere Application Server instance in the same node remains monitored by a version of the Data Collector without Fix Pack 4, or a superceding PTF, installed.
13. The script will unconfigure the Data Collector. The runtime unconfiguration script creates a log of all the unconfiguration operations that it performs. You can review the log for any error conditions, and you might be requested to provide the log contents to IBM software support. The log file is called unconfig.log and is located under the *config_home*. For example, /u/itcam71/runtime/unconfig.log .

For successful unconfiguration look for messages similar to the following text: Successfully unconfigured data collector for server ibm001

14. If you selected to have SMF records to be written when you ran the configuration program, use the IBM WebSphere Application Server administrative console to disable the SMF activity and interval records (if they were not enabled prior to installing ITCAM for Application Diagnostics).

Unconfiguring the Data Collector in batch (auto-run) mode

Executing the unconfiguration script in batch (auto-run) mode eliminates the need for command-line-execution prompting. You can either enter values for environmental variables in the `cynzucfg.cntl` batch job and submit it as a z/OS JCL job that uses BPXBATCH, or you can execute the `unconfig.sh` script through a command line.

Perform one of the following procedures to execute the unconfiguration script in batch (auto-run) mode:

- “Editing the `cynzucfg.cntl` batch job and submitting it as a z/OS JCL job that uses BPXBATCH”
- “Executing the `unconfig.sh` script through a command line” on page 95

Editing the `cynzucfg.cntl` batch job and submitting it as a z/OS JCL job that uses BPXBATCH

Perform the following procedure to execute the unconfiguration script in batch (auto-run) mode by editing the `cynzucfg.cntl` batch job and submitting it as a z/OS JCL job that uses BPXBATCH:

1. If WebSphere Global Security is enabled, log in as a WebSphere administrator, which will be able to administer the application server configuration.
2. If you are running the application server in a Network Deployment environment, make sure the Deployment Manager and the node agent are running. If you need to restart the node agent, instructions are at the following Web site:
http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.zseries.doc/info/zseries/ae/txml_restartnodeagent.html
3. If you are running the application server in a non-ND environment, make sure the instance of the application server that is being monitored by the Data Collector is running. If it is not, start the instance of the application server that is being monitored by the Data Collector.
4. Copy the sample batch job, `cynzucfg.cntl`, from the `config_home/bin` directory to a location of your choice.
5. In the sample batch job, modify the environment variables appropriately. See Table 18 on page 88 for the list of environment variables.
6. Save the batch job file you modified in Step 5.
7. In TSO, submit a z/OS JCL job using the contents of the file you modified in Step 5, which uses BPXBATCH.

Using a z/OS JCL submitted job with BPXBATCH is advantageous if you want to produce a record or do not want to tie up your terminal.

Resolve any security issues you encounter when running the job.

8. The runtime unconfiguration script creates a log of all the unconfiguration operations that it performs. You can review the log for any error conditions, and you might be requested to provide the log contents to IBM software support. The log file is called `unconfig.log` and is located under the `config_home`. For example, `/u/itcam71/runtime/unconfig.log`.

For successful unconfiguration look for messages similar to the following text:

Successfully unconfigured data collector for server `ibm001`

9. If you selected to have SMF records to be written when you ran the configuration program, use the IBM WebSphere Application Server

administrative console to disable the SMF activity and interval records (if they were not enabled prior to installing ITCAM for Application Diagnostics).

Executing the `unconfig.sh` script through a command line

Perform the following procedure to execute the unconfiguration script in batch (auto-run) mode by executing the `unconfig.sh` script through a command line:

1. If WebSphere Global Security is enabled, log in as a WebSphere administrator, which will be able to administer the application server configuration.
2. If you are running the application server in a Network Deployment environment, make sure the Deployment Manager and the node agent are running. If you need to restart the node agent, instructions are at the following Web site:

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.zseries.doc/info/zseries/ae/txml_restartnodeagent.html

3. If you are running the application server in a non-ND environment, make sure the instance of the application server that is being monitored by the Data Collector is running. If it is not, start the instance of the application server that is being monitored by the Data Collector.
4. Run `unconfig.sh` from a command line.

Perform the same procedure as you would for running `unconfig.sh` in prompt mode (see “Unconfiguring the Data Collector in prompt mode” on page 91), but indicate all the options you want to specify at the command line (or by exporting the corresponding environment variable prior to running `unconfig.sh`). Make sure to indicate options that are required for running in batch mode (see Table 18 on page 88 for the list of options, especially those that are required for running in batch mode).

The script will unconfigure the Data Collector.

5. The runtime unconfiguration script creates a log of all the unconfiguration operations that it performs. You can review the log for any error conditions, and you might be requested to provide the log contents to IBM software support. The log file is called `unconfig.log` and is located under the `config_home`. For example, `/u/itcam71/runtime/unconfig.log`.

For successful unconfiguration look for messages similar to the following text:
Successfully unconfigured data collector for server ibm001

6. If you selected to have SMF records to be written when you ran the configuration program, use the IBM WebSphere Application Server administrative console to disable the SMF activity and interval records (if they were not enabled prior to installing ITCAM for Application Diagnostics).

Unconfiguring the Data Collector manually

If you tried to run the `unconfig.sh` script to unconfigure it and it failed, you need to unconfigure the Data Collector manually.

Perform the following procedure to manually unconfigure the Data Collector:

1. Log into the IBM WebSphere Application Server administrative console.
2. Click **Server > Application Servers** and select the `server_name`.
3. In the **Configuration** tab, navigate to **Server Infrastructure > Java and Process Management > Process Definition > Servant > Additional Properties: Java Virtual Machine**.

4. In the **Generic JVM arguments** field, remove the values that were added as a result of the Data Collector configuration. Make sure you do not remove the values that are not related to the Data Collector configuration.
5. For JVM custom properties, select and remove the values that were added as a result of the Data Collector configuration. Make sure you do not remove the values that are not related to the Data Collector configuration.
6. Click **Server > Application Servers** and select the *server_name*.
7. In the **Configuration** tab, navigate to **Process Definition > Servant > Custom Properties**.
8. For custom properties, select and remove the values that were added as a result of the Data Collector configuration. Make sure you do not remove the values that are not related to the Data Collector configuration.
9. Click **Server > Application Servers** and select the *server_name*.
10. Navigate to **Server Infrastructure: Administration > Custom Services**.
11. For custom services, select and remove the **am** custom service.
12. Click **Server > Application Servers** and select the *server_name*.
13. Navigate to **Performance: Performance Monitoring Infrastructure (PMI)**.
14. Modify the Performance Monitoring Service to the **none** level and set the startup to false.
15. Navigate to the page for environment variables at the server level: in the Navigation Pane, select **Environment > WebSphere Variables**, and navigate to the server level variables.
16. Select and remove the ITCAMDCHOME, ITCAM61HOME, ITCAM71HOME, MS_AM_HOME, and CCLOG_COMMON_DIR variables.
17. Edit the NLSPATH and LIBPATH environment variables to remove the ITCAM for Application Diagnostics paths.
18. If you selected to have SMF records to be written when you ran the configuration program, use the IBM WebSphere Application Server administrative console to disable the SMF activity and interval records (if they were not enabled prior to installing ITCAM for Application Diagnostics).
19. Save your changes.
20. For a Network Deployment (ND) environment, synchronize the changes with the node agent so that the changes at dmgr can be applied to individual server instances.
21. Run the IBM WebSphere Application Server wsc2n.sh script to process the options and verify that processing will be successful.

Part 3. Installing and Configuring the monitoring agent on z/OS

Chapter 6. Installing and configuring the monitoring agent on IBM z/OS

For instructions on installing the ITCAM Tivoli Enterprise Monitoring Agent on z/OS, see the *Program Directory for IBM Tivoli Composite Application Monitor (ITCAM) for Application Diagnostics on z/OS, Tivoli Enterprise Monitoring Agent V7.1.0*. You will also need to apply the latest maintenance for the monitoring agent, see Appendix A, “Applying the latest maintenance,” on page 157

This chapter provides complete instructions for configuring the ITCAM Tivoli Enterprise Monitoring Agent on z/OS. These steps are performed using Tivoli Monitoring's Installation and Configuration Assistance Tool, ICAT.

Configuring the monitoring agent on z/OS

These instructions assume that you have already installed and configured a Tivoli Enterprise Monitoring Server (monitoring server), either on z/OS, Windows, or a Linux or UNIX system, that this agent can communicate with. See either the *IBM Tivoli Monitoring: Installation and Setup Guide* (for Windows and UNIX) or the *Configuring IBM Tivoli Enterprise Monitoring Server on z/OS*.

Steps for configuring the monitoring agent on z/OS

Perform the following steps to configure the monitoring agent on z/OS.

- “Step 1: Invoke ICAT”
- “Step 2: Define the ICAT work environment” on page 103
- “Step 3: Begin the configuration” on page 106
- “Step 4: Begin configuring the monitoring agent” on page 107
- “Step 5: Build the monitoring agent runtime environment” on page 108
- “Step 6: Define RTE parameters” on page 110
- “Step 7: Build RTE libraries” on page 112
- “Step 8: Configure your new runtime environment” on page 113
- “Step 9: Configure the monitoring agent connection to the Data Collector” on page 116
- “Step 10: Create application server runtime members” on page 119
- “Step 11: Define the RTE address space parameters” on page 120
- “Step 12: Build the agent JCL” on page 126
- “Step 13: Configure the z/OS Persistent Datastore” on page 127
- “Step 14: Complete the agent configuration” on page 137
- “Step 15: Copy remaining product libraries” on page 143

Step 1: Invoke ICAT

To run ICAT, you need the *itmhlq.INSTLIB* dataset. You need this dataset first configuring any product running in the IBM Tivoli Monitoring framework. If the dataset has not yet been created, create one by running a batch job with a step as in the following example:

```
//MAKEINST EXEC PGM=IEBCOPY,REGION=0M
//SYSPRINT DD SYSOUT=*
//TKCIINST DD DSN=itmhlq.TKCIINST,DISP=SHR
//INSTLIB DD DSN=itmhlq.INSTLIB,DISP=(,CATLG),
```

```
//          UNIT=SYSALLDA,VOLUME=SER=yourvolume,
//          SPACE=(CYL,(10,2,132)),
//          DSORG=PO,RECFM=FB,LRECL=80,BLKSIZE=27920
//SYSIN      DD  *
//          COPY      INDD=TKCIINST,OUTDD=INSTLIB
/*
```

The following screen shows how you may invoke ICAT.



Figure 4. TSO Screen

When you have finished installing the Tivoli Enterprise Monitoring Agent, invoke ICAT from an ISPF option 6 or equivalent environment:

```
EXEC 'itmhlq.INSTLIB'
```

where *itmhlq* is the high-level qualifier you defined for your site's Tivoli Monitoring environment.

The ICAT welcome screen is displayed:

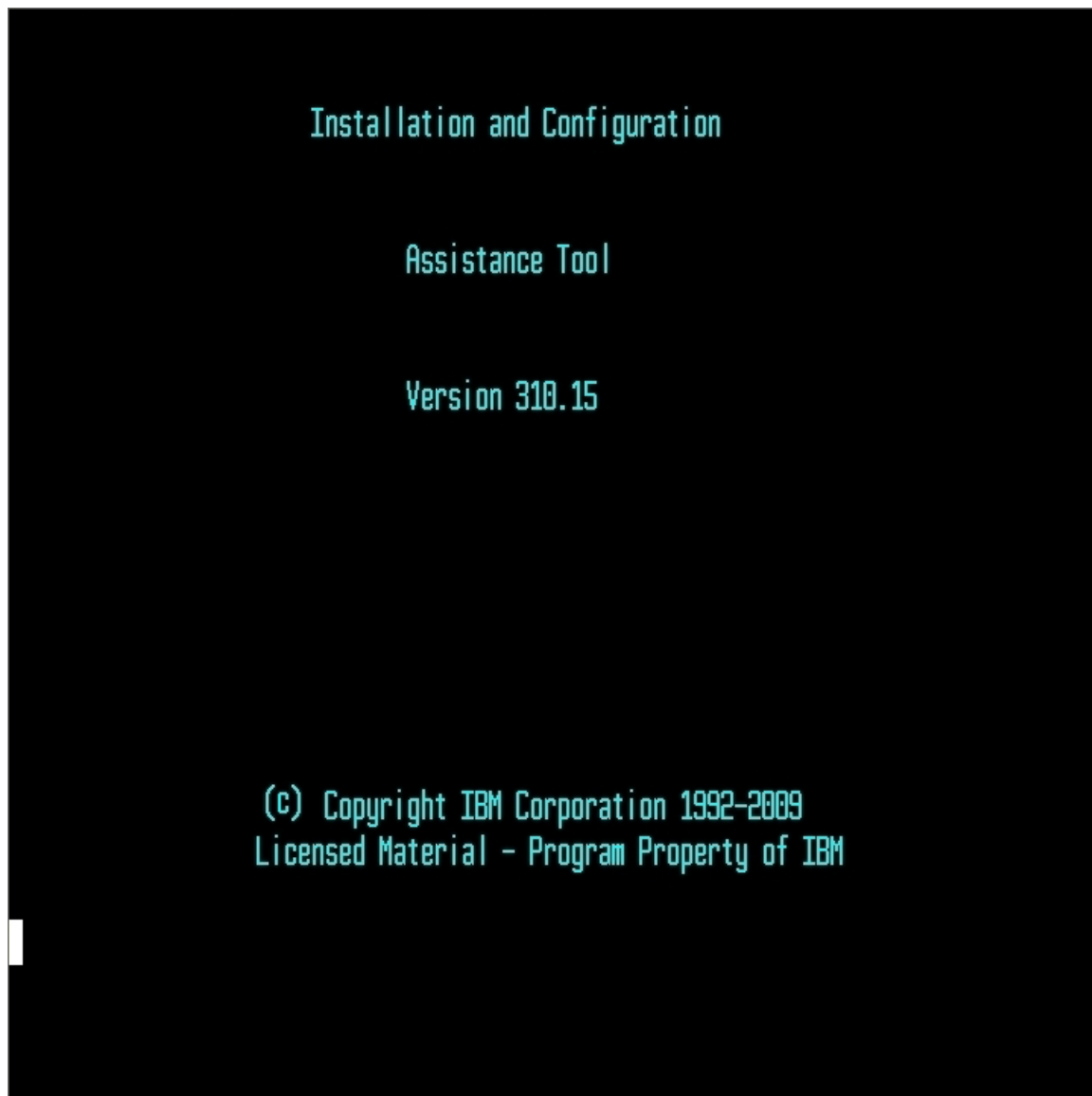


Figure 5. ICAT welcome screen

After a few seconds, this screen is replaced by the primary ICAT screen:

```
----- MAIN MENU -----
OPTION ==> 1

Enter the number to select an option:

1  Set up work environment

2  Install products

3  Configure products

I  Installation information          <=== Revised
S  Services and utilities

Installation and Configuration Assistance Tool Version 310.15
      (c) Copyright IBM Corp. 1992-2009
      Licensed Material - Program Property of IBM

F1=Help F3=Back
```

Figure 6. Primary ICAT screen

Enter 1 to set up your ICAT environment on z/OS. The Set Up Work Environment screen is displayed:

```
----- SET UP WORK ENVIRONMENT -----
OPTION ==> 1

Enter the number to select an option:

1  Specify JCL options
2  Set up configuration environment
3  Allocate work libraries

Last selected
Date      Time

Note: Once you create and submit the "Allocate work libraries" job,
      you must exit the installer and allow the job to run before
      restarting the installer.

F1=Help  F3=Back
```

Figure 7. Set Up Work Environment screen

Note: If you have already defined these ICAT options, skip to “Step 3: Begin the configuration” on page 106.

Step 2: Define the ICAT work environment

Enter 1 to define default JCL options; the Specify Options screen is displayed:

```

----- SPECIFY JCL OPTIONS -----
COMMAND ==> █

Specify allocation and processing options:

JCL REGION value ==> OM (Specify K/M suffix)

Installation work datasets .....
Unit/VolSer      Storclas/  PDSE
                Mgmtclas
3390
T60080
N

Specify the job statement for generated JCL:

==> //YN#?JOBS JOB , 'ERIC JACKSON',MSGCLASS=X,NOTIFY=EJACK
==> //*
==> //*
==> //*

Note: Press F1=Help for Batch Mode considerations when modifying
      jobcard values.

Enter=Next F1=Help F3=Back

```

Figure 8. Setting up work options

Specify the appropriate region, the DASD parameters for work datasets, and the JOB statements for submitted batch jobs; then press **Enter**. You return to the Set Up Work Environment screen, Figure 7 on page 103.

Note: To allocate ICAT's work libraries as PDSEs rather than standard PDSs, specify Y for the PDSE option. It is best practice to specify Y to avoid library space issues.

Enter 2 to define necessary configuration datasets (note that completing this one-time task fixes certain dataset names within the installed environment you are building). The Set Up Configuration Environment screen is displayed:

```

----- SET UP CONFIGURATION ENVIRONM      Enter required field
COMMAND ==>

*** Verify changes, then press ENTER to continue.

RTE allocation routine ==> IKJEFT01 (IKJEFT01/IEFBR14)

Runtime                                     Unit/   Storclas/
Datasets   High-Level Qualifier           VolSer  Mgmtclas  PDSE
VSAM        TDKYNT.HKYN710.TARGET          3390
                                           T60080
Non-VSAM    TDKYNT.HKYN710.TARGET          3390                N
                                           T60080
Work        .....                        3390

SMP/E
Datasets   High-Level Qualifier
Target     tdkynt.hkyn710.target

Enter=Next F1=Help F3=Back

```

Figure 9. Set Up Configuration Environment screen

Specify the tool you want to use to allocate these datasets, batch TSO or the IEFBR14 utility. Also specify the high-level qualifiers for allocating VSAM and, optionally, non-VSAM datasets (if you specify no non-VSAM entry, the VSAM entry is used) and their allocation parameters, as well as the allocation parameters for work datasets. The high-level qualifiers for SMP/E target libraries were defined when you loaded the product tape; supply that dataset prefix (it is possible that the VSAM, non-VSAM and SMP/E entries will all be the same).

When you press **Enter**, the screen is displayed again showing all supplied values for you to verify. Correct these values if necessary, and press **Enter** again. The updated parameters are saved, and you return to the Set Up Work Environment screen, Figure 7 on page 103. .

Note: When you press **Enter**, dataset names are fixed for this installation library and all the runtime environments it defines. You can, however, return to this screen to change such storage options as unit or volume serial number for future dataset allocations.

Enter option 3 to allocate necessary ICAT libraries. You enter the ISPF editor on the JCL script:

```
EDIT ---- TDKYNT.HKYN710.TARGET.INSTLIB(CI$UPG2) - 01.00 ----- Columns 001 072
COMMAND ==> sub                                SCROLL ==> CSR
***** IF YOU WISH TO SUBMIT THIS JOB NOW, TYPE 'SUBMIT' AND PRESS ENTER. *****
***** NOTE: JOBCARD REQUIRES ALL CAPS. *****
***** ***** Top of Data *****
==MSG> -Warning- The UNDO command is not available until you change
==MSG> your edit profile using the command RECOVERY ON.
000001 //YN#0JOBS JOB , 'ERIC JACKSON',MSGCLASS=X,NOTIFY=EJACK
000002 //*
000003 //*****
000004 //* DATE: 2009/10/22
000005 //* TIME: 17:07
000006 //*****
000007 //*
000008 //* JOB: TDKYNT.HKYN710.TARGET.INSTLIB(CI$UPG2)
000009 //*
000010 /***
000011 /*** IMPORTANT: AFTER YOU SUBMIT THIS JOB, YOU MUST EXIT THE
000012 /*** INSTALLATION TOOL AND ALLOW THE JOB TO RUN BEFORE
000013 /*** STARTING THE INSTALLATION TOOL.
000014 /***
000015 /*** READ NOTES SECTION BEFORE PROCEEDING.
000016 /***
```

Figure 10. JCL for allocating ICAT work libraries

Customize the JCL as necessary, and enter SUBMIT.

Note: After you submit this job, it cannot complete until you press End twice to leave ICAT, because this job requires exclusive access to the INSTLIB dataset.

After the job completes, examine its output, and ensure that each step ended with a return code of either 0 or 4.

Step 3: Begin the configuration

When you re-enter ICAT after defining the ICAT JCL parameters and work libraries in “Step 2: Define the ICAT work environment” on page 103, you return to the primary ICAT screen shown in Figure 6 on page 102. Enter option 3 to begin configuring the monitoring agent. The Configure Products screen is displayed:

```
----- CONFIGURE PRODUCTS -----
OPTION ==> 1

Enter the number to select an option:

1  Select product to configure

I  Configuration information          <=== Revised
S  Services and utilities

F1=Help  F3=Back
```

Figure 11. Configure Products screen

Step 4: Begin configuring the monitoring agent

Enter option 1. The Product Selection Menu screen is displayed, listing the products available for configuration:

```
----- PRODUCT SELECTION MENU -----  
COMMAND ==>  
  
Actions: S Select product  
  
_ IBM Tivoli Management Services on z/OS V6.2.2  
S ITCAM for Application Diagnostics on z/OS  
I ITCAM for Transactions, File Transfer Enabler for z/OS V7.1.0  
F1=Help F3=Back F5=Refresh F7=Up F8=Down
```

Figure 12. Product Selection Menu

Select **IBM Tivoli Composite Application Manager for WebSphere V7.1.0**, and press **Enter**.

Note: You do not need to select IBM Tivoli Monitoring Services on z/OS V6.2.2 to configure Tivoli Monitoring. You can configure Tivoli Monitoring at the same time as the monitoring agent itself is configured.

Step 5: Build the monitoring agent runtime environment

When you select the ITCAM for WebSphere Tivoli Enterprise Monitoring Agent for configuration, the Runtime Environments screen is displayed so you can build its runtime environment (RTE):

```
----- RUNTIME ENVIRONMENTS (RTEs) -----
COMMAND ==>

*** Current product entry selected: ***
    ITCAM for Application Diagnostics on z/OS

Actions: A Add RTE, B Build libraries, C Configure,
         L Load all product libraries after SMP/E,
         D Delete, U Update, V View values, Z Utilities
         R README Table of Contents

Action Name      Type      Sharing Description
  a    TEMA      sharing smp    ITCAM 7.1 TEMA Agent
F1=Help F3=Back (No RTEs defined, use Action A to Add)
```

Figure 13. Runtime Environments screen

For **Action**, enter A to name the RTE and define its structure. For **Name**, specify a name that is 1 - 8 characters in length (this name is appended to dataset names created for this RTE, and must be unique for the set of *itmhlq* datasets; the safest bet is to make it unique for the sysplex); supply any description you choose. For **Type**, specify either SHARING (which allows sharing of libraries across RTEs) or FULL (separate SMP/E and RTE libraries are built for each RTE).

If you specify SHARING, for **Sharing** enter the libraries to be shared, either SMP (as shown in Figure 13) or the name of an existing RTE. If you enter SMP, the RTE will use the library datasets installed by SMP/E. If you enter the name of another RTE, the new RTE will use the library files of that existing RTE. If that RTE was created as type FULL, it will have its own copy of the library datasets, and the new RTE will now use this copy as well.

Press **Enter**. The Add Runtime Environment screen is displayed.

Step 6: Define RTE parameters

When you press **Enter** on the Runtime Environments screen, the Add Runtime Environment (1 of 2) screen is displayed:

```
----- ADD RUNTIME ENVIRONMENT (1 of 2) -----
COMMAND ==>

RTE: TEMA      Type: SHARING Desc: ITCAM 7.1 TEMA Agent

  Libraries  High-level Qualifier  Volser Unit  Storclas Mgmtclas PDSE
  Non-VSAM   TDKYNT.HKYN710.TARGET        T6008D 3390      _____ N
  VSAM       TDKYNT.HKYN710.TARGET        T6008D      _____
  Mid-level qualifier ==> TEMA

  JCL suffix      ==> jobs          Remote RTE for transport ==> N (Y, N)
  STC prefix      ==> tema          Runtime members analysis ==> Y (Y, N)
  SYSOUT class    ==> X             Diagnostic SYSOUT class ==> X
  Load optimization ==> N (Y, N)

  Will this RTE have a Tivoli Enterprise Monitoring Server ==> n (Y, N)
    If Y, TEMS name ==> _____ (Case sensitive)

  Copy configuration values from RTE ==> _____ (Optional)

Enter=Next F1=Help F3=Back
```

Figure 14. Add Runtime Environment screen (1 of 2)

On this screen, you define dataset-allocation parameters for this RTE's new libraries, as well as the suffix for new JCL members and the prefix for started tasks. You also specify SYSOUT classes for submitted jobs and whether load optimization is active (when load optimization is in effect, only those modules that have changed are updated whenever the RTE libraries are refreshed). This can reduce the amount of DASD space required, but there is some overhead in determining which modules are unchanged.

If you want to create an RTE on the local system for transporting it to another system, enter Y in **Remote RTE for transport**. In this case, runtime libraries will not be allocated and configuration batch jobs will not be run.

If **Runtime members analysis** is set to Y, the configuration program will check if any values previously modified by the user are going to be overwritten; if so, it will display a warning. Reports on this information can also be generated from the RTE Utilities panel (RTE action Z).

Press **Enter**. The Add Runtime Environment (2 of 2) screen is displayed:

```
----- ADD RUNTIME ENVIRONMENT (2 of 2) -----
COMMAND ==>

Use z/OS system variables? ==> N (Y, N)   Use VTAM model applids? ==> N (Y, N)
RTE name specification      ==> &SYSNAME
RTE base alias specification ==> _____ n/a
Applid prefix specification ==> K&SYSCLONE.

Security system             ==> NONE (RACF, ACF2, TSS, NAM, None)
ACF2 macro library          ==> _____
Fold password to upper case ==> Y (Y, N)

If you require VTAM communications for this RTE, complete these values:
Applid prefix               ==> kyn      Network ID           ==> net1
Logmode table               ==> KDSMTAB1 LU6.2 logmode        ==> CANCTDCS

If you require TCP/IP communications for this RTE, complete these values:
Hostname                    ==> tv16008

Started task                ==> * (Recommended default = *)
Port number                 ==> 1918
Enter=Next F1=Help F3=Back
```

Figure 15. Add Runtime Environment screen (2 of 2)

Complete this screen as follows:

1. Use **z/OS system variables** field, you specify whether the variables set by the individual z/OS system image be used to make the RTE values unique; for more information, see the *IBM Tivoli Monitoring: Installation and Setup Guide*.
2. For **Security system**, specify the security system this RTE will run under and, if appropriate, the ACF2 macro library. Specify NONE if no security software is to be activated.

3. If this monitoring agent must communicate to other Tivoli Monitoring components (such as a z/OS monitoring server) using VTAM®, complete the VTAM communications section.
 - The **Applid prefix** is required and you must set it to some string of your choice; a good string to use is **kyn**, to represent the ITCAM for WebSphere agent (whose product prefix is kyn).
 - For the **Network ID**, check the ATCSTRxx member of VTAMLST library of your site. Consult VTAM systems programmer of your site for assistance with all these parameters.
 - Use Create LU6.2 logmode to create the **LU6.2 logmode** and **Logmode table** required by the monitoring server.

Note: Running this job requires update access to VTAMLIB load library of your site.

Whatever VTAM values you specify, make sure that they are consistent with those defined for other Tivoli Monitoring components.

4. If this monitoring agent requires TCP/IP to communicate to other Tivoli Monitoring components (such as a monitoring server running on Windows, Linux, or UNIX), complete the TCP/IP communications section. Enter the hostname or address of the IP interface which the TEMA will use, and the port number to be used in the communication. Make sure that the values you specify here are consistent with those defined for your Tivoli Monitoring environment TCP/IP communications.

When all the items are correctly defined, press **Enter**. You return to the Runtime Environments definition screen shown in Figure 13 on page 109.

Step 7: Build RTE libraries

On the Runtime Environments screen (shown in Figure 13 on page 109), on the line showing the new RTE, specify option B to build the necessary RTE libraries. You enter the ISPF editor on the JCL shown in Figure 16 on page 113:

```

EDIT ---- TDKYNT.HKYN710.TARGET.INSTJOBS(YN#1JOBS) - 01.00 --- Columns 001 072
COMMAND ==> sub                                SCROLL ==> CSR
***** IF YOU WISH TO SUBMIT THIS JOB NOW, TYPE 'SUBMIT' AND PRESS ENTER. *****
***** NOTE: JOBCARD REQUIRES ALL CAPS. *****
***** ***** Top of Data *****
==MSG> -CAUTION- Profile changed to CAPS ON (from CAPS OFF) because the
==MSG> data does not contain any lower case characters.
==MSG> -Warning- The UNDO command is not available until you change
==MSG> your edit profile using the command RECOVERY ON.
000001 //YN#1JOBS JOB , 'ERIC JACKSON',MSGCLASS=X,NOTIFY=EJACK
000002 //*
000003 //*****
000004 //* DATE: 2009/10/22
000005 //* TIME: 17:14
000006 //*****
000007 //*
000008 //* JOB: TDKYNT.HKYN710.TARGET.INSTJOBS(YN#1JOBS)
000009 //*
000010 //*****
000011 //* DATE: 2009/10/22
000012 //* TIME: 17:14
000013 //*
000014 //*
000015 //* PURPOSE: ALLOCATE A RUNTIME ENVIRONMENT FOR THIS PRODUCT.

```

Figure 16. JCL for allocating a new RTE's libraries

Customize the JCL as necessary, and enter SUBMIT. Press F3 to return to the Runtime Environments definition screen shown in Figure 13 on page 109.

Step 8: Configure your new runtime environment

On the Runtime Environments screen (shown in Figure 13 on page 109), specify option C to configure your new RTE. The Product Component Selection Menu screen is displayed:

```
----- PRODUCT COMPONENT SELECTION MENU -----
COMMAND ==> 2

The following list of components requires configuration to make the product
operational. Refer to the appropriate configuration documentation if you
require additional information to complete the configuration.
To configure the desired component, enter the selection number on the command
line. You should configure the components in the order they are listed.

Note: It may not be necessary to configure Tivoli Enterprise Monitoring Server
      (TEMS) component, if listed below. Press F1 for more information.

      COMPONENT TITLE

1  Tivoli Enterprise Monitoring Server
2  ITCAM for Application Diagnostics, TEMA
```

Figure 17. Product Component Selection menu

You already have configured a monitoring server for use with this new agent; if you have, skip option 1, and specify the Composite Application Manager for WebSphere Agent option.

Note: If you have not yet configured a monitoring server for this agent and you plan to run your monitoring server on z/OS, specify option 1, and follow the instructions in the *Configuring IBM Tivoli Enterprise Monitoring Server on z/OS* guide.

Select option 2 and press **Enter**. The Product RTE configuration screen is displayed:

```
----- CONFIGURE ITCAM for Application Diagnostics / RTE: TEMA -----
OPTION ==> 2

Perform the appropriate configuration steps in order:
If you have a TEMS in this RTE that this Agent will
communicate with, start with option 1; otherwise with 2.

I Configuration information (What's New)                <=== Revised

1 Register with local TEMS

2 Specify Java SubAgent parameters
3 Specify agent collection options
4 Create application server runtime members

5 Specify agent address space parameters
6 Create runtime members

7 Configure persistent datastore (in Agent)

8 Complete the configuration

F1=Help  F3=Back
```

Figure 18. Product RTE configuration screen

Note: If your agent connects to a local monitoring server, enter 1 to define the new agent to the monitoring server. Customize the JCL as necessary, and enter SUBMIT. You return to the Configure *prodname* RTE screen shown in Figure 18. If your agent connects to a remote monitoring server, skip option 1.

Enter 2 to specify Java SubAgent parameters. The following screen is displayed:

```
----- UPDATE OPTIONS / RTE: TEMA -----
COMMAND ==>

Update the Java SubAgent options.

Java SubAgent STC name ==> TEMAYNSA      (Default: TEMAYNSA )

Application port    ==> 63337            (Default: 63337)

SubAgent Timeout    ==> 60              (Default: 60 seconds)

Java home directory:                                (Default: /usr/lpp/java/J5.0)
==> /usr/lpp/java/J5.0
Note: A Java 5.0 or later JVM is required for the Java SubAgent.

Product home directory:                            (Default: /u/itcam71/TEMA)
==> /u/itcam71/TEMA

Normal job spawn    ==> Y   y or n      (Default: y - Normal job spawn)

*** Warning: You are about to update the DEFAULT entry.
              (F3 to cancel, Enter to proceed)
Enter=Next F1=Help F3=Back
```

Figure 19. Specify Java SubAgent Parameters screen

Enter values for the following fields:

Java home directory: the home directory (JAVA_HOME) for a Java Virtual Machine (JVM). This JVM will be used by the Java Subagent component of the monitoring agent.

Product home directory: the path for the home directory for this RTE. This must be unique for every RTE. If this directory does not exist, it will be created.

After specifying the values, press **Enter**. You will return to the Product RTE configuration screen (Figure 18 on page 115)

Step 9: Configure the monitoring agent connection to the Data Collector

On the Product RTE configuration screen (Figure 18 on page 115), enter option 3 to define the data the new ITCAM for WebSphere Tivoli Enterprise Monitoring Agent will collect from the Data Collector.

The Update Agent Collection Options screen is displayed:

```
----- UPDATE AGENT COLLECTION OPTIONS / RTE: TEMA -----
COMMAND ==>

Update required data for instance.

Agent identification string ==> TVT6008 Collector port ==> 63335
Garbage collection data (Y/N) ==> Y GC polling freq. ==> 60
Maximum log error events ==> 50 Log scan interval ==> 60

Request data collection method (D=On Demand/F=Fixed Int) ==> F
Monitoring level (N/1/2) ==> 1 Sample rate (0-100) ==> 2
On-demand max sample age ==> 60 Fixed-interval time ==> 60
Resource data collection method (D=On Demand/F=Fixed Int) ==> D
Monitoring active (Y/N) ==> Y
On-demand max sample age ==> 60 Fixed-interval time ==> 60
Application Dashboard Completion Rate Percentages
Fair completion ==> 99 Bad completion ==> 95
Application Dashboard Automatic Thresholding Percentages
Baseline Selection ==> 50 Deviation ==> 200
Fair Projection ==> 150 Bad Projection ==> 300

*** Warning: You are about to update the DEFAULT entry.
(F3 to cancel, Enter to proceed)
Enter=Next F1=Help F3=Back
```

Figure 20. Update Agent Collection menu

Update these fields as follows:

Agent Identification string

A name to be used in place of the system host name for identification purposes within the portal client.

Collector port

The port number the monitoring agent will use for retrieving monitoring data from the ITCAM for WebSphere Data Collector.

Garbage Collection Data

Enter Y to collect statistics about the Java virtual machine's invocation of its garbage-collection algorithm; otherwise enter N.

GC Polling Freq.

The time, in seconds, between scans of the verboseGC logs for garbage-collection statistics; the value is meaningful only if you set **Collect Garbage Collection Data** to Y.

Maximum log error events

The maximum number of WebSphere Application Server log messages the monitoring agent can store before overwriting them.

Log scan interval

The time, in seconds, between scans of the WebSphere Application Server message logs for key events.

Request data collection method

This parameter controls how frequently data is collected on service requests made by your site's WebSphere applications:

Specify F (Fixed Interval) to collect request data at a fixed interval.

Specify D (On Demand) to collect request data only when the portal user requests them.

Monitoring level

The monitoring level for request data:

Specify N to disable collection of request data.

Specify 1 to collect data only about Level1 requests (also called edge requests), such as servlets and JSPs.

Specify 2 to collect data about Level2 requests (that is, both edge requests and subsidiary requests), such as JDBC and JMS requests. If you request Level2 monitoring, all subsidiary requests for the selected edge requests are monitored.

Sample rate

The percentage of all edge (Level1) requests to be monitored, in the range 1 - 100.

On-demand max sample age

The maximum length of time, in seconds, for which on-demand request data be collected. This value is meaningful only if you set **Request data collection method** to **On Demand**.

Fixed-interval time

The interval between collections of request data, in seconds. The value is meaningful only if you set **Request data collection method** to **Fixed**.

Resource data collection method

This parameter controls how frequently resource (that is, Performance Monitoring Infrastructure - PMI) data is collected about your site's WebSphere applications:

Specify F (Fixed Interval) to collect resource data at a fixed interval.

Specify D (On Demand) to collect resource data only when the portal user requests them.

Monitoring active

This parameter turns monitoring on or off for resource (that is, PMI) data:

Specify Y to enable collection of resource data.

Specify N to disable collection of resource data.

On-demand max sample age

The maximum length of time, in seconds, that for which resource (PMI) data be collected. This value is meaningful only if you set **Resource data collection method** to **On Demand**.

Fixed-interval time

The interval, in seconds, between collections of resource (that is, PMI) data. This value is meaningful only if you set Resource data collection method to Fixed.

Application Dashboard Completion Rate Percentages

The default request completion rates to be used as Fair and Bad threshold for Application Health Summary dashboards. For details, see the online Help document in the Tivoli Monitoring portal.

Application Dashboard Automatic Thresholding Percentages

The values used for determining automatic thresholds for request response times, in the baselining process. For details, see the online Help document in the Tivoli Monitoring portal.

After you have defined all data-collection parameters, press **Enter** to save your changes. Then press F3 to exit this screen (do *not* press F3 until you have saved your updates) and return to the Product RTE configuration screen (Figure 18 on page 115).

Step 10: Create application server runtime members

From the Product RTE configuration screen (Figure 18 on page 115), enter option 4 to create the application server runtime members. These members contain parameter values that control agent execution and effectively implement the agent definitions you created in “Step 9: Configure the monitoring agent connection to the Data Collector” on page 116. You enter the ISPF editor on the JCL shown in figure 59:

```

EDIT ---- TDKYNT.HKYN710.TARGET.INSTJOBS(YN#6JOBS) - 01.00 --- Columns 001 072
COMMAND ==> sub                                SCROLL ==> CSR
***** IF YOU WISH TO SUBMIT THIS JOB NOW, TYPE 'SUBMIT' AND PRESS ENTER. *****
***** NOTE: JOBCARD REQUIRES ALL CAPS. *****
***** ***** Top of Data *****
==MSG> -CAUTION- Profile changed to CAPS OFF (from CAPS ON) because data
==MSG>           contains lower case characters.
==MSG> -Warning- The UNDO command is not available until you change
==MSG>           your edit profile using the command RECOVERY ON.
000001 //YN#6JOBS JOB , 'ERIC JACKSON',MSGCLASS=X,NOTIFY=EJACK
000002 //*
000003 //*****
000004 //* DATE: 2009/10/22
000005 //* TIME: 17:28
000006 //*****
000007 //*
000008 //* JOB: TDKYNT.HKYN710.TARGET.INSTJOBS(YN#6JOBS)
000009 //*
000010 //*****
000011 //*
000012 //*
000013 //* PURPOSE: CREATE APPLICATION SERVER RUNTIME MEMBERS
000014 //*

```

Figure 21. JCL for creating agent runtime members

Customize the JCL as necessary, and enter SUBMIT.

After this job runs, press F3 to return to the Product RTE configuration screen (Figure 18 on page 115).

Step 11: Define the RTE address space parameters

From the Product RTE configuration screen (Figure 18 on page 115), enter option 5 to define the address space within which the new ITCAM for WebSphere Tivoli Enterprise Monitoring Agent will run. The Specify Agent Address Space Parameters screen is displayed:

```
----- SPECIFY AGENT ADDRESS SPACE PARAMETERS -----
COMMAND ==>

The following information is needed to define the Agent address space.
Agent started task          ==> TEMAYN
Connect to TEMS in this RTE ==> N      (Y, N)
Name of Primary TEMS       ==> None

Specify the communication protocols in priority sequence.
IP.PIPE ==> 1 (Non-secure NCS RPC)
IP.UDP  ==> 2 (Non-secure NCS RPC)
SNA.PIPE ==> _ (Non-secure NCS RPC)
IP6.PIPE ==> _ (IP.PIPE for IPV6)
IP6.UDP  ==> _ (IP.UDP for IPV6)
IP.SPIPE ==> _ (Secure IP.PIPE)
IP6.SPIPE ==> _ (Secure IP.PIPE for IPV6)

Note: Enable only protocol(s) in use by the Primary TEMS.

Enter=Next F1=Help F3=Back F5=Advanced F10=CMS List
```

Figure 22. Specify Agent Address Space Parameters screen

If you want to, change the name assigned to the address-space started task. If your monitoring agent will connect to a monitoring server defined within this runtime environment, specify Y for the **Connect to TEMS in this RTE** field, and define that monitoring server's name, in the same format you used when completing the Add Runtime Environment (1 of 2) screen in "Step 6: Define RTE parameters" on page 110 (for example, Z:CMS). When specifying the communications protocols this agent can use for communicating with the monitoring server, ensure that you specify only protocols defined for that monitoring server when you built it. The numbers you enter indicate the priority sequence.

If you wish to use the monitoring server installed in the same RTE (see *IBM Tivoli Management Services on z/OS: Configuring the Tivoli Enterprise Monitoring Server on z/OS*), specify Y for the **Connect to TEMS in this RTE** field. Otherwise, specify N.

In this panel, you may also press F5 to move to the Specify Advanced Agent Configuration Values screen:

```
----- SPECIFY ADVANCED AGENT CONFIGURATION VALUES -----
COMMAND ==>

Specify the advanced configuration options for this Agent.

Enable secondary TEMS          ==> N (Y, N)
  Name of secondary TEMS       ==> None
Enable startup console messages ==> N (Y, N)
Enable WTO messages            ==> N (Y, N)
Reconnect after TCP/IP recycle ==> N (Y, N)
Intervals (hh:mm):
  Storage detail logging: Hours ==> 24 (0-24) Minutes ==> 00 (0-60)
  Flush VSAM buffers:      Hours ==> 24 (0-24) Minutes ==> 00 (0-60)
Virtual IP Address (VIPA) type ==> N (S=Static, D=Dynamic, N=None)
Minimum extended storage       ==> 256000 K
Language locale ==> 1a (Press F1=Help for a list of codes)
Program to Program Interface (PPI) information:
  Forward Take Action commands to NetView for z/OS? ==> N (Y, N)
  NetView PPI receiver          ==> CNMPCMDR
  Agent PPI sender              ==> _____

Enter=Next F1=Help F3=Back F5=Advanced F10=CMS List
```

Figure 23. Specify Advanced Agent Configuration Values screen

On this screen, you may specify the following options:

1. Whether you want to assign a secondary monitoring server to this agent and, if so, its name.
2. Whether you want console and write-to-operator messages displayed.
3. How frequently you want details written out about the current consumption of storage subpools (the smaller the number, the more frequent the console messages).

Note: The **Flush VSAM buffers** option does not apply to the ITCAM for WebSphere agent; set it to the maximum (24 hours). Similarly the **Virtual IP Address (VIPA) type** does not apply; set it to N (None).

In the **Minimum Extended Storage**, the default of 6 MB be sufficient to run the ITCAM for WebSphere agent under most circumstances. If you need to increase this value for some reason, you will probably need to increase the region size of the agent started task.

Do not change the **Language locale** field unless you have special requirements.

If the monitoring agent is to forward Take Action commands to IBM Tivoli NetView® for z/OS (version 5.2 or later), enter Y in **Forward Take Action commands to NetView for z/OS?**. In this case, you also need to set the **NetView PPI receiver** and **Agent PPI sender** names.

When you press **Enter** to save your updates, you return to the Specify Agent Address Space Parameters screen (Figure 22 on page 121).

Press F10 to display the Communication Selection panel. On this screen, you can select the monitoring server and RTE that you want to use:

```
----- COMMUNICATION SELECTION PANEL FOR T          TEMS LIST EMPTY
COMMAND ==> █

Select the primary TEMS to connect to this agent.

The TEMS table below lists eligible TEMS that you have configured in
this TDKYNT.HKYN710.TARGET.INSTLIB.
Enter S next to the TEMS that you wish to connect to this agent.
Important: To manually enter the *TEMS information, press F5-Advanced.
           * Typically applicable to non-local TEMS in another platform
             or in another RTE not known to this installation environment.

-----
      TEMS      RTE name      RTE
      Type      (mid-level)  Description
-----
F1=Help F3=Back F5=Advanced F7=Up  F8=Down
```

Figure 24. Tivoli Enterprise Monitoring Server selection screen

If the list is empty or does not list the monitoring server that you need to use, press F5. A panel for the monitoring server information for the monitoring server is displayed.

```

----- SPECIFY AGENT PRIMARY TEMS VALUES -----
COMMAND ==>

Primary TEMS name    ==> NONAME (case sensitive)

Complete this section if the Agent is connecting to its primary TEMS using:
SNA protocol (Enter applicable VTAM values of its primary TEMS):
  LU6.2 logmode      ==> _____
  Logmode table name ==> _____
  Local location broker applid ==> _____
  Network ID         ==> _____

IP protocol (Enter applicable network address and respective port number(s)):
* Network address (Hostname of Primary TEMS):
  ==> tems.hostname
      IP.PIPE port number ==> 1918 (Non-secure NCS RPC)
      IP6.PIPE port number ==> _____ (IP.PIPE for IPV6)
      IP.SPIPE port number ==> _____ (Secure IP.PIPE)
      IP6.SPIPE port number ==> _____ (Secure IP.PIPE for IPV6)
      IP.UDP port number ==> 1918 (Non-secure NCS RPC)
      IP6.UDP port number ==> _____ (IP.UDP for IPV6)
* Note: See F1=Help for TSO HOMETEST command instructions.
Enter=Next F1=Help F3=Back

```

Figure 25. Panel for the monitoring server information

In this panel, you need to specify the TEMS name, as well as the TEMS parameters for the selected communication system - SNA or TCP/IP. If using TCP/IP, you only need to enter port numbers for the protocols that will be used, as set in the Specify Agent Address Space Parameters screen (see Figure 22 on page 121). After entering the settings, press **Enter** to return to the Communication Selection panel (see Figure 24 on page 123).

In the Communication Selection panel, select the monitoring server to use. Then press **Enter** to save the selection and move to the screens where you define communications parameters for each of the monitoring server communications protocols you listed. One or more of the protocol specification screens will be displayed, such as those shown in Figure 26 on page 125 and Figure 27 on page 126.

```
----- SPECIFY AGENT IP.PIPE CONFIGURATION VALUES -----
COMMAND ==>

Specify the IP.PIPE communication values for this Agent.  These network
address-related values are for the z/OS system where the Agent runs on.

* Network address (Hostname):
  ==> VT6008
  Started task ==> * (Recommended default = *)
  Network interface list: (If applicable)
  ==> _____

Specify additional configuration values.

  Address translation      ==> N      (Y, N)
  Partition name          ==> _____
* Note: See F1=Help for TSO HOMETEST command instructions.

Enter=Next F1=Help F3=Back
```

Figure 26. Specify Agent IP.PIPE Configuration Values screen

```
----- SPECIFY AGENT IP.UDP CONFIGURATION VALUES -----
COMMAND ==> █

Specify the IP.UDP communication values for this Agent.  These network
address-related values are for the z/OS system where the Agent runs on.

* Network address (Hostname):
  ==> TVT6008
Started task ==> * (Recommended default = *)
Network interface list: (If applicable)
  ==>

* Note: See F1=Help for TSO HOMETEST command instructions.

Enter=Next F1=Help F3=Back
```

Figure 27. Specify Agent IP.UDP Configuration Values screen

Complete these screens using the values that are set up on the monitoring server.

When you press **Enter** on the third and final protocol screen, you return to the Configure *prodname* RTE screen (Figure 18 on page 115).

Step 12: Build the agent JCL

Enter 6 on the Configure *prodname* RTE screen (Figure 18 on page 115) to configure the runtime environment's JCL members for the agent. You enter the ISPF editor on the JCL shown in figure 65:

```

EDIT ---- TDKYNT.HKYN710.TARGET.INSTJOBS(YN#3JOBS) - 01.00 --- Columns 001 072
COMMAND ==> sub                                SCROLL ==> CSR
***** IF YOU WISH TO SUBMIT THIS JOB NOW, TYPE 'SUBMIT' AND PRESS ENTER. *****
***** NOTE: JOBCARD REQUIRES ALL CAPS. *****
***** ***** Top of Data *****
==MSG> -Warning- The UNDO command is not available until you change
==MSG> your edit profile using the command RECOVERY ON.
000001 //YN#3JOBS JOB , 'ERIC JACKSON',MSGCLASS=X,NOTIFY=EJACK
000002 //*
000003 //*****
000004 //* DATE: 2009/10/22
000005 //* TIME: 17:40
000006 //*****
000007 //*
000008 //* JOB: TDKYNT.HKYN710.TARGET.INSTJOBS(YN#3JOBS)
000009 //*
000010 //*****
000011 //* DATE: 2009/10/22
000012 //* TIME: 17:40
000013 //*
000014 //*
000015 //* PURPOSE: THIS JOB CREATES ALL THE RUNTIME MEMBERS FOR:
000016 //*

```

Figure 28. JCL for allocating the agent's runtime members

Customize the JCL as necessary, and enter SUBMIT. Press F3; you return to the Configure *prodname* RTE screen (Figure 18 on page 115).

Step 13: Configure the z/OS Persistent Datastore

Enter 7 on the Configure *prodname* RTE screen (Figure 18 on page 115) to configure the ITCAM for WebSphere Tivoli Enterprise Monitoring Agent's storage of historical data within the z/OS Persistent Datastore (PDS).

Note: The acronym PDS for the z/OS Persistent Datastore is distinct from, and should not be confused with, the z/OS Partitioned Dataset (dataset library) commonly known as PDS.

The Specify Persistent Datastore Values screen is displayed:

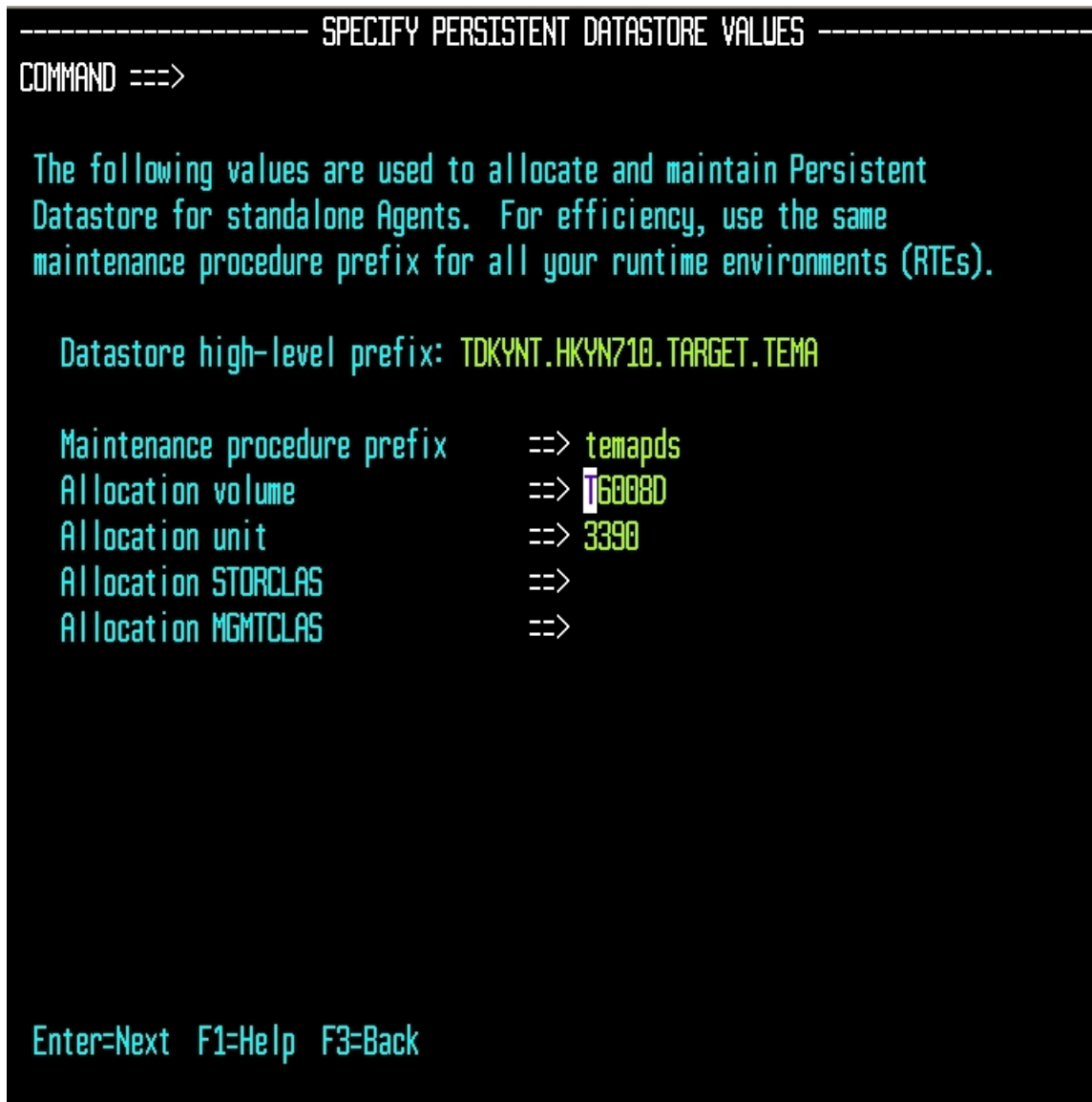


Figure 29. Specify Persistent Datastore Values menu

If the monitoring server was configured locally, the values initially displayed are those defined for the PDS when you built the monitoring server. You can change them now, for those files that will be allocated for the ITCAM for WebSphere Tivoli Enterprise Monitoring Agent. (You might especially want to specify a new prefix—one specific to the ITCAM for WebSphere Tivoli Enterprise Monitoring Agent—for the started tasks that will be submitted to maintain the PDS files.) When finished, press Enter; the Allocate Persistent Datastore Menu screen is displayed:

```
----- CONFIGURE PERSISTENT DATASTORE -----
OPTION ==> 1

Perform these configuration steps in order:

1 Modify and review datastore specifications
2* Create or edit PDS maintenance jobcard
3 Create runtime members
4 Allocate and initialize datastore files
5 Complete persistent datastore configuration

* Note: The initial PDS maintenance jobcard defaults to the jobcard
set on the Set up work environment option. This jobcard is
shared by all products that configured historical collection
within this RTE=TEMA. Change to a generic jobcard, as
necessary.

F1=Help F3=Back
```

Figure 30. Allocate Persistent Datastore Menu

Enter 1 to define the allocation of PDS files. The Persistent Datastore Specifications screen is displayed:

```

----- MODIFY AND REVIEW DATASTORE SPECIFICATIONS Row 1 to 1 of 1
COMMAND ==> █

Modify persistent datastore allocation and maintenance information as required.
Press Enter to accept values and then F3 to return.

Datastore high-level qualifier: TDKYNT.HKYN710.TARGET.TEMA

Group   -Datasets in Group- Volser/  Storclas/ -Est Cyl-  -Maintenance-
Name    Lowlev   Count   Unit      Mgmtclas  Space  Backup Export Extract
-----
KYN     RKYNPDS    3   T60080  _____ 427_    N      N      N
          3390_____

F1=Help F3=Back

```

Figure 31. Persistent Datastore Specifications screen

Specify the allocation and maintenance parameters for these datasets.

Note the two subheadings, **Lowlev** and **Count**, under the heading Datasets in Group. The **Lowlev** value is the suffix for the PDS dataset. The **Count** value is the number of PDS datasets for this group. The PDS rotates the use of these datasets; when one fills up, data recording begins on the next dataset, and a PDS maintenance job is started to clear the filled dataset.

When you have finished, press **Enter** and then F3; you return to the Allocate Persistent Datastore Menu screen (Figure 30 on page 129).

Enter 2 to update the PDS maintenance job's JOB information. You enter the ISPF editor on the JCL shown in figure 69:

```
----- CREATE OR EDIT PDS MAINTENANCE JOBCARD -----  
COMMAND ==>  
  
Specify the job statement for Persistent Datastore jobs:  
  
Job statement for RTE TEMA:  
==> //TEMAPDS2 JOB , 'ERIC JACKSON',MSGCLASS=X,NOTIFY=EJACK  
==> //*  
==> //*  
==> /*  
  
Note: This jobcard is shared by all products within this RTE.  
  
Enter=Next F1=Help F3=Back
```

Figure 32. Create or Edit PDS Maintenance Jobcard screen

This job information is saved in the RKANSAM library, member KPDJOB and used to run the PDS maintenance jobs. Update the statements as necessary, and press **Enter** to return to the Allocate Persistent Datastore Menu (Figure 30 on page 129). Alternatively, you may press F3 to return to the Allocate Persistent Datastore Menu without updating the JCL.

Enter 3 to create the PDS maintenance JCL members. A PDS information panel is displayed.

```
----- UPGRADE PERSISTENT DATASTORE MAINTENANCE PROCEDURES -----
OPTION ==> █

The Configure persistent datastore (PDS) historical data collection
facility now supports a more simplified PDS maintenance procedure. It
no longer requires the submission of a TEMAPDS2 batch job and the PDS
jobcard (KPDJOBBC) in TDKYNT.HKYN710.TARGET.TEMA.RKANSAMU is no longer required

The enhancement requires recreating the following PDS members:
- TDKYNT.HKYN710.TARGET.TEMA.RKANSAMU(TEMAPDS1)
- TDKYNT.HKYN710.TARGET.TEMA.RKANSAM(TEMAPDSC)

Important:
1. TEMAPDS1 maintenance procedure must be refreshed in your system
   procedure library to implement the new support.
2. Since the REXX procedure associated with the improved persistent
   datastore processing runs in a TSO environment, the KPDDSCO
   program must be enabled to execute as an authorized program under
   TSO. This can be done by adding the KPDDSCO name to the system
   PARMLIB(IKJTSONn) member under the AUTHPGM section.

Press F1=Help for more information on important migration considerations.

Enter=Next F1=Help
```

Figure 33. PDS information panel

Press **Enter**. You enter the ISPF editor on the JCL shown in Figure 34 on page 133.

```

EDIT ---- TDKYNT.HKYN710.TARGET.INSTJOBS(YN#PJOB) - 01.00 --- Columns 001 072
COMMAND ==> sub                                SCROLL ==> CSR
**** IF YOU WISH TO SUBMIT THIS JOB NOW, TYPE 'SUBMIT' AND PRESS ENTER. ****
****                                     NOTE: JOBCARD REQUIRES ALL CAPS.                                     ****
***** ***** Top of Data *****
==MSG> -Warning- The UNDO command is not available until you change
==MSG>                your edit profile using the command RECOVERY ON.
000001 //YN#PJOB JOB , 'ERIC JACKSON',MSGCLASS=X,NOTIFY=EJACK
000002 //*
000003 //*****
000004 //* DATE: 2009/10/22
000005 //* TIME: 17:44
000006 //*****
000007 //*
000008 //* JOB: TDKYNT.HKYN710.TARGET.INSTJOBS(YN#PJOB)
000009 //*
000010 //*****
000011 //* DATE: 2009/10/22
000012 //* TIME: 17:44
000013 //*
000014 //*
000015 //* PURPOSE: THIS JOB CREATES PERSISTENT DATASTORE MEMBERS
000016 //*

```

Figure 34. JCL for creating PDS maintenance members

Customize the JCL as necessary, and enter SUBMIT. Then press F3 to return to the Allocate Persistent Datastore Menu (Figure 30 on page 129).

Enter 4 to submit the job that allocates the PDS files. You enter the ISPF editor on the JCL shown in Figure 35 on page 134

```

EDIT ---- TDKYNT.HKYN710.TARGET.INSTJOBS(YN#QJOBS) - 01.00 --- Columns 001 072
COMMAND ==> sub                                SCROLL ==> CSR
***** IF YOU WISH TO SUBMIT THIS JOB NOW, TYPE 'SUBMIT' AND PRESS ENTER. *****
***** NOTE: JOBCARD REQUIRES ALL CAPS. *****
***** ***** Top of Data *****
==MSG> -CAUTION- Profile changed to CAPS ON (from CAPS OFF) because the
==MSG> data does not contain any lower case characters.
==MSG> -Warning- The UNDO command is not available until you change
==MSG> your edit profile using the command RECOVERY ON.
000001 //YN#QJOBS JOB , 'ERIC JACKSON',MSGCLASS=X,NOTIFY=EJACK
000002 //*
000003 //*****
000004 //* DATE: 2009/10/22
000005 //* TIME: 17:45
000006 //*****
000007 //*
000008 //* JOB: TDKYNT.HKYN710.TARGET.INSTJOBS(YN#QJOBS)
000009 //*
000010 //*****
000011 //* DATE: 2009/10/22
000012 //* TIME: 17:45
000013 //*
000014 //*

```

Figure 35. JCL for allocating Persistent Datastore files

Customize the JCL as necessary, and enter SUBMIT. Then press F3 to return to the Allocate Persistent Datastore Menu (Figure 30 on page 129).

Note: This action will normally take some time to complete while it formats the datasets for persistent storage. It may instead complete quickly because the PDS datasets already exist from a prior configuration. In this case, you need to delete these datasets, so that the job can reformat or reallocate them, and then submit the job again. The datasets to delete are named *itmhlq.rtename.RKYNPDSx* and *itmhlq.rtename.RYNSGRP_x*, where *itmhlq* is the high-level qualifier you defined for your site's Tivoli Monitoring environment, *rtename* is the name you gave this runtime environment, and *x* is a digit, usually 1 to 3.

Enter 5 to complete PDS allocation. The first screen of the Complete Persistent Datastore Configuration process is displayed. Press DOWN (F8) to scroll through the screens:

```

+-----+
+-----+ Persistent Datastore +-----+
+-----+

                COMPLETE THE CONFIGURATION

After configuring the Persistent Datastore (PDS) component for this
product, you must perform the following procedure outside of the
Configuration tool to finalize configuration.

Perform the following steps for each of the items listed below,
if applicable:

Step 1 - Copy procedures to PROCLIB.

    Copy the following members from:

        TDKYNT.HKYN710.TARGET.TEMA.RKANSAMU

    to your system procedure library (usually SYS1.PROCLIB):

        TEMAPDS1 - Sample PDS maintenance procedure

Step 2 - Provide access to the datastore files.

    The TEMAPDS1 procedure is used to maintain the physical files that
    constitute the PDS. Datastore files are archived, exported or
    recycled according to the maintenance strategy that you specified
    for PDS file groups for this product.

    The PDS subsystem automatically submits maintenance jobs whenever
    a datastore file becomes full. The maintenance procedure must be
    available in a system procedure library for this to operate. The
    procedure is generic so it may be used by all RTEs using this
    version of the PDS.

    Ensure that TEMAPDS1 procedure has the necessary authority to read,
    write, and update the datastore files.

Step 3 - Authorize the KPDDSCO module.

    Authorize the KPDDSCO module by adding KPDDSCO to the system

```

Figure 36. Complete Persistent Datastore Configuration screen (1 of 2)

PARMLIB(IKJTSOnn) under the AUTHPGM section and refresh the IKJTSOnn member by issuing the set command (T IKJTSO=nn). You may also request your site's authorized system programmers to perform this step so it can be scheduled with the LPAR's change control processes. This change is required because the TEMAPDSC REXX procedure runs in a TSO environment. The KPDDSCO program has to be enabled to execute as an authorized program under TSO.

Step 4 - Verify persistent datastore configuration.

1. Bring up the started task (TEMS's or Agent's) that will collect historical data into this product's persistent datastore libraries. In the started task's RKPLOG DDNAME, find any persistent datastore libraries in a **non-Offline** status (for example, Partial or Full status):

2. From a z/OS operator console, issue the following z/OS MODIFY command as follows:
/F &stcname,KPDCMD RECOVER FILE=DSN:&pds_dataset

(where: &stcname = Started task name performing the persistent datastore collection
&pds_dataset = Persistent datastore dataset)

For example, issue the following MODIFY command for the TEMS:
/F TEMADSST,KPDCMD RECOVER FILE=+
DSN:TDKYNT.HKYN710.TARGET.TEMA.RGENHIS1

3. Wait 5 minutes.

4. In the started task's RKPLOG DDNAME, find the following Command: and KPDDSTR: references as shown in the TEMS RKPLOG DDNAME example below:

```
Command: RESUME FILE=DSN:TDKYNT.HKYN710.TARGET.TEMA.RGENHIS1
KPDDSTR: CONNECT processing started for DataStore file
DSN:TDKYNT.HKYN710.TARGET.TEMA.RGENHIS1
KPDDSTR: CONNECT processing ended for DataStore file
DSN:TDKYNT.HKYN710.TARGET.TEMA.RGENHIS1
```

5. If these references are not found, then view the TEMAPDS1 started task in SDSF and look for any obvious errors.

Please refer to the IBM Tivoli Monitoring Administrator's Guide and the Configuring Tivoli Enterprise Monitoring Server on z/OS documentation for more information.

Figure 37. Complete Persistent Datastore Configuration screen (2 of 2)

While these screens are displayed, perform the following steps outside ICAT (for example, using an ISPF split):

1. Copy JCL members xxxxPDS1 and xxxxPDS2 (where xxxx is the STC prefix, see Figure 14 on page 110) from the RKANSAM dataset listed to your system proclib (for example, SYS1.PROCLIB) so they can be submitted as started tasks.
2. Using your site's security system (such as RACF), authorize the user ID under which these started tasks will run to be able to delete, allocate, and update all PDS datasets for this RTE. These datasets are named *itmhlq.rtename.RKYNPDSx* and *itmhlq.rtename.RYNSGRPx*, where *itmhlq* is the high-level qualifier you defined for your site's Tivoli Monitoring environment, *rtename* is the name you gave this runtime environment, and *x* is a digit, usually 1 to 3.

3. Verify persistent datastore configuration.

Refer to the text on the screens for details of these steps.

When you have finished these steps, press F3 to return to the Allocate Persistent Datastore Menu (Figure 30 on page 129). You have completed the allocation and initialization of the Persistent Datastore for this agent; press F3 again to return to the Configure *prodname* RTE screen (Figure 18 on page 115).

Step 14: Complete the agent configuration

From the Configure *prodname* RTE screen, enter 8 to complete the configuration phase. The first screen of the Complete the Configuration process is displayed. Use the DOWN (F8) button to scroll through the screens.

```
+-----+
| ITCAM for Application Diagnostics on z/OS |
+-----+

                COMPLETE THE CONFIGURATION

After initial configuration of this product, perform the Load all
product libraries after SMP/E step from the Runtime Environments
(RTE) panel (for interactive Configuration tool users).  If you use
the Batch Mode facility, the RTE Load job (pp#2JOBS), typically
generated from the Load all product libraries after SMP/E step, is
automatically generated as part of the CICATB Batch Mode run.

If you have additional products that you plan to configure in this RTE
also, then perform the RTE Load step after you have completed the
configuration of all products in this RTE.  If you intend to start
using this product operationally before the additional products are
initially configured in this RTE, then you must perform the RTE Load
step for this product before startup.

In the same manner, if you have additional products that you plan to
configure in this RTE also, then typically, you would want to
complete configuration of all products first before performing the
common procedures done outside of the Configuration tool.

After all required steps for this product (or any additional
products) within the Configuration tool have been performed, then you
must execute the following procedures outside of the Configuration
tool to finalize installation and configuration.

Note:
Type README RTE for more information.

Perform the following steps for each of the items listed below,
if applicable:

Step 1 - Support SYSTCPD in TEMAYN and TEMAYNSA started tasks

    In order for the agent to successfully use TCP/IP, it may be
```

Figure 38. Complete the Configuration screen (1 of 7)

necessary to activate the SYSTCPD dd statement to get the correct values of TCP/IP parameters. The name of the SYSTCPD dataset is installation dependent; you will need to inquire of your local system programmer for the correct specification.

If you are certain that SYSTCPD is not needed at your installation, you may skip this step. However, note that you may gain a small performance benefit if you supply a SYSTCPD dd statement by avoiding multiple dynamic dataset allocations.

To support SYSTCPD, update the TEMAYN and TEMAYNSA members in RKANSAMU (before they have been copied to PROCLIB) to uncomment the SYSTCPD dd statements as described below. You must also change the dataset name in both members to your local requirement.

The Configuration tool generated the TEMAYN and TEMAYNSA started tasks with the following commented out lines. Customize the SYSTCPD DDNAMEs accordingly if this scenario fits your environment:

```
/* SYSTCPD explicitly identifies which dataset to use to obtain
/* the parameters defined by TCPIP.DATA when no GLOBALTCPIPDATA
/* statement is configured. Refer to the IP Configuration Guide
/* for information on the TCPIP.DATA search order. The dataset
/* can be any sequential dataset or a member of a partitioned
/* dataset. TCPIP.SEZAINST(TCPDATA) is the default sample file.
/* TCPIVP.TCPPARMS(TCPDATA) is another sample and is created as
/* part of the Installation Verification Program for TCP/IP.
/* Note: Uncomment out this DDNAME and point to appropriate
/*      TCPDATA library name supported at your site if domain
/*      name resolution is not fully configured.
/*SYSTCPD DD DISP=SHR,
/*      DSN=TCPIP.SEZAINST(TCPDATA)
```

Note: If this is a reconfiguration, refresh the agent started tasks (TEMAYN) and (TEMAYNSA) from RKANSAMU to PROCLIB if you uncomment the SYSTCPD DD statement.

Step 2 - Copy procedures to PROCLIB.

The Configuration tool created started task procedures in RKANSAMU which you must copy to your procedure library. When you copy, you may rename the procedures to meet your site's requirements. Update your started task library as follows:

- a) If you have configured an agent address space, copy the agent started task (TEMAYN) from RKANSAMU to PROCLIB.
- b) You should copy the Java SubAgent started task (TEMAYNSA) from RKANSAMU to PROCLIB.

Figure 39. Complete the Configuration screen (2 of 7)

Both of these started tasks must be running for the agent to function. It does not matter which starts first, although startup will complete slightly more quickly if they are both started at the same time.

Step 3 - APF-authorize libraries (if applicable).

Add the following runtime load libraries to your list of APF-authorized libraries.

Load library name:

- TDKYNT.HKYN710.TARGET.TEMA.RKANMODU
- TDKYNT.HKYN710.TARGET.TEMA.RKANMOD
- TDKYNT.HKYN710.TARGET.TKANMOD
- TDKYNT.HKYN710.TARGET.TKANMODL

Note: All runtime libraries concatenated in the STEPLIB DDNAME or in the RKANMODL DDNAME of the TEMAYN started task must be APF-authorized.

Step 4 - Install Catalog and Attribute Members (if applicable).

If this Agent's TEMS has been created within the current RTE, this step is not necessary. However, if the TEMS is created in another RTE without support for this product installed, it will be necessary to copy this product's catalog and attribute members to the TEMS, including both the hub and any remote. This must also be done when maintenance has distributed new versions of the catalog and attribute files.

This Agent's catalog and attribute files are as follows:

- TDKYNT.HKYN710.TARGET.TEMA.RKANDATV(KYNCAT)
- TDKYNT.HKYN710.TARGET.TEMA.RKANDATV(KYNATR)

For the non-local z/OS TEMS, copy these members manually to the RKANDATV dataset of the TEMS. Refresh these members in the respective RKANDATV libraries when SMP/E maintenance that changes these members is applied.

Alternatively, the TEP Advanced Utility FTP function may be used to copy the catalog and attribute files. Follow these steps to FTP the catalog and attributes to the TEMS using "Manage Tivoli Monitoring Services":

1. The TEMS does not have to be running, and if it is running it will have to be restarted after this procedure.
2. On the workstation "Manage Tivoli Monitoring Services" select **Actions**

Figure 40. Complete the Configuration screen (3 of 7)

```

Advanced
Utilities
FTP Catalog and Attribute files...
3. Select both the Catalog and the Attribute data for "ITCAM for
Application Diagnostics on z/OS" and continue by pressing OK.
4. Enter the host name or IP address, the user ID, the password for
that user, and the RKANDATV data set name for the TEMS on the
target system. You then click OK to initiate the upload.
5. If the TEMS is running, it must be restarted at this time.

Step 5 - Verify installation and configuration (if applicable).

a) Start the ITCAM for Application Diagnostics on z/OS TEMA Agent
and the Java subagent started tasks:

    S TEMAYN
    S TEMAYNSA

b) Stop the ITCAM for Application Diagnostics on z/OS TEMA Agent
started task:

    P TEMAYN

(The TEMAYNSA started task should stop when TEMAYN stops.)

The following steps only apply if the Tivoli Enterprise Monitoring Agent
(TEMA) is running in its own Agent address space and connects to
a non-local z/OS TEMS:

Note: A non-local z/OS TEMS pertains to a TEMS defined in
another RTE based on the following scenarios:
1. The TEMS (Hub or Remote) is known to this
   TDKYNT.HKYN710.TARGET.INSTLIB installation library.
2. The TEMS (Hub or Remote) is defined in another INSTLIB
   (or another CSI) that is not accessible to this
   TDKYNT.HKYN710.TARGET.INSTLIB installation library.

Important:
If the Agent's primary TEMS is a non-local z/OS TEMS (Hub or
Remote) or if the Agent's primary TEMS is a Remote TEMS and
this Remote TEMS is reporting to a non-local z/OS Hub TEMS,
then the Agent must also be installed in the non-local INSTLIB or CSI
environment where the z/OS TEMS is installed. In the non-local
installation environment where the z/OS TEMS is configured,
perform one of two required steps.

Step 6 - Copy and refresh the Agent's catalog and attribute files
in the non-local z/OS TEMS.

```

Figure 41. Complete the Configuration screen (4 of 7)

Perform one of two steps below:

- Execute the RTE Load step in the non-local TEMS RTE ("Load all product libraries after SMP/E" option from the RTE panel) -or-
- Execute the "Upgrade attribute and catalog members" option from the RTE Utility menu.

Alternative: Applicable if the Agent is not installed in the same CSI as the non-local z/OS TEMS's CSI:

You must copy this Agent's catalog and attribute files into the z/OS TEMS' RKANDATV library manually. This Agent's catalog and attribute files are as follows:

- TDKYNT.HKYN710.TARGET.TEMA.RKANDATV(KYNCAT)
- TDKYNT.HKYN710.TARGET.TEMA.RKANDATV(KYNATR)

These members are required in both the Agent's RKANDATV library and in the non-local TEMS' RKANDATV dataset. Refresh these members in the respective RKANDATV libraries when SMP/E maintenance that changes these members is applied.

Step 7 - Seed the TEMS using Manage Tivoli Monitoring Services (if applicable).

Seed the Hub Tivoli Enterprise Monitoring Server (TEMS) using Manage Tivoli Monitoring Services.
The term Seed is also used interchangeably with Add TEMS application support.
This step is only applicable to the Hub TEMS that the Agent reports to.

Note: The Agent is currently connected to a non-local TEMS. Ensure that the TEMS seeding steps below are performed for the non-local Hub TEMS.
The currently selected primary TEMS CMS_NODEID is set to:
NONAME

Before seeding the Hub TEMS, verify that:

- the support* for the z/OS-based products is installed and available with Tivoli Enterprise Portal Server (TEPS)
- the same versions of the z/OS-based products are installed and available with TEPS

* When you install "support" for the products on Tivoli Enterprise Portal Server (TEPS), you install the files that the TEPS requires for presenting data and well as the files required to seed the Hub TEMS.

Follow these steps to seed the TEMS using Manage Tivoli Monitoring Services:

Figure 42. Complete the Configuration screen (5 of 7)

1. Ensure that the Hub TEMS is running.
2. On the workstation where you installed Manage Tivoli Monitoring Services, select Start menu
>Programs
>IBM Tivoli Monitoring
>Manage Tivoli Monitoring Services
3. On the Manage Tivoli Monitoring Services dialog box, select Actions drop-down menu
>Advanced
>Add TEMS application support
4. On the Add application support to the TEMS dialog, select the location of the Hub TEMS (On this computer or On a different computer radio button) and click OK.
5. On the Non-Resident TEMS Connection window, provide the TEMS Node ID. You can find the Node ID as the value of the CMS_NODEID variable in the Hub TEMS' RKANPARU(KDSENV) environment member.
6. Select the appropriate communications protocol and click OK.
7. On the next window, provide any values required by your communications protocol.
8. On the Select the application support to add to the TEMS window, select the products whose seed data you want to add to the Tivoli Enterprise Monitoring Server configuration, and click OK.
Result: Manage Tivoli Monitoring Services seeds the TEMS and displays a dialog box indicating whether or not the seeding completed successfully.
9. Stop and restart the Hub TEMS.

Step 8 - Run the ITMSUPER Tools (recommended).

The ITMSUPER Tools give you information about the health of your managed systems, situations, and environment configuration. You can find the tools by searching for ITMSUPER on the Tivoli Open Process Automation Library (OPAL) Web site at <http://www.ibm.com/software/tivoli/opal>.

Step 9 - Configure History Collection Configuration window of the Tivoli Enterprise Portal (TEP) (if applicable).

Relationship between TEP History Collection Configuration and z/OS Configure persistent datastore options:

The Configure persistent datastore option on the product main menu is a component of the History Collection Configuration option of the TEP. If you configured the persistent datastore option on the product main menu, type README PDS on the command line to review the considerations to determine if the TEP's historical collection options match the

Figure 43. Complete the Configuration screen (6 of 7)

persistent datastore collection options configured for this product.

For more information, please refer to the product documentation.

Figure 44. Complete the Configuration screen (7 of 7)

To complete this process, perform the following steps:

1. Complete “Step 15: Copy remaining product libraries” to copy the remaining product libraries to your RTE.
2. Complete the optional configuration steps, outlined in “Optional postconfiguration steps” on page 144, as necessary.

Attention: the names of the affected members in RKANSAMU, referenced in the screenshots in this document as TEMAYN and TEMAYNSA, might be different on your system. Make sure to check these names in the instructions displayed on your system.

Important: You may wish to print these fifteen screens so you can have the instructions after closing ICAT. You will need these instructions when you complete the postconfiguration tasks described in “Optional postconfiguration steps” on page 144.

Step 15: Copy remaining product libraries

Press F3 to leave the Complete the Configuration screens. Press F3 again to return to the Product Component Select Menu screen (Figure 17 on page 114). Press F3 a third time to return to the Runtime Environments definition screen (Figure 13 on page 109).

Enter L to load postconfiguration product libraries. You enter the ISPF editor on the JCL shown in figure 90:

```

EDIT ---- TDKYNT.HKYN710.TARGET.INSTJOBS(YN#2JOBS) -      BATCH PARMs CREATED
COMMAND ==> sub      SCROLL ==> CSR
***** IF YOU WISH TO SUBMIT THIS JOB NOW, TYPE 'SUBMIT' AND PRESS ENTER. *****
***** NOTE: JOBCARD REQUIRES ALL CAPS. *****
***** ***** Top of Data *****
==MSG> -CAUTION- Profile changed to CAPS OFF (from CAPS ON) because data
==MSG> contains lower case characters.
==MSG> -Warning- The UNDO command is not available until you change
==MSG> your edit profile using the command RECOVERY ON.
000001 //YN#2JOBS JOB , 'ERIC JACKSON',MSGCLASS=X,NOTIFY=EJACK
000002 //*
000003 //*****
000004 //* DATE: 2009/10/22
000005 //* TIME: 17:47
000006 //*****
000007 //*
000008 //* JOB: TDKYNT.HKYN710.TARGET.INSTJOBS(YN#2JOBS)
000009 //*
000010 //*****
000011 //* DATE: 2009/10/22
000012 //* TIME: 17:47
000013 //*
000014 //*
000015 //* PURPOSE: THIS JOB LOADS ALL PRODUCT LIBRARIES IN THIS RUNTIME

```

Figure 45. JCL for copying postconfiguration agent libraries

Customize the JCL as necessary, and enter SUBMIT. Press F3 to return to the Product Selection Menu screen (Figure 12 on page 108). Press F3 again to return to the Configure Products screen (Figure 11 on page 107). Press F3 once more to return to the primary ICAT screen (Figure 6 on page 102); then press F3 a fourth time to leave ICAT.

Optional postconfiguration steps

The postconfiguration processes described in the Complete the Configuration screens (Figure 38 on page 137 through Figure 44 on page 142) are performed outside ICAT.

1. If you created started task members for the agent and the Java subagent, copy those members from the RTE's RKANSAMU library to a system proclib (for example, SYS1.PROCLIB.)
2. Copy the agent's VTAM major-node definition, KYNYYN, from the RTE's RKANSAMU library to your VTAMLST library.
3. Active the VTAM major node, KYNYYN:

V NET,ACT,ID=KYNNNN

Note: The VTAM major node must be activated every time VTAM is started. You might want to add the vary command to the agent's started-task JCL.

4. All runtime libraries defined to the agent's started task by the STEPLIB or the RKANMODL DD statements must be APF-authorized. Usually this means that you have to add these libraries to your site's list of APF-authorized libraries:

- *itmhlq.rtename.RKANMOD*
- *itmhlq.rtename.RKANMODU*
- *itmhlq.TKANMOD*
- *itmhlq.TKANMODL*

where *itmhlq* is the list of high-level qualifiers you defined for your site's Tivoli Monitoring environment, and *rtename* is the name you gave this runtime environment.

5. Verify both the installation and configuration of your monitoring agent by starting and then stopping the agent started task:

S *procmem*

S *javaprocmem*

where *procmem* is the member name within your site's proclib that defines the agent started task, and *javaprocmem* is the name of the Java subagent started task member. The *javaprocmem* started task terminate automatically when the *procmem* task is stopped.

6. If your agent does not communicate with a local z/OS monitoring server (in other words, it instead communicates with a monitoring server defined in another INSTLIB's RTE), register the agent with the non-local hub or remote monitoring server; launch the Register with local monitoring server step in the monitoring agent's RTE (Figure 18 on page 115).
7. Install Application Support files for the ITCAM for WebSphere monitoring agent onto any monitoring server that runs as a hub. For monitoring servers that run on z/OS, see *Tivoli Management Services on z/OS: Configuring the Tivoli Enterprise Monitoring Server on z/OS*. For monitoring servers on other systems, see *IBM Tivoli Monitoring: Installation and Setup Guide*.
8. If you want this agent to collect historical data, ensure that feature has been turned on in your site's Tivoli Enterprise Portal server; see *IBM Tivoli Composite Application Manager: Agent for WebSphere Applications Installation and Configuration Guide*.

Enter ICAT subcommand README PDS for more information about PDS requirements and the persistent datastore's relationship to historical reporting; the following panels are displayed:

```

----- README -----
COMMAND ==> █ SCROLL ==> CSR

***** Top of Data *****
**:-----:
**:Licensed Materials - Property of IBM:
**:5698-A39, 5698-A40, 5698-A46, 5698-A57, 5698-A58,:
**:5698-A59, 5698-A67, 5698-A72, 5698-A78, 5698-A79:
**:4 Copyright IBM Corporation 2005, 2008. All rights reserved:
**:
**:US Government Users Restricted Rights - Use, duplication or:
**:disclosure restricted by GSA ADP Schedule Contract with IBM Corp.:
**:-----DA24039-----:

Relationship Between Tivoli Enterprise Portal (TEP)
History Collection Configuration and z/OS Configure Persistent
Datastore Options

The Configure persistent datastore option on the product main
menu is a component of the History Collection Configuration
option of the TEP. If you configured the persistent
datastore option on the product main menu, review the following
considerations below to determine if the TEP's historical
collection options match the persistent datastore collection
options configured for this product.

TEP History Collection Configuration's collection options:

In TEP's History Collection Configuration window,
historical data collection may be set as follows:
- Collection Location=TEMA or
- Collection Location=TEMS

The collection interval set in the History Collection
Configuration window of the TEP can be as short as a minute
or as long as a day. The shorter the interval, the faster and
larger the history files will grow at the collection location.
Short collection intervals also increase CPU consumption and
network traffic. Do not set a one-minute collection interval
unless your work requires it. If you need frequent collection of

Up or Down to browse or End to return. Type Print to print, Save to save.

```

Figure 46. README PDS output (1 of 8)

```
----- README -----
COMMAND ===> █ SCROLL ===> CSR

historical data, be sure to allocate extra space for the
persistent datastore datasets. Insufficient allocation of space
results in inability to view short-term data and can result in
loss of historical data. Allocate enough space for 24 hours of
short-term historical data at the location of the persistent
datastore.

TEP Collection Location and z/OS persistent datastore
collection options:

The Collection Location options available for selection in
TEP directly relate to the z/OS Configure persistent
datastore option(s) within the z/OS Configuration tool.
The "Configure persistent datastore" option allocates the
product-specific, TEP historical datasets on z/OS and these
datasets are used by the following z/OS product started tasks:

- the z/OS TEMS address space:
  applicable if a local TEMS is configured in the runtime
  environment (RTE) and if customer enabled History Collection
  Configuration on TEP, with Collection Location set
  to TEMS. It is also applicable if the Agent in the RTE is
  configured to run in the TEMS address space and if customer
  enabled History Collection Configuration on TEP, with
  Collection Location set to TEMS.
- the z/OS Tivoli Enterprise Monitoring Agent
  (TEMA) address space:
  applicable if the Agent in the RTE is configured to run in its
  own standalone Agent address space and if customer enabled
  History Collection Configuration on TEP, with Collection
  Location set to TEMA.

z/OS-based Applications that support persistent datastore:

The persistent datastore option on z/OS is available for
configuration under the following products:
- Tivoli Enterprise Monitoring Server (TEMS)

Up or Down to browse or End to return. Type Print to print, Save to save.
```

Figure 47. README PDS output (2 of 8)

```

----- README -----
COMMAND ===> █ SCROLL ===> CSR

- A number of TMS:Engine-based applications
  (OMEGAMON II, OMEGAMON XE TEMAs, certain ITCAM TEMAs,
   NetView TEMA, System Automation TEMA, and other
   Agents)

TEMS persistent datastore configuration on z/OS:

Under the TEMS "Configure persistent datastore" configuration
on the TEMS main menu, this step is required if the customer
enabled History Collection Configuration on TEP, with
Collection Location set to TEMS. It is also required
because the option allocates the datasets required for recording
generic history data for distributed Agents connected to a z/OS
TEMS. These datasets are as follows:
- TDKYNT.HKYN710.TARGET.Z.RPD5GRP1
- TDKYNT.HKYN710.TARGET.Z.RGENHISx
In addition, the option is used as part of the data warehouse
controls.
Note: The Configuration tool enables the persistent datastore by
default at the TEMS (i.e., the TEMS started task is
generated with persistent datastore enabled) because
several z/OS and non-z/OS Agents connecting to a z/OS
TEMS depend on the TEMS started task to collect
historical data. This ensures that the historical
datasets listed above are always available.

TEMA application persistent datastore configuration on z/OS:

Under the TEMA's "Configure persistent datastore"
configuration, the z/OS Configuration tool typically presents
two separate "Configure persistent datastore" options on the
Agent's main menu, and the appropriate "Configure persistent
datastore" option should be selected based on two factors:

1. How the z/OS TEMA is configured:
   a. running in its standalone Agent address
      space (recommended)

Up or Down to browse or End to return. Type Print to print, Save to save.

```

Figure 48. README PDS output (3 of 8)

```

----- README -----
COMMAND ===>                                SCROLL ===> CSR

    NetView TEMA, System.Automation.TEMA, and other
    Agents)

TEMS persistent datastore configuration on z/OS:

Under the TEMS "Configure persistent datastore" configuration
on the TEMS main menu, this step is required if the customer
enabled History Collection Configuration on TEP, with
Collection Location set to TEMS. It is also required
because the option allocates the datasets required for recording
generic history data for distributed Agents connected to a z/OS
TEMS. These datasets are as follows:
- TDKYNT.HKYN710.TARGET.Z.RPDGRP1
- TDKYNT.HKYN710.TARGET.Z.RGENHISx
In addition, the option is used as part of the data warehouse
controls.
Note: The Configuration tool enables the persistent datastore by
default at the TEMS (i.e., the TEMS started task is
generated with persistent datastore enabled) because
several z/OS and non-z/OS Agents connecting to a z/OS
TEMS depend on the TEMS started task to collect
historical data. This ensures that the historical
datasets listed above are always available.

TEMA application persistent datastore configuration on z/OS:

Under the TEMA's "Configure persistent datastore"
configuration, the z/OS Configuration tool typically presents
two separate "Configure persistent datastore" options on the
Agent's main menu, and the appropriate "Configure persistent
datastore" option should be selected based on two factors:

1. How the z/OS TEMA is configured:
   a. running in its standalone Agent address
      space (recommended)
      -or-
   ** b. running in the TEMS address space (alternative)

Up or Down to browse or End to return. Type Print to print, Save to save.

```

Figure 49. README PDS output (4 of 8)

```

----- README -----
COMMAND ===> █ SCROLL ===> CSR

    Note: Certain TEMA applications support running in
           the TEMS address space only

2. How TEP History Collection Configuration is configured:
** a. enabled to collect data at the monitoring Agent
    (Collection Location=TEMA)
    -or-
    b. enabled to collect data at the TEMS
    (Collection Location=TEMS)

** Note: See "Special Considerations" section below.

If the Agent is configured to run in its own Agent address space,
the corresponding "Configure persistent datastore (in Agent)"
option typically under "To run in an Agent address space:" main
menu heading should be selected, only if customer enabled
History Collection Configuration on TEP, with Collection
Location set to TEMA. The option allocates the
product-specific, historical datasets that the Agent address
space will use to collect the data. Additional product-specific
datasets are also allocated for generic history data and data
warehousing.

Alternatively, if the Agent is configured to run in the TEMS
address space, the corresponding "Configure persistent datastore
(in TEMS)" option typically under "To run in the TEMS
address space:" main menu heading should be selected, only if
customer enabled History Collection Configuration on TEP,
with Collection Location set to TEMS. The option allocates
the product-specific, historical datasets that the TEMS
address space will use to collect the data.

Depending on the TEMA product requirements for
historical data collection, certain z/OS products only support
configuration of the persistent datastore to collect at the
TEMS address space only, or at the Agent address space only
(i.e., the "Configure persistent datastore" options on the Agent

Up or Down to browse or End to return. Type Print to print, Save to save.

```

Figure 50. README PDS output (5 of 8)

```

----- README -----
COMMAND ===> █ SCROLL ===> CSR

main menu are mutually exclusive options and only one is allowed
for configuration depending on how the Agent is configured to
run.)).

In most cases though, the z/OS Configuration tool allows
configuration of both "Configure persistent datastore" options if
the Agent is configured to run in its own Agent address space. A
customer may configure both of these options on the product menu:
- "Configure persistent datastore (in TEMS)"
- "Configure persistent datastore (in Agent)"
Configuring both options allocates two unique sets of
product-specific, historical datasets that the TEMS address
space and/or the Agent address space will use to collect the
data.

Unique historical files are allocated so that there is no
contention in the usage of these datasets when the TEMS
address space and/or the Agent address space takes an exclusive
enqueue on these datasets to record data. One would configure
both options at initial product configuration to allocate the
datasets ahead of time, so when the TEP History Collection
Configuration is enabled, the Configuration program may be
configured to collect data at the TEMA one day, and may be
reconfigured to collect data at the TEMS at another time. In
either case, there would be no reconfiguration necessary on the
z/OS TEMA because both "Configure persistent datastore"
options on the product main menu have already been configured
ahead of time.

Special Considerations:

A. TEP Collection Location
Certain z/OS TEMA applications support running in the TEMS
address space only. An example of a product that runs in the
TEMS address space only is IBM Tivoli OMEGAMON XE on z/OS
V3.1.0 (M5310) and higher versions.

Up or Down to browse or End to return. Type Print to print, Save to save.

```

Figure 51. README PDS output (6 of 8)

```

----- README -----
COMMAND ===> █ SCROLL ===> CSR

In the TEP History Collection Configuration, ensure that you
enable to collect data at the TEMS only (Collection
Location=TEMS)

Setting Collection Location=TEMA at the TEP History
Collection Configuration to collect historical data for attribute
groups from a z/OS product that runs in the TEMS address space
only may result in abnormal end of task error (ABEND) in the
TEMS started task. This error might be caused by the default
TEP setting for collection of historical data, which is to
collect data at the TEMA. Change the settings for collection
of historical data in the History Configuration dialog box of the
TEP. Instead of the default settings, configure collection
of historical data to occur at the TEMS for all of the
attribute groups of z/OS products that only run in the TEMS
address space.

B. DATACLAS SMS Parameter
When configuring the persistent datastore for any of the z/OS
components, the "Modify and review datastore specifications"
option on the "CONFIGURE PERSISTENT DATASTORE" main menu does not
currently allow for the datasets to be allocated as
extended-format sequential datasets. If your data center ACS
routines are using extended-format for allocations, the DATACLAS
parameter may be specified in the persistent datastore
pp#PJOB generated jobs. Edit the job or edit the resulting
TDKYNT.HKYN710.TARGET.Z.RKANPARU(KppAL)
persistent datastore allocation member for each product.
In each KppAL member, add the DATACLAS=xxxxxxx parameter, where
xxxxxxx is the data class that will be used to allocate standard
sequential datasets.

Please refer to the IBM Tivoli Monitoring Administrator's Guide
and the Configuring Tivoli Enterprise Monitoring Server
on z/OS documentation for more information.

Up or Down to browse or End to return. Type Print to print, Save to save.

```

Figure 52. README PDS output (7 of 8)

```

----- README -----
COMMAND ===>                                SCROLL ===> CSR

TEP. .Instead of the default settings, configure collection
of historical data to occur at the TEMS for all of the
attribute groups of z/OS products that only run in the TEMS
address space.

B. DATACLAS SMS Parameter
When configuring the persistent datastore for any of the z/OS
components, the "Modify and review datastore specifications"
option on the "CONFIGURE PERSISTENT DATASTORE" main menu does not
currently allow for the datasets to be allocated as
extended-format sequential datasets. If your data center ACS
routines are using extended-format for allocations, the DATACLAS
parameter may be specified in the persistent datastore
pp#PJOB generated jobs. Edit the job or edit the resulting
TDKYNT.HKYN710.TARGET.Z.RKANPARU(KppAL)
persistent datastore allocation member for each product.
In each KppAL member, add the DATACLAS=xxxxxxx parameter, where
xxxxxxx is the data class that will be used to allocate standard
sequential datasets.

Please refer to the IBM Tivoli Monitoring Administrator's Guide
and the Configuring Tivoli Enterprise Monitoring Server
on z/OS documentation for more information.

***** Bottom of Data *****

Up or Down to browse or End to return. Type Print to print, Save to save.

```

Figure 53. README PDS output (8 of 8)

Part 4. Appendixes

Appendix A. Applying the latest maintenance

Perform the following procedure to apply the latest maintenance to a Data Collector that has already been installed and configured:

1. Apply all newly required Program Temporary Fixes (PTFs) for the Data Collector and for ITCAM Common Services. To see a list of recent PTFs and to acquire them, find the IBM Tivoli Composite Application Manager for Application Diagnostics support site.

Select **Download**, then **Fixes by version**.

For Data Collector maintenance, click the "PSP buckets": *z/OS Data Collectors V7.1 PSP (WAS DC)* and *z/OS Data Collectors V7.1 PSP (Common Services)*.

For Monitoring Agent maintenance, click the "PSP bucket": *z/OS Data Collectors V7.1 PSP (TEMA)*. Read the *Service Recommendation Summary* in each of these documents.

If you have installed multiple Data Collectors on different profiles that share the same IBM WebSphere Application Server SMP/E base, and you are applying the latest interim fix or fix pack to the Data Collectors, unexpected problems might occur if you do not install the fix for all the Data Collectors at the same time. Do not restart any of the application server instances until all of them have had the same interim fix or fix pack applied to them.

2. If the cover letter for any newly installed PTFs for the Data Collector requires this, for every configuration home directory, run the `amupdate.sh` script from `config_home/bin`:

```
./amupdate.sh [-config config_home] [-debug] [-batch] [-?]
```

The parameters are:

-config

Set a different `config_home` directory. Not needed when the script is started from `config_home/bin`.

-debug

Output debug information.

-batch

Run the script without any prompts.

-? Display help on the script syntax.

Appendix B. Environment Checking Utility for z/OS

Overview

The ITCAM Environment Checking Utility (ECU) for z/OS is an interactive tool designed to examine a WebSphere environment and determine whether there are any features or third party products that may be incompatible with ITCAM Data Collector. The utility examines several aspects of the WebSphere operating environment and configuration, including:

- OS version
- WebSphere product and version
- WebSphere JVM version and Service Release
- Installed database management systems and version
- JVM options, system properties and environment variables
- Installed third party products (including other Tivoli products)

On z/OS the utility is an interactive command line script that runs under UNIX System Services (USS).

Installation

ECU for z/OS is distributed as a tar file, ITCAM_ZWAS_ENVCHECK.tar. To install the utility, create a new directory on a read-write filesystem (HFS or zFS), and copy the tar file there. To extract the files, use the command:

```
tar -xof ITCAM_ZWAS_ENVCHECK.tar
```

The following directories will be created:

```
<ecu-root>
|
+-----+-----+-----+
|       |       |       |
bin/    etc/   lib/    logs/
```

Running the Environment Checking Utility

You must use ECU with a user ID that has at least read access to the WebSphere configuration files. If your WebSphere has Global Security enabled, you must also use a user ID that has authority to use the WebSphere Scripting Client (wsadmin.sh), and uses an SSL key store that includes CA keys that the cell was signed with.

The ECU requires a Java Runtime Environment. You must set environment variable JAVA_HOME to a JDK 1.4.2 or higher. For example:

```
export JAVA_HOME=/usr/lpp/java/J1.4
```

To start the utility, change to the ecu-root directory you created, and execute the script:

```
./envcheck.sh -logPath logs -reportPath logs
```

These are the minimum start options required to run the utility.

The available options are:

`-reportPath Report save path [-logPath Log path] [-tmpPath Tmp path]
[-showSteps] [-noWizard] [-dumpDir (Dump dir)] [-jcfile (path/filename)]
[-jcdebug] [-help]`

Parameter description:

`-reportPath Report save path`

The Environment Checking Utility will generate a report of checking content. The *Report save path* indicates the path to save the report.

`-logPath Log path`

Optional. Indicates the log path for Environment Checking Utility. Default log directory is `/var/ibm/tivoli/common`.

`-tmpPath Tmp path`

Optional. Indicates the temporary directory for Environment Checking Utility. Default temporary directory is `/tmp`.

`-showSteps`

Optional. If this parameter is in the command line, the Environment Checking Utility will print wizard steps.

`-noWizard`

Optional. If this parameter is in the command line, the Environment Checking Utility will not prompt wizard navigation inputs.

`-dumpDir Dump directory`

Optional. Indicates the directory where the ECU will look for the javacore dump. Example: `-dumpDir /u/WSSR1`.

`-jcfile Path/filename of a javacore`

Optional. Indicates the directory and file name of the javacore to use. No javacore dump is taken. Example: `-jcfile /u/WSSR1/javacore.20081107.180633.50331817.0001.txt`

`-jcdebug`

Optional. Activates javacore debug mode, generating more logging and more console display messages.

`-help`

Optional. Print an option guide.

The utility then prompts the user of information needed to examine the environment:

Select WebSphere Home

Please wait while the Env Checking Utility searches for WebSphere Application Servers installed on your system ...

Select WebSphere installation or profile to check. If necessary, select "Manually specify a WebSphere installation" and specify the appropriate installation directory.

1. Manually specify a WebSphere installation root.

Items marked with "[X]" are selected, Please Input your selection (input ",", between each index, e.g. 1,3,4)

On some platforms, the WebSphere install directory can be determined from a registry. On z/OS you must supply this information manually. Select option 1. Specify WebSphere Application Server Installation Directory:

You must specify the fully qualified path to the configuration home directory, for example:/u/WAS510/Servers/AppServer

The utility uses this information to examine the WebSphere environment. It will determine the servers defined:

Select Application Server Instance

Select WebSphere installation or profile to check. If necessary, select "Manually specify a WebSphere installation" and specify the appropriate installation directory.

```
/u/WAS510/Servers/AppServer/  
[ ] 1. cells/TVT6006/nodes/TVT6006/servers/server1  
[ ] 2. cells/TVT6006/nodes/TVT6006/servers/BBOSBVT  
[ ] 3. cells/TVT6006/nodes/TVT6006/servers/BBOSMCS  
[ ] 4. cells/TVT6006/nodes/TVT6006/servers/cb60001  
[ ] 5. cells/TVT6006/nodes/TVT6006/servers/cb60002  
[ ] 6. cells/TVT6006/nodes/TVT6006/servers/cb61001  
[ ] 7. cells/TVT6006/nodes/TVT6006/servers/ab  
[ ] 8. cells/TVT6006/nodes/TVT6006/servers/bbosims  
[ ] 9. cells/TVT6006/nodes/TVT6006/servers/BBOSELJ  
[ ] 10. cells/TVT6006/nodes/TVT6006/servers/BBOSNVW
```

Items marked with "[X]" are selected, Please Input your selection (input ",", between each index, e.g. 1,3,4)

You can select one or more servers to be examined. The utility then determines the default connection attributes for the WebSphere scripting client: You can select one or more servers to be examined. The utility then determines the default connection attributes for the WebSphere scripting client:

WebSphere Connection (wsadmin)

Validating WebSphere connection (wsadmin) of
cells/TVT6006/nodes/TVT6006/servers/server1 - /u/WAS510/Servers/AppServer/

Current connection parameters:

Host Name: localhost

Connector Type: SOAP

SOAP Connector Port: 8880

Do you want to modify the existing connection information? [YES or NO]
(default is: No)

For each server selected, the utility will generate a javacore. The javacore file is then examined to identify installed frameworks, applications and third party products that might be incompatible with ITCAM.

When the utility terminates, a report will be generated in the specified report path directory containing the information gathered. You can use this report to determine whether ITCAM can safely be installed.

Special considerations

Execution environment requirements

In Network Deployment (ND) environments, the Deployment Manager must be running. In base environments, the Admin Service must be running.

Application Servers selected for checking by the ECU also need to be running.

Javacores

To take javacore dumps, the ECU will issue a command using `wsadmin`. The dump will be scanned for the presence of third party software and frameworks. The ECU of course must be able to locate the javacore dump after it has been generated.

Specifying the location of the javacore

In some cases, the ECU will not be able to find the javacore. Therefore, you can supply an override directory location using `-dumpDir` or supply the location of an existing javacore using `-jcfile`.

The default location where ECU looks for the javacore is `/tmp` unless the environmental variable `_CEE_DMPTARG`, specifying the location of javacores, is defined in the admin console for the servant region.

In most cases with WebSphere 6.0, the ECU will be able to locate these javacore dumps without runtime overrides. However, in WebSphere 6.1, if `_CEE_DMPTARG` is not defined, the JVM usually will write the dump to the “current working directory”, whose name is not available to ECU. In this case, you can examine the java property “`user.home`”, usually displayed in the JES2 joblog of the servant region, and use the `-dumpDir` argument for `envcheck.sh` to specify the actual javacore dump directory.

The most reliable way to determine the directory where javacores are written is to look at the SYSOUT DD output file of the servant region. This file contains messages that indicate the directory and filename of the javacore dumps. For example:

```
JVMDUMP010I Java Dump written to /u/WSSR1/javacore.20081109.211531.50331817.0024.txt
```

Processing a javacore if the connection times out

In the z/OS version of IBM WebSphere Application Server 6.1, prior to APAR PK58669 bringing WebSphere to 6.1.0.17, javacore dumps can take a very long time (6-8 minutes), usually causing the SOAP or RMP connections to fail before dump generation completes.

In this situation, you can generate the javacore outside the ECU, and then instruct the ECU where the javacore is located, using the `envcheck.sh` argument `-jcfile`.

Perform the following steps:

- a. Generate a javacore. Issue a modify command to the control region:

```
F <ctn_region_name>,JAVACORE
```

Example: `F BB0S001,JAVACORE`. In the SYSLOG, you will see the message:

```
BB000211I MODIFY COMMAND JAVACORE COMPLETED SUCCESSFULLY
```

b. Locate the name and location of the resulting javacore file. Look in the servant region's SYSOUT DD output for message JVMDUMP010I. Example:

```
JVMDUMP007I JVM Requesting Java Dump using  
'/u/WSSR1/javacore.20081116.182936.16779055.txt'
```

c. Pass this file to the ECU. Invoke `envcheck.sh` , specifying the `-jcfile` option. Example:

```
envcheck.sh -jcfile /u/WSSR1/javacore.20081116.182936.16779055.txt
```

Javacore summary

If the ECU does not seem to be processing a javacore dump:

1. Locate the directory where javacores are written, and specify it using the `-dumpDir` argument when invoking `envcheck.sh`.
2. If that does not work, or if the javacore step takes a long time and does not work properly, generate a javacore using the command:

```
F <ctl-region-name>,JAVACORE
```

Then re-run `envcheck.sh` specifying the resulting javacore path/filename using the `-jcfile` parameter.

Appendix C. Setting up security

Setting up optional security for ITCAM for Application Diagnostics is described in this chapter.

Because security for ITCAM for Application Diagnostics often involves integration of the various components, this chapter contains information pertaining to both Managing Servers and Data Collectors on IBM z/OS.

Perform the procedures in each of the following sections, if they apply.

Setting up the user ID and password for the Data Collector with IBM WebSphere Application Server Global Security enabled

Installing, configuring, and running the ITCAM for Application Diagnostics on z/OS Data Collector with Global Security turned on might require additional steps, depending on your security configuration.

If WebSphere Global Security has been turned on, perform the following steps prior to running the `setupwas.sh` script:

1. Make sure the user ID you will use to log on to UNIX System Services (USS) and to run the `setupwas.sh` script has read and write access to the IBM WebSphere Application Server configuration files. This user ID must also have permission to execute the WebSphere Scripting Client script (`wsadmin.sh`). It is recommended that you use an administrative user ID (such as `WSADMIN`) to run the `setupwas.sh` runtime setup script. If you do not want to use an administrative user ID to run the `setupwas.sh` runtime setup script, define a user using the same commands that were used to define an administrative userid.
2. Make sure the user ID you will use to run `setupwas.sh` is a member of the same UNIX group as an administrative user ID. This user ID will create the ITCAM for Application Diagnostics runtime directories for the server. This user ID must also have read and write access to these directories. It is recommended that you use an administrative user ID (such as `WSADMIN`) to run the `setupwas.sh` runtime setup script. If you do not want to use an administrative user ID to run the `setupwas.sh` runtime setup script, define a user using the same commands that were used to define an administrative userid.
3. Make sure the user ID you will use to run `setupwas.sh` fulfills the requirements for Secure Sockets Layer (SSL) security.

Background information:

When Global Security is enabled, SSL security is always used by the administrative subsystem to secure administrative commands, the IBM WebSphere Application Server administrative console, and communications between IBM WebSphere Application Server processes (which includes the `wsadmin.sh` scripting facility). SSL support always provides a mechanism by which the server proves its identity.

In addition, SSL support on IBM WebSphere Application Server for z/OS allows the following ways for a client to prove its identity:

- Basic authentication (also known as SSL Type 1 authentication), in which a client proves its identity to the server by passing a user identity and password known by the target server

- Client certificate support, in which both the server and client supply digital certificates to prove their identities to each other

For the client to authenticate the server, the server (actually, the Controller user ID) must possess a signed certificate created by a certificate authority. The server passes the signed certificate to prove its identity to the client. The client must possess the Certificate Authority (CA) certificate from the same CA that issued the server's certificate. The IBM WebSphere Application Server customization dialogs generate jobs that, amongst other things, define the user IDs for the various IBM WebSphere Application Server regions (Deployment Manager, Node Agent, Server Controller, and Servant tasks). These jobs also specify user IDs that can be used to log on to the IBM WebSphere Application Server administrative console. The RACF customization jobs create key rings for each of these user IDs and connects certificates to them. You may use one of these user IDs to perform the ITCAM for Application Diagnostics Data Collector setup if it also has the necessary permissions to access the IBM WebSphere Application Server configuration root files mentioned in Step 1 on page 165.

Procedure:

An administrative user ID (typically WSADMIN, but it could be different) is set up to have the necessary privileges when the cell is configured, so any user ID you use must be set up in the same way. It is recommended that you use an administrative user ID to run the `setupwas.sh` runtime setup script.

If you cannot use the administrative user ID that was created when the security domain was set up for the cell, you can create a new user ID, or alter your personal user ID, so that it has the same characteristics. Find the jobs BBOSBRK and BBOCBRAK that defined the WebSphere administrative user ID to RACF and created its keyring. Then use those RACF commands to create a new user ID or update your personal user ID so it has the same characteristics. (Your RACF Administrator will probably need to run the RACF commands for you.)

If you cannot locate the BBOSBRK and BBOCBRAK jobs that set up the security domain for the cell, perform the following procedure:

- Find the following information:
 - The user ID and group of the IBM WebSphere Application Server Controller or administrator started task
 - The name of the CA certificate that was used to sign the controller user ID's server certificate. (If configuring a server in a Network Deployment, find the name of the CA certificate that was used to sign the Deployment Manager server certificate).

If you don't know the group ID of the Controller or administrator ID, issue the TSO RACF command LISTUSER (LU) for servant task owner. For example:

```
LU ASCR1
```

```
USER=ASCR1  NAME=WAS APPSVR CR          OWNER=IBMUER  CREATED=05.043
DEFAULT-GROUP=WSCFG1  PASSDATE=N/A      PASS-INTERVAL=N/A
ATTRIBUTES=PROTECTED
REVOKE DATE=NONE  RESUME DATE=NONE
```

This shows that the group default group name for the ID is WSCFG1.

- Define a user ID that you will use exclusively for running the ITCAM for Application Diagnostics setup configuration using the TSO RACF command ADDUSER (AU). For example:

```

AU ITCAMWS NAME('ITCAM for WAS USER') PASSWORD(password) -
  OWNER(IBMUSER) DFLTGRP(WSCFG1) UACC(READ) -
  TSO(ACCTNUM(ACCT#) PROC(GENERAL) -
    SIZE(200000) MAXSIZE(200000)) -
  OMVS(HOME(/u/itcam71) PROGRAM(/bin/sh) UID(00001234))

```

The TSO segment for this user profile is required if you intend to run the ITCAM for Application Diagnostics setup from TSO OMVS. This same user ID will be used for the ITCAM for Application Diagnostics Java Management Extensions (JMX) client.

- c. Create a keyring for this user ID, and have the cell signing CA certificate placed on it, as follows:

```

RACDCERT ID(ITCAMWS) CONNECT -
  (RING(WASKeyring) LABEL('WebSphereCA') CERTAUTH)

```

Access to keyrings and certificates is protected by RACF by a set of profiles in the FACILITY class. Although the keyring is associated with the user ID, the user must have read authority to the IRR.DIGTCERT.LISTRING profile in order to access its keyring. The user must also have read access to the IRR.DIGTCERT.LIST profile to be able to access its certificate.

4. If you selected Use SAF EJBROLE profiles to enforce J2EE roles during security domain setup in the IBM WebSphere Application Server Customization Dialogs, make sure the user ID you will use to run setupwas.sh has read access to the EJBROLE administrator profile. The following administrative roles were defined by the customization jobs:

```

RDEFINE EJBROLE (optionalSecurityDomainName.) administrator UACC(NONE)
RDEFINE EJBROLE (optionalSecurityDomainName.) monitor UACC(NONE)
RDEFINE EJBROLE (optionalSecurityDomainName.) configurator UACC(NONE)
RDEFINE EJBROLE (optionalSecurityDomainName.) operator UACC(NONE)

```

Ideally, your user ID will be a member of the administrative or Controller ID group, which is already granted permission to these profiles.

5. For any RACF classes whose profiles have been added or modified, refresh the RACF cache. To do this, an authorized RACF administrator must issue the following command:

```

SETROPTS RACLIST(classname) GENERIC(classname) REFRESH

```

6. Use the WebSphere Scripting Client directly to see if the user ID is set up correctly. From a USS session, change to the bin directory of IBM WebSphere Application Server and issue the following command:

```

./wsadmin.sh -user itcamws -password itcamws

```

You will normally see messages similar to the following text if the user ID is set up correctly (This example is from a Network Deployment environment):

```

WASX7209I: Connected to process "dmgr" on node PLEX1Manager using SOAP
connector; The type of process is: DeploymentManager WASX7029I: For
help, enter: "$Help help"

```

Enter quit to terminate the WebSphere Scripting Client.

Setting up RACF access to FACILITY profile ERBSDS.MON2DATA

RACF access to FACILITY class profile ERBSDS.MON2DATA is required for z/OS Data Collectors to access SMF CPU and paging data if that profile has been defined to RACF. If RACF resource FACILITY class profile ERBSDS.MON2DATA has been defined, normally to protect access to RMF™ type 79 record data, ITCAM

for Application Diagnostics will be unable to obtain SMF CPU and paging information when it invokes the RMF service ERBSMFI and does not have read access.

The following message is issued because of security checks by RMF Security Access Facility (SAF) calls:

```
ICH408I USER(userid) GROUP(group_id) NAME(user name )
        ERBSDS.MON2DATA CL(FACILITY)
        INSUFFICIENT ACCESS AUTHORITY
        FROM ERBSDS.* (G)
        ACCESS INTENT(READ  )
        ACCESS ALLOWED(NONE  )
```

Failure occurs when the owner IDs of z/OS Data Collectors hosting applications have not been granted READ access to the profile ERBSDS.MON2DATA.

Owner IDs for all regions running the Data Collector need to be granted READ access to the ERBSDS.MON2DATA profile. These regions include the ITCAM CYN1 subsystem, and all IBM WebSphere Application Server Servant, CICS, and IMS regions that run ITCAM Data Collectors.

For example, suppose the profile ERBSDS.MON2DATA has been defined using the following command:

```
RDEFINE FACILITY ERBSDS.MON2DATA UACC(NONE)
```

Then take the following actions:

1. Grant the user ID READ access:

```
PERMIT ERBSDS.MON2DATA CLASS(FACILITY) ID(userid) ACC(READ)
```
2. Activate the changes:

```
SETOPTS REFRESH RACLIST(FACILITY)
```

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 or Data Collectors 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 property `security.enabled` on that particular component. You can use the following combinations:

- Managing server in secure mode and the data collector in non secure mode.
- Data collector in secure mode and the managing server in non secure mode.
- Managing server and data collector in secure or non secure mode.

Script to run if your SSL certificates have expired

All SSL certificates have an expiration time. For some certificates, the expiration time is 4 years, after which the product will not function if you have enabled Node Authentication and SSL. If this is the case, to increase the expiration time, perform the procedure at “Script to run if your SSL certificates have expired” on page 175.

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 `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 managing server components with security enabled configuration by default with the exception of 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`) take the following actions:

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 7.1.0.2, in the Kernel properties file (`MS_home/etc/kl1.properties`), set
`codebase.security.enabled=false`.

If you have more than one instance of the Kernel, set
`codebase.security.enabled=false` in `kl2.properties` as well.

3. Restart the Managing Server.

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 (`config_home/runtime/app_server_version.node_name.server_name/custom/datacollector_custom.properties`) complete the following steps:

1. Set `security.enabled=true`
2. Then restart the application server.

Keystore management and populating certificates

You do not have to take the following actions unless you want to create unique certificates with a new storepass and keypass. These commands will populate a new store with those certificates.

For populating all new keystores: there are 2 stores used by ITCAM for Application Diagnostics: `CyaneaMgmtStore` to run on the managing server and `CyaneaDCStore` to run on the data collectors.

CyaneaMgmtStore contains: `mgmttomgmt.cer` (`cn=cyaneamgmt`)
`dctomgmt.cer` (`cn=cyaneadc`)

CyaneaDCStore contains: `mgmttodc.cer` (`cyaneamgmt`)

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:

Note: Replace "oakland1" with your custom keypass and "oakland2" with your custom storepass. Replace "CyaneaMgmtStore" and "CyaneaDCStore" 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:

After creating the 2 Stores, extract the certificates by taking the following actions:

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
```

When you have extracted your files, copy the following certificates and Stores to the following locations:

*MS_home/etc:*CyaneaMgmtStore mgmttomgmt.cer mgmttodc.cer

*install_home/itcamdc/etc:*CyaneaDCStore dctomgmt.cer

Configuring components to use new keystores and certificates

Configure components to use new keystores and certificates:

1. Modify *MS_home/bin/setenv.sh*. At the end of the script you will need to modify the following lines with the new keystore name, storepass, and keypass:

```
KEYSTR_LOC=MS_home/etc/CyaneaMgmtStore
KEYSTR_PASS=oakland2
KEYSTR_KEYPASS=oakland1
```

2. Modify the Visualization Engine (Application Monitor) user interface with the new keystore name, storepass and keypass. Perform the following procedure:
 - a. Start the Managing Server and the Visualization Engine (Application Monitor) user interface.
 - b. Log into the IBM WebSphere Application Server administrative console.
 - c. Depending on your application server version, perform one of the following procedures:

Table 19. Navigation to JVM custom properties in the IBM WebSphere Application Server administrative console

IBM WebSphere Application Server 6	1. Click Server > Application Servers and select the <i>server_name</i>. 2. In the Configuration tab, navigate to Server Infrastructure: Java and Process Management > Process Definition > Additional Properties: Java Virtual Machine > Additional Properties: Custom Properties.
IBM WebSphere Application Server 5	1. Click Server > Application Servers and select the <i>server_name</i>. 2. Navigate to Additional Properties: Process Definition > Additional Properties: Java Virtual Machine > Additional Properties: Custom Properties.

- d. 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
- e. Restart the application server.
3. Modify *config_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 *config_home /runtime/app_server_version.node_name.server_name/custom/ datacollector_custom.properties*.
 - c. Set the following property definitions:

Note: All the following properties are set during the installation or at configuration time. By default you do not need to do anything. You only need to change the following properties if you have changed items that the

following properties are referring to. All the keywords in angle (< >) brackets need to 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 should 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. Start the instance of the application server that is monitored by the data collector for the property changes to take effect.
4. Restart the Managing Server.

Secure Socket Layer communications

On distributed platforms, ITCAM for Application Diagnostics uses the SSL security protocol for integrity and confidentiality. You have the option of configuring all monitoring components to utilize SSL for communications. The following sequence describes a sample HTTP-based SSL transaction using server-side certificates:

1. The client requests a secure session with the server.
2. The server provides a certificate, its public key, and a list of its ciphers to the client.
3. The client uses the certificate to authenticate the server (verify that the server is who it claims to be).
4. The client picks the strongest common cipher and uses the server's public key to encrypt a newly-generated session key.
5. The server decrypts the session key with its private key.
6. From this point forward, the client and server use the session key to encrypt all messages.

The monitoring software uses the Java Secure Sockets Extensions (JSSE) API to create SSL sockets in Java applications.

Note: If you performed an embedded installation of the IBM WebSphere Application Server with the Managing Server, use the IBM WebSphere Application Server default key. For more information on 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 Application Diagnostics.

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, perform the following procedure:

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*. The complete instructions for changing the JDBC user ID and password for the database Schema user are located in the *ITCAM Managing Server Installation and Customization Guide*.
 - keystore.storepass, keystore.keypass using the same method mentioned in the Step 2 on page 171.
 - keystore.storepass and keystore.keypass in *config_home/runtime/app_server_version.node_name.server_name/custom/datacollector_custom.properties* file.
3. Restart the Managing Server to activate the changes.
 4. Restart the VE application server to activate the changes.

Properties file encryption

Take the following actions:

1. To encrypt a properties file, use:

```
amcrypto.sh -encryptPropertyFile file
```

The *file* is *kl1.properties* or *kl2.properties* in *MS_home/etc*. This command encrypts the given input file and stores it in a file with different name. The user can back up the existing properties file and have it replaced by the encrypted file for more security.

2. To decrypt a properties file, use:

```
amcrypto.sh -decryptPropertyFile file
```

The *file* is *kl1.properties* or *kl2.properties* in *MS_home/etc*. This command decrypts the given file and writes the decrypted file to another file with a different name.

3. Restart the Managing Server to activate the changes

Enabling Secure Socket Layer at the Data Collector level

To enable SSL, enable Node Authentication first (See “Node Authentication” on page 168). 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 *config_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.

Verifying secure communications

To verify SSL is properly configured, look for the message labeled CYND4051I in one of the following files:

Table 20. Location of the CYND4051I message

Windows	C:\Program Files\IBM\tivoli\common\CYN\logs\node_name.server_name\ java_msg_log_file. For example: C:\Program Files\IBM\tivoli\common\CYN\logs\IBMNode01.server1\ msg-dc-Ext.log
UNIX and Linux	/var/ibm/tivoli/common/CYN/logs/node_name.server_name/ java_msg_log_file. For example: /var/ibm/tivoli/common/CYN/logs/IBMNode01.server1/msg-dc-Ext.log
z/OS	[ITCAM_CONFIG]/runtime/wasXX.node.server/logs/CYN/logs

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 21. Classification of the data processed on the CommandAgent channel

Classification	Data
Command and control data	Configuring and unconfiguring the Data Collector
User actions related to threads	- Starting and stopping JVM threads - 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 *config_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 4 years, after which the product will not function if you have enabled Node Authentication and SSL. If this is the case, to increase the expiration time, perform the following procedure:

1. Open the script located at *MS_home/bin/security_cert.sh* with a text editor. The 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
# ITCAMFAS 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 dctopproxy -file ./dctopproxy.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 it occurs in the script. For example, change all instances of -validity 7000 to -validity 3500.
4. Save the changes and run the script.

Settings for the Data Collector if Java 2 security is used

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, perform 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 *config_home/runtime/appserver_version.node_name.server_name/datacollector.policy*. You must edit this file in the following way:

- Remove all existing content.
- Copy the sample security policy for the Data Collector from the file *config_home/itcamdc/etc/datacollector.security.policy*.
- 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.
- Add your required security policy settings.

Save the file, and create a backup copy.

Attention: If you configure, reconfigure, or unconfigure the Data Collector for an application server instance using the -clean option, the file *config_home/runtime/appserver_version.node_name.server_name/datacollector.policy* might be overwritten. To ensure that your security policy remains active, restore this file from the backup copy after using the -clean option for any application server instance.

Appendix D. Common Services Address Space command reference

The Common Services Address Space (CYN1) serves as a repository for SMF records generated by the application server and captured by the SMF address space. This repository takes copies of SMF records and provides the basis for real time analysis when used in conjunction with the Visualization Engine (Application Monitor) user interface. It also provides other functions that are unique to the IBM z/OS environment.

This appendix describes the CYN1 commands.

Starting the Common Services Address Space

CYN1 is defined as an IBM MVS subsystem; it also runs as a started task and the JCL resides in one of the system PROCLIB data sets. The PROCLIB member name and the subsystem name do not have to be the same. If they are, the sub parameter SUB=JES2 must be added to the start command to inform the system to start the job under the JES2 procedure library, instead of the MSTR library, which is the default when the task being started is a subsystem.

The syntax of the start command is as follows:

```
START xxxx[.yy][,SUB=JES2][,PARM=zzzz][SMFWRITE=ON | OFF]
```

xxxx The name of the PROCLIB member containing the JCL for CYN1. *CYN1* is also the name of the IBM MVS subsystem. The PROCLIB member is usually called *CYN1*, but it does not have to be. In fact, in order to avoid specifying SUB=JES2, it is recommended to keep those names distinct and use *CYN1PROC* as the name for the Proclib member.

yy The optional identifier of the started task for future reference is the MODIFY or STOP commands. For short yy=CC. If yy is not specified, the system uses xxxx as the identifier.

SUB=JES2

If the PROCLIB member and the subsystem share the same name, *CYN1*. This specification is required so that the JCL to be selected is to be found in the JES2 procedure library, for example, USER.PROCLIB, instead of the default MSTR.

PARM=zzzz

It is appended to the string CYNP to form the name of a parameter module Data Section (DSECT), member of the STEPLIB library, in which the run parameters are specified. If omitted, the name specified in the PARM keyword, in the JCL EXEC statement will be selected. If there is no PARM keyword, this specification is required.

SMFWRITE=ON | OFF

Either ON or OFF must be used if the SMFWRITE directive is specified. If omitted, the name specified in the SMFWRITE keyword, in the JCL EXEC statement will be selected. If there is no SMFWRITE keyword, this specification is required. This specification sets the initial value of the SMFWRITE variable, which can be subsequently changed with the SMFWRITE command. If SMFWRITE is ON, application server generated

SMF records (type 120, subtypes 3, 6, and 8) will be written to the SMF data sets. If SMFWRITE is OFF, writing of these records will be disabled.

Examples:

```
START CYN1.CC,SUB=JES2
START CYN1PROC.DS
START CYN1PROC,PARM=BIG
START CYN1PROC,SMFWRITE=ON
START CYN1PROC.CC,SMFWRITE=OFF,PARMS=TEST
```

Stopping the Common Services Address Space

The syntax of the stop command is as follows:

P xxxx or P yy

xxxx The name of the PROCLIB member containing the JCL for CYN1. This form is required when no identifier name was supplied in the start command.

yy The optional identifier for the started task, in the start command. If yy is not specified, the system uses xxxx as the identifier.

Note: When stopping CYN1, outstanding requests will be completed. Subsequent requests, however, might produce unpredictable results. Therefore use the INACT command (See “The INACT command” on page 181.) prior to issuing this command to insure that no additional requests will be initiated.

Modifying the Common Services Address Space

The following syntax options are available for the modify command:

- F xxxx,verb[,param...[,param]...]

- F yy,verb[,param...[,param]...]

xxxx The name of the PROCLIB member containing the JCL for CYN1. This form is required when no identifier name was supplied in the start command.

yy The optional identifier for the started task, in the start command. If yy is not specified, the system uses xxxx as the identifier.

verb The command verb. Currently there are eight verbs: ACT, INACT, DUMP, TRACE, SPINLOG, ZAP, STAMP, VER, for the CYN1 commands.

param The CYN1 command parameters. They are command dependent and their presence is optional.

The ACT command

The form of the ACT command is as follows:

F xxxx,ACT

Or,

F yy,ACT

The ACT command is only useful to render CYN1 active again in the event the INACT command has been issued. When CYN1 is started, it is initiated in active mode, ready to process Client requests.

The CPU command

The CPU command is used to display CPU information about a particular address space identified by its address space identification (asid). The CPU information consists in the accumulated CPU time in central processors expressed in seconds. Additionally, under IBM z/OS V1R6 and later, some IBM zSeries® Application Assist Processor (zAAP) data is given. They are the accumulated CPU time in zAAP, also known as Integration Facility for Applications (IFA) processors, the accumulated CPU time in central processors (CP), and the accumulated CPU time in CP which could have been spent in zAAP. All CPU times are normalized and expressed in seconds.

The form of the CPU command is as follows:

```
F {xxxx | yy}, asid
```

asid

It specifies the asid of the address space for which the CPU information will be given. It is a four-digit hexadecimal number.

Example:

```
F CC,CPU 006A
```

will output CPU information for the address space whose asid is 006A.

The INACT command

The form of the INACT command is as follows:

```
F xxxx,INACT
```

Or,

```
F yy,INACT
```

The INACT command puts CYN1 in a state where no further Client requests will be accepted. However, currently active requests will be completed. The use of the INACT command is recommended when problems are detected, either at the Server, or the Client level, or when CYN1 is about to be brought down.

The DUMP command

The DUMP command is used to display in hexadecimal and character format areas of storage in the CYN1PROC address space.

The form of the DUMP command is as follows:

```
F {xxxx | yy},DUMP,AS,hexaddr[,length]
```

AS AS stands for address space.

Hexaddr

It specifies an eight-digit hexadecimal starting address of the memory location to be displayed. Alternately, the starting address can be specified with keywords describing what control blocks to be displayed.

The current valid keywords are:

\$CYNCYNA	The CYN1 anchor area in CSA
\$CYNSETB	The server directory table
\$CYNSTITB	The server or container interval table
\$CYNSSPL	The server section entry pool
\$CYNBSPL	The bean section entry pool
\$CYNBMPL	The bean method section entry pool
\$CYNHSPL	The HttpSessionManager section entry pool
\$CYNWSPL	The WebApplication section entry pool
\$CYNVPL	The Servlet section entry pool
\$LOGBOOK	The in-core SYSLOG book
\$CMDBOOK	The in-core command book

Note: The corresponding DSECTs are part of the macro library.

length

It specifies the length in bytes of the area to be displayed. The length is specified in decimal and has a maximum of 4 digits (9999 bytes). The default is 16 bytes (one dump line).

Example:

Table 22. Example of Dump command output

F CC,DUMP,AS,00000000	It displays 16 bytes of the Prefixed Storage Area (PSA).
F CC,DUMP,AS,\$CYNSETB,192	It displays entries 0 and 1 of the server directory table.
F CC,DUMP,AS,02A0C100,4096	It displays one memory page starting at location 02A0C100.

The SMFWRITE command

The SMFWRITE command is used to turn on or off the writing of application server generated SMF records (type 120, subtypes 3, 6, and 8) to the SMF data sets. It is also used to display the current value of SMFWRITE.

The form of the SMFWRITE command is as follows:

F {xxxx | yy},SMFWRITE {ON | OFF | SHOW}

Note: ON will turn the SMF writing on, while OFF will turn it off. When CYN1 comes up, the writing is governed by the SMFWRITE specification in the START command, or is hardcoded in the JCL of the corresponding PROCLIB member JCL. SHOW displays the current value (ON or OFF) of SMFWRITE.

The TRACE command

The TRACE command is used to turn on or off the SYSLOG trace, which currently consists of information messages regarding the reception of SMF records. The SYSLOG data set is buffered in a circular in-core book, the size of which is specified in the PARM member.

The form of the TRACE command is as follows:

F {xxxx | yy},TRACE {ON | OFF}

Note: ON will turn the trace on, while OFF will turn it off. When CYN1 comes up, the trace is off.

The SPINLOG command

The SPINLOG command is used to reset pointers to the in-core SYSLOG book, close the current SYSLOG data set, and reopen a new one. The closed SYSLOG data set can be subsequently retrieved by report writer programs. SYSLOG traces can be separated.

The form of the SPINLOG command is as follows:

F {xxxx | yy},SPINLOG

The ZAP command

The ZAP command is used to modify areas of storage in the CYN1 address. The form of the ZAP command is as follows:

F {xxxx | yy},ZAP,{AS|SS},hexaddr,hexcont,hexrepl

AS|SS

AS stands for address space dump. SS stands for address space authorized. Either one must be specified.

hexaddr

It specifies an eight-digit hexadecimal address of the word to be zapped. Low core (4 kilobyte PSA) zapping is always disabled. System region, for example, virtual addresses 00001001 through 00005000 can only be zapped if SS address space authorized option is specified.

hexcont

It specifies the eight-digit hexadecimal current contents of the word to be zapped, for verification.

Hexrepl

It specifies the eight-digit hexadecimal value to replace hexcont with at address hexaddr.

Examples:

Table 23. Examples of Zap command

Valid	Invalid
F CC,ZAP,SS,0000100F,E8000000,00000000	F CC,ZAP,AS,00000000,040C0000,00000000 F CC,ZAP,SS,00000000,040C0000,00000000 Note: It is invalid because the area to be zapped is in the PSA.
F CC,ZAP,AS,028AC300,001F007A,00000000 zeroes the word at virtual address 028AC300 location.	F CC,ZAP,AS,0000100F,E8000000,00000000 Note: It is invalid because the area to be zapped is in the system region.

The STAMP command

The STAMP command is used to turn on or off time stamping, which consists in outputting to the SYSLOG data set stamp records corresponding to critical events in processing client requests. The SYSLOG data set is buffered in a circular in-core book, the size of which is specified in the PARM member.

The form of the STAMP command is as follows:

```
F {xxxx | yy},STAMP {ON | OFF}
```

Note: ON will turn the STAMP on, while OFF will turn it off. When CYN1 comes up, time stamping is off.

The VER command

The VER command is used to display the version information in CYN1 main task entry module CYN1DRVR. The information consists of the name of the module followed by the *version.level.change* number followed by the date and time of the module assembly.

The form of the VER command is as follows:

```
F {xxxx | yy},VER
```

The STATS command

The STATS command is used to reset the statistical information that is gathered by CYN1 from the application server generated SMF records. SMF records of type 120 are generated on a regular basis (recommended every 300 seconds) by every application server instance, summarizing server activity (subtype 3), EJB container activity (subtype 6) and Web container activity (subtype 8) for that period. Normally CYN1 gathers this information and accumulates or averages these statistics across periods for each server instance, so that what the user sees on the System Resource screen is a running activity history for that server instance. The RESET option of the STATS command will cause the next generated statistics to override the current accumulated statistics for all server instances, thereby starting a new history interval. After the override, statistics accumulation resumes until the next time the RESET option is used. If the RESET option was entered by mistake, the CUMUL option will nullify it provided the CUMUL option is entered prior to application server generation of the next SMF records.

The form of the STATS command is as follows:

```
F {xxxx | yy},STATS {RESET | CUMUL}
```

Note: RESET will reset the start of the statistics accumulation interval. CUMUL will undo RESET if entered before the next SMF record cycle. CUMUL has no effect if RESET was not entered.

Appendix E. Using regular expressions

Regular expressions are sets of symbols and characters that are used to match patterns of text. You can use regular expressions to search specific IP addresses across your Web environment. Regular expressions also enable you to search a simple, fixed URI or a complex URI pattern that matches one or more groups of transactions.

Regular expression library

An extensive library of regular expression characters and operators is available for your URI filters and IP address specifications. The International Components for Unicode (ICU) open-source development project provides this library for your use. The next section provides the most frequently used expressions for this product. However, you can refer to the following Web page for a full description of the ICU regular expression library and an explanation of how to use the characters and operators for complex expressions: <http://oss.software.ibm.com/icu/userguide/regex.html>

Frequently used regular expressions

The following list highlights characters and operators most frequently used in regular expressions:

**** Quotes the character that follows it, which treats that character as a literal character or operator (not a regular expression). When you want the following characters to be treated as literal, you must precede them with a backslash:

*** ? + [() { } ^ \$ | \ . /**

In other words, use a backslash followed by a forward slash (\/) to include a forward slash in a URI filter. Use a backslash followed by a period (\.) to include a period in a URI filter.

Example: to specify the URI pattern `http://www.ibm.com/`, use the following regular expression:

`http:\\www\\.ibm\\.com\\`

To specify all URIs that begin with `http://www.ibm.com/`, use the following regular expression:

`http:\\www\\.ibm\\.com\\.*`

. Matches any one character.

Example: to match both `ibm2` and `ibm3` within a string, use `ibm.` such as in the following example: **`http:\\www\\.ibm\\.com\\`**

(?: ...)

Non-capturing parentheses. Groups the included pattern, but does not provide capturing of matching text. Somewhat more efficient than capturing parentheses.

Example: you can use the non-capturing parenthesis to group expressions to form more complicated regular expressions. To match a URI that starts

with one of the following 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)

Note: This section applies to the entry of URI and client IP filters for Quality of Service listening policies only.

You can use an exclamation point (!), also called the *bang* operator, to filter out transactions that might match the regular expressions already entered, but that 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. Support information

This chapter describes options for obtaining support for IBM products.

Searching knowledge bases

If you have a problem with your IBM software, you want it resolved quickly. Begin by searching the available knowledge bases to determine whether the resolution to your problem is already documented.

Finding Release Notes

You can find Release Note information online by viewing IBM Technotes. Technotes replace the Release Notes[®] manual for this product. *Technotes* are short documents that cover a single topic. You can search the Technote collection for common problems and solutions, as well as known limitations and workarounds. Technotes are continuously updated to provide current product information.

The following two procedures describe how to view Technotes and subscribe to have future Technotes e-mailed to you. Alternatively, you can watch demos of these procedures at the following Web site:

<http://www.ibm.com/software/support/sitetours.html>

Viewing Technotes

Perform the following actions to access Technotes for this product:

1. Launch the IBM Software Support Web site: <http://www.ibm.com/software/support>
2. Follow the instructions on the screen to search for the Technotes related to the issue encountered.

Subscribing to new Technotes

You can subscribe to an RSS feed of the product support page or subscribe to receive e-mail notification about product tips and newly published fixes through My support. To subscribe to an RSS news feed of the product support page, click the orange **RSS** button under the **Stay up to date** pane.

My Support is a personalized portal that enables you to:

- Specify the products for which you want to receive notifications
- Create a personalized page that provides product information for the products you use
- Choose from flashes, downloads, and Technotes
- Receive an e-mail update in your inbox

Perform the following actions to subscribe to My support e-mails:

1. Launch an IBM support Web site such as the following site:
<http://www.ibm.com/support/>
2. Click **My support** in the upper-right section of the page.
3. If you have not yet registered, click **register** in the upper-right corner of the support page to create your user ID and password.
4. Sign in to **My support**.

5. On the My support page, click **Add products**.
6. Make the following selections from the lists to add this product to your personal page:
 - a. Software
 - b. Systems Management
 - c. Application Performance & Availability
7. Click **Add products**.
8. Click **Subscribe to email**.
9. Set your preferences to specify the information you want in your e-mails.
10. Click **Update**.
11. Click **Submit**.

Searching the information center on your local system or network

IBM provides extensive documentation that can be installed on your local computer or on an intranet server. You can use the search function of this information center to query conceptual information, instructions for completing tasks, reference information, and support documents.

Searching the Internet

If you cannot find an answer to your question in the information center, search the Internet for the latest, most complete information that might help you resolve your problem. To search multiple Internet resources for your product, expand the product folder in the navigation frame to the left and select **Web search**. From this topic, you can search a variety of resources including:

- IBM technotes
- IBM downloads
- IBM Redbooks®
- IBM DeveloperWorks
- Forums and newsgroups
- Google

Obtaining fixes

A product fix might be available to resolve your problem. To determine what fixes are available for your IBM software product, follow these steps:

1. Go to the IBM Software Support Web site at <http://www.ibm.com/software/support>.
2. Click **Downloads** in the **Software** section.
3. Under the **Updates, drivers, and fixes** section, select **Fixes, fixpacks and utilities**.
4. Navigate to ITCAM for WebSphere or ITCAM for J2EE to obtain a list of available fixes.

For more information about the types of fixes that are available, see the *IBM Software Support Handbook* at <http://techsupport.services.ibm.com/guides/handbook.html>.

Receiving Weekly support updates

To receive e-mail notifications about software support news and updates, follow these steps:

1. Go to the IBM Software Support Web site at <http://www.ibm.com/software/support>.
2. On the right hand side, click **My Notifications**.
3. If you have already registered for **My Notifications**, login. If you have not registered, click **register now**. Complete the registration form using your e-mail address as your IBM ID. When you have logged in, the **My notifications for IBM technical support** home page is displayed.
4. Select the **Subscribe** tab.
5. Under the **Software** list, select **Tivoli**.
6. Select **Tivoli Composite Application Manager for J2EE** and/or **Tivoli Composite Application Manager for WebSphere**. Click **Continue**.
7. In the **Options** section, enter a folder name, update notifications will be saved in this folder.
8. In the **Notify me by** section, choose if you want to be notified of updates daily or weekly.
9. In the **Notify me by** section, choose if you want to receive notifications in plain text or html.
10. In the **Document Types** section, customize the types of information you want to be updated on, for example, white papers, drivers etc. Click **Submit**.

If you experience problems with the **My Notifications** feature, you can obtain help in one of the following ways:

Online

Send an e-mail message to erchelp@ca.ibm.com, describing your problem.

By phone

Call 1-800-IBM-4You (1-800-426-4968).

Contacting IBM Software Support

IBM Software Support provides assistance with product defects.

Before contacting IBM Software Support, your company must have an active IBM software maintenance contract, and you must be authorized to submit problems to IBM. The type of software maintenance contract that you need depends on the type of product you have:

- For IBM distributed software products (including, but not limited to, IBM Tivoli, IBM Lotus®, and IBM Rational® products, as well as IBM DB2 and IBM WebSphere Application Server products that run on Windows, UNIX, or Linux operating systems), enroll in IBM Passport Advantage® in one of the following ways:
 - **Online:** go to the IBM Passport Advantage Web page (<http://www.ibm.com/software/passportadvantage>) and click **How to Enroll**
 - **By phone:** for the phone number to call in your country, go to the IBM Software Support Web site (<http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html>) and click the name of your geographic region.
- For IBM eServer™ software products (including, but not limited to, IBM DB2 and IBM WebSphere Application Server products that run in IBM zSeries, IBM

pSeries®, and IBM iSeries® environments), you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for eServer software products, go to the IBM Technical Support Advantage Web page (<http://www.ibm.com/servers/eserver/techsupport.html>).

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States or, from other countries, go to the contacts page of the IBM Software Support Handbook on the Web (<http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html>) and click the name of your geographic region for phone numbers of people who provide support for your location.

Follow the steps in this topic to contact IBM Software Support:

1. Determine the business impact of your problem.
2. Describe your problem and gather background information.
3. Submit your problem to IBM Software Support.

Determining the business impact of your problem

When you report a problem to IBM, you are asked to supply a severity level. Therefore, you need to understand and assess the business impact of the problem you are reporting. Use the following criteria:

Table 24. Criteria for assessing the business impact of your problem

Severity 1	Critical business impact: you are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.
Severity 2	Significant business impact: the program is usable but is severely limited.
Severity 3	Some business impact: the program is usable with less significant features (not critical to operations) unavailable.
Severity 4	Minimal business impact: the problem causes little impact on operations, or a reasonable circumvention to the problem has been implemented.

Describing your problem and gathering background information

When explaining a problem to IBM, be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently. To save time, know the answers to these questions:

- What software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can the problem be re-created? If so, what steps led to the failure?
- Have any changes been made to the system? (For example, hardware, operating system, networking software, and so on.)
- Are you currently using a workaround for this problem? If so, please be prepared to explain it when you report the problem.

Submitting your problem to IBM Software Support

You can submit your problem in one of two ways:

- **Online:** go to the "Submit and track problems" page on the IBM Software Support site (<http://www.ibm.com/software/support/probsub.html>). Enter your information into the appropriate problem submission tool.
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can the problem be re-created? If so, what steps led to the failure?
- Have any changes been made to the system? (For example, hardware, operating system, networking software, and so on.)
- Are you currently using a workaround for this problem? If so, please be prepared to explain it when you report the problem.

If the problem you submit is for a software defect or for missing or inaccurate documentation, IBM Software Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Software Support provides a workaround for you to implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM product support Web pages daily, so that other users who experience the same problem can benefit from the same resolutions.

For more information about problem resolution, see Searching knowledge bases and Obtaining fixes.

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 Web site: http://www.ibm.com/software/sysmgmt/products/support/supp_tech_exch.html

Appendix G. Accessibility

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. These are the major accessibility features you can use with ITCAM for Application Diagnostics when accessing it through the *IBM Personal Communications* terminal emulator:

- You can operate all features using the keyboard instead of the mouse.
- You can read text through interaction with assistive technology.
- You can use system settings for font, size, and color for all user interface controls.
- You can magnify what is displayed on your screen.

For more information on viewing PDFs from Adobe, go to the following Web site:
<http://www.adobe.com/enterprise/accessibility/main.html>

Index

A

- accessibility xiv, 193
- ACT command 180
- addressing mode 74
- AMODE 74
- analyzing JVM 117, 118
- analyzing WebSphere 118
- application server
 - changing version 73
- AppServer_home xvi
- ASSIZEMAX parameter 20
- Asynchronous Bean requests 62
- authorizing data sets 16
- autoconfiguration 78

B

- books xi
- Byte Code Instrumentation, disabling
 - types of 50

C

- CICS 76
- commands
 - ACT 180
 - CPU 181
 - CYN1 179
 - DUMP 181
 - INACT 181
 - SMFWRITE 182
 - SPINLOG 183
 - STAMP 183
 - STATS 184
 - TRACE 182
 - VER 184
 - ZAP 183
- Common Services Address Space
 - commands 179
- communications protocols
 - z/OS 121, 124
- config_home xv, 18
 - creating 13
- configuration directory 18
 - creating 13
- configuring
 - CYN1 subsystem 15
 - Data Collector 17
 - Monitoring Agent 99
 - overview of steps 7
- conventions
 - typeface xv
- CPU command 181
- CTG 76
- custom MBeans 63, 64
- custom requests 60
- customer support 189
- CYN1
 - commands 179
 - modifying 180

- CYN1 (*continued*)
 - starting 179
 - stopping 180
- CYN1 subsystem
 - configuring 15
 - customizing for SMF 67
 - verifying definition of 70

D

- data collector
 - z/OS 116
- Data Collector 5
 - configuring 17
 - installing 7, 13
 - moving to a different host
 - computer 75
 - upgrading 32
- Data Collector buffering 47
- Data Collector properties 45
- data sets, authorizing 16
- datacollector_custom.properties 45
- datacollector.properties 45
- directories, variables for xv
- DUMP command 181
- dynamic subsystem 15

E

- edge request data 118
- encryption 172

F

- firewall
 - ports 20
- fixes, obtaining 188

G

- garbage collection
 - interval 82

H

- heap analysis, disabling 59
- historical data collection 145
 - Persistent Datastore 127, 145
- hub TEMS
 - identifying 145

I

- ICAT 99
 - invoking 99
- identifying hub TEMS
 - z/OS 145

- identifying remote TEMS
 - z/OS 145
- IEFU83 exit, installing 67
- INACT command 181
- information centers, searching to find
 - software problem resolution 188
- install_home xv
- Installation and Configuration Assistance Tool 99
- installing
 - Data Collector 7, 13
 - Monitoring Agent 9
- instrumentation 52
- integration with ITCAM for Transactions 79
- Internet, searching to find software
 - problem resolution 188
- invoking
 - ICAT 99
- IP address 23, 74
- ISA xiv

K

- keystore management 169
- knowledge bases, searching to find
 - software problem resolution 187

L

- Level2 request data 118
- lock analysis 52, 53
- log files
 - runtime setup script 41, 42, 43, 93, 94, 95
- log messages 118
- LogCmd 86

M

- Managing Server 16, 44, 84
 - changing 73
- manuals xi
- MBeans 63
- memory leak analysis 55
- memory leak diagnosis 52
- memory monitoring 72
- method entry and exit analysis 52, 57
- method tracing 52, 57
- modifying
 - CYN1 180
- Monitoring Agent 6
 - configuring 99
 - disabling Data Collector
 - communication with 84
 - installing 9

N

- NATs 76
- Network Deployment 19, 78
- network interfaces 76
- Node Authentication 168
 - Data Collector 169
 - Managing Server 169

O

- ordering publications xiii

P

- PARMLIB, updating 15
- password 22
- PDS 127
- Performance Monitoring Infrastructure
 - customizing 65
 - Service Integration Bus 66
 - settings after running the runtime setup script 20
- Persistent Datastore 127
 - configuring 127, 145
- physical disability 193
- populating certificates 169
- ports
 - default 20
- privacy filtering 175
- problem determination
 - describing problem for IBM Software Support 190
 - determining business impact for IBM Software Support 190
 - submitting problem to IBM Software Support 190
- procedure library
 - z/OS system 136, 144, 145
- PROCLIB, updating 16
- product home directory, Monitoring Agent 113
- properties files 45
- publications xi
 - ordering xiii

Q

- Quality of Service
 - using regular expressions 186

R

- RACF, updating 16
- reader requirements xi
- regular expressions 185
 - bang (!) operator 186
 - frequently used 185
 - library 185
 - Quality of Service 186
- Release Notes 187
- remote TEMS
 - identifying 145
- requirements for readers xi
- resource data
 - WebSphere 118, 119

- RMI/IIOP requests, enabling instrumentation 49
- Runtime Environment 108
- runtime setup script 17
 - auto-run mode 42
 - batch mode 42
 - log files 41, 42, 43, 93, 94, 95
 - prompt mode 36

S

- script, runtime setup 17
 - auto-run mode 42
 - batch mode 42
 - log files 41, 42, 43, 93, 94, 95
- secure communications, verifying 173
- security 165
- server alias 73
- Service Integration Bus
 - Performance Monitoring Infrastructure settings 66
- SMF 83, 85
- SMF, customizing 67
 - CYN1 subsystem 67
- SMFWRITE command 182
- Software Support
 - contacting 189
 - describing problem for IBM Software Support 190
 - determining business impact for IBM Software Support 190
 - receiving weekly updates 189
 - submitting problem to IBM Software Support 190
- SPINLOG command 183
- SSL 172
 - Data Collector 173
- STAMP command 183
- started task
 - z/OS 110, 121, 128, 136, 145
- starting
 - CYN1 179
- STATS command 184
- stopping
 - CYN1 180
- SYS1.PROCLIB 136
- SYSPLEX 7
- system procedure library
 - z/OS 136, 144, 145

T

- Technotes
 - e-mail subscriptions 187
 - viewing 187
- The IBM Support Assistant xiv
- Tivoli Enterprise Portal
 - benefits 3
- Tivoli Monitoring Services
 - z/OS 108
- Tivoli Support Technical Exchange 191
- toolkit properties 45
 - toolkit_custom.properties 45
 - toolkit_global_custom.properties 45
 - toolkit.properties 45
- TRACE command 182

- TTAPI 79
- Turbo Mode 48
- typeface conventions xv

U

- unconfiguring
 - Data Collector 87
- updating
 - PARMLIB 15
 - PROCLIB 16
 - RACF 16
- upgrading 10
 - Data Collector 32

V

- variables for directories xv
- VER command 184
- verboseGC trace 118
- verifying installation 17
 - verifying installation and configuration 44
- VIPA 23

W

- Web Services 72
- wsadmin.sh scripting engine 19

Z

- ZAP command 183

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Adobe is either a registered trademark or a trademark of Adobe Systems Incorporated in the United States, other countries, or both.

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

Windows is a registered trademark of Microsoft Corporation in the United States, other countries, or both.

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



Java and all Java-based trademarks are trademarks or registered trademarks of Oracle and/or its affiliates.

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

Notices

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

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

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

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

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to

IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.



Printed in USA

SC27-2820-00

