Tivoli® System Automation for z/OS
Version 3 Release 3

Monitoring Agent Configuration and User's Guide

IBM

Tivoli® System Automation for z/OS
Version 3 Release 3

*Monitoring Agent Configuration and
User's Guide*

IBM

Contents

Figures

Tables

Dotted decimal syntax diagrams

Syntax diagrams are provided in dotted decimal format for users accessing the Information Center using a screen reader. In dotted decimal format, each syntax element is written on a separate line. If two or more syntax elements are always present together (or always absent together), they can appear on the same line, because they can be considered as a single compound syntax element.

Each line starts with a dotted decimal number; for example, 3 or 3.1 or 3.1.1. To hear these numbers correctly, make sure that your screen reader is set to read out punctuation. All the syntax elements that have the same dotted decimal number (for example, all the syntax elements that have the number 3.1) are mutually exclusive alternatives. If you hear the lines 3.1 USERID and 3.1 SYSTEMID, you know that your syntax can include either USERID or SYSTEMID, but not both.

The dotted decimal numbering level denotes the level of nesting. For example, if a syntax element with dotted decimal number 3 is followed by a series of syntax elements with dotted decimal number 3.1, all the syntax elements numbered 3.1 are subordinate to the syntax element numbered 3.

Certain words and symbols are used next to the dotted decimal numbers to add information about the syntax elements. Occasionally, these words and symbols might occur at the beginning of the element itself. For ease of identification, if the word or symbol is a part of the syntax element, it is preceded by the backslash (\) character. The * symbol can be used next to a dotted decimal number to indicate that the syntax element repeats. For example, syntax element *FILE with dotted decimal number 3 is given the format 3 * FILE. Format 3* FILE indicates that syntax element FILE repeats. Format 3* * FILE indicates that syntax element * FILE repeats.

Characters such as commas, which are used to separate a string of syntax elements, are shown in the syntax just before the items they separate. These characters can appear on the same line as each item, or on a separate line with the same dotted decimal number as the relevant items. The line can also show another symbol giving information about the syntax elements. For example, the lines 5.1*, 5.1 LASTRUN, and 5.1 DELETE mean that if you use more than one of the LASTRUN and DELETE syntax elements, the elements must be separated by a comma. If no separator is given, assume that you use a blank to separate each syntax element.

If a syntax element is preceded by the % symbol, this indicates a reference that is defined elsewhere. The string following the % symbol is the name of a syntax fragment rather than a literal. For example, the line 2.1 %OP1 means that you should refer to separate syntax fragment OP1.

The following words and symbols are used next to the dotted decimal numbers:
- ? means an optional syntax element. A dotted decimal number followed by the ? symbol indicates that all the syntax elements with a corresponding dotted decimal number, and any subordinate syntax elements, are optional. If there is only one syntax element with a dotted decimal number, the ? symbol is displayed on the same line as the syntax element, (for example 5? NOTIFY). If there is more than one syntax element with a dotted decimal number, the ? symbol is displayed on a line by itself, followed by the syntax elements that are

optional. For example, if you hear the lines 5 ?, 5 NOTIFY, and 5 UPDATE, you know that syntax elements NOTIFY and UPDATE are optional; that is, you can choose one or none of them. The ? symbol is equivalent to a bypass line in a railroad diagram.

- ! means a default syntax element. A dotted decimal number followed by the ! symbol and a syntax element indicates that the syntax element is the default option for all syntax elements that share the same dotted decimal number. Only one of the syntax elements that share the same dotted decimal number can specify a ! symbol. For example, if you hear the lines 2? FILE, 2.1! (KEEP), and 2.1 (DELETE), you know that (KEEP) is the default option for the FILE keyword. In this example, if you include the FILE keyword but do not specify an option, default option KEEP will be applied. A default option also applies to the next higher dotted decimal number. In this example, if the FILE keyword is omitted, default FILE(KEEP) is used. However, if you hear the lines 2? FILE, 2.1, 2.1.1! (KEEP), and 2.1.1 (DELETE), the default option KEEP only applies to the next higher dotted decimal number, 2.1 (which does not have an associated keyword), and does not apply to 2? FILE. Nothing is used if the keyword FILE is omitted.

- * means a syntax element that can be repeated 0 or more times. A dotted decimal number followed by the * symbol indicates that this syntax element can be used zero or more times; that is, it is optional and can be repeated. For example, if you hear the line 5.1* data area, you know that you can include one data area, more than one data area, or no data area. If you hear the lines 3*, 3 HOST, and 3 STATE, you know that you can include HOST, STATE, both together, or nothing.

    Notes:

    1. If a dotted decimal number has an asterisk (*) next to it and there is only one item with that dotted decimal number, you can repeat that same item more than once.

    2. If a dotted decimal number has an asterisk next to it and several items have that dotted decimal number, you can use more than one item from the list, but you cannot use the items more than once each. In the previous example, you could write HOST STATE, but you could not write HOST HOST.

    3. The * symbol is equivalent to a loop-back line in a railroad syntax diagram.

- + means a syntax element that must be included one or more times. A dotted decimal number followed by the + symbol indicates that this syntax element must be included one or more times; that is, it must be included at least once and can be repeated. For example, if you hear the line 6.1+ data area, you must include at least one data area. If you hear the lines 2+, 2 HOST, and 2 STATE, you know that you must include HOST, STATE, or both. Similar to the * symbol, the + symbol can only repeat a particular item if it is the only item with that dotted decimal number. The + symbol, like the * symbol, is equivalent to a loop-back line in a railroad syntax diagram.

How to send your comments to IBM

We appreciate your input on this publication. Feel free to comment on the clarity, accuracy, and completeness of the information or give us any other feedback that you might have.

Use one of the following methods to send us your comments:

1. Send an email to s390id@de.ibm.com
2. Visit the SA z/OS home page at http://www.ibm.com/systems/z/os/zos/features/system_automation/
3. Visit the Contact z/OS web page at http://www.ibm.com/systems/z/os/zos/webqs.html
4. Mail the comments to the following address:
   > IBM Deutschland Research & Development GmbH
   > Department 3248
   > Schoenaicher Str. 220
   > D-71032 Boeblingen
   > Federal Republic of Germany
5. Fax the comments to us as follows:
   > From Germany: 07031-16-3456
   > From all other countries: +(49)-7031-16-3456

Include the following information:
- Your name and address
- Your email address
- Your telephone or fax number
- The publication title and order number:
   > IBM Tivoli System Automation for z/OS V3R3.0 Monitoring Agent
   > Configuration and User's Guide
   > SC34-2581-00
- The topic and page number related to your comment
- The text of your comment.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you submit.

If you have a technical problem

Do not use the feedback methods listed above. Instead, do one of the following:
- Contact your IBM service representative
- Call IBM technical support
- Visit the IBM zSeries support web page at www.ibm.com/systems/z/support/.

About this book

The IBM® Tivoli® System Automation for z/OS® (SA z/OS) monitoring agent monitors the automation environment and the resources it contains in systems and sysplexes.

The SA z/OS monitoring agent collects information about the status of automation on z/OS systems and z/OS sysplexes, and reports it in the Tivoli Enterprise Portal (formerly named CandleNet Portal) graphical user interface. The product workspaces provide the following types of information about your enterprise:

- Resource overview and detail information
- Resource requests inserted into the automation
- The current automation environment, that is, the location and status of automation managers and automation agents within the sysplex
- System and application health information through monitor resources
- User-defined status items for installation-specific monitoring
- Exceptional messages that are captured by SA z/OS
- Gateway definitions and statuses for a system in the sysplex
- Outstanding WTORs in the SA z/OS subplex

This book describes how to plan your deployment of the SA z/OS monitoring agent and how to install and configure it in your environment.

This book also describes how to use the SA z/OS monitoring agent to monitor z/OS systems and sysplexes. It also presents several usage scenarios and explains product messages.

Who should use this book

Parts 1 and 2 of this guide are intended for the system programmer or administrator who is responsible for installing and configuring new programs on z/OS systems. The procedures in this guide require familiarity with the following:

- The z/OS operating system
- The Microsoft® Windows® operating system

No previous experience with Tivoli OMEGAMON® products or with IBM Tivoli Monitoring is required; in fact, the SA z/OS monitoring agent is intended as an introduction to the zSeries® monitoring agents that run in the IBM Tivoli Monitoring environment. Therefore, the procedures for configuring this product are somewhat simpler and involve fewer choices than those for the other Tivoli OMEGAMON zSeries monitoring products.

Part 3 of this guide is intended primarily for operators. However, system administrators, programmers and help desk personnel may find it helpful for installation, maintenance, and investigating and correcting problems.

Where to find more information

The System Automation for z/OS library

The following table shows the information units in the System Automation for z/OS library:

Table 1. System Automation for z/OS Library

Title	Order Number
IBM Tivoli System Automation for z/OS Planning and Installation	SC34-2571
IBM Tivoli System Automation for z/OS Customizing and Programming	SC34-2570
IBM Tivoli System Automation for z/OS Defining Automation Policy	SC34-2572
IBM Tivoli System Automation for z/OS User's Guide	SC34-2573
IBM Tivoli System Automation for z/OS Messages and Codes	SC34-2574
IBM Tivoli System Automation for z/OS Operator's Commands	SC34-2575
IBM Tivoli System Automation for z/OS Programmer's Reference	SC34-2576
IBM Tivoli System Automation for z/OS TWS Automation Programmer's Reference and Operator's Guide	SC34-2579
IBM Tivoli System Automation for z/OS Product Automation Programmer's Reference and Operator's Guide	SC34-2569
IBM Tivoli System Automation for z/OS End-to-End Automation Adapter	SC34-2580
IBM Tivoli System Automation for z/OS Monitoring Agent Configuration and User's Guide	SC34-2581
IBM Tivoli System Automation for z/OS: GDPS/PPRC HyperSwap® Manager Installation Guide	SC33-8270

The System Automation for z/OS books are also available on CD-ROM as part of the following collection kit:

IBM Online Library z/OS Software Products Collection (SK3T-4270)

SA z/OS Home Page

For the latest news on SA z/OS, visit the SA z/OS home page at http://www.ibm.com/systems/z/os/zos/features/system_automation/

The z/OS library

You can find books in related product libraries that may be useful for support of the SA z/OS base program by visiting the z/OS Internet Library at http://www.ibm.com/systems/z/os/zos/bkserv/

IBM Tivoli Monitoring publications

Basic instructions for installing and setting up the IBM Tivoli Monitoring (also called Tivoli Monitoring Services or Tivoli Management Services) components of the product are provided in this guide. You can find more detailed information about the IBM Tivoli Monitoring components in the following publications:

- *Installation and Setup Guide*, GC32-9407

  Provides information on installing and setting up the Tivoli Enterprise Monitoring Server and the Tivoli Enterprise Portal Server and client.

- *Configuring IBM Tivoli Enterprise Monitoring Server on z/OS*, SC32-9463

  Describes how to configure and customize the Tivoli Enterprise Monitoring Server on z/OS. The book also contains platform planning information and information about setting up security on your monitoring server.
- *Administrator's Guide*, SC32-9408

  Describes how to perform administrative tasks associated with the Tivoli Enterprise Portal Server and client.
- *User's Guide*, SC32-9409

  Describes how to use the Tivoli Enterprise Portal client interface. This book includes a monitoring tutorial that covers workspaces, navigation, views, and responding to alerts. Different types of views and situations for event-based monitoring are also included, as well as information on automation policies.
- *Problem Determination Guide*, GC32-9458.

  Lists and explains IBM Tivoli Monitoring messages, and offers troubleshooting guidance.

You can also find useful information about setting up and deploying the IBM Tivoli Monitoring components in the following IBM Redbooks®:
- *Deployment Guide Series: IBM Tivoli Monitoring 6.2*, SG24-7444

Getting Started with IBM Tivoli Monitoring 6.2 on Distributed Environments

Accessing publications online

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

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 Website. Access the Tivoli software information center at the following Web address:

http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp

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

Reading *CCR2* Online

IBM publishes *CCR2*, a useful monthly e-newsletter for the System z® and zSeries software community. You can find the latest issue of *CCR2* at http://www-306.ibm.com/software/tivoli/features/ccr2/info.html.

Ordering publications

You can order many Tivoli publications online at the following Website:

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

You can also order by telephone by calling one of these numbers:
- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, contact your software account representative to order Tivoli publications.

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 Website:

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

Access the glossary by clicking the **Glossary** link on the left pane of the Tivoli software library window.

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

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

Using LookAt to look up message explanations

LookAt is an online facility that lets you look up explanations for most of the IBM messages you encounter, as well as for some system abends and codes. Using LookAt to find information is faster than a conventional search because in most cases LookAt goes directly to the message explanation.

You can use LookAt from these locations to find IBM message explanations for z/OS elements and features, z/VM®, z/VSE™, and Clusters for AIX® and Linux®:
- The Internet. You can access IBM message explanations directly from the LookAt Website at www.ibm.com/systems/z/os/zos/bkserv/lookat/index.html
- Your z/OS TSO/E host system. You can install code on your z/OS or z/OS.e systems to access IBM message explanations using LookAt from a TSO/E command line (for example: TSO/E prompt, ISPF, or z/OS UNIX® System Services).
- Your Microsoft Windows workstation. You can install LookAt directly from the *z/OS Collection* (SK3T-4269) or the *z/OS and Software Products DVD Collection* (SK3T-4271) and use it from the resulting Windows graphical user interface (GUI). The command prompt (also known as the DOS > command line) version can still be used from the directory in which you install the Windows version of LookAt.
- Your wireless handheld device. You can use the LookAt Mobile Edition from www.ibm.com/systems/z/os/zos/bkserv/lookat/lookatm.html with a handheld device that has wireless access and an Internet browser (for example: Internet Explorer for Pocket PCs, Blazer or Eudora for Palm OS, or Opera for Linux handheld devices).

You can obtain code to install LookAt on your host system or Microsoft Windows workstation from:
- A CD-ROM in the *z/OS Collection* (SK3T-4269).
- The *z/OS and Software Products DVD Collection* (SK3T-4271).
- The LookAt Website (click **Download** and then select the platform, release, collection, and location that suit your needs). More information is available in the LOOKAT.ME files available during the download process.

Accessibility

Publications for this product are offered in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties when using PDF files, you may view the information through the z/OS Internet Library Web site or the z/OS Information Center. If you continue to experience problems, send an e-mail to mhvrcfs@us.ibm.com or write to:

IBM Corporation
Attention: MHVRCFS Reader Comments
Department H6MA, Building 707
2455 South Road
Poughkeepsie, NY 12601-5400
U.S.A.

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features in z/OS enable users to:

- Use assistive technologies such as screen readers and screen magnifier software
- Operate specific or equivalent features using only the keyboard
- Customize display attributes such as color, contrast, and font size

Using assistive technologies

Assistive technology products, such as screen readers, function with the user interfaces found in z/OS. Consult the assistive technology documentation for specific information when using such products to access z/OS interfaces.

Keyboard navigation of the user interface

Users can access z/OS user interfaces using TSO/E or ISPF. Refer to *z/OS TSO/E Primer*, *z/OS TSO/E User's Guide*, and *z/OS ISPF User's Guide Vol I* for information about accessing TSO/E and ISPF interfaces. These guides describe how to use TSO/E and ISPF, including the use of keyboard shortcuts or function keys (PF keys). Each guide includes the default settings for the PF keys and explains how to modify their functions.

z/OS information

z/OS information is accessible using screen readers with the BookServer or Library Server versions of z/OS books in the Internet library at:

http://www.ibm.com/systems/z/os/zos/bkserv/

Tivoli technical training

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

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

Support information

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

- Searching knowledge bases: You can search across a large collection of known problems and workarounds, Technotes, and other information.

- Obtaining fixes: You can locate the latest fixes that are already available for your product.
- Contacting IBM Software Support: If you still cannot solve your problem, and you need to work with someone from IBM, you can use a variety of ways to contact IBM Software Support.

For more information about these three ways of resolving problems, see Part 4, "Problem determination," on page 187.

Participating in newsgroups

User groups provide software professionals with a forum for communicating ideas, technical expertise, and experiences related to the product. They are located on the Internet and are available using standard news reader programs. These groups are primarily intended for user-to-user communication and are not a replacement for formal support.

To access a newsgroup, use the instructions appropriate for your browser.

Conventions used in this guide

This guide uses several conventions for special terms and actions and for operating system-dependent commands and paths.

In the books that discuss configuration and in the Configuration Tool, the following abbreviations are used:

Table 2. Configuration Tool abbreviations

Abbreviation	Meaning
&hilev	High-level qualifier
&rhilev	Runtime high-level qualifier (non-VSAM)
&rte	Runtime environment name; used in conjunction with &rhilev
&rvhilev	Runtime high-level qualifier (VSAM)
&shilev	Installation high-level qualifier of the INST* libraries
&thilev	SMP/E target high-level qualifier

Typeface conventions

This guide 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

- Words defined in text
- Emphasis of words (words as words)
- New terms in text (except in a definition list)

- Variables and values you must provide

Monospace

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

Operating system-dependent variables and paths

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

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

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

Part 1. Planning your SA z/OS monitoring agent installation

Chapter 1. Introduction to the SA z/OS monitoring agent

The SA z/OS monitoring agent is a member of the IBM Tivoli Monitoring Services family of mainframe monitoring products. It monitors the automation environment and the resources it contains in systems and sysplexes.

The SA z/OS monitoring agent displays the following types of automation data:
- Resources, their type and location, their status, such as compound status, desired status, and observed status, and a resource description
- Any request that is issued against a resource, such as start and stop requests
- Detailed information about Monitor Resources and their health states
- Installation-defined status items and their individual values
- The automation environment with automation agents and automation managers, including their states as well as detailed automation manager configuration information

On individual systems the monitoring agent shows:
- Automation agent information
- Automation statistics, such as messages and commands
- OMEGAMON sessions that are in use and their activity

The SA z/OS monitoring agent has a flexible, easy-to-use Java-based interface called the Tivoli Enterprise Portal, which transforms systems data into the business knowledge that you can use to run your enterprise. With the SA z/OS monitoring agent you can also set threshold levels and flags as desired to alert you when the systems reach critical points.
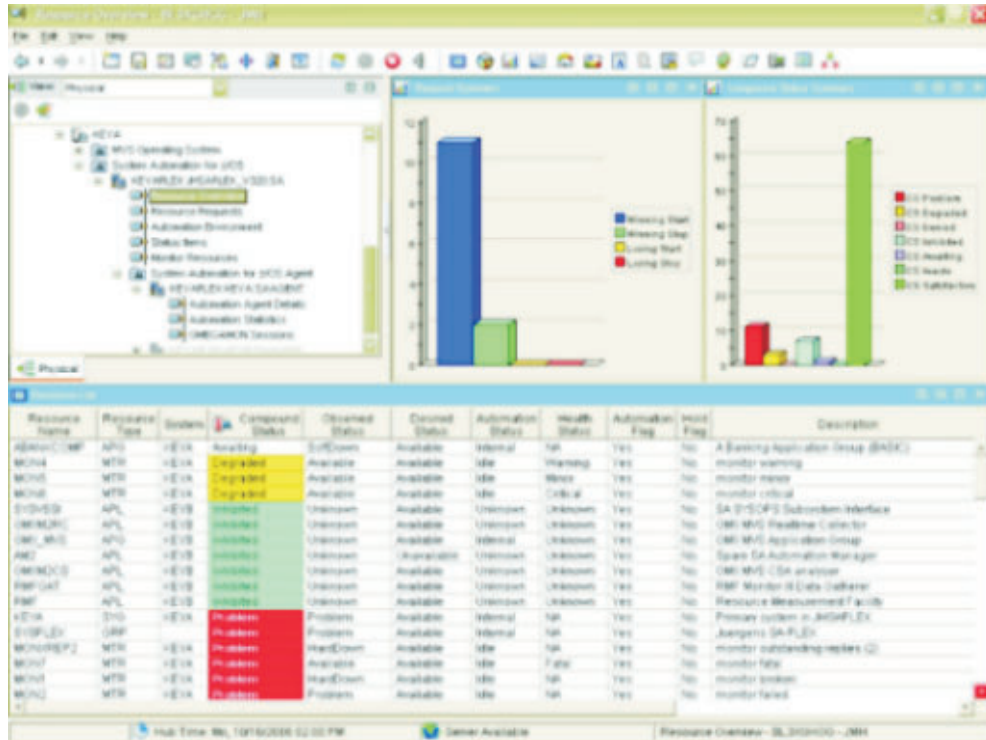
Figure 1. Tivoli Enterprise Portal sample workspace for the SA z/OS monitoring agent

Figure 1 shows the Tivoli Enterprise Portal application window for the monitoring agent. The Tivoli Enterprise Portal presents information in a single window comprising a Navigator and a workspace:

- The *Navigator* in the upper left corner of Figure 1 shows the hierarchy of your monitored enterprise, from the top level (Enterprise) down to the *nodes* that represent the systems in the enterprise, and then to the *subnodes* that represent groupings of information collected by the monitoring agents. The Navigator lights up with critical, warning, and informational alerts so you can instantly identify problems as they occur. When you click an item in the Navigator, its default workspace displays in the Tivoli Enterprise Portal window.
- *Workspaces* such as the one shown in Figure 1 can be divided into multiple *views* containing reports in the form of tables and charts, TN3270 emulator views, Web browsers, text boxes, graphic views, and event message logs.

You can use the SA z/OS monitoring agent features to:
- Monitor the automation environment and its resources from a single, integrated browser-based interface that you can customize with filters to display only the data you want to see
- Create comprehensive online reports about resource conditions
- Define your own queries, using the attributes provided by a monitoring agent, to monitor conditions and data and customize workspaces
- Create *situations*, which let you set up monitoring for particular conditions and flag the condition with an alert when detected
- Trace the causes leading up to an alert
- Create and send commands to systems in your managed enterprise with the *Take Action* feature

- Embed information about problem resolution in the product interface using *Expert Advice*, which can be edited to include knowledge and solutions specific to your environment

Components of the SA z/OS monitoring agent

The SA z/OS monitoring agent is considered a client-server-agent implementation. For information about the components of the monitoring agent, see "Designing your SA z/OS monitoring agent configuration" on page 9.

SA z/OS monitoring agent features

The following features are available with the SA z/OS monitoring agent and the Tivoli Enterprise Portal:

- **Customized workspaces for each information group:** Tivoli Enterprise Portal retrieves data from the monitoring agent and displays the results in the workspace in the form of charts and tables. You can start monitoring activity and system status immediately with the predefined workspaces and tailor your own workspaces to look at specific conditions, display critical threshold values in red, and filter incoming data according to your needs.
- **Workspace views:** Each workspace consists of one or more views. There are several types of views:
  - *Table views* display data in table format where rows represent monitored resources and columns represent data collected for each resource.
  - *Chart views* allow you to view data in graphical formats. Pie, bar, and plot charts and a gauge format are supported.
  - *Take action view* lets you enter a command or select a predefined command, and run it on any system in your managed network.
  - *Message log view* shows the status of the situations running on your managed network.
  - *Notepad view* opens a simple text editor for writing text that can be saved with the workspace.
  - *Terminal view* starts a 3270 or 5250 session for working with z/OS applications.
  - *Browser view* opens the integrated Web browser.
- **Navigator views or *navigators*** provide hierarchical views of the systems, resources, and applications you are monitoring. Navigators help you structure your enterprise information to reflect the interests and responsibilities of the user. The Tivoli Enterprise Portal comes with a default navigator called the physical navigator. The Tivoli OMEGAMON DE on z/OS product, which can be ordered separately, comes with the same default navigator, but allows you to create additional navigators for viewing enterprise information representing your business systems.
- **Linked workspaces**: If you often go from one workspace to another, you can build a link between them to speed the transition. You can also build links that originate from a table or from a bar or pie chart, and use relevant data from the source table or graph to determine the target workspace.
- **Custom queries:** Every monitoring agent comes with a set of predefined queries. These queries tell the monitoring server what monitoring data to retrieve from the agent for the chart or table view. You can create your own queries to specify exactly which attributes to retrieve, thus saving valuable resources. For example, you can build a filter into the Connections query to retrieve only records from a particular remote port. Additionally, you can write SQL queries to ODBC data

sources and display the results in any chart or table. This enables you to show monitoring data and data from other sources (such as third-party databases) in a single workspace.

- **Interaction with systems from your console:** The Take Action feature lets you enter a command or select a predefined command, and run it on any system in your managed network.
- **Monitor system conditions and send alerts**: You can use the situation editor to create situations. A situation notifies you when an event occurs on a managed system. The monitoring server sends an alert when the conditions in a situation are evaluated to be true. The alert is displayed on the portal client with visual and sound indicators.
- **Managed system lists:** You can create and maintain named lists of managed systems that can be applied to:
  - Situation distribution lists
  - Policies correlated by business application group
  - Queries
  - Customer Navigator-managed system assignments
- **User administration:** The Tivoli Enterprise Portal provides a user administration feature for adding new user IDs, complete with selectable permissions for the major features and specific managed systems.

IBM Tivoli Monitoring products

You can use the SA z/OS monitoring agent with any of the IBM Tivoli Monitoring products. These products include solutions for z/OS-based applications, database products, and applications such as CICS®, storage, and networks. Some of the IBM Tivoli Monitoring products provide features that are not included with the SA z/OS monitoring agent, such as historical data.

You can see the complete list of IBM Tivoli Monitoring products at the following Website:

http://www.ibm.com/software/tivoli/solutions/availability/

Standards supported

IBM Tivoli Monitoring products provide a number of integration facilities and adhere to a range of industry standards to make integration with other applications easier for you. These products use industry-standard languages and protocols to facilitate integration with third-party components and tools. The product also uses strategic IBM and Tivoli tools and platforms. These standards and platforms include the following:

- A Web-based user interface implemented with industry-standard Web content languages, such as Java™, XML, and HTML
- Simple Network Management Protocol
- Web Services and Web Management Interface (WMI) standard
- TCP/IP-based communication between components and systems
- Support for the DB2® product, an industry-standard relational database
- Use of Structured Query Language (SQL '92, ISO/IEC 9075:1992), the standard interface for relational database access
- Use of standard shell scripts and SMP/E to assist in installation

Interoperability with other products

Interoperability is the capability of an application to integrate with other IBM and non-IBM applications that are used in the same customer environment.

IBM Tivoli Monitoring products are compatible with each other and can coexist in a single IBM Tivoli Monitoring environment (that is, with a common Tivoli Enterprise Monitoring Server). These products, including the SA z/OS monitoring agent, also interoperate with Tivoli Enterprise Monitoring Agents running on distributed systems and communicating through the same monitoring server.

For more information on possible deployments of the monitoring products, see the following publications:

- *Installation and Setup Guide*
- *Configuring IBM Tivoli Enterprise Monitoring Server on z/OS*
- *Deployment Guide Series: IBM Tivoli Monitoring 6.2*

Interoperability with other products

Chapter 2. Planning your SA z/OS monitoring agent configuration

In this chapter, you will learn about the components of the SA z/OS monitoring agent, and gather the information you need to make decisions about your configuration.

Before you begin the tasks of installing and configuring the monitoring agent, be sure to complete these prerequisite steps covered in this chapter:

1. Read the *Program Directory* and complete all the installation requirements listed there.

2. Read "Designing your SA z/OS monitoring agent configuration" to determine how you want your monitoring agent configuration to look. For example, you must decide:
   - Where you want to deploy Tivoli Enterprise Monitoring Servers and monitoring agent monitoring agents
   - What kind and how many runtime environments you need for your configuration

3. To get ready for configuration, make all the decisions called out in decision points in "Designing your SA z/OS monitoring agent configuration" and fill out the worksheets in "Worksheets for SA z/OS monitoring agent configuration" on page 21.

4. Once you've designed your configuration and filled out the work sheets, see "A road map for installation and configuration of the SA z/OS monitoring agent" on page 38 to determine your next step in installation and configuration.

Designing your SA z/OS monitoring agent configuration

The SA z/OS monitoring agent uses the Tivoli Monitoring Services infrastructure (also referred to as IBM Tivoli Monitoring, or Tivoli Management Services). The Tivoli Monitoring Services infrastructure provides security, data transfer and storage, notification mechanisms, user interface presentation, and communication services for products in the IBM Tivoli Monitoring and OMEGAMON XE suites in an agent-server-client architecture (see Figure 2 on page 10.)
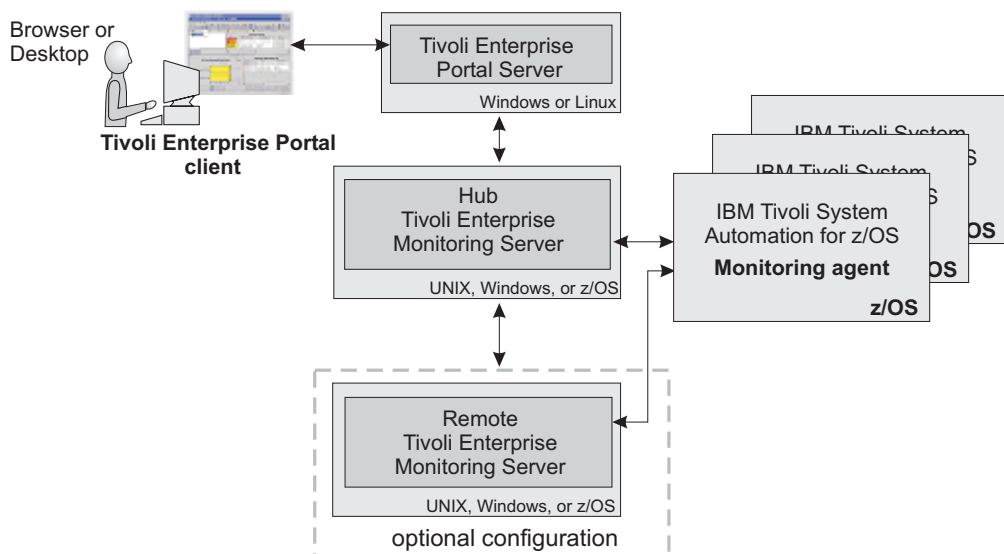
Figure 2. Components of the SA z/OS monitoring agent

The components include:
- "Tivoli Enterprise Monitoring Servers: hub and remote"
- "The SA z/OS monitoring agent" on page 12
- "Tivoli Enterprise Portal client and Tivoli Enterprise Portal Server" on page 13

Some components, such as the Tivoli Enterprise Portal, run only on distributed operating systems (Windows, Linux, or UNIX). The Tivoli Enterprise Monitoring Server can run on either distributed or mainframe systems. The SA z/OS monitoring agent runs only on mainframe systems.

The required versions of the Tivoli Monitoring Services infrastructure components are not distributed with the SA z/OS monitoring agent software. See "Understanding product packaging" on page 40 for more details.

As you read through these sections, fill out the following worksheets to get ready for the configuration process:
- "Worksheet: Your overall configuration" on page 22
- "Worksheets: Information to gather when you put your hub monitoring server on a distributed system" on page 31
- "Worksheets: Information to gather when you put your hub monitoring server on a z/OS system" on page 23
- "Worksheet: Information for configuring your runtime environment" on page 36

Tivoli Enterprise Monitoring Servers: hub and remote

All requests and data for IBM Tivoli Monitoring products, such as the SA z/OS monitoring agent, flow through a hub Tivoli Enterprise Monitoring Server (monitoring server). The monitoring server component does the following:
- Retrieves data from the monitoring agents and delivers data to the portal server
- Sends alerts to the portal server when conditions specified in situations are met
- Receives commands from the portal client and passes them to the appropriate monitoring agents

You can install this component on z/OS, Windows, and some UNIX operating systems. See the *IBM Tivoli Monitoring: Installation and Setup Guide* for a complete list of supported platforms.

Decision point:
Should you install a monitoring server on z/OS, Windows, or UNIX systems?

Many organizations prefer the reliability and availability characteristics of the z/OS platform for the monitoring server. For the SA z/OS monitoring agent, z/OS might be an attractive place for the monitoring server because it is close to the monitoring agent on z/OS, which can shorten the communications path.

On the other hand, if you have other IBM Tivoli Monitoring product monitoring agents on your Windows or UNIX systems, you might prefer Windows or UNIX platforms. If you install the hub monitoring server on Windows, you have the option of deploying the portal server on the same system, which can shorten the communications path.

This decision influences the way you configure the SA z/OS monitoring agent, depending on where you choose to install the monitoring server:
- On a distributed system, fill out "Worksheets: Information to gather when you put your hub monitoring server on a distributed system" on page 31.
- On z/OS, fill out "Worksheets: Information to gather when you put your hub monitoring server on a z/OS system" on page 23.

The two basic types of monitoring servers are *hub* and *remote*:
- The *hub* monitoring server is the focal point for managing your environment. You can configure only one hub monitoring server. It communicates with the portal server, with monitoring agents, and optionally with monitoring servers running remotely.
- You can optionally configure a *remote* monitoring server to distribute the workload of the hub monitoring server, but it is not required.

  Each remote monitoring server must be installed on its own system or workstation. A remote monitoring server communicates with the hub monitoring server and with monitoring agents running on the same or different systems. Note that a remote monitoring server is remote only with respect to the hub monitoring server, not necessarily with respect to the monitoring agents. A monitoring agent can be installed on the same system as a remote monitoring server. The monitoring server is then local to the monitoring agent, but it is still a remote monitoring server. See also "The SA z/OS monitoring agent" on page 12.

  The configuration scenarios in this guide assume that the monitoring server being configured with the SA z/OS monitoring agent is a *hub* monitoring server. For instructions on configuring remote monitoring servers, see the *IBM Tivoli Monitoring: Configuring IBM Tivoli Enterprise Monitoring Server on z/OS* and *IBM Tivoli Monitoring: Installation and Setup Guide*.

> **Decision point:**
> **Should you configure a remote monitoring server or servers for your environment?**
>
> A remote monitoring server is designed to offload work from the hub. Whether or not your hub gets overloaded enough to slow down hub processing of situations and other data depends on the complexity of your environment. The following factors tend to boost strain on the hub and increase the likelihood that you might want a remote server to help out the hub:
>
> – Monitoring many z/OS images. The more monitoring agents you have installed on z/OS systems, the more work for the hub.
> – Monitoring many situations. The SA z/OS monitoring agent does not come with a great many situations to consume hub cycles, so unless you have other IBM Tivoli Monitoring products with lots of situations, this is probably not a factor that will push you into needing remote monitoring servers.
>
> Configuring a remote monitoring server can also give you scalability potential and failover protection, which might be especially important when you add the SA z/OS monitoring agent to an environment with multiple IBM Tivoli Monitoring products and agents. For more information on these issues, see the *IBM Redbooks: Deployment Guide Series: IBM Tivoli Monitoring 6.2* at the following Website:
>
> http://www.redbooks.ibm.com/Redbooks.nsf/RedbookAbstracts
> /sg247188.html?Open
>
> Look for the following topics:
> – Small/medium installation
> – Scalability

The SA z/OS monitoring agent

The SA z/OS monitoring agent, like all IBM Tivoli Monitoring monitoring agents, monitors and collects data from a managed system. Here the scope of data is an SA z/OS sysplex that is monitored from one single system in that sysplex. Monitoring agents are installed on the systems or subsystems you want to monitor, pass data to monitoring servers (remote or hub), and receive instructions from the monitoring servers. A monitoring agent is also able to issue commands to the managed system.

The SA z/OS monitoring agent is installed on at least one z/OS system in your SA z/OS sysplex, but the agent can also collect automation data for the entire sysplex. It is recommended that you install the monitoring agent in a separate address space.

Note: You only need configure multiple SA z/OS monitoring agents in order to define backup monitoring agents in a SA z/OS sysplex should the primary monitoring agent fail.

Tivoli Enterprise Portal client and Tivoli Enterprise Portal Server

The *Tivoli Enterprise Portal client* (portal client) is the user interface for SA z/OS monitoring agent. The portal client is a thin Java application that communicates with the Tivoli Enterprise Portal Server to send requests and retrieve data.

Tip

The portal client requires IBM Java Runtime Environment (JRE) 1.4.2. You do not need to install this JRE; it is installed automatically when you install a Tivoli Monitoring Services component that requires it.

You can access all portal client function through the desktop client or an Internet Explorer browser connected to an embedded Web server in the Tivoli Enterprise Portal Server. You should, however, have access to both the desktop and the browser client.

* The desktop portal client allows access to portal client function and is required for configuration. In the operations environment, you must install the portal client on at least one desktop. Then individual SA z/OS monitoring agent users can either install the portal client on their desktops, or use the browser portal client to access the portal client function. The desktop client can run on Windows or Linux (Red Hat or SUSE Intel® Linux only).
* The browser portal client allows you to leverage an existing deployment of Internet Explorer without installing the client component on every user's workstation. The browser client can run on Windows only, with Internet Explorer 6 as the only supported browser.

See the *IBM Tivoli Monitoring: Installation and Setup Guide* for complete information about supported operating system version support.

The *Tivoli Enterprise Portal Server* (portal server) is a Java application server that enables retrieval, manipulation, and analysis of data from agents. The portal server holds all the information needed to format the workspaces viewed in the portal client.

The portal server communicates with the portal clients (default port is 1920) and with the hub monitoring server (default port is 1918). You can provide fault tolerance by connecting more than one portal server to the same hub monitoring server.

You can install the portal server on a Windows, Linux for Intel, 31-bit Linux for z/OS, or AIX system.

> **Decision point:**
> **How do you choose among Windows, Linux, and AIX for installation of the portal server, and between Windows and Linux for installation of the portal desktop client?**
>
> Base this decision on conditions and preferences at your site, such as:
> - The operating systems already in use in the existing environment
> - Familiarity and comfort level with the Windows and Linux operating systems
> - Whether you want to bring additional operating systems into your site's current configuration
>
> Note that you can run with mixed portal server and desktop client components. For example, you can have a desktop client on Linux and a portal server on AIX, or a desktop client on Windows and a portal server on Linux.

The portal server requires that you have already installed DB2 Universal Database™ (DB2 UDB) Workgroup Server Edition. The DB2 UDB Workgroup Server Edition is provided as part of the Tivoli Monitoring Services infrastructure that is a prerequisite for installing the SA z/OS monitoring agent. If you already have DB2 UDB version 8 or higher on the workstation where you will be installing the portal server, you do not need to install it again for the monitoring agent.

See the *IBM Tivoli Monitoring: Installation and Setup Guide* and *IBM Tivoli Monitoring: Administrator's Guide* for complete information about planning for Tivoli monitoring platform components on Windows.

Understanding runtime environments

After you determine which z/OS images need to be monitored and decide whether to deploy the hub monitoring server and monitoring agent in the same address space, in separate address spaces, or on different systems, your next choice is deciding what types of runtime environments to use to configure the components you plan to deploy on your z/OS images.

A runtime environment is a logical grouping of runtime libraries that are referenced by started tasks as they run on a z/OS image. When you run the Configuration Tool to configure the SA z/OS monitoring agent, you start this process by defining a runtime environment of a certain type that determines the number and types of runtime libraries required.

> **Tip**
> You must define a runtime environment on each z/OS image that the SA z/OS monitoring agent may be started on.
>
> **Note:** This is for high availability only. Otherwise it is sufficient to configure one RTE for the whole SA z/OS sysplex. However monitoring is lost if that system goes down unless another system can resume monitoring for the SA z/OS sysplex.

Table 3 summarizes the types of libraries created during installation and configuration of the SA z/OS monitoring agent.

Table 3. Types of libraries

Type of Library	Description
Runtime libraries	General term for libraries referenced by started task procedures. Includes SMP/E target, base, and LPAR-specific libraries.
SMP/E target libraries Abbreviated *&thilev*.	SMP/E maintained target libraries.
Base libraries Abbreviated *&rhilev* or *&rhilev.&rte*.	Runtime libraries that the configuration process does not alter and that are shareable between systems. These libraries physically exist in a full or base runtime environment, or as SMP/E target libraries (if a runtime environment shares with SMP/E).
LPAR-specific libraries Abbreviated *&rhilev.&rte*.	Runtime libraries that are built during configuration to run on a specific logical partition (LPAR). These libraries contain the unique elements required for a particular LPAR and cannot be shared among z/OS images.

Table 4 explains the types of runtime environments that you can create during product configuration.

Table 4. Types of runtime environments

Type of runtime environment	Description
Full (self-contained) runtime environment	Configuration containing a full set of dedicated libraries consisting of both LPAR-specific libraries and base libraries eligible for sharing with other runtime environments. See "Example 1. Full (self-contained) runtime environment" on page 16.
Base runtime environment	Configuration containing only shareable runtime libraries (base libraries) that are a subset of the libraries needed to run OMEGAMON and other monitoring products that are based on the Tivoli Monitoring Services infrastructure. Therefore, they must be shared by another runtime environment. See "Example 2. Base runtime environment" on page 17.
Sharing-with-base runtime environment	Configuration containing LPAR-specific libraries and referencing the base libraries configured in a base runtime environment. See "Example 3. Sharing-with-base runtime environment" on page 18.
Sharing-with-full runtime environment	Configuration containing LPAR-specific libraries and referencing the base libraries configured in a full runtime environment. See "Example 4. Sharing-with-full runtime environment" on page 19.
Sharing-with-SMP/E runtime environment	Configuration containing LPAR-specific libraries and referencing the libraries managed by SMP/E. See "Example 5. Sharing-with-SMP/E runtime environment" on page 20.

The distinction among library types allows you to optimize your product environment. For example, by allocating common base libraries to a single runtime environment that can be shared by other runtime environments, you can

substantially reduce the amount of disk space required, as well as simplify the application of Tivoli Monitoring Services product maintenance across remote z/OS images.

Quick start suggestion for a runtime environment configuration

There are many variables and lots of information to consider when deciding on a runtime environment configuration for your installation. To get you started quickly, here are a couple of suggestions:

- In most cases, when you are monitoring multiple z/OS images, you should get good results with a sharing-with-base or sharing-with-SMP/E type of runtime environment.
- If you want to test the SA z/OS monitoring agent on an isolated test system, use a full, self-contained type of runtime environment.

Possible configurations using runtime environments

The following five examples show different types of runtime environment configurations. The way you choose to set up your runtime environments depends on your site requirements and maintenance procedures.

Tip

The data set name (DSN) is composed of the high-level qualifier (*&hilev*), followed by the mid-level qualifier (&rte), followed by the low-level qualifier. The field settings and library names shown are for illustrative purposes only.

Example 1. Full (self-contained) runtime environment: The full runtime environment contains all libraries required by a particular IBM product and is the easiest runtime environment to create. This type of runtime environment can be defined in any situation but is most suitable if at least one of the following statements is true:

- Your installation comprises only a single z/OS image.
- You want each z/OS image to be independent.
- You are creating a runtime environment for a specific combination of Tivoli Monitoring Services products that does not exist in any other runtime environment.

The following example represents a full runtime environment called RTE1 that is completely self-contained. All base libraries and LPAR-specific libraries are allocated within RTE1.

```
RTE Name: RTE1
Type: FULL
Hilev: SYS.SA
Midlev: RTE1
Shares with: (none)
```

LPAR-specific library DD DSNAME resolution:

```
//RKANPAR DD DSN=SYS.SA.RTE1.RKANPAR
```

Base library DD DSNAME resolution:

```
//RKANMODL DD DSN=SYS.SA.RTE1.RKANMODL
```

This type of runtime environment is illustrated in Figure 3 on page 17.
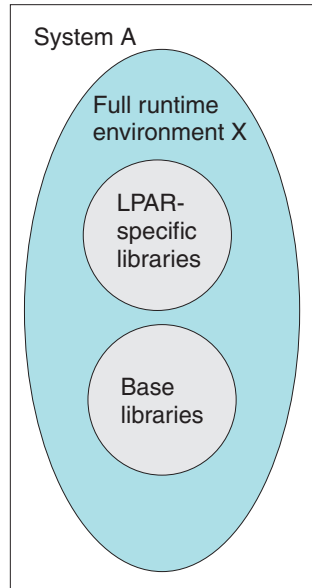
Figure 3. Full runtime environment on a single system

Figure 4 shows the way a full runtime environment can be expanded to more than one z/OS image. Each runtime environment is self-contained; the three runtime environments X, Y, and Z on systems A, B, and C do not share any libraries.
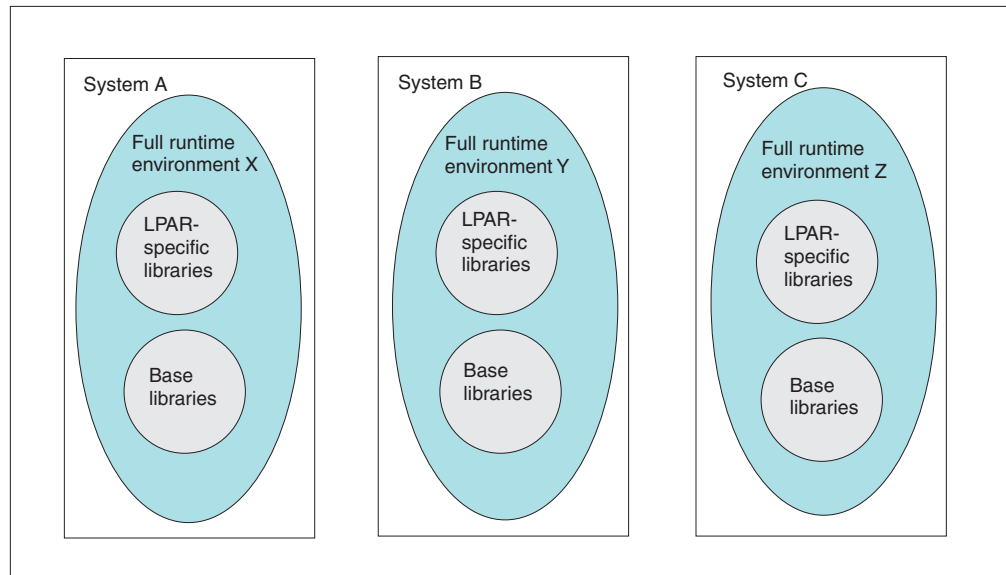
Figure 4. Full runtime environments on several systems

Example 2. Base runtime environment: The base runtime environment allocates shareable base libraries only. A base runtime environment must be used in conjunction with a sharing-with-base runtime environment (see "Example 3. Sharing-with-base runtime environment" on page 18) to provide the complete set of libraries required to run the installed Tivoli Monitoring Services products. The base runtime environment and the sharing-with-base runtime environment must be defined for the same combination of Tivoli Monitoring Services products.

Understanding runtime environments

A base runtime environment is typically used when storage devices are shared or when Tivoli Monitoring Services product maintenance synchronization across systems is desired. Sharing base libraries avoids unnecessary duplication, saves disk space, and simplifies the application of Tivoli Monitoring Services product maintenance to a common point.

The following example represents a base runtime environment called RTE2.

```
RTE Name: RTE2
Type: BASE
Hilev: SYS.SA
Midlev: (none)
Shares with: (none)
```

LPAR-specific library DD DSNAME resolution:

```
*There are no LPAR-specific libraries in a BASE RTE.
```

Base library DD DSNAME resolution:

```
//RKANMODL DD DSN=SYS.SA.RKANMODL
```

This type of runtime environment is illustrated in Figure 5.
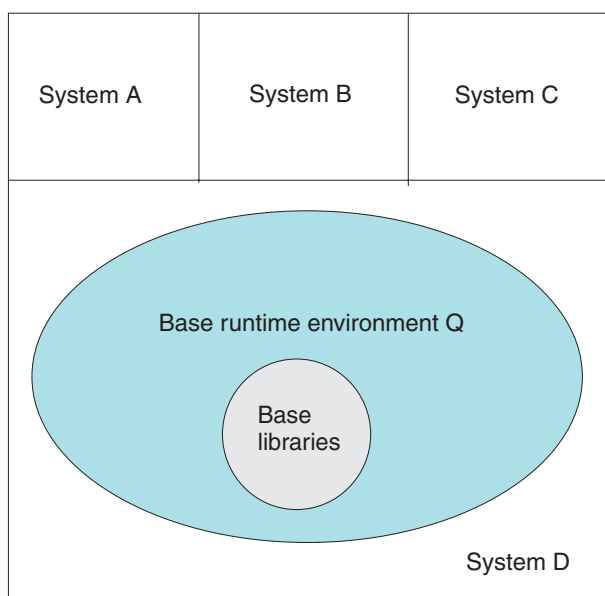
Figure 5. Base runtime environment

Example 3. Sharing-with-base runtime environment: The sharing-with-base configuration is a good choice for environments where storage devices are shared. Using the base runtime environment for common data sets, the sharing-with-base runtime environment contains only LPAR-specific libraries. The base runtime environment cannot contain the LPAR-specific libraries required to run the installed Tivoli Monitoring Services products. The base runtime environment and the sharing-with-base runtime environment must be defined for the same combination of Tivoli Monitoring Services products.

The Configuration Tool resolves product configuration elements to point at the LPAR-specific libraries and the base runtime environment libraries as necessary.

The following example represents a sharing-with-base runtime environment called RTE3, which obtains its base library information from the base runtime environment (RTE2).

```
RTE Name: RTE3
Type: SHARING
Hilev: SYS.SA
Midlev: RTE3
Shares with: BASE RTE2
```

LPAR-specific library DD DSNAME resolution:

```
//RKANPAR DD DSN=SYS.SA.RTE3.RKANPAR
```

Base library DD DSNAME resolution:

```
//RKANMODL DD DSN=SYS.SA.RKANMODL
```

This type of runtime environment is illustrated in Figure 6.
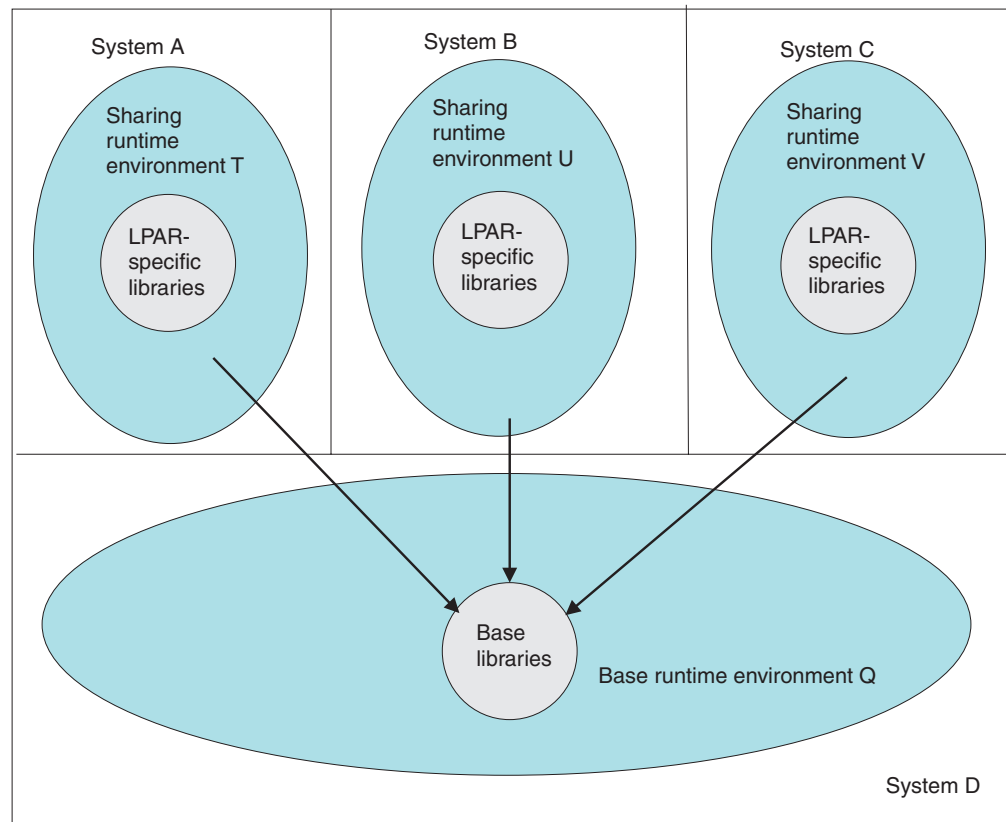
Figure 6. Sharing-with-base runtime environment

Example 4. Sharing-with-full runtime environment: The sharing-with-full runtime environment allocates LPAR-specific libraries only, and in this example, obtains its base library information from a full runtime environment that contains the same combination of Tivoli Monitoring Services products.

This configuration can also be used for environments where storage devices are shared, although the base/sharing pair is the preferred approach.

The following example represents a sharing-with-full runtime environment called RTE4, which obtains its base library information from the full runtime environment (RTE1).

```
RTE Name: RTE4
Type: SHARING
Hilev: SYS.SA
Midlev: RTE4
Shares with: FULL RTE1
```

LPAR-specific library DD DSNAME resolution:

```
//RKANPAR DD DSN=SYS.SA.RTE4.RKANPAR
```

Base library DD DSNAME resolution:

```
//RKANMODL DD DSN=SYS.SA.RTE1.RKANMODL
```

This type of runtime environment is illustrated in Figure 7.
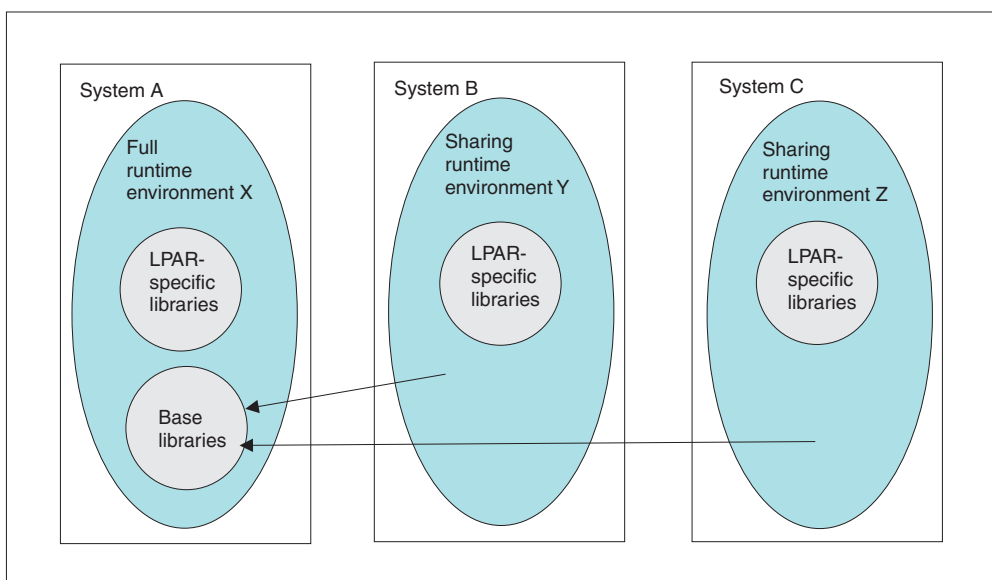
Figure 7. Sharing-with-full runtime environment

Example 5. Sharing-with-SMP/E runtime environment: The sharing-with-SMP/E runtime environment allocates LPAR-specific libraries only and obtains its base library information from target libraries managed by SMP/E. Note that the target SMP/E libraries must be copies (cloned) rather than the system libraries. See the appendix on making a copy of your system software (cloning) in *z/OS and z/OS.e Planning for Installation*.

Use the sharing-with-SMP/E configuration if at least one of the following statements is true:

• Space is limited on storage devices. This configuration method does not allocate base libraries in the runtime environment, thereby reducing storage requirements.
• You want to activate SMP/E applied Tivoli Monitoring Services product maintenance immediately.

The following example represents a sharing-with-SMP/E runtime environment called RTE5, which obtains its base library information from SMP/E target libraries.

```
RTE Name: RTE5
Type: SHARING
Hilev: SYS.SA
Midlev: RTE5
Shares with: SMP/E Target Libraries
Hilev (SMP): INSTALL.SMPE
```

LPAR-specific library DD DSNAME resolution:

```
//RKANPAR DD DSN=SYS.SA.RTE5.RKANPAR
```

Base library DD DSNAME resolution:

```
//RKANMODL DD DSN=SYS.SA.SMPE.TKANMODL
```

The sharing-with-SMP/E type of runtime environment is illustrated in Figure 8.
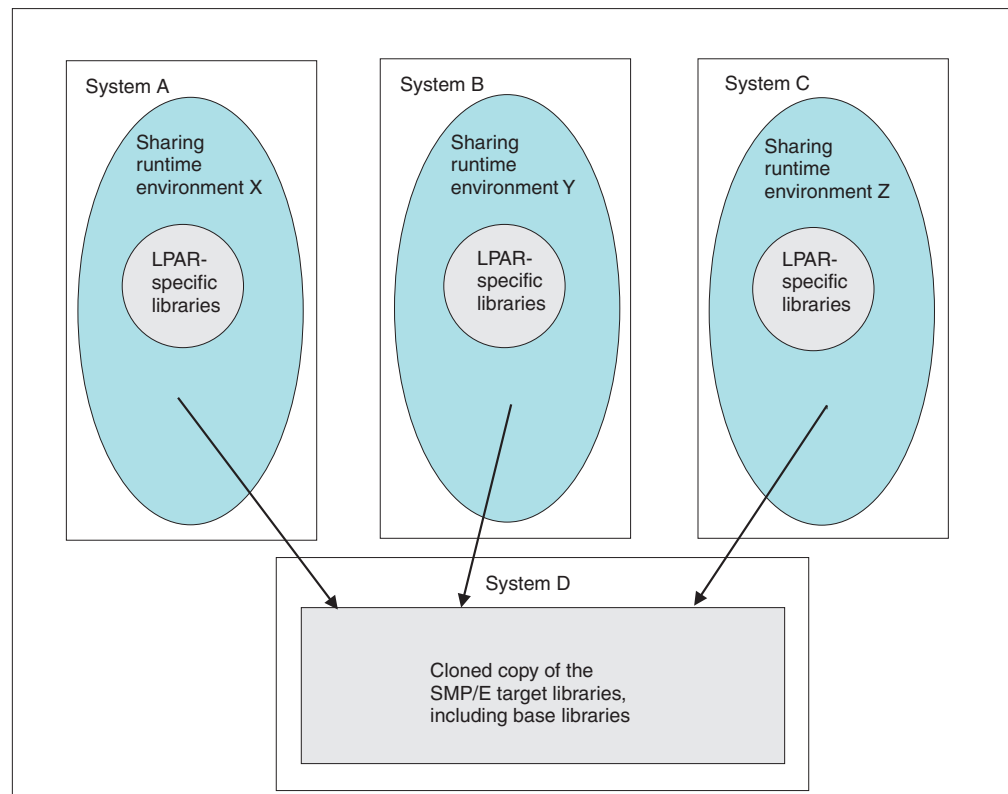
Figure 8. Sharing-with-SMP/E runtime environment

Worksheets for SA z/OS monitoring agent configuration

- "Worksheet: Your overall configuration" on page 22
- "Worksheets: Information to gather when you put your hub monitoring server on a distributed system" on page 31
- "Worksheets: Information to gather when you put your hub monitoring server on a z/OS system" on page 23
- "Worksheet: Information for configuring your runtime environment" on page 36

Worksheets for SA z/OS monitoring agent configuration

Worksheet: Your overall configuration

As you read the following sections, you can start to fill in your own overall SA z/OS monitoring agent configuration, using the worksheet below. Fill in the system name where you plan to install each component, using "Designing your SA z/OS monitoring agent configuration" on page 9 as a guide:

Table 5. Worksheet for designing your overall configuration

Components of the SA z/OS monitoring agent	Values

SA z/OS monitoring agents (z/OS)
 	
See "The SA z/OS monitoring agent" on page 12
	Number of images: _____
	
	Image 1:
	   • Host name: _____
	   • IP address: _____
	
	Image 2:
	   • Host name: _____
	   • IP address: _____
	
	Image 3:
	   • Host name: _____
	   • IP address: _____
	
	Image 4:
	   • Host name: _____
	   • IP address: _____
	
	Image 5:
	   • Host name: _____
	   • IP address: _____

Hub Tivoli Enterprise Monitoring Server
 	
See "Tivoli Enterprise Monitoring Servers: hub and remote" on page 10
	Hub Tivoli Enterprise Monitoring Server is located on (check one):
	__ Windows server
	__ Linux server
	__ UNIX server
	__ z/OS server:
	  – Host name: _____
	  – IP address: _____

Remote Tivoli Enterprise Monitoring Server?
 	
See "Tivoli Enterprise Monitoring Servers: hub and remote" on page 10
 	
Optional
	__ Yes
	__ No
	If yes, indicate where you plan to put remote Tivoli Enterprise Server or Servers:
	__ Windows server
	__ Linux server
	__ UNIX server
	__ z/OS server:
	  – Host name: _____
	  – IP address: _____

Table 5. Worksheet for designing your overall configuration (continued)

Components of the SA z/OS monitoring agent	Values

Tivoli Enterprise Portal Server
 	
See "Tivoli Enterprise Portal client and Tivoli Enterprise Portal Server" on page 13
	Tivoli Enterprise Portal Server is located on (check one):
	   — Windows
	   — Linux
	   — AIX
	• Host name: _____
	• IP address: _____

Tivoli Enterprise Portal desktop client
 	
See "Tivoli Enterprise Portal client and Tivoli Enterprise Portal Server" on page 13
	Desktop client is located on (check one):
	   — Windows
	   — Linux

Tivoli Enterprise Portal browser client See "Tivoli Enterprise Portal client and Tivoli Enterprise Portal Server" on page 13	Windows

For complete information about operating system version support for each Tivoli Monitoring Services component, see the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Worksheets: Information to gather when you put your hub monitoring server on a z/OS system

If you are putting your hub monitoring server on a z/OS system, fill out the tables below:

- "Configuration worksheet if the monitoring server is on a z/OS system"
- "Configuration worksheet for communication protocols if the monitoring server is on a z/OS system" on page 25

For information about general requirements for using the TCP/IP communication protocols, see "Requirements for TCP/IP communication protocols" on page 39.

Configuration worksheet if the monitoring server is on a z/OS system

Note that all fields are required, unless otherwise indicated.

Table 6. Configuration worksheet if the monitoring server is on a z/OS system

Value	Description	Value for your configuration
Runtime environment settings		
Host name	Host name of the z/OS system where the hub monitoring server is installed. To obtain the host name, enter TSO HOMETEST at the command line of the z/OS system where the hub monitoring server is installed. If the z/OS domain name resolver configuration specifies a search path that includes the target domain suffix, specify only the first qualifier of the host name. (Example: sys is the first qualifier of the fully qualified host name sys.ibm.com.) Otherwise, specify the fully qualified host name.	

Worksheets for SA z/OS monitoring agent configuration

Table 6. Configuration worksheet if the monitoring server is on a z/OS system (continued)

Value	Description	Value for your configuration
Port number	Address of the IP port for the z/OS system where the monitoring server is installed. **Note:** The same TCP/IP port number must be used for every monitoring server in the enterprise. Also, make sure that the monitoring server well-known port is not on the TCP/IP reserved port list.	
LU6.2 logmode settings: You must associate an SNA logmode with each monitoring server on z/OS. You can either use an existing logmode or create a new one.		
LU6.2 logmode name	Name of the LU6.2 logmode defined for use by the monitoring server. The default value is **CANCTDCS**.	
Logmode table name	Name of the logmode table that contains the LU6.2 logmode. The default name is **KDSMTAB1**.	
VTAMLIB load library	Name of the system library used to contain VTAM® logmode tables. This is usually SYS1.VTAMLIB. You can specify any load library if you do not want to update you VTAMLIB directly.	
VTAM macro library	Name of the system library that contains the VTAM macros. The default is SYS1.SISTMAC.	
Configuration value settings		
Tivoli Enterprise Monitoring Server started task name	Define a name for the started task (procedure name) for the monitoring server. Follow the naming conventions used at your installation, making sure that the value has a maximum of eight characters. Check the IEFSSN*xx* member of SYS1.PARMLIB to make sure that the name you are picking has not been used before.	
Is this a hub or remote Tivoli Enterprise Monitoring Server?	Indicate whether this is a hub or remote monitoring server.	
Do you want to use z/OS Integrated Cryptographic Service Facility (ICSF) on the z/OS hub system?	Ask your security team whether ICSF is installed and configured on the z/OS system where the hub monitoring server is installed. If so, answer Y. The portal server assumes that the monitoring server is using ICSF encryption. If you set the ICSF value to N, the monitoring server uses an alternative, less secure encryption scheme. In that case, you must use a workaround to ensure communication between the monitoring server on z/OS and the portal server. See "Specifying configuration values" on page 67 for instructions.	__ Yes __ No
ICSF load library	If ICSF is installed and configured on the z/OS system, specify the load library that contains the CSNB* modules used for password encryption.	

Table 6. Configuration worksheet if the monitoring server is on a z/OS system (continued)

Value	Description	Value for your configuration
Encryption key	You are prompted for a 32-byte ICSF encryption key. You can use the default key. Be sure to document the value you use for the key, because you must use the same key during the installation of any components that communicate with this monitoring server.	__ Use default key: _____ __ Define your own key: _____
Enable Web Services SOAP Server	The Web Services SOAP Server must be enabled for a hub monitoring server, even though the SA z/OS monitoring agent does not use the SOAP Server. You must accept the default value of Y for the **Enable Web Services SOAP Server** field if you are configuring a hub monitoring server.	
Language locale	Specify 1 for United States English. This is the only language that SA z/OS supports.	
Do you want to forward Take Action commands to NetView for z/OS	You can enable forwarding of z/OS console commands issued from the Tivoli Enterprise Portal to NetView for user authorization and command execution. See "Setting up NetView authentication of Take Action commands" on page 114 for instructions.	
VTAM network ID	A VTAM network ID is required for any monitoring server on z/OS. You can locate this value on the NETID parameter in the VTAMLST startup member ATCSTR*nn*.	

Configuration worksheet for communication protocols if the monitoring server is on a z/OS system

Fill out the following communication protocols worksheet for your hub monitoring server on z/OS as well as for each remote monitoring server on z/OS. For information about general requirements for using the TCP/IP communication protocols, see "Requirements for TCP/IP communication protocols" on page 39.

Worksheets for SA z/OS monitoring agent configuration

Table 7. Configuration worksheet for communication protocols if the monitoring server is on a z/OS system

Value	Description	Value for your configuration

Communication protocols for the monitoring server on z/OS:
 	
You specify the communication protocols for the monitoring server in "Specifying communication protocols" on page 69.
	You can choose from all the protocols shown in the list below. You must specify SNA.PIPE as one of the protocols for a Tivoli Enterprise Monitoring Server on z/OS. However, it need not be Protocol 1 (the highest-priority protocol).
	
	For a hub monitoring server on z/OS, you must specify a TCP/IP protocol as one of your protocols, for use by the Web Services SOAP Server, which must be enabled.
	
	Choose from the following protocols:
	IP.PIPE
	    Uses the TCP/IP protocol for underlying communications.
	IP.UDP
	    Also a TCP/IP protocol. Uses the User Datagram Protocol (UDP).
	IP6.PIPE
	    IP.PIPE protocol with IPV6 installed and operational. This protocol is available only for a monitoring server on a z/OS system at release level V1R7 or higher with IPV6 installed and operational.
	IP6.UDP
	    IP.UDP protocol with IPV6 installed and operational. This protocol is available only for a monitoring server on a z/OS system at release level V1R7 or higher with IPV6 installed and operational.
	IP.SPIPE
	    Secure IP.PIPE protocol. This protocol is available only for a monitoring server on a z/OS system at release level V1R7 or higher.
	IP6.SPIPE
	    Secure IP.PIPE for IPV6. This protocol is available only for a monitoring server on a z/OS system at release level V1R7 or higher with IPV6 installed and operational.
	SNA.PIPE
	    Uses the SNA Advanced Program-To-Program Communications (APPC). Because some IBM Tivoli Monitoring products require SNA, it must be one of the protocols for a Tivoli Enterprise Monitoring Server on z/OS. However, it need not be Protocol 1 (the highest-priority protocol).
		• Protocol 1: _____
		
		Highest-priority communication protocol. IP.PIPE, IP.SPIPE, IP6.PIPE, or IP6.SPIPE is generally the best choice for Protocol 1 in firewall environments. These protocols enable the monitoring server on z/OS to communicate with other components on other systems, even if all components are running behind firewalls.
		
		• Protocol 2: _____
		• Protocol 3: _____
		• Protocol 4: _____
		• Protocol 5: _____
		• Protocol 6: _____
		• Protocol 7: _____

IP.* and IP6.* settings		
Host name	Host name of the z/OS system where the Tivoli Enterprise Monitoring Server is installed. See "Configuration worksheet if the monitoring server is on a z/OS system" on page 23.	

Table 7. Configuration worksheet for communication protocols if the monitoring server is on a z/OS system (continued)

Value	Description	Value for your configuration
Address	IP address of the z/OS system where the Tivoli Enterprise Monitoring Server is installed. To obtain the IP address, enter TSO HOMETEST at the command line of the z/OS system where the monitoring agent is installed.	
Started task	Started task name of the TCP/IP server. You can specify * to allow the IP stack to dynamically find the TCP/IP image. * is the suggested value for the started task.	
Network interface list	A list of network interfaces for the monitoring agent to use. This parameter is required for sites that are running more than one TCP/IP interface or network adapter on the same z/OS image. Setting this parameter allows you to direct the monitoring agent to connect to a specific TCP/IP local interface. Specify each network adapter by the host name or IP address to be used for input and output. Use a blank space to separate the entries. If your site supports DNS, you can enter IP addresses or short host names. If your site does not support DNS, you must enter fully qualified host names. If you specify an interface address or a list of interface addresses, the Configuration Tool generates the KDEB_INTERFACELIST parameter in the KDSENV member of the *&rhilev.&rtename*.RKANPARU library.	
HTTP server port number	Accept the default value of 1920. This field is required for the SOAP Server, which must be enabled for a hub monitoring server on z/OS, even though the SA z/OS monitoring agent does not use the SOAP Server.	
Access TEMS list via SOAP Server?	Accept the default value of Y. The Web Services SOAP Server must be enabled for a hub monitoring server on z/OS, even though the SA z/OS monitoring agent does not use the SOAP Server.	
Address translation	By default, Ephemeral Pipe Support (EPS) is enabled automatically to allow IP.PIPE connections to cross a (network address) translating firewall. This feature obviates the need for a broker partition file (KDC_PARTITIONFILE=KDCPART). If you specifically want to disable EPS, specify Y for **Address translation**.	
Partition name	If you specified Y for **Address translation**, specify the partition name that identifies the monitoring server relative to the firewall used for address translation.	

Worksheets for SA z/OS monitoring agent configuration

Table 7. Configuration worksheet for communication protocols if the monitoring server is on a z/OS system (continued)

Value	Description	Value for your configuration
SNA.PIPE setting		
Applid prefix	Specify the applid prefix you want for all the VTAM applids required by the monitoring server. These applids begin with a prefix, and end with a unique applid value. The applids are contained in the VTAM major node. The default is CTDDSN.	
Communication protocols for the monitoring agent You specify the communication protocols for the monitoring agent in "Step 5. Configure the monitoring agent" on page 98.	You must plan communication protocols for the monitoring agent to send data to the monitoring server. **Tip:** Make sure that at least one of the protocols you specify for the monitoring agent corresponds to a protocol specified for the agent's primary monitoring server. Choose from the following protocols: **IP.PIPE** Uses the TCP/IP protocol for underlying communications. **IP.UDP** Also a TCP/IP protocol. Uses the User Datagram Protocol (UDP). **IP6.PIPE** IP.PIPE protocol with IPV6 installed and operational. This protocol is available only on a z/OS system at release level V1R7 or higher with IPV6 installed and operational. **IP6.UDP** IP.UDP protocol with IPV6 installed and operational. This protocol is available only on a z/OS system at release level V1R7 or higher with IPV6 installed and operational. **IP.SPIPE** Secure IP.PIPE protocol. This protocol is available only on a z/OS system at release level V1R7 or higher. **IP6.SPIPE** Secure IP.PIPE for IPV6. This protocol is available only on a z/OS system at release level V1R7 or higher with IPV6 installed and operational. **SNA.PIPE** Uses the SNA Advanced Program-To-Program Communications (APPC).	• Protocol 1: _____ Highest-priority communication protocol. IP.PIPE, IP.SPIPE, IP6.PIPE, or IP6.SPIPE is generally the best choice for Protocol 1 in firewall environments. These protocols enable the monitoring agent on z/OS to communicate with a monitoring server on a different system, even if both components are running behind firewalls. • Protocol 2: _____ • Protocol 3: _____
TEMS name (node ID)	Node ID of the hub monitoring server. Note that the node ID is generally not the same as the host name. It is an arbitrary name assigned during Tivoli Enterprise Monitoring Server configuration. On z/OS systems, look for the value of CMS_NODEID in this location: &rhilev.&rte.RKANPARU(KDSENV)	
IP.* or IP6.* settings		

Table 7. Configuration worksheet for communication protocols if the monitoring server is on a z/OS system (continued)

Value	Description	Value for your configuration
Host name	Host name of the system where the monitoring agent is installed. To obtain the host name, enter TSO HOMETEST at the command line of the z/OS system where the monitoring agent is installed. If the z/OS domain name resolver configuration specifies a search path that includes the target domain suffix, specify only the first qualifier of the host name. (Example: sys is the first qualifier of the fully qualified host name sys.ibm.com.) Otherwise, specify the fully qualified host name.	
Address	IP address of the system where the monitoring agent is installed. To obtain the IP address, enter TSO HOMETEST at the command line of the z/OS system where the monitoring agent is installed.	
Started task	Started task name of the TCP/IP server. You can specify * to allow the IP stack to dynamically find the TCP/IP image. * is the suggested value for the started task.	
Network interface list	A list of network interfaces for the monitoring agent to use. This parameter is required for sites that are running more than one TCP/IP interface or network adapter on the same z/OS image. Setting this parameter allows you to direct the monitoring agent to connect to a specific TCP/IP local interface. Specify each network adapter by the host name or IP address to be used for input and output. Use a blank space to separate the entries. If your site supports DNS, you can enter IP addresses or short host names. If your site does not support DNS, you must enter fully qualified host names. If you specify an interface address or a list of interface addresses, the Configuration Tool generates the KDEB_INTERFACELIST parameter in the KDSENV member of the *&rhilev.&rtename*.RKANPARU library.	
Address translation	By default, Ephemeral Pipe Support (EPS) is enabled automatically to allow IP.PIPE connections to cross a (network address) translating firewall. This feature obviates the need for a broker partition file (KDC_PARTITIONFILE=KDCPART). If you specifically want to disable EPS, specify Y for **Address translation**.	

Worksheets for SA z/OS monitoring agent configuration

Table 7. Configuration worksheet for communication protocols if the monitoring server is on a z/OS system (continued)

Value	Description	Value for your configuration
Partition name	If you specified Y for **Address translation**, specify the partition name that identifies the monitoring agent relative to the firewall used for address translation.	
SNA settings		
Applid prefix	Specify the applid prefix to create the VTAM node and applids required by the monitoring agent. These applids begin with a prefix, and end with a unique applid value. The applids are contained in the VTAM major node. The default prefix is CTDAH.	
Communication protocols for the portal server You specify the communication protocols for the portal server in "Installing and configuring the Tivoli Monitoring Services components" on page 85.	You must plan communication protocols for the portal server to receive data from the monitoring server. Choose from the following protocols: **IP.PIPE** Uses the TCP/IP protocol for underlying communications. **IP.UDP** Uses the TCP/IP User Datagram Protocol (UDP). **IP.SPIPE** Secure IP.PIPE protocol. **SNA.PIPE** Uses the SNA Advanced Program-To-Program Communications (APPC).	• Protocol 1: _____ Highest-priority communication protocol. IP.PIPE or IP.SPIPE is generally the best choice for Protocol 1 in firewall environments. These protocols enable the portal server to communicate with a monitoring server on another system, even if both components are running behind firewalls. • Protocol 2: _____ • Protocol 3: _____
IP.PIPE or IP.SPIPE settings (See "Configuration worksheet if the monitoring server is on a z/OS system" on page 23.)		
Host name or IP address	Host name or IP address of the monitoring server.	
Port number	Listening port for the hub monitoring server to use in communicating with the portal server. The default port number is 1918 for IP.PIPE and 3660 for IP.SPIPE.	
IP.UDP settings (See "Configuration worksheet if the monitoring server is on a z/OS system" on page 23.)		
Host name or IP address	Host name or IP address of the monitoring server.	
Port or pool number	Listening port for the hub monitoring server to use in communicating with the portal server, or the pool from which the port is to be selected. The default number is 1918.	
SNA settings		
Network name	SNA network identifier for your location	
LU name	LU name for the monitoring server. This LU name corresponds to the Local LU Alias in your SNA communications software.	
LU 6.2 logmode	The name of the LU6.2 logmode. The default value is **CANCTDCS**.	

Table 7. Configuration worksheet for communication protocols if the monitoring server is on a z/OS system (continued)

Value	Description	Value for your configuration
TP name	Transaction program name for the monitoring server. The default value is **SNASOCKETS**.	

Worksheets: Information to gather when you put your hub monitoring server on a distributed system

If you are putting your hub monitoring server on a distributed system, fill out the tables below:

- "Configuration worksheet if the hub monitoring server is on a distributed system"
- "Configuration worksheet for communication protocols if the hub monitoring server is on a distributed system" on page 32

If you are putting your hub monitoring server on z/OS, fill out the worksheets in "Worksheets: Information to gather when you put your hub monitoring server on a z/OS system" on page 23.

Note that all fields are required, unless otherwise indicated.

Configuration worksheet if the hub monitoring server is on a distributed system

Table 8. Configuration worksheet if the hub monitoring server is on a distributed system

Field	Description	Value for your configuration
Monitoring server host name	Host name of the system where the hub monitoring server is installed. You need both the short host name (without the domain name) and the fully qualified host name of the monitoring server workstation (with the domain name).	
Monitoring server port number	Port number of the system where the hub monitoring server is installed. The default is 1918. **Note:** The same TCP/IP port number must be used for every monitoring server in the enterprise. Also, make sure that the monitoring server well-known port is not on the TCP/IP reserved port list.	

Worksheets for SA z/OS monitoring agent configuration

Table 8. Configuration worksheet if the hub monitoring server is on a distributed system (continued)

Field	Description	Value for your configuration
Monitoring server name (node ID)	Name (node ID) of the monitoring server. The default name for the hub monitoring server is **HUB_***host_name*. For example, for host ITMSERV61, the default hub name is **HUB_ITMSERV61**. The node ID is generally not the same as the host name. It is an arbitrary name assigned during monitoring server configuration. • On Windows systems, you can find the node ID in **Manage Tivoli Monitoring Services**. Right-click **Tivoli Enterprise Monitoring Server** and select **Browse Settings**, and look for the value of CMS_NODEID. • On Linux and UNIX systems, you can find the value of CMS_NODEID in the KBBENV file located in the $itmhome/tables/*cms_name* subdirectory.	
Encryption key	You are prompted for a 32-byte encryption key when you begin configuration of components on a distributed system. You can use the default key. Be sure to document the value you use for the key, because you must use the same key in configuring any monitoring server and the portal servers that communicate.	__ Use default key: _____ __ Define your own key: _____

Configuration worksheet for communication protocols if the hub monitoring server is on a distributed system

Fill out the following communication protocols worksheet if you plan to put your hub monitoring server on a distributed system. For information about general requirements for using the TCP/IP communication protocols, see "Requirements for TCP/IP communication protocols" on page 39.

Table 9. Configuration worksheet for communication protocols if the hub monitoring server is on a distributed system

Field	Description	Value for your configuration
Communication protocols for a monitoring server on a distributed system You specify the communication protocols for the monitoring server in "Specifying communication protocols" on page 69.	You must plan communication protocols for a monitoring server on a distributed system to send data to other components of the SA z/OS monitoring agent, such as remote monitoring servers and portal servers. Choose from the following protocols: **IP.PIPE** Uses the TCP/IP protocol for underlying communications. **IP.UDP** Uses the TCP/IP User Datagram Protocol (UDP). **IP.SPIPE** Secure IP.PIPE protocol. The z/OS system must be V1R7 or higher. **SNA.PIPE** Uses the VTAM SNA Advanced Program-To-Program Communications (APPC).	• Protocol 1: _____ Highest-priority communication protocol. The IP.PIPE or IP.SPIPE protocol is generally the best choice for Protocol 1 in firewall environments. These protocols enable the monitoring server to communicate with the monitoring agent on z/OS and with other components on other systems, even if the components are running behind firewalls. • Protocol 2: _____ • Protocol 3: _____
IP.PIPE or IP.SPIPE Settings (See "Configuration worksheet if the hub monitoring server is on a distributed system" on page 31.)		

Table 9. Configuration worksheet for communication protocols if the hub monitoring server is on a distributed system (continued)

Field	Description	Value for your configuration
Host name or IP address	Host name or IP address of the system where the monitoring server is installed.	
Port number	Listening port for the hub monitoring server to use in communicating with the monitoring agent. The default port number is 1918 for IP.PIPE and 3660 for IP.SPIPE. **Note:** The same TCP/IP port number must be used for every monitoring server in the enterprise. Also, make sure that the monitoring server well-known port is not on the TCP/IP reserved port list.	
IP.UDP Settings (See "Configuration worksheet if the hub monitoring server is on a distributed system" on page 31.)		
Host name or IP address	Host name or IP address of the system where the monitoring server is installed.	
Port or pool number	Listening port for the hub monitoring server to use in communicating with the monitoring agent, or the pool from which the port is to be selected. The default number is 1918.	
SNA Settings		
Network Name	SNA network identifier for your location.	
LU name	LU name for the monitoring server. This LU name corresponds to the Local LU Alias in your SNA communications software.	
LU 6.2 logmode	Name of the LU6.2 logmode. The default value is **CANCTDCS**.	
TP name	Transaction program name for the monitoring server. The default value is **SNASOCKETS**.	

Worksheets for SA z/OS monitoring agent configuration

Table 9. Configuration worksheet for communication protocols if the hub monitoring server is on a distributed system (continued)

Field	Description	Value for your configuration
Communication protocols for the monitoring agent You specify the communication protocols for the monitoring agent in "Step 5. Configure the monitoring agent" on page 98.	You must plan communication protocols for the monitoring agent to send data to the monitoring server. **Tip:** Make sure that at least one of the protocols you specify for the monitoring agent corresponds to a protocol specified for the agent's primary monitoring server. Choose from the following protocols: **IP.PIPE** 　　Uses the TCP/IP protocol for underlying communications. **IP.UDP** 　　Uses the TCP/IP User Datagram Protocol (UDP). **IP6.PIPE** 　　Uses the TCP/IP protocol for underlying communications. IPV6 must be installed and operational. **IP6.UDP** 　　Uses the TCP/IP User Datagram Protocol (UDP). IPV6 must be installed and operational. **IP.SPIPE** 　　Secure IP.PIPE protocol. The z/OS system must be V1R7 or higher. **IP6.SPIPE** 　　Secure IP.PIPE protocol. IPV6 must be installed and operational, and the z/OS system must be V1R7 or higher. **SNA.PIPE** 　　Uses the VTAM SNA Advanced Program-To-Program Communications (APPC).	• Protocol 1: _____ Highest-priority communication protocol. IP.PIPE, IP.SPIPE, IP6.PIPE, or IP6.SPIPE is generally the best choice for Protocol 1 in firewall environments. These protocols enable the monitoring agent on z/OS to communicate with the monitoring server on a distributed system, even if both components are running behind firewalls. • Protocol 2: _____ • Protocol 3: _____
Language locale	Specify 1 for United States English. This is the only language that SA z/OS supports.	
TEMS name (node ID)	Node ID of the hub monitoring server. Note that the node ID is generally not the same as the host name. It is an arbitrary name assigned during Tivoli Enterprise Monitoring Server configuration. Find the node ID as follows, depending on where the monitoring server is installed: • On Windows systems, you can find the node ID in Manage Tivoli Monitoring Services. Right-click **Tivoli Enterprise Monitoring Server** and select **Browse Settings**, and look for the value of CMS_NODEID. • On Linux and UNIX systems, you can find the value of CMS_NODEID in the KBBENV file located in the $itmhome/tables/cms_name subdirectory.	
IP.* or IP6.* protocols		

Table 9. Configuration worksheet for communication protocols if the hub monitoring server is on a distributed system (continued)

Field	Description	Value for your configuration
Host name	Host name of the system where the monitoring agent is installed. To obtain the host name, enter TSO HOMETEST at the command line of the z/OS system where the monitoring agent is installed. If the z/OS domain name resolver configuration specifies a search path that includes the target domain suffix, specify only the first qualifier of the host name. (Example: sys is the first qualifier of the fully qualified host name sys.ibm.com.) Otherwise, specify the fully qualified host name.	
Address	IP address of the system where the monitoring agent is installed. To obtain the IP address, enter TSO HOMETEST at the command line of the z/OS system where the monitoring agent is installed.	
Started task	Started task name of the TCP/IP server. You can specify * to allow the IP stack to dynamically find the TCP/IP image. * is the suggested value for the started task.	
Network interface list	A list of network interfaces for the monitoring agent to use. This parameter is required for sites that are running more than one TCP/IP interface or network adapter on the same z/OS image. Setting this parameter allows you to direct the monitoring agent to connect to a specific TCP/IP local interface. Specify each network adapter by the host name or IP address to be used for input and output. Use a blank space to separate the entries. If your site supports DNS, you can enter IP addresses or short host names. If your site does not support DNS, you must enter fully qualified host names. If you specify an interface address or a list of interface addresses, the Configuration Tool generates the KDEB_INTERFACELIST parameter in the KDSENV member of the *&rhilev.&rtename*.RKANPARU library.	
Address translation	By default, Ephemeral Pipe Support (EPS) is enabled automatically to allow IP.PIPE connections to cross a (network address) translating firewall. This feature obviates the need for a broker partition file (KDC_PARTITIONFILE=KDCPART). If you specifically want to disable EPS, specify Y for **Address translation**.	
Partition name	If you specified Y for **Address translation**, specify the partition name that identifies the monitoring agent relative to the firewall used for address translation.	
SNA settings		

Worksheets for SA z/OS monitoring agent configuration

Table 9. Configuration worksheet for communication protocols if the hub monitoring server is on a distributed system (continued)

Field	Description	Value for your configuration
VTAM applid prefix	Specify the applid prefix to create the VTAM node and applids required by the monitoring agent. These applids begin with a prefix, and end with a unique applid value. The applids are contained in the VTAM major node. The default prefix is CTDAH.	

Communication protocols for the portal server
 	
You specify the communication protocols for the portal server in "Installing and configuring the Tivoli Monitoring Services components" on page 85.
	You must plan communication protocols for the portal server to receive data from the monitoring server. Choose from the following protocols:
	
	IP.PIPE
	    Uses the TCP/IP protocol for underlying communications.
	
	IP.UDP
	    Uses the TCP/IP User Datagram Protocol (UDP).
	
	IP.SPIPE
	    Secure IP.PIPE protocol.
	
	SNA.PIPE
	    Uses the SNA Advanced Program-To-Program Communications (APPC).
		• Protocol 1: _____
		Highest-priority communication protocol. The IP.PIPE or IP.SPIPE protocol is generally the best choice for Protocol 1 in firewall environments. These protocols enable the portal server to communicate with a monitoring server on another system, even if both components are running behind firewalls.
		• Protocol 2: _____
		• Protocol 3: _____

IP.* settings (See "Configuration worksheet if the hub monitoring server is on a distributed system" on page 31.)		
Host name or IP address	Host name or IP address of the hub monitoring server.	
Port number	Same port number you specified for the hub monitoring server.	
SNA settings		
Network name	SNA network identifier for your location.	
LU name	LU name for the monitoring server. This LU name corresponds to the Local LU Alias in your SNA communications software.	
LU 6.2 logmode	Name of the LU6.2 logmode. The default value is **CANCTDCS**.	
TP name	Transaction program name for the monitoring server. The default value is **SNASOCKETS**.	

Worksheet: Information for configuring your runtime environment

Using the information about runtime environments above, you can decide what type of runtime environment configuration you need for your SA z/OS monitoring agent configuration. You must define a runtime environment on each z/OS system you monitor. In most cases, you start with one full or base type and sharing types (that share either the full or base runtime environment) for subsequent z/OS images you monitor. For each runtime environment, gather the following information:

Table 10. Worksheet for defining runtime environments

Value	Description	Value for your configuration
Runtime environment name	Unique identifier of up to 8 characters. **Tip:** If you specify a runtime environment name no more than 4 characters long, you can specify the same name for the JCL suffix (used as the suffix of the name of the member containing the JCL in the INSTJOBS data set). This setup makes the output of Configuration Tool batch jobs easier to find in the Spool Display and Search Facility (SDSF) queue.	
Runtime environment type	Explained above in "Understanding runtime environments" on page 14	
The base or full runtime environment associated with a sharing runtime environment	For a sharing runtime environment type, list the name of the base or full runtime environment from which the sharing runtime environment obtains its base library information.	
Runtime environment description	Information for your installation's use.	
Security system for the runtime environment	For each runtime environment, the Configuration Tool prompts you for a security system. You can specify None, RACF, TSS, or NAM. Specifying a security system here does not enable security validation of users signing on to the Tivoli Enterprise Portal. Security validation of users is enabled in a Tivoli Enterprise Monitoring Server configuration panel.	
VTAM network ID	VTAM network ID for the monitoring server on z/OS as identified in "Worksheets: Information to gather when you put your hub monitoring server on a z/OS system" on page 23. This is optional for a monitoring server on a distributed system, see "Worksheets: Information to gather when you put your hub monitoring server on a distributed system" on page 31.	
TCP/IP host name	TCP/IP host name of the z/OS system where the runtime environment is being defined. To obtain the host name, enter TSO HOMETEST at the command line of the z/OS system. If the z/OS domain name resolver configuration specifies a search path that includes the target domain suffix, specify only the first qualifier of the host name. (Example: sys is the first qualifier of the fully qualified host name sys.ibm.com.) Otherwise, specify the fully qualified host name.	
IP address	IP address of the z/OS system where the runtime environment is defined. To obtain the IP address, enter TSO HOMETEST at the command line of the z/OS system.	
Started task	Started task of the TCP/IP server for the z/OS system.	
Port number	Address of the IP port. The default is 1918 for nonsecure communication and 3660 for secure communication.	

A road map for installation and configuration of the SA z/OS monitoring agent

Use the following roadmap to steer you though the installation process:

1. **Plan your installation**, using the information in Chapter 3, "Planning for prerequisites, packaging, and tools," on page 39.
2. **Perform the steps** in Chapter 4, "Beginning the installation and configuration," on page 47.
3. **Select** a configuration procedure to perform, depending on your configuration design:
   a. Chapter 5, "Configuring the hub monitoring server and the monitoring agent on z/OS," on page 57
   b. Chapter 6, "Configuring the hub monitoring server on a Windows system and the monitoring agent on a z/OS image," on page 89
4. **Perform the steps** in Chapter 7, "Setting up security," on page 109.
5. **Optionally make your configuration system-independent**, using the information in Chapter 8, "Enabling system variable support," on page 119.
6. **Optionally replicate runtime environments in batch mode**, using the information in Chapter 9, "Using batch mode processing," on page 125.

Chapter 3. Planning for prerequisites, packaging, and tools

This chapter describes:

- "Understanding software and hardware prerequisites for installation"
- "Understanding product packaging" on page 40
- "Understanding the SA z/OS monitoring agent installation" on page 41
- "Understanding the Configuration Tool" on page 42

You will need to understand this information before beginning the installation process in Part 2, "Installation and configuration," on page 45.

Understanding software and hardware prerequisites for installation

The SA z/OS monitoring agent has the following prerequisites:

- The SA z/OS monitoring agent has a conditional operational prerequisite to IBM Tivoli Monitoring Services (5698-A79), if you want to exploit the SA z/OS monitoring agent.
- A complete list of other SA z/OS hardware and software prerequisites is located in the *IBM Tivoli System Automation for z/OS: Program Directory*.
- Prerequisites for the distributed IBM Tivoli Monitoring Services components are located in the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Requirements for TCP/IP communication protocols

Review the following TCP-related requirements before you configure the SA z/OS monitoring agent.

Default OMVS segment

To use the TCP/IP communication protocols, both the Tivoli Enterprise Monitoring Server and the SA z/OS monitoring agent require a default OMVS segment. See the *z/OS Communications Server IP Configuration Guide* for an explanation of how to provide an OMVS segment.

Using the IP.PIPE communication protocol

IP.PIPE is the default protocol for product components. If you choose IP.PIPE as a protocol for the monitoring server and monitoring agent, be aware of the following limitations:

- The maximum number of IP.PIPE processes per host is 16.
- IP.IPIPE uses only one physical port per process. Port numbers are allocated using a well-known port allocation algorithm. The first process for a host is assigned port 1918, which is the default.

> **Important**
>
> The same TCP/IP port number must be used on every monitoring server in the enterprise. Also, the monitoring server well-known port cannot be on the TCP/IP reserved port list.

Configuring domain name resolution

If the monitoring server and monitoring agent on a z/OS system are using any IP.* or IP6.* communication protocols for connection, but the IP domain name

resolution is not fully configured on the system, you must specify the SYSTCPD DDNAME in the CANSDSST started task.

The Configuration Tool generates the CANSDSST started task with the following commented out lines. Customize the SYSTCPD DDNAME to your environment.

```
//*SYSTCPD explicitly identifies which data set 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 data set
//*can be any sequential data set or a member of a partitioned
//*data set. TCPIP.SEZAINST(TCPDATA) is the default sample file.
//* TCPIP.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 your appropriate
//*      TCPDATA library name supported at your site if domain
//*      name resolution is not fully configured.
//*SYSTCPD DD DISP=SHR,
>//*      DSN=TCPIO.SEZAINST(TCPDATA)
```

After you finish, copy the procedures to PROCLIB.

Prerequisite for Take Action command forwarding

NetView authentication of z/OS console commands forwarded from the Tivoli Enterprise Portal requires NetView on z/OS V5.2 with APAR OA18449 applied.

Checking for fixes

To make sure that you have the latest version of all components, check for any fix packs that might be available. See Part 4, "Problem determination," on page 187.

Understanding product packaging

If you are installing the SA z/OS monitoring agent for the first time, you will find familiar IBM packaging types (such as Passport Advantage®), installation tools (such as SMP/E or InstallShield), and installation documentation, including a program directory. You will also find a new z/OS-based Configuration Tool that streamlines the transition between the SMP/E installation and a running system. This tool works with SMP/E to save files that will be used in later steps to configure the products.

If you are an existing OMEGAMON customer, you will find some differences but a lot of familiar tools and processes as well. Here are the key differences you can anticipate:

- CICAT (the Candle Installation and Configuration Assistance Tool) is now called the Configuration Tool, but the configuration functionality is relatively unchanged.
- The tape format used by the Candle products, called the Candle Universal Tape Format, included four files in front of the SMP/E Modification Control Statements (SMPMCS) file. The tapes provided with the SA z/OS monitoring agent are in the standard IBM relfile format that IBM software manufacturing uses to create the tape images for installation systems such as ServerPac and Custom-Built Product Delivery Offering (CBPDO).
- z/OS maintenance is delivered electronically or on tape in the form of program temporary fixes (PTFs) that are installed using SMP/E. Refer to Appendix C, "Support," on page 239 for more information. If you receive your product tape through the custom-built product delivery offering (CBPDO) process,

maintenance is included on the tape for you to install. If you receive your product tape as part of a ServerPac or SystemPac®, then product maintenance is preinstalled.

Each Tivoli Monitoring Services product provides a program directory that describes the z/OS installation steps required to move the product code from the distribution media to your DASD, whether it is distributed on tape or electronically.

The contents of the SA z/OS monitoring agent package are shown in Table 11:

Table 11. SA z/OS monitoring agent packaging

Media	Name and description	Target
Media set 1 of 4: Prerequisite installation (z/OS and distributed)		
5698-A79 media	*IBM Tivoli Monitoring* (multi-CD set) includes subdirectories and installation procedures for the Tivoli Monitoring Services components on Windows, UNIX, Intel Linux, and Linux on zSeries operating systems.	Workstation & z/OS
	IBM DB2 Universal Database Workgroup Server Edition (multi-CD set) provides database functions to Tivoli Monitoring Services components on Windows, UNIX, and Intel Linux, and Linux on zSeries operating systems.	
Media set 2 of 4: Distributed installation		
CD	*IBM Tivoli System Automation for z/OS Workspace Enablement Version 3.3.0* contains the predefined workspaces and situations, online help, expert advice, and System Automation for z/OS data for the Tivoli Enterprise Portal. This CD also contains data for adding System Automation for z/OS application support to the Tivoli Enterprise Monitoring Server.	Workstation
Media set 3 of 4: z/OS installation		
Hardcopy	The z/OS media set includes the following hardcopy publication: • *IBM Tivoli System Automation for z/OS Version 3 Release 3 Monitoring Agent Configuration and Users Guide*, SC34-2581	—
Media set 4 of 4: Product Documentation		
CD	*IBM Tivoli System Automation for z/OS Documentation CD*	—

Understanding the SA z/OS monitoring agent installation

The System Modification Program/Extended (SMP/E) is the basic tool for installing and maintaining software in z/OS systems and subsystems. It controls these changes at the element level by:

• Selecting the proper levels of elements to be installed from a large number of potential changes

• Calling system utility programs to install the changes

• Keeping records of the installed changes

SMP/E is an integral part of the installation, service, and maintenance processes for z/OS and OS/390® software products and product packages, such as CBPDO, ProductPac®, RefreshPac, and selective follow-on service for CustomPac. In addition, SMP/E can be used to install and service any software that is packaged in SMP/E system modification (SYSMOD) format.

SMP/E can be run either using batch jobs or using dialogs under Interactive System Productivity Facility/Program Development Facility (ISPF/PDF). SMP/E dialogs help you interactively query the SMP/E database, as well as create and submit jobs to process SMP/E commands.

The guidance for doing an SMP/E installation is a program directory. Every monitoring agent product is accompanied by a program directory.

Understanding the Configuration Tool

The Installation and Configuration Assistance Tool (also known as the Configuration Tool) creates and customizes all the runtime data sets, and creates the JCL member in SYS1.PROCLIB, to support the SA z/OS monitoring agent. If the Tivoli Enterprise Monitoring Server is installed on a z/OS system or if you select SNA as one of your communication protocols, the Configuration Tool also creates the VTAM major node member in SYS1.VTAMLST. The members have the started task name and major node name you specify during the configuration process.

The Configuration Tool is restartable. If necessary, you can end the dialog, start it again, and continue from the point of interruption.

If you have an earlier version of the Configuration Tool on your z/OS system, it is automatically replaced by the IBM Configuration Tool version 3.3.0 during SMP/E installation. For information about supported levels of the SMP/E program and other related installation software, refer to the *IBM Tivoli System Automation for z/OS: Program Directory*.

> **Tip**
>
> Some Configuration Tool menus contain items that apply only to the former Candle products. On the Main Menu of the Configuration Tool (Figure 9 on page 51), only options **1** (**Set up work environment**) and **3** (**Configure products**) apply to the SA z/OS monitoring agent.

The Configuration Tool provides defaults wherever possible. These defaults are sufficient to complete the installation of products and maintenance. Change the defaults to reflect the needs of your enterprise. The tool operates in two modes:
- **Interactive mode** where an ISPF panel-driven facility assists you in specifying parameters and tailoring jobs for configuring new products and new versions of products.
- A **Batch facility** that creates a single batch job that you can use to build, configure, and load a *runtime environment* (RTE). This single job performs all of the same RTE processing as the interactive Configuration Tool. Batch mode is a simple and useful way of replicating RTEs to other z/OS systems.

Using the Configuration Tool

The Configuration Tool provides defaults for most fields and options. The defaults can be changed to values specific to your site.

Whenever possible, the Configuration Tool checks the values you specify and verifies that you have specified the required values. If the Configuration Tool detects an error or omission, it displays a short message.

Display requirements in ISPF

If you are using a 3270 Model 2 (24 x 80) display, you must turn off the predefined function (PF) keys so that the Configuration Tool panels are not truncated. To turn off the predefined function keys, type PFSHOW on any ISPF command line and press Enter until the function keys are no longer displayed.

Restrictions

The following restrictions apply to the Configuration Tool:

- The length of the high-level qualifier for the runtime libraries must be 26 characters or less.
- You cannot use the ISPF feature for edit recovery. If you enter the ISPF RECOVERY ON command, edits produce a recovery error message. Enter the RECOVERY OFF command to suppress the error messages.

Commands and function

You can use the following commands for navigation and display control in the Configuration Tool:

End key
> Returns to the previous panel.

Enter key
> Accepts the values you have specified and displays the next panel in the process.

HELP Displays information about a panel or the extended description for a message.

README
> Displays the README for the Configuration Tool.

README APP
> Displays information about VTAM applids.

README ERR
> Displays a list of CLIST error codes and descriptions (for both interactive and batch mode).

README SYS
> Displays information about system variable support.

UTIL Displays the **Installation Services and Utilities** menu.

Online help for the Configuration Tool

Online help contains detailed information about using the Configuration Tool panels. To display help from any Configuration Tool panel, press the Help key (F1) or enter HELP on the command line.

You can also display help for the help. For example, you can display information about the command to use to return to the previous topic in the help system. To display the help for help from any help panel, press the Help key (F1) or enter HELP on the command line.

Understanding the Configuration Tool

Part 2. Installation and configuration

Chapter 4. Beginning the installation and configuration

If you are installing the SA z/OS monitoring agent software for the first time, follow the instructions in this chapter.

First steps: Installing the z/OS components and beginning the configuration

For any deployment you choose, you must complete the first steps in the same way:

__ "Step 1. Perform the SMP/E installation of the z/OS-based components"

__ "Step 2. Configure SA z/OS and NetView"

__ "Step 3. Set up the Configuration Tool" on page 49

__ "Step 4. Start the Configuration Tool" on page 50

__ "Step 5. Set up the Configuration Tool environment" on page 51

The rest of this chapter provides instructions for these steps.

Step 1. Perform the SMP/E installation of the z/OS-based components

Follow the instructions in the *IBM Tivoli Monitoring Services: Program Directory* to install the following components:

- Configuration Tool
- Tivoli Enterprise Monitoring Server on z/OS (if your planned deployment includes a hub Tivoli Enterprise Monitoring Server on z/OS)
- Common components

  This product includes several common components that are also included in other Tivoli Monitoring Services products. If you install into an existing environment, you might need to delete the FMIDs for the common components from the SMP/E installation jobs to avoid errors. See the *IBM Tivoli Monitoring Services: Program Directory* for a list of the common components.

If an earlier version of a product component is installed in the same consolidated software inventory (CSI), the earlier version is automatically replaced by the new version provided with the product.

Step 2. Configure SA z/OS and NetView

The SA z/OS monitoring agent communicates with the SA z/OS agent running in NetView for z/OS using the NetView Program-to-Program Interface (PPI). A new task has to be started in NetView to receive requests from the SA z/OS monitoring agent. One or more additional autotasks are required to process such requests. Finally, the SA z/OS automation policy must be modified to define the automated functions and the autotasks assigned to them.

Perform the following to configure the communication between SA z/OS and NetView:

Step 1. Perform the SMP/E installation of the z/OS-based components

1. Define the name of the PPI receiver that receives requests from the SA z/OS monitoring agent. This name must match the name that you assign to the SA z/OS monitoring agent configuration option KAH_PPI_RECEIVER. The default name is INGAHRCV.

2. Define the name of the PPI receiver that receives events from the SA z/OS automation agent. This name must match the name that you assign to the SA z/OS monitoring agent configuration option KAH_PPI_LISTENER. The default name is KAHNVLIS.

3. Define the timeout interval that is used to monitor the duration of a request to the SA z/OS automation agent. If the timeout expires, the current request is discarded and the monitoring agent is notified. The default value is 45 seconds.

4. Create an initialization member for the NetView PPI receiver task or take the sample member, INGAHINI, that is shipped with the product and set the following options:

   ```
   KAH_PPI_RECEIVER=name from 1 above
   KAH_PPI_LISTENER=name from 2 above
   TIMEOUT=value from 3 above
   ```

5. Enter the SA z/OS customization dialog to modify the SA z/OS automation policy and add one or more automated functions under entry type AOP:

   a. Select entry type AOP.

   b. Create a new entry, for example new KAH_AUTOOPS, and fill out the description as needed.

   c. Select the OPERATORS policy and then enter one or more automated functions in the corresponding field. The automated functions must be named AOFKAH*nn*.

   d. Next select each individual AOFKAH*nn* automated function and specify a primary automation operator. SA z/OS ships the sample member AOFOPFSO that, when included in the DSIOPF library concatenation, defines three automation operators: AUTKAH01, AUTKAH02, and AUTKAH03.

   e. Select the WHERE USED policy and link the newly created entry to the system (or systems) of your choice.

   f. Build the System Operations configuration file that includes the new automated functions.

6. Unless you use the AOFOPFSO member that is shipped with the SA z/OS product, make sure you have configured the automation operators that are assigned to your new automated functions in the DSIOPF library. After adding new automation operators, refresh the operators to activate them.

7. Refresh the automation agent configuration using the newly built configuration file.

8. Start the NetView PPI receiver task. There are several ways that this task can be started. Once started, pass the name of the initialization member located in the DSIPARM library that you have created in step 4. Otherwise, default values are used.

   • You can start the task automatically when NetView is started. To do this, remove the comments for the INGAHPPI task in the AOFSTYLE member that is shipped with the SA z/OS product.

   • You can also define the task in the automation policy to manage it using SA z/OS operator commands.

   • You can start the task manually using the NetView START command. Use the following command:

```
        START TASK=INGAHPPI,MOD=INGAHPPI,MEM=INGAHINI
```

9. Once the NetView PPI receiver task is active, validate the status of the PPI receiver using the DISPPI command.

10. If you want to run multiple copies of the SA z/OS monitoring agent within the same physical sysplex, but each one within its own SA z/OS subplex, then you must create a unique group entry (GRP) in the SA z/OS customization dialog for each SA z/OS subplex.

   This is even true for SA z/OS subplexes that consist of a single system only, for example, a Geographically Dispersed Parallel Sysplex® (GDPS®) Controlling system. This ensures that the managed system name of the SA z/OS monitoring agent is unique and so multiple copies of the SA z/OS monitoring agent can register at the TEMS at the same time.

Step 3. Set up the Configuration Tool

Your first step after installing the contents of the product tape is to copy the contents from one of the target libraries into the appropriate Configuration Tool work library. If you are using an existing CSI that already has the Configuration Tool installed, copy the contents of the target library into your existing Configuration Tool work library. If you are using a new CSI, copy the contents of the target library to a newly created Configuration Tool library.

Tip

The **Prepare user libraries** utility generates a batch job to create, from the existing target libraries, the user libraries that are new in this release. You can access the utility by selecting **Services and utilities** from the Configuration Tool **Configure Products** menu, and then entering 6 (**Prepare user libraries**). See "Utilities: Preparing user libraries" on page 233.

If you use a CSI that the Configuration Tool is already installed in

If you use an existing CSI that already has the Configuration Tool installed, copy the contents of the *&thilev*.TKCIINST library to the *&shilev*.INSTLIBW library as follows:

```
//COPY     EXEC  PGM=IEBCOPY
//SYSPRINT DD SYSOUT=*
//IN       DD DSN=&thilev.TKCIINST,DISP=SHR
//OUT      DD DSN=&shilev.INSTLIBW,DISP=SHR
//SYSIN    DD *
  C O=OUT,I=((IN,R))
```

where *&thilev* is the SMP/E target high-level qualifier and *&shilev* is the installation high-level qualifier.

Tip

To receive notification of the results of a job, add this option to your job card:

```
NOTIFY=userid
```

If you use a new CSI

If you are using a new CSI, perform the following steps to copy the contents of the target library to the newly created Configuration Tool library:

Step 3. Set up the Configuration Tool

1. Allocate the *&shilev*.INSTLIB library using the sample JCL below:

```
//JOBCARD
//ALLOCDS EXEC PGM=IEFBR14
//*
//INSTLIB DD DSN=&shilev.INSTLIB,
//        DISP=(NEW,CATLG,DELETE),
//        UNIT=&tunit,
//        VOL=SER=&tvol,
//        DCB=(RECFM=FB,LRECL=80,BLKSIZE=8880),
//        SPACE=(TRK,(90,15,132))
```

Replace the following parameters with the values specific to your site:

JOBCARD is your job card.

&shilev is the high-level qualifier for the installation environment.

&tunit is the disk unit type for the target library.

&tvol is the disk volser for the target library.

2. Copy the contents of the *&thilev*.TKCIINST library into the *&shilev*.INSTLIB library:

```
//COPY     EXEC  PGM=IEBCOPY
//SYSPRINT DD SYSOUT=*
//IN       DD DSN=&thilev.TKCIINST,DISP=SHR
//OUT      DD DSN=&shilev.INSTLIB,DISP=SHR
//SYSIN    DD *
  C O=OUT,I=((IN,R))
```

where *&thilev* is the SMP/E target high-level qualifier and *&shilev* is the installation high-level qualifier.

Step 4. Start the Configuration Tool

To start the Configuration Tool, complete the following steps:

1. Log on to a TSO session on the target system.
2. Invoke ISPF.
3. Go to a TSO command line. (In most cases, this is option 6 on the ISPF Primary Option Menu.)
4. Enter the following command:

```
EX '&shilev.INSTLIB'
```

where *&shilev* is the high-level qualifier you specified for the Configuration Tool.

> **Tip**
>
> You do not need to specify a member name in this command.

The Configuration Tool displays the copyright panel and then the Main Menu.

```
-------------------------------- MAIN MENU ----------------------------------
OPTION ===>

 Enter the number to select an option:

    1    Set up work environment

    2    Install products

    3    Configure products

    I    Installation information
    S    Services and utilities




        Installation and Configuration Assistance Tool Version 310.12
                      (C) Copyright IBM Corp. 1992-2008
                  Licensed Material - Program Property of IBM

 F1=Help   F3=Back
```

Figure 9. Configuration Tool: Main Menu

> **Tip**
>
> Some Configuration Tool menus contain items that apply only to the
> former Candle products. On the Main Menu, only options **1** (**Set up work
> environment**, for setting up a new Configuration Tool environment) and **3**
> (**Configure products**) apply to the SA z/OS monitoring agent.

If you are configuring the SA z/OS monitoring agent in an existing runtime
environment, skip the next step and go to Chapter 5, "Configuring the hub
monitoring server and the monitoring agent on z/OS," on page 57.

If this is the first time that you are setting up a runtime environment in this
CSI, you need to set working and configuration values before you define the
runtime environment. Continue to "Step 5. Set up the Configuration Tool
environment."

Step 5. Set up the Configuration Tool environment

Setting up the Configuration Tool environment involves two short procedures:

1. Setting up the work environment, by specifying the allocation and processing
   values that the tool uses to create the work data sets it needs and to allocate its
   work libraries.
2. Setting up the configuration environment, by specifying the values the tool uses
   to customize the JCL it creates.

Setting up the work environment

To set up the work environment, complete the following steps:

1. From the Configuration Tool Main Menu, enter 1 (Set up work environment).
   This displays the Set Up Work Environment menu, which has three options.
   a. Select **Specify JCL options** to specify allocation and processing values that
      are used to create the work data sets that are needed by the Configuration
      Tool. This provides operational values for generating batch jobs.

Step 5. Set up the Configuration Tool environment

b. Select **Set up configuration environment** to specify the high-level qualifiers for the VSAM, non-VSAM, and SMP/E runtime libraries for the JCL that is created by the Configuration Tool.

c. Select **Allocate work libraries** to allocate the Configuration Tool work libraries. The initial library, INSTLIB, contains both the operational code and the tables and jobs created by the installer. This job creates additional libraries and populates them with the data initially stored in INSTLIB.

2. From the Set Up Work Environment menu, enter 1 (Specify Options).

```
----------------------------- SPECIFY JCL OPTIONS ------------------------------
COMMAND ===>

 Specify allocation and processing options:

   JCL REGION value    ==> 0M        (Specify K/M suffix)

                                                 Unit/     Storclas/
                                                 VolSer    Mgmtclas    PDSE
   Installation work datasets ...............    3390      OMG         N
                                                 name

 Specify the job statement for generated JCL:

   ==> //useridA JOB (ACCT),'NAME',CLASS=A
   ==> //* DEFAULT JCL
   ==> //*
   ==> //*

   Note: Press F1=Help for Batch Mode considerations when modifying
         jobcard values.

 Enter=Next  F1=Help  F3=Back
```

Figure 10. Configuration Tool: Specify JCL Options panel

The **Specify JCL options** panel shows the defaults for your system.

> **Tip**
> To receive notification of the results of the job, add this option to your job card:
> NOTIFY=*userid*

Use the following information to complete this panel:

JCL REGION value
SMP/E batch jobs contain the REGION= parameter on the EXEC statement The value of this parameter is taken from the CIGSMREG variable. Change this value as required by your installation. The default is 0M.

Unit Specify the unit name to be used when allocating the installation data sets. If the installation data sets are not to be SMS-managed, this field is required. If your installation does not use the unit name or if it is optional, you can leave this field blank.

Volser Specify the volume serial numbers to be used when allocating the installation data sets. If the installation data sets are not to be SMS-managed, this field is required. If your installation does not use the volume serial number or if it is optional, you can leave this field blank.

Storclas

If the installation data sets are to be SMS-managed, specify the SMS storage class to be used for allocation. If your installation does not use the SMS Storclas parameter, or if it is optional, leave this field blank.

Mgmtclas

If the installation data sets are to be SMS-managed, specify the SMS management class to be used for allocation. If your installation does not use the SMS Storclas parameter, or if it is optional, leave this field

PDSE If the installation data sets are to be SMS-managed, you can specify Y to allocate PDSE data sets instead of standard PDS data sets. IBM recommends using PDSE.

Job statement

Enter the standard job card that will be used for each of the batch jobs that the Configuration Tool builds. This job card information is saved in the PROFILE pool for each user. Specify your own job statement by overwriting:

```
// jobstatement
```

In this field, *jobstatement* is the JCL appropriate to your environment for job submission. Each input field represents one line of JCL.

Note: During the configuration process, you will submit several jobs where the JCL is generated for you. By default, install-generated JCL does not include the NOTIFY option. However, if you add this option, you can verify that each job completes successfully before continuing to the next configuration step. The notation `CLASS=A, MSGCLASS=A, NOTIFY=&SYSUID` in Figure 10 on page 52 enables the NOTIFY option.

Because SMS can be implemented in different ways, the Configuration Tool does not attempt to validate these parameters. The data set allocation jobs will use all parameters that you enter. Before allocating SMS-managed data sets, verify the following:

- SMS is active on the MVS™ image where the data sets are allocated.
- The high-level qualifier that you specify is eligible for SMS-managed volumes.
- The combination of Unit/Volser and Storclas/Mgmtclas that you specify is valid at your site.

3. When you have entered the relevant information, press Enter to return to the Set Up Work Environment menu.

4. From the Set Up Work Environment menu, enter 3 (Allocate Work Libraries). The JCL is displayed for you to review, edit if necessary, and submit.

5. After submitting the job, exit the Configuration Tool and allow the job to run. (It will not run while you are in the tool.) Verify that the job completes successfully. All return codes must be zero.

Setting up the configuration environment

When the Allocate Work Libraries job completes, perform the following steps:

1. Start the Configuration Tool:

```
EX '&shilev.INSTLIB'
```

Step 5. Set up the Configuration Tool environment

2. From the Main Menu of the Configuration Tool (Figure 9 on page 51), enter 1 (Set up work environment). This displays the Set Up Work Environment panel. Then enter 2 (Set up configuration environment).

   This displays the Set Up Configuration Environment panel, where you specify values for the JCL that is created by the Configuration Tool. For details of the parameters, press F1 (Help).

```
---------------------- SET UP CONFIGURATION ENVIRONMENT ----------------------
COMMAND ===>

 *** High-level qualifiers are locked.

 RTE allocation routine   ==> IKJEFT01   (IKJEFT01/IEFBR14)

 Runtime                                        Unit/     Storclas/
 Datasets      High-Level Qualifier             VolSer    Mgmtclas    PDSE
 VSAM          hilev                             3390      NONSMS
                                                 name
 Non-VSAM      hilev                             3390      NONSMS      N
                                                 name
 Work     ...............................        3390


 SMP/E
 Datasets      High-Level Qualifier
 Target        hilev



 Enter=Next  F1=Help  F3=Back
```

Figure 11. Configuration Tool: Set Up Configuration Environment panel

This panel includes the following options:

RTE allocation routine
> The allocation steps that the Configuration Tool generates for the runtime environments are designed to use one of two techniques:
>
> - Batch TMP in which the JCL that is generated creates a CLIST using a temporary data set and then executes that CLIST to create the libraries. This process ensures that the JCL can be resubmitted without change and does not fail with JCL errors. This is the recommended method.
> - DD allocation in which the JCL that is generated uses DD statements. If the step requires a re-submission, you must first modify the JCL to eliminate DD statements for data sets that have already been allocated.

Unit   Specify the unit name to be used when allocating the runtime data sets. This field is required if the runtime data sets are not to be SMS-managed. If your installation does not use the unit name or if it is optional, you can leave this field blank.

Volser   Specify the volume serial numbers to be used when allocating the runtime data sets. This field is required if the runtime data sets are not to be SMS-managed. If your installation does not use the volume serial number or if it is optional, you can leave this field blank.

Storclas
> If the runtime data sets are to be SMS-managed, specify the SMS storage class to be used for allocation. If your installation does not use the SMS Storclas parameter, or if it is optional, leave this field blank.

Mgmtclas
If the runtime data sets are to be SMS-managed, specify the SMS management class to be used for allocation. If your installation does not use the SMS Storclas parameter, or if it is optional, leave this field blank.

PDSE If the runtime data sets are to be SMS-managed, you can specify Y to allocate PDSE data sets instead of standard PDS data sets. It is recommended to use PDSE.

SMP/E datasets target
Enter the high-level qualifier of your SMP/E target data sets (*&hilev*).

3. Press Enter to accept the values.

Tip
If you enter the Set Up Configuration Environment panel again after specifying values, the high-level qualifiers are locked and cannot be modified. If you need to modify these values, you can unlock them by selecting **Unlock runtime high-level qualifiers** on the Configuration Services and Utilities menu.

Step 5. Set up the Configuration Tool environment

Chapter 5. Configuring the hub monitoring server and the monitoring agent on z/OS

This procedure describes the steps to follow in configuring a hub Tivoli Enterprise Monitoring Server and SA z/OS monitoring agent in different address spaces of the same z/OS image, as shown in Figure 12. This deployment is recommended for most installations.
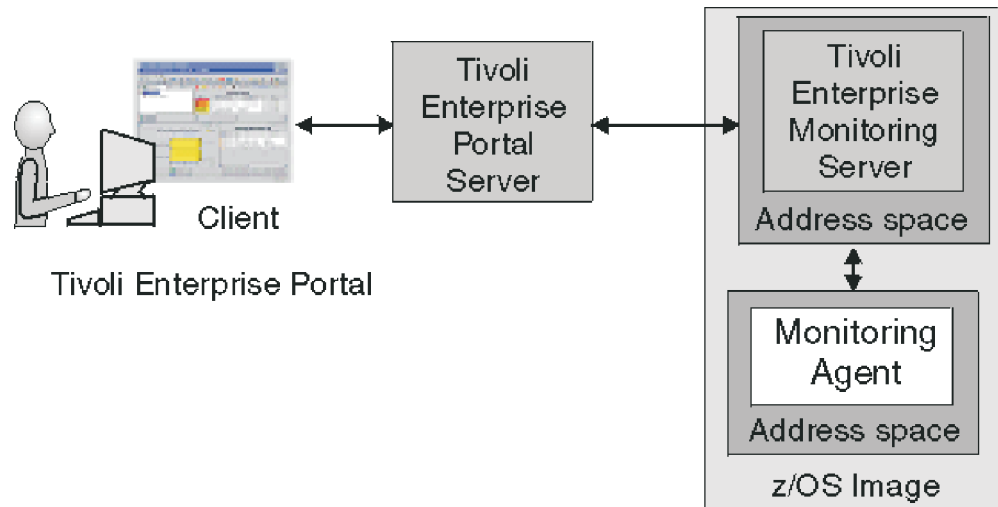
Figure 12. Hub monitoring server and monitoring agent in different address spaces of a single z/OS image

This configuration monitors status, performance and availability on the z/OS system image where the product components are installed. You can add agents in the same monitoring agent address space or in separate address spaces. This configuration is a basic one that can be expanded easily to accommodate multiple systems. (See "Expanding your configuration" on page 88.)

Configuration steps

To configure the product, complete the following steps in order:
- "Step 1. Define the runtime environment" on page 58
- "Step 2. Build the runtime libraries" on page 64
- "Step 3. Configure the hub Tivoli Enterprise Monitoring Server" on page 64
- "Step 4. Configure the monitoring agent" on page 75
- "Step 5. Load the runtime libraries" on page 82
- "Step 6. Complete the configuration of the Tivoli Enterprise Monitoring Server and the monitoring agent" on page 83
- "Step 7. Install the Tivoli Enterprise Portal Server and client on a Windows workstation" on page 84
- "Step 8. Install SA z/OS application support" on page 86
- "Step 9. Verify the configuration" on page 87

Step 1. Define the runtime environment

In this step you define the runtime environment for configuring the SA z/OS monitoring agent.

> **Tip**
>
> Be sure you have completed the steps in "First steps: Installing the z/OS components and beginning the configuration" on page 47 before beginning this procedure.

- If you installed the SA z/OS monitoring agent on a z/OS image that contains no other OMEGAMON products, you must add the runtime environment and then build its libraries. This procedure is described below.
- If you installed the SA z/OS monitoring agent on a z/OS image that already contains another OMEGAMON product, and you want to use an existing runtime environment (rather than creating a new one) to configure the SA z/OS monitoring agent, you do not need to add a runtime environment. Go directly to "Step 2. Build the runtime libraries" on page 64 and continue from there.
- If you have installed preventive service planning (PSP) maintenance for the SA z/OS monitoring agent, browse the PSPHL*vvv* file to see whether it indicates changes to the configuration values for the product. If so, go directly to "Step 4. Configure the monitoring agent" on page 75 and continue from there. If not, go directly to "Step 5. Load the runtime libraries" on page 82 and continue from there.

To define the runtime environment for the SA z/OS monitoring agent, complete the following procedure:

1. On the Configure Products panel (Figure 13), enter 1 (Select product to configure).

```
---------------------------- CONFIGURE PRODUCTS ----------------------------
OPTION ===> 1

 Enter the number to select an option:

    1    Select product to configure

    I    Configuration information
    S    Services and utilities



  F1=Help  F3=Back
```

Figure 13. Configuration Tool: Configure Products panel

The Product Selection Menu is displayed (Figure 14 on page 59), listing the products that are available for configuration.

```
-------------------------- PRODUCT SELECTION MENU --------------------------
COMMAND ===>

Actions: S Select product

  _    IBM Tivoli Monitoring Services on z/OS V6.2.0
  s    IBM Tivoli System Automation for z/OS V3.3.0

F1=Help   F3=Back   F5=Refresh   F7=Up   F8=Down
```

Figure 14. Configuration Tool: Product Selection Menu panel

2. Type S to the left of **IBM Tivoli System Automation for z/OS V3.3.0** and press Enter.

   The Runtime Environments (RTEs) panel is displayed (Figure 15). This panel lists all the runtime environments defined to the Configuration Tool, along with the actions you can perform to create and manage runtime environments.

```
------------------------ RUNTIME ENVIRONMENTS (RTEs) ------------------------
  COMMAND ===>

  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     SAT1      FULL             Full RTE for SYS1.INSTALL.V330.T02
  ---------------------------------------------------------------------------
         SVTBASE1 BASE             Base RTE for the SVT environment
  ---------------------------------------------------------------------------
  Enter=Next  F1=Help  F3=Back  F7=Up  F8=Down
```

Figure 15. Configuration Tool: Runtime Environments (RTEs) panel

3. On the Runtime Environments (RTEs) panel, type A (Add RTE) in the **Action** field beside the first (empty) row and type a name for your new runtime environment in the **Name** field.

   The runtime environment name is a unique identifier of up to 8 characters. It is automatically used as the mid-level qualifier for full and sharing runtime environments. You can optionally specify a mid-level qualifier for base runtime environments.

> **Tips**
>
> If you specify a runtime environment name that is no more than 4 characters long, you can specify the same name for the JCL suffix (used as the suffix of the name of the member that contains the JCL in the INSTJOBS data set). This setup makes it easy to associate the jobs in INSTJOBS with the runtime environment.
>
> When you enter a C (Configure), B (Build), or L (Load) next to a runtime environment that has a previous version of the Tivoli Enterprise Monitoring Server installed, the Configuration Tool prompts you to confirm that you want to migrate to the newer version. A batch migration job completes the upgrade and retains all previously configured values for the Configuration Tool.
---

4. In the **Type** field specify the type of runtime environment being created. If you intend to add sharing runtime environments later on, start by creating either a base or full type.

   Valid RTE types are:

   FULL Allocates both private and base libraries. Use this if only one RTE will be defined for your environment, or if you add an RTE for a unique set of products.

   BASE Allocates base libraries only, and does not execute alone. Use this only in conjunction with sharing RTEs populated with the same products.

   SHARING
   Allocates private libraries only. This type can share base libraries with a base or full RTE populated with the same products, or use SMP/E target libraries for its base libraries. Define one sharing RTE for each z/OS image if you have multiple images.

   Tip

   In most cases, when you are monitoring multiple z/OS images, you should get good results with a sharing-with-base or sharing-with-SMP/E type of runtime environment.

   A base runtime environment is not configurable. For information about the different types of runtime environments, see "Understanding runtime environments" on page 14.

   ---

5. (For *sharing* runtime environments only) In the **Sharing** field specify the name of the base or full runtime environment that this runtime environment obtains its base library information from. If SMP/E target libraries are to be shared, type SMP.

6. In the **Description** field type a description for this runtime environment.

   The description can be any information that is useful for you and others at your site.

7. When you have specified all required values on the Runtime Environments (RTEs) panel, press Enter.

8. This displays the first (Figure 16 on page 61) of two Add Runtime Environment panels (for base runtime environments, there is only one panel). This panel shows the defaults for your system.

   Tip

   If you enter this panel again after specifying values, the high-level qualifiers are locked and cannot be modified. If you need to modify these values, you can unlock them by selecting **Unlock runtime high-level qualifiers** on the Configuration Services and Utilities menu.

```
-------------------- ADD RUNTIME ENVIRONMENT (1 of 2) ------------------------
COMMAND ===>

RTE: RTEname   Type: SHARING Desc: RTE with TEMS

  Libraries   High-level Qualifier       Volser Unit     Storclas Mgmtclas PDSE
  Non-VSAM    hilev                       P2OMG1 3390                       N
  VSAM        hilev                       P2OMG1
  Mid-level qualifier ==> RTEname

  JCL suffix          ==> suffix        Remote RTE for transport ==> N  (Y, N)
  STC prefix          ==> CANS          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      ==> Y  (Y, N)
     If Y, TEMS name    ==> RTEname:CMS                      (Case sensitive)

  Copy configuration values from RTE ==>          (Optional)


 Enter=Next  F1=Help  F3=Back
```

Figure 16. Configuration Tool: Add Runtime Environment (1 of 2) panel

Use the information below to complete this panel.

Non-VSAM libraries

- Type the high-level qualifier.
- Type valid values for your enterprise for either the Volser Unit parameters or the Storclas/Mgmtclas parameters.
- Indicate whether PDSE libraries are to be used.
- PDSEs do not require compression, and are not limited by a predefined number of directory entries. The default of N signifies that PDS libraries are to be used.

    Note: Supply SMS values for libraries specified as PDSEs.

VSAM libraries

- Type the high-level qualifier.
- Type valid values for your enterprise for the Volser Unit or the Storclas/Mgmtclas parameters.

Mid-level qualifier

- For full and sharing RTEs, accept the mid-level qualifier default value (which is the RTE name you previously specified) or specify a unique mid-level qualifier.
- For base RTEs, specify a unique mid-level qualifier or optionally leave this field blank.

JCL suffix

Type a suffix for the JCL. The suffix (up to four characters) is appended to all JCL that is generated in INSTJOBS. The JCL suffix uniquely identifies the batch job members created by the Configuration Tool for this RTE.

STC prefix

For a full or sharing RTE, type a global STC Prefix (from 1–4 characters) to be used in building started task names for products in this RTE, or accept the default value of *CANS*.

Step 1. Define the runtime environment

SYSOUT class / Diagnostic SYSOUT class
Specify values for the non-diagnostic and diagnostic output DDNAMES.

Note: These values were previously hardcoded.

Load optimization
Indicate whether you want to optimize loading of this RTE. The default is N. Refer to the online help (F1) for more details.

Will this RTE have a Tivoli Enterprise Monitoring Server
This applies only to full or sharing RTEs. Specify whether a monitoring server will be configured within this runtime environment. The default of Y allocates Tivoli Enterprise Monitoring Server libraries. Type Y for deployment.

If a monitoring server is to be configured for this runtime environment, you must enter its name. It is used by the other components that need to communicate with this Tivoli Enterprise Monitoring Server. The name of the RTE is used as a default.

Copy configuration values from RTE
This is optional and applies only to full or sharing RTEs. Type the name of an existing RTE that configuration values are copied from and used for this RTE.

This procedure makes an exact copy of the existing runtime environment. If you will not be using the same products in the new runtime environment, do not use this procedure.

For further details of the parameters, press F1 (Help).

9. `12345678901234567890123456789012345678901234567890`
   `install_dir/logs/hostname_ms_timestamp.log`

10. From the Add Runtime Environment (1 of 2) panel, press Enter. This displays the Add Runtime Environment (2 of 2) panel (for full or sharing RTEs only), as shown in Figure 17.

```
------------------- ADD RUNTIME ENVIRONMENT (2 of 2) -----------------------
 COMMAND ===>

 Use z/OS system variables? ==> Y (Y, N)    Use VTAM model applids? ==> N (Y, N)
    RTE name specification       ==> &SYSNAME.
    RTE base alias specification ==>                      n/a
    Applid prefix specification  ==>

 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     ==> CTD       Network ID      ==> Netid
    Logmode table     ==> KDSMTAB1  LU6.2 logmode   ==> CANCTDCS

 If you require TCP/IP communications for this RTE, complete these values:
    Hostname      ==>

    Started task ==>  *       (Recommended default = *)
    Port number  ==>
  Enter=Next  F1=Help  F3=Back
```

Figure 17. Configuration Tool: Add Runtime Environment (2 of 2) panel

Use the following information to complete this panel:

Use z/OS system variables?

Specify Y if this runtime environment will use z/OS system variables.

Security system

You can leave `NONE` as the value of this field, or specify the security system of your choice. You will return to the Configuration Tool later to enable security validation, and you can specify a security system at that time.

VTAM communication values

If you intend to use the SNA communication protocol, supply the name of your network ID in the VTAM section.

- Type a global VTAM applid prefix (of from 1–4 characters) to be used in building the VTAM applids for products in this runtime environment. The default is `CTD`.

- Identify your VTAM network.

- Type the Logmode table name for LU6.2 logmode entries. The default is `KDSMTAB1`.

- Type the LU6.2 logmode for this runtime environment. The default is `CANCTDCS`.

> **Important**
>
> If you do not intend to use SNA, clear the system defaults displayed in the **VTAM** section. Otherwise, you will be required to define SNA as one of your communication protocols during "Step 5. Configure the monitoring agent" on page 98.

TCP/IP communication values

For TCP/IP communications between the monitoring agent and the Tivoli Enterprise Monitoring Server, supply the following information:

Hostname

The TCP/IP host name of the z/OS system where this runtime environment is being added.

> **Tip**
>
> To obtain the host name and IP address values, enter `TSO HOMETEST` at the command line on the z/OS system where this runtime environment is being added.

Started task

The started task name of the TCP/IP server. The default value of ***** (asterisk) allows the IP stack to find the TCP/IP image dynamically, if it is available.

Port number

The address of the IP port. The default is 1918.

11. When you have finished defining your runtime environment, press Enter. This returns you to the Runtime Environments (RTEs) panel (Figure 15 on page 59).

> **Tip**
> Select **View Values** (**V**) to verify the runtime environment information and **Update** (**U**) to make any necessary changes.

12. You must define a runtime environment on each z/OS image where the SA z/OS monitoring agent might be running. Note that only one instance of the monitoring agent is required for monitoring an SA z/OS sysplex.

This completes the creation or addition of your runtime environment.

Step 2. Build the runtime libraries

Complete the following steps to allocate the required runtime libraries:

1. Type B next to the name of the runtime environment that you want to build the libraries for, and press Enter.

   The JCL is displayed for you to review, edit if necessary, and submit. Verify that the job completes successfully and that all return codes are zero.

2. Press F3 to return to the Runtime Environments (RTEs) panel (Figure 15 on page 59).

Step 3. Configure the hub Tivoli Enterprise Monitoring Server

Before you configure SA z/OS monitoring agent, configure the hub Tivoli Enterprise Monitoring Server.

> **Tip**
> If you completed the worksheets in Chapter 2, "Planning your SA z/OS monitoring agent configuration," on page 9, refer to them for the values to supply on the configuration panels.

Configuring the hub Tivoli Enterprise Monitoring Server consists of the following steps:

1. "Beginning the configuration"
2. "Creating a logmode" on page 66
3. "Specifying configuration values" on page 67
4. "Specifying communication protocols" on page 69
5. "Creating the runtime members" on page 74

Beginning the configuration

Perform the following steps to begin the configuration:

1. On the Runtime Environments (RTEs) panel (Figure 15 on page 59), type C (Configure) next to the runtime environment that you want to configure the SA z/OS monitoring agent in .

   This displays the Product Component Selection Menu.

```
---------------------- PRODUCT COMPONENT SELECTION MENU ----------------------
COMMAND ===>

  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   System Automation Monitoring Agent
```

Figure 18. Configuration Tool: Product Component Selection Menu

2. From the Product Component Selection Menu, enter 1 to select Tivoli Enterprise Monitoring Server.

   The Configure the TEMS menu is displayed. There are six options that you must complete to configure the hub Tivoli Enterprise Monitoring Server. These options should be selected in the order shown in the panel.

```
- ------------------- CONFIGURE THE TEMS / RTE: RTEname -----------------------
 OPTION ===>

  Each RTE can contain only one TEMS.  To configure          Last selected
  the TEMS for this RTE, perform these steps in order:       Date     Time

   I  Configuration information (What's New)                  <=== Revised

   1  Create LU6.2 logmode
   2  Specify configuration values                          09/10/05  12:40
   3  Specify communication protocols                       09/10/21  10:11
   4  Create runtime members                                09/10/05  13:03
   5  Configure persistent datastore
   6  Complete the configuration                            09/10/05  13:04

 Optional:

   7  View TEMS list and registration status
   8  Generate sample migration JCL



  F1=Help  F3=Back
```

Figure 19. Configuration Tool: Configure the TEMS menu

> **Tips**
> - Option 5 (**Configure persistent datastore**) on the Configure the TEMS menu is not required for the SA z/OS monitoring agent and is omitted from these instructions.
> - Option 6 (**Complete the configuration**) on the Configure the TEMS menu can be performed for both the Tivoli Enterprise Monitoring Server and the SA z/OS monitoring agent after you configure the monitoring agent. Therefore, the instructions are provided later in this chapter ("Step 6. Complete the configuration of the Tivoli Enterprise Monitoring Server and the monitoring agent" on page 83).

Creating a logmode

To create a logmode, complete the following procedure:

1. From the Configure the TEMS menu (Figure 19 on page 65), enter 1 (Create LU 6.2 logmode).

    This displays the Create LU6.2 Logmode panel (as shown in Figure 20) that lets you specify the name of the LU6.2 logmode and logmode table required by the Tivoli Enterprise Monitoring Server.

```
---------------------------- CREATE LU6.2 LOGMODE ----------------------------
COMMAND ===>

 The TEMS requires an LU6.2 logmode.  Complete the items on this panel and
 press Enter to create a job that will assemble and link the required logmode.

   LU6.2 logmode         ==> CANCTDCS
   Logmode table name    ==> KDSMTAB1

   VTAMLIB load library ==> SYS1.VTAMLIB
   VTAM macro library    ==> SYS1.SISTMAC1
```

Figure 20. Configuration Tool: Create LU6.2 Logmode panel

> **Tip**
>
> If you use an existing LU6.2 logmode, you do not need to submit the job created from this panel. However, you must ensure that the existing logmode has the same VTAM attributes as the logmode contained in the job. Be sure to provide the logmode information, even if you do not intend to submit the job.

2. Review the values in the following fields and specify site-specific values as needed. Use the information below to complete the panel.

    LU6.2 logmode
    > This is the name of the LU6.2 logmode. The default name is CANCTDCS.

    Logmode table name
    > This is the name of the logmode table that contains the LU6.2 logmode. This is required even if you do not submit the JCL job generated by the information that you provide on this panel.

    VTAMLIB load library
    > This is the name of the system library that is used to contain VTAM logmode tables. This is usually SYS1.VTAMLIB. You can specify any load library if you do not want to update your VTAMLIB directly.

    VTAM macro library
    > This is the name of the system library that contains the VTAM macros. This library is usually SYS1.SISTMAC1.

    For the full list of parameters, press F1 (Help).
3. To accept the values, press Enter.

    The JCL to create the logmode is displayed.
4. Review the JCL, edit it if necessary, and submit it. Verify that the job completes successfully and that all return codes are zero.

    You are returned to the Configure the TEMS menu (Figure 19 on page 65).

Specifying configuration values

To specify the configuration values for the Tivoli Enterprise Monitoring Server, complete the following procedure:

1. From the Configure the TEMS menu (Figure 19 on page 65), enter 2 to display the Specify Configuration Values panel.

```
----------------------- SPECIFY CONFIGURATION VALUES -----------------------
COMMAND ===>

 Started task          ==> CANSDSST
 Type (Hub or Remote)  ==> HUB

 Security settings:
   Validate security?  ==> N  (Y, N)

   TMS password encryption information:
     Integrated Cryptographic Service Facility (ICSF) installed? ==> N (Y, N)
       ICSF load library
       ==> CSF.SCSFMOD0
       TMS encryption key
       ==> IBMTivoliMonitoringEncryptionKey


   Program to Program Interface (PPI) information:
     Forward Take Action commands to NetView for z/OS? ==> N (Y, N)
       NetView PPI receiver ==> CNMPCMDR
       TEMS PPI sender       ==>

 Enter=Next  F1=Help  F3=Back  F5=Advanced
```

Figure 21. Configuration Tool: Specify Configuration Values panel

2. Accept the defaults or provide the values appropriate for your site:

   TEMS started task

   This is the name of the started task for the Tivoli Enterprise Monitoring Server. This started task must be copied to your system procedure library. The default is CANSDSST.

   Note: If you have many RTEs on your site, you need to be sure that the name of the started task is unique. Follow the guidelines for your site.

   Hub or Remote?

   Specify whether the Tivoli Enterprise Monitoring Server you are creating is a Hub or a Remote. If this is your first Tivoli Enterprise Monitoring Server, you must define it as a hub.

   Security settings

   Follow these guidelines for the **Security settings** section:

   Validate security?

   Leave the value N. If you set security validation to Y at this point, you will have difficulty completing the configuration steps and verifying the configuration. You can return to this panel and set security validation to Y later, after you set up security for the monitoring server (see Chapter 7, "Setting up security," on page 109).

   Integrated Cryptographic Service Facility (ICSF) installed?

   If the IBM Integrated Cryptographic Service Facility (ICSF) is installed and configured on the z/OS system, set the value to Y.

Step 3. Configure the hub Tivoli Enterprise Monitoring Server

> **Important**
>
> The Tivoli Enterprise Portal Server assumes that the Tivoli Enterprise Monitoring Server is using ICSF encryption. If you set the ICSF value to N, the Tivoli Enterprise Monitoring Server uses an alternative, less secure encryption scheme.
>
> Perform the following steps so that the portal server can connect to a monitoring server without ICSF:
>
> a. When you specify configuration values for the hub monitoring server on z/OS, answer N to the prompt **Integrated Cryptographic Service Facility (ICSF) installed?**
>
> b. After the monitoring server has been configured and is running, modify the portal server configuration to use the older, less robust encoding algorithm used by the hub monitoring server in the absence of ICSF:
>
> > 1) In a text editor, edit the **kfwenv** file in *drive*:\IBM\ITM\CNPS.
> >
> > 2) In a line by itself, type the text USE_EGG1_FLAG=1
> >
> > 3) Save the file and exit.
> >
> > 4) Stop and restart the portal server.

ICSF load library

> If ICSF is installed and configured on the z/OS system, specify the ICSF load library that contains the CSNB* modules used for password encryption.
>
> If ICSF is not installed on the system, clear the field.

TMS encryption key

> Specify a unique, 32-byte password encryption key. Once written to the key file, the encryption key value cannot be changed. The value is case-sensitive.
>
> **Note:** Be sure to document the value you use for the key. You must use the same key during the installation of any components that communicate with this monitoring server.
>
> If ICSF is not installed on the system, clear the field.

The Program to Program Interface (PPI) information section is optional. If desired, specify the PPI values that enable forwarding of Take Action commands to NetView for z/OS for authorization and execution. If you enable forwarding, you must also enable NetView to authorize the commands. See "Setting up NetView authentication of Take Action commands" on page 114.

NetView® PPI receiver:

> Specify the name of the PPI receiver on NetView for z/OS that will receive Take Action commands. This value is required if you specified Y in the **Forward Take Action commands to NetView for z/OS** field.

TEMS PPI sender:

> Specify the optional name of the PPI sender.

For a full description of the parameters, press F1 (Help).

3. Press F5 to display the Specify Advanced Configuration Values panel.

```
------------------ SPECIFY ADVANCED CONFIGURATION VALUES ------------------
COMMAND ===>

   Enable Web Services SOAP Server            ==> Y  (Y, N)
   Enable Tivoli Event Integration Facility (EIF) ==> N (Y, N)
   Enable startup console messages ==> Y  (Y, N)
   Enable communications trace     ==> N  (Y, N, D, M, A)
   Enable storage detail logging   ==> Y  (Y, N)
     Storage detail logging: Hours ==> 0  (0-24)  Minutes ==> 60 (0-60)
     Flush VSAM buffers:     Hours ==> 0  (0-24)  Minutes ==> 30 (0-60)
   Virtual IP Address (VIPA) type  ==> N  (S=Static, D=Dynamic, N=None)
   Minimum extended storage        ==> 150000  K
   Maximum storage request size    ==> 16 (Primary)  ==> 23 (Extended)
   Language locale     ==> 1            (Press F1=Help for a list of codes)

 Persistent datastore parameters:
   Maintenance procedure prefix     ==> KPDPROC
   Datastore file high-level prefix ==> hilev
   Volume  ==> PRI140     Storclas  ==>
   Unit    ==> 3390       Mgmtclas  ==>


 Enter=Next F1=Help F3=Back F5=Advanced F10=CMS List
```

Figure 22. Configuration Tool: Specify Advanced Configuration Values panel

Accept the defaults or specify other values.

Enable Web Services SOAP Server
> Accept the default value of Y. The Web Services SOAP Server is required to be enabled for a hub monitoring server, even though the SA z/OS monitoring agent does not use the SOAP Server. Press F1 for information about the SOAP Server.

Language locale
> This is a required field and has no default. Specify 1 for United States English.

Persistent datastore parameters
> The first two parameters in this section of the panel are required, even though the SA z/OS monitoring agent does not include historical data collection. Accept the default values.

4. Press Enter twice to return to the Configure the TEMS menu (Figure 19 on page 65).

Specifying communication protocols

To specify protocols for communications between the Tivoli Enterprise Monitoring Server and the other components of the SA z/OS monitoring agent, complete the following procedure:

1. From the Configure the TEMS menu, enter 3 to display the Specify Communication Protocols panel.

Step 3. Configure the hub Tivoli Enterprise Monitoring Server

```
--------------------- SPECIFY COMMUNICATION PROTOCOLS ----------------------
 COMMAND ===>

 Specify the communication protocols in priority sequence for
 TEMS RTEname:CMS.

    IP.PIPE   ==> 1  (Non-secure NCS RPC)
    IP.UDP    ==> 2  (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)
    SNA.PIPE  ==> 3  (Non-secure NCS RPC)

 Note:  One of the protocols chosen must be SNA.PIPE.
        * Web Services SOAP Server is enabled: TCP protocol is required.

 Enter=Next  F1=Help  F3=Back
```

Figure 23. Configuration Tool: Specify Communication Protocols panel

This panel lists the communication protocols to be used by the monitoring server. The number beside each protocol indicates its priority. When communication with another component is initiated, the monitoring server tries Protocol 1 first and goes to Protocol 2 and then to Protocol 3 in case of failure.

2. Supply the priority number for each protocol you want to select. SNA.PIPE must be one of the protocols chosen but need not be Protocol 1. At least one of the protocols chosen must match a protocol that you intend to specify for the SA z/OS monitoring agent (see "Communications protocols for a monitoring agent (hub on distributed system)" on page 34).

   IP.PIPE
   > Uses the TCP/IP protocol for underlying communications. The IP.PIPE protocol is generally the best choice for Protocol 1 in firewall environments. It enables the monitoring server to communicate with the portal server on a distributed system, even if both are running behind firewalls.

   IP.UDP
   > Uses the User Datagram Protocol (UDP), a TCP/IP protocol.

   IP6.PIPE
   > Uses the IP.PIPE protocol with IP version 6.

   IP6.UDP
   > Uses the IP.UDP protocol with IP version 6.

   IP.SPIPE
   > Uses the secure IP.PIPE protocol. Requires z/OS version is V1.7 or higher.

   IP6.SPIPE
   > Uses the secure IP.PIPE for IP version 6. Requires z/OS version is V1.7 or higher.

   SNA.PIPE
   > Uses the SNA Advanced Program-To-Program Communications (APPC). Because some zSeries OMEGAMON products require SNA, it must be one of the protocols for the monitoring server on z/OS. However, it need not be Protocol 1 (the highest-priority protocol).

> **Tip**
>
> If your site is using TCP/IP, network services (such as NIS, DNS, and the
> /etc/hosts file) must be configured to return the fully qualified host
> name of the Tivoli Enterprise Monitoring Server and the SA z/OS
> monitoring agent.

3. When you have numbered the protocols, press Enter. You are presented with
   panels for the protocols that you have just specified. Complete the panels and
   press Enter to continue to the panel for the next communication protocol.

   a. **IP.PIPE**

      Figure 24 shows the **Specify IP.PIPE Communication Protocol** panel.

```
------------------- SPECIFY IP.PIPE COMMUNICATION PROTOCOL -------------------
COMMAND ===>

 Specify the IP.PIPE communication values for this TEMS.

 * Network address (Hostname):
      ==>
   Started task            ==> *          (Recommended default = *)
   Network interface list:                (If applicable)
      ==>

 Specify IP.PIPE and Web Services SOAP Server configuration.
   Port number             ==> 1918   (IP.PIPE)
   Port number             ==>        (IP.PIPE for IPV6)
   Port number             ==>        (Secure IP.PIPE)
   Port number             ==>        (Secure IP.PIPE for IPV6)
   HTTP server port number ==> 1920
   Access TEMS list via SOAP Server?   ==> Y (Y, N)
   Address translation     ==> N          (Y, N)
      Partition name       ==>

 * Note: See F1=Help for TSO HOMETEST command instructions.
 Enter=Next  F1=Help  F3=Back
```

Figure 24. Configuration Tool: Specify IP.PIPE Communication Protocol panel

Network address (Hostname)
> The TCP/IP host name of the z/OS system that the Tivoli
> Enterprise Monitoring Server is running on.

> **Tip**
>
> To obtain the host name and IP address values, enter TSO
> HOMETEST at the command line of the z/OS system to be
> monitored.

Started task
> The started task name of the TCP/IP server. The default value of *
> (asterisk) allows the IP stack to find the TCP/IP image dynamically,
> if it is available.

Network interface list
> A list of network interfaces for the monitoring server to use. This
> parameter is required for sites that are running more than one
> TCP/IP interface or network adapter on the same z/OS image.

Step 3. Configure the hub Tivoli Enterprise Monitoring Server

Setting this parameter allows you to direct the monitoring server to connect to a specific TCP/IP local interface.

Specify each network adapter by the host name or IP address to be used for input and output. Use a blank space to separate the entries. If your site supports DNS, you can enter IP addresses or short host names. If your site does not support DNS, you must enter fully qualified host names. If you specify an interface address or a list of interface addresses, the Configuration Tool generates the KDEB_INTERFACELIST parameter in the KDSENV member of the *&rhilev.&rtename*.RKANPARU library.

Port number
The address of the IP port. The default port number is 1918 for nonsecure IP protocols and 3660 for secure IP protocols.

Note: The same TCP/IP port number must be used for every monitoring server in the enterprise. Also make sure that the monitoring server well-known port is not on the TCP/IP reserved port list.

HTTP server port number
Accept the default value of 1920. This field is required but is used only for the SOAP Server, which is not used by the SA z/OS monitoring agent.

Access TEMS list via SOAP Server?
Accept the default value of Y, The Web Services SOAP Server is required to be enabled for a hub monitoring server, even though the SA z/OS monitoring agent does not use the SOAP Server. Press F1 for information about the SOAP Server.

Address translation
Specify Y to configure IP.PIPE support for communication across firewalls using address translation.

By default, Ephemeral Pipe Support (EPS) is enabled automatically to allow IP.PIPE connections to cross a (network address) translating firewall. This feature obviates the need for a broker partition file (KDC_PARTITIONFILE=KDCPART). If you specifically want to disable EPS, specify Y for **Address translation**.

When you press Enter after providing the IP.PIPE configuration values, you are presented with the Specify TEMS KSHXHUBS Values panel.

```
-------------- SPECIFY TEMS KSHXHUBS VALUES / RTE: RTEname ------------------

COMMAND ===>

 Action: Add
   Hub TEMS SOAP Server values for RTEname :
   TEMS name          ==> RTEname:CMS                     (case sensitive)
   Protocol 1         ==> IPPIPE    (IPPIPE,IP,IP6PIPE,IP6,IPSPIPE,IP6SPIPE,SNA)

   TCP hostname       ==>
   TCP port number    ==> 1918

   SNA network ID                   ==>
   SNA global location broker applid  ==>
   SNA LU6.2 logmode                ==>

   Alias name ==> RTEname:CMS
   Note: IBM recommends that the Alias name is the same as the TEMS name.




 Enter=Next F1=Help F3=Back
```

Figure 25. Configuration Tool: Specify TEMS KSHXHUBS Values panel

This panel is displayed if the TEMS that you are adding has not yet been created. All the values are already filled in according to your previous input. Verify these values and provide any missing values. Press Enter to add your new TEMS and display the SOAP Server KSHXHUBS List panel.

```
------------------ SOAP SERVER KSHXHUBS LIST / RTE: RTEname ----- Row 1 from 1
COMMAND ===>

 The following Hub TEMS list is eligible for SOAP Server access.

 RTE: RTEname     Local SOAP Server:  RTEname:CMS

 Actions:    A Add TEMS, U Update TEMS, D Delete TEMS,
             V View TEMS, S Secure TEMS,
             G Grant global security access, C Copy TEMS

      RTE name   TEMS name                         Preferred  TEMS
                                                   protocol   secured
   _   RTEname    RTEname:CMS                       IPPIPE     N

 F1=Help  F3=Back  F7=Up  F8=Down
```

Figure 26. Configuration Tool: SOAP Server KSHXHUBS List panel

This panel lists the hub monitoring servers that are eligible for SOAP Server access. The list is maintained in the KSHXHUBS member of the RKANPAR library. The monitoring server you are configuring is shown on the list. Verify that your newly added TEMS is included.

Press F3 to continue to the next communication protocol configuration panel.

b. **IP.UDP**

The field definitions and instructions for the IP.UDP protocol are the same as those for the IP.PIPE protocol, except that address translation does not apply to IP.UDP.

Press F3 to continue to the next communication protocol configuration panel.

c. **SNA.PIPE**

Step 3. Configure the hub Tivoli Enterprise Monitoring Server

Figure 27 shows the Specify SNA Communication Protocol panel.

```
--------------------- SPECIFY SNA COMMUNICATION PROTOCOL ---------------------
COMMAND ===>

 Specify the SNA communication values for this TEMS.

   Applid prefix        ==> DS
   Network ID           ==>            (NETID value from SYS1.VTAMLST(ATCSTRnn))



 Enter=Next  F1=Help  F3=Back  F6=Applids
```

Figure 27. Configuration Tool: Specify SNA Communication Protocol panel

Applid prefix

This value is used to create the VTAM applids required by the monitoring server. These applids begin with the prefix, and end with a specific value that makes each applid unique. The applids are contained in the VTAM major node.

> **Tip**
>
> Enter README APP on the command line for more information on how the Configuration Tool processes VTAM applids. If System Variable support is enabled, enter README SYS on the command line for more information on how the Configuration Tool processes VTAM applids using z/OS system symbols. Press F6 for a list of the VTAM major node and applid values.

Network ID

The identifier of your VTAM network. You can locate this value on the NETID parameter in the VTAMLST startup member ATCSTR*nn*.

For detailed help about the required values, press F1.

When you press Enter on the last communication protocol panel, you are returned to the Configure the TEMS menu.

Creating the runtime members

To create the runtime members required by Tivoli Enterprise Monitoring Server, complete the following procedure:

1. From the Configure the TEMS menu, enter 4 to display the job that creates the runtime members required by Tivoli Enterprise Monitoring Server. These members are created in the runtime libraries for this runtime environment.
2. Review the JCL, edit if necessary, and submit. Verify that the job completes successfully and that all return codes are zero.
3. When the job finishes, return to the Configure the TEMS menu and then to the Product Component Selection Menu.

> **Tip**
> Even though **Configure persistent datastore** and **Complete the configuration**
> are included in the list of required steps on the Configure the TEMS menu,
> you do not need to perform them now. Option 5 (**Configure persistent
> datastore**) does not apply to the SA z/OS monitoring agent, and Option 6
> (**Complete the configuration**) can be performed for both the Tivoli Enterprise
> Monitoring Server and the SA z/OS monitoring agent after you have
> configured the monitoring agent (see "Step 6. Complete the configuration of
> the Tivoli Enterprise Monitoring Server and the monitoring agent" on page
> 83).

Step 4. Configure the monitoring agent

To configure the SA z/OS monitoring agent to communicate with a hub Tivoli
Enterprise Monitoring Server, complete the following steps:

1. On the Runtime Environments (RTEs) panel (Figure 15 on page 59), type `C`
   (Configure) next to the runtime environment that you want to configure the
   SA z/OS monitoring agent in.

   This displays the Product Component Selection Menu.

```
---------------------- PRODUCT COMPONENT SELECTION MENU ----------------------
COMMAND ===>

 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   System Automation Monitoring Agent
```

Figure 28. Configuration Tool: Product Component Selection Menu

2. From the Product Component Selection Menu, enter 2 to select the System
   Automation Monitoring Agent.

   The Configure IBM Tivoli System Automation for z/OS menu shown in
   Figure 29 on page 76 is displayed.

Step 4. Configure the monitoring agent

```
------ CONFIGURE IBM Tivoli System Automation for z/OS / RTE: RTEname ----------
OPTION ===>
                                                        Last selected
 Perform these configuration steps in order:           Date     Time

 I  Configuration information (What's New)

 1  Specify NetView PPI parameters

 If you have defined a TEMS in this RTE that this Agent
 will communicate with, select option 2.
   2  Register with local TEMS

 3  Specify Agent address space parameters
 4  Create runtime members

 5  Complete the configuration

Note: Press F5=Advanced to configure Agent to runin the TEMS address space.



 F1=Help  F3=Back  F5=Advanced
```

Figure 29. Configuration Tool: Configure IBM Tivoli System Automation for z/OS panel

Perform the following configuration steps in order:

    1. Specify NetView PPI parameters

    2. Register with local TEMS

    3. Specify Agent address space parameters

    4. Create runtime members

Note: You complete the configuration (option 5) later, after completing the other options and then loading the runtime libraries.

3. **Option 1, Specify NetView PPI parameters:**

   From the Configure IBM Tivoli System Automation for z/OS menu, enter 1 to display the Specify Configuration Parameters panel, as shown in Figure 30.

```
---------------------- SPECIFY CONFIGURATION PARAMETERS ----------------------
Command ===>

 Specify the following Program-To-Program Interface (PPI) information:

    NetView Agent PPI Receiver Name      ==> INGAHRCV
    Monitoring Agent PPI Listener Name   ==> KAHNVLIS
    NetView PPI Buffer Size              ==> 1024K
    NetView PPI Timeout                  ==> 60


 Specify the following communication monitoring information:

    Heartbeat Interval      ==> 60
    Check Active Interval   ==> 10


 Enter=Next  F1=Help  F3=Back
```

Figure 30. Configuration Tool: Specify Configuration Parameters panel

You can accept the defaults as shown, or provide the required information:

NetView Agent PPI Receiver Name
        Specify the name of the PPI receiver that processes requests from the SA z/OS monitoring agent within SA z/OS or NetView.

Monitoring Agent PPI Listener Name

Specify the name of a listener that is used by the SA z/OS monitoring agent to listen for events, such as systems that join or leave the automation manager's XCF group.

NetView PPI Buffer Size

Set the PPI buffer size that is used for communication between the SA z/OS monitoring agent and NetView.

NetView PPI Timeout

The interval after which the monitoring agent stops waiting for data from SA z/OS. It is specified in seconds and can be between 1 and 3600. The default interval is 60 seconds.

Heartbeat Interval

The interval used to periodically check for the availability of the SA z/OS automation agent on the local system. The heartbeat interval is specified in seconds and may be set to any value between 1 and 3600. The default interval is 60 seconds.

Check Active Interval

Once a communication problem has been detected, this interval is used to periodically check for the SA z/OS automation agent being restarted for the communication to resume. The check active interval is specified in seconds and may be set to any value between 1 and 3600. The default interval is 10 seconds.

Complete this panel and press Enter to return to the Configure IBM Tivoli System Automation for z/OS panel.

4. **Option 2, Register with local TEMS:**

From the Configure IBM Tivoli System Automation for z/OS panel, enter 2 to produce and display a JCL job that enables the SA z/OS monitoring agent to transmit data to the Tivoli Enterprise Monitoring Server, and allocates and initializes the VSAM file containing the workload definitions for the monitoring agent.

   a. Review the JCL, edit if necessary, and submit. Verify that the job completes successfully. All return codes must be zero.

   b. After the job completes, press F3 to return to the Configure IBM Tivoli System Automation for z/OS panel.

5. **Option 3, Specify Agent address space parameters:**

From the Configure IBM Tivoli System Automation for z/OS panel, enter 3 to display the Specify Agent Address Space Parameters panel, as shown in Figure 31 on page 78.

Step 4. Configure the monitoring agent

```
------------------- SPECIFY AGENT ADDRESS SPACE PARAMETERS ------------------
COMMAND ===>

 The following information is needed to define the Agent address space.
  Agent started task            ==> agent_started_taskname
  Connect to TEMS in this RTE   ==> Y          (Y, N)
     Name of Primary TEMS       ==> RTEname:CMS

 Specify the communication protocols in priority sequence.
     IP.PIPE   ==> 1  (Non-secure NCS RPC)
     IP.UDP    ==> 2  (Non-secure NCS RPC)
     SNA.PIPE  ==> 3  (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.
            IP6.* and *.SPIPE protocols do not apply to this Agent.


 Enter=Next  F1=Help  F3=Back  F5=Advanced  F10=CMS List
```

Figure 31. Configuration Tool: Specify Agent Address Space Parameters panel

a. Provide the required information:

Agent started task
> Supply the started task name for the agent. This started task must be copied to your system procedure library at a later time. The default is CANSAH.

Connect to TEMS in this RTE
> Specify Y for this procedure.

Name of Primary TEMS
> Leave the name of the primary Tivoli Enterprise Monitoring Server blank for now.

Communication protocols
> Specify the communication protocols in priority sequence. When communication with the monitoring server is initiated, the monitoring agent tries Protocol 1 first and goes to Protocol 2 and then to Protocol 3, and so on, in case of failure. Be sure to specify the same protocols that you specified for the monitoring server (see "Installing and configuring the Tivoli Monitoring Services components" on page 85).

> Refer to the online help for a description of the protocols.

Press F5 (Advanced) to display the Specify Advanced Agent Configuration Values panel, as shown in Figure 32 on page 79.

```
---------------- 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            ==> Y  (Y, N)
   Reconnect after TCP/IP recycle  ==> N  (Y, N)
   Intervals (hh:mm):
     Storage detail logging: Hours ==> 0  (0-24)  Minutes ==> 60 (0-60)
     Flush VSAM buffers:     Hours ==> 0  (0-24)  Minutes ==> 30 (0-60)
   Virtual IP Address (VIPA) type  ==> N  (S=Static, D=Dynamic, N=None)
   Minimum extended storage       ==> 150000  K
   Language locale ==> 1           (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 32. Configuration Tool: Specify Advanced Agent Configuration Values panel

Accept the defaults or specify other values.

Language locale
> This is a required field and has no default. Specify 1 for United States English.

The Program to Program Interface (PPI) information section is optional. If desired, specify the PPI values that enable forwarding of Take Action commands to NetView for z/OS for authorization and execution. If you enable forwarding, you must also enable NetView to authorize the commands. See "Setting up NetView authentication of Take Action commands" on page 114.

NetView PPI receiver:
> Specify the name of the PPI receiver on NetView for z/OS that will receive Take Action commands. This value is required if you specified Y in the **Forward Take Action commands to NetView for z/OS** field.

TEMS PPI sender:
> Specify the optional name of the PPI sender.

Press Enter twice.

b. The following panels are displayed where you can specify the configuration values for the communication protocols that you specified in the Specify Agent Address Space Parameters panel.

IP.PIPE, IP6.PIPE, IP.SPIPE
> Uses the TCP/IP protocol for underlying communications. IP.PIPE is the best choice for Protocol 1 in a firewall environment.

Step 4. Configure the monitoring agent

```
----------------- 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 Agents runs on.

* Network address (Hostname):
      ==>
  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 33. Configuration Tool: Specify Agent IP.PIPE Configuration Values panel

Use the information below to complete this panel, which also applies to the IP.PIPE for IPV6 and IP.SPIPE protocols.

Network address (Hostname)
Specify the TCP ID of the z/OS system that the SA z/OS monitoring agent will connect to. To get this value, issue the TSO HOMETEST command and use the first qualifier of the TCP hostname.

Started task
Specify the started task name of TCP that is running on the z/OS system, for example, TCPIP.

Network interface list
A list of network interfaces for the monitoring agent to use. This parameter is required for sites that are running more than one TCP/IP interface or network adapter on the same z/OS image. Setting this parameter allows you to direct the monitoring agent to connect to a specific TCP/IP local interface.

Specify each network adapter by the host name or IP address to be used for input and output. Use a blank space to separate the entries. If your site supports DNS, you can enter IP addresses or short host names. If your site does not support DNS, you must enter fully qualified host names. If you specify an interface address or a list of interface addresses, the Configuration Tool generates the KDEB_INTERFACELIST parameter in the KDSENV member of the *&rhilev.&rtename*.RKANPARU library.

Address translation
Specify Y to configure IP.PIPE support for communication across firewalls using address translation.

By default, Ephemeral Pipe Support (EPS) is enabled automatically to allow IP.PIPE connections to cross a (network address) translating firewall. This feature obviates

the need for a broker partition file
(KDC_PARTITIONFILE=KDCPART). If you specifically want to
disable EPS, specify Y for **Address translation**.

Complete this panel and press Enter to configure the next
communication protocol in your sequence.

IP.UDP
Uses the UDP protocol.

```
------------------ SPECIFY AGENT IP.UDP CONFIGURATION VALUES ------------------
COMMAND ===>

 Specify the IP.UDP communication values for this Agent.

 * Network address (Hostname):
       ==>
   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 34. Configuration Tool: Specify Agent IP.UDP Configuration Values panel

See the description of the "Specify Agent IP.PIPE Configuration
Values panel" on page 80 for details of these communication values.

Complete this panel and press Enter to configure the next
communication protocol in your sequence.

SNA Uses the SNA Advanced Program-To-Program Communications
(APPC).

```
-------------------- SPECIFY AGENT SNA CONFIGURATION VALUES --------------------
COMMAND ===>

 Specify the SNA communication value for this Agent.

   VTAM applid prefix    ==> AH


 Enter=Next  F1=Help  F3=Back  F6=Applids
```

Figure 35. Configuration Tool: Specify Agent SNA Configuration Values panel

Use the information below to complete this panel.

VTAM applid prefix
Specifies the value is used to create all of the VTAM applids
required by the monitoring server. These applids begin with
the prefix, and end with a specific value that makes each
applid unique. These applids are contained in the VTAM
major node.

When you have provided these values, press Enter to save them and return
to the Configure IBM Tivoli System Automation for z/OS panel.

6. **Option 4, Create runtime members:**

   This step creates the runtime members that are required by the SA z/OS monitoring agent. These members are created in the runtime libraries for this RTE.

   From the Configure IBM Tivoli System Automation for z/OS menu, enter 4 (Create runtime members).

   A JCL job is generated and displayed. Review the sample JCL and submit the job. Verify that the job completes successfully with a return code of 0.

7. After the job has completed, press F3 to return to the Configure IBM Tivoli System Automation for z/OS menu.

> **Tip**
>
> Even though **5 Complete the configuration** is an option on the Configure IBM Tivoli System Automation for z/OS menu, you must load the runtime libraries from the SMP/E target libraries *before* you perform the tasks required to complete the configuration.
>
> If you select **Complete the configuration** (option 5 on the Configure IBM Tivoli System Automation for z/OS menu), the Configuration Tool displays a list of the steps you must take outside the Configuration Tool. You can examine and print the list now. Instructions for completing the configuration are in "Step 6. Complete the configuration of the Tivoli Enterprise Monitoring Server and the monitoring agent" on page 83.

Step 5. Load the runtime libraries

Before you complete the configuration of the product outside the Configuration Tool, you must load the runtime libraries from the SMP/E target libraries. The load job requires exclusive access to the runtime libraries.

You must load the runtime libraries after you have done any of the following:
* Installed and configured the products you want in a new RTE
* Installed and configured an additional product in an existing RTE
* Installed maintenance, whether or not you re-configured a product
* Changed the configuration of the SA z/OS monitoring agent

To load the runtime libraries from the SMP/E target libraries, complete the following steps:

1. Go to the Runtime Environments (RTEs) panel (Figure 15 on page 59).
2. Type L in the **Action** field to the left of the runtime environment that you have just configured the SA z/OS monitoring agent in, and press Enter.

   Note: If you are sharing RTEs, you must perform this loading step on both the base RTE and the sharing RTE.

3. If you specified usage of system variables on the Add Runtime Environment (2 of 2) panel (Figure 17 on page 62) you may receive a warning to run the CB#V*xxxx* system variable members job (see Creating the system variable members on page 83). Press Enter to continue with loading the runtime libraries job.
4. Review the JCL and submit the job. Verify that the job completes successfully and that the return code is 04 or less.

5. When you finish loading the libraries, press F3 to return to the Runtime Environments (RTEs) panel.

Step 6. Complete the configuration of the Tivoli Enterprise Monitoring Server and the monitoring agent

To complete the configuration, perform the following steps in the order shown.

1. Copy the started task procedures to your procedure library.

   a. From the Runtime Environments (RTEs) panel (Figure 15 on page 59), enter Z (Utilities) next to your runtime definition to open the RTE Utility Menu, as shown in Figure 36.

```
----------------------- RTE UTILITY MENU / RTE: RTEname -------------------
OPTION ===>

 Specify the number of the desired utility.

   1  Create batch mode parameters
   2* Create System Variable parameter member
   3  Create System Variable VTAM major node rename job
   4  Create VTAM major node (one node for all products)
   5  Generate sample transport JCL
   6  Generate sample system procedure copy JCL
   7  Generate sample system VTAMLST copy JCL
   8  Analyze user modified elements
   9  Create consolidated complete the configuration and README reports
  10  Process Edit subcommands for INSTJOBS or RKANPARU members
  11  Verify configuration and generate parameter map
  12  Upgrade attribute and catalog members


 * Important: After the CB#VSA job runs, review/edit RKANPAR(midlvl)
   See F1=Help topic for more info.: Create System Variable parameter member

 F1=Help  F3=Back
```

Figure 36. Configuration Tool: RTE Utility Menu

   b. On the RTE Utility Menu, enter 6 to display the **Generate sample system procedure copy JCL** panel.

   c. Type the name of your procedure library (for example, USER.PROCLIB). Press Enter.

   d. The JCL is displayed for you to review, edit if necessary, and submit. Verify that the job completes successfully and that all return codes are zero.

   This job creates a member called KCISYPJB in the RKANSAMU library.

   e. Edit KCISYPJB and submit the job. Verify that the job completes successfully and that all return codes are zero.

   This job copies all the required started tasks from your RKANSAMU library to the specified procedure library. The code contains the names of all the started tasks that were created during configuration.

2. Create the system variable members.

   If you have enabled system variable support, you must run the CB#V*xxxx* system variable members job to create the system variable parameter member and other components.

   Note: If a new product is added to the RTE or an existing product is reconfigured to change any of the system variable values, rerun the CB#V*xxxx* job.

Step 6. Complete the configuration

3. Copy the VTAM definitions to your SYS1.VTAMLST.

   Note: This step is only applicable if system variables mode has been *disabled*.

   Even if you have not configured the monitoring agent to use SNA, the Tivoli Enterprise Monitoring Server on z/OS requires SNA as one of its communication protocols, so you must copy the VTAM definitions from your Tivoli Enterprise Monitoring Server configuration to SYS1.VTAMLST.

   a. On the RTE Utility Menu, enter 7 to display the **Generate sample system VTAMLST copy JCL** panel.

   b. Type the name of your VTAM major node and press Enter.

   c. The JCL is displayed for you to review, edit if necessary, and submit. Verify that the job completes successfully and that all return codes are zero.

   This job creates a member called KCISYNJB in the RKANSAMU library.

   d. Edit KCISYNJB and submit the job. Verify that the job completes successfully and that all return codes are zero.

   This job copies all the required VTAM definitions from your RKANSAMU library to the specified VTAMLST.

4. Vary the VTAM major node active. For example:

   `V NET,ACT,ID=CTDDSN`

5. APF-authorize the runtime load libraries.

   These are concatenated in the STEPLIB DDNAME and in the RKANMODL DDNAME of the CANSAH started task. Ask your security administrator to grant the appropriate authorizations.

6. Verify successful installation and configuration.

   a. Start the started tasks for the Tivoli Enterprise Monitoring Server and the SA z/OS monitoring agent.

   b. Verify successful startup.

      1) In the RKLVLOG for the monitoring server address space, look for the following messages to indicate successful startup:

         ```
         KDSMA001 Tivoli Enterprise Monitoring Server (TEMS) data collection server started.
         KO4SRV032 Tivoli Enterprise Monitoring Server (TEMS) startup complete.
         ```

      2) Look also for the following messages to indicate successful establishment of a communications path by local and global location brokers:

         ```
         KDSNC004 Bind of local location broker complete= protocol_name:address
         KDSNC004 Bind of global location broker complete= protocol_name:address
         ```

      3) In the RKLVLOG for the monitoring agent address space, look for the following message to indicate successful startup:

         ```
         KAHM024I SYSTEM AUTOMATION MONITORING AGENT VERSION V310 (BUILD LEVEL level) HAS STARTED
         ```

      If you do not find these messages, review the steps performed and look for errors. If you need assistance, see Part 4, "Problem determination," on page 187.

Step 7. Install the Tivoli Enterprise Portal Server and client on a Windows workstation

In this step, you install at least one Tivoli Enterprise Portal Server for each hub Tivoli Enterprise Monitoring Server. You can connect more than one Tivoli Enterprise Portal Server to a hub Tivoli Enterprise Monitoring Server, for example, to provide a test environment and a production environment.

Install only the Tivoli Enterprise Portal Server and desktop client components. You do not need to install Tivoli Enterprise Monitoring Server on the Windows system, because you have already installed and configured it on a z/OS system. If you plan to install the hub Tivoli Enterprise Monitoring Server on Windows, UNIX, or Linux, see Chapter 6, "Configuring the hub monitoring server on a Windows system and the monitoring agent on a z/OS image," on page 89.

The instructions assume that the operating system on the workstation is Windows XP Professional Edition with Service Pack 1. For complete information about hardware and software requirements for the Tivoli Monitoring Services components, and for instructions for installing and configuring the components on a UNIX system, see the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Installing the DB2 Universal Database software

Tivoli Enterprise Portal Server requires DB2 Universal Database (DB2 UDB) Workgroup Server Edition. DB2 UDB is provided in the Tivoli Monitoring Services installation package. If DB2 UDB is already installed on the workstation where you plan to install a Tivoli Enterprise Portal Server, you can skip this procedure and go directly to "Installing and configuring the Tivoli Monitoring Services components."

For more details about installing DB2 Workgroup Server Edition, see the relevant documentation in the DB2 Information Center for the version of DB2 that you are installing at:
http://www.ibm.com/support/docview.wss?rs=71&uid=swg27009474

> **Important**
>
> DB2 UDB requires the user name and password for all administrative tasks, including installation and configuration of the Tivoli Enterprise Portal Server.
>
> - If the Local Security Settings on the Windows system require complex or long passwords, use a password that fits the requirements. For information about Local Security Settings and password complexity, see the Windows system help.
> - If you change the **db2admin** password after DB2 UDB installation, you receive error messages when you try to install the Tivoli Enterprise Portal Server. If your Local Security Settings require you to change the password, wait to do so until you finish installing the Tivoli Enterprise Portal Server. See Part 4, "Problem determination," on page 187 for troubleshooting information.

Installing and configuring the Tivoli Monitoring Services components

You must install the following features on a Windows workstation where DB2 UDB is already installed and running:
- Tivoli Enterprise Monitoring Agent framework
- Tivoli Enterprise Portal Server framework
- Tivoli Enterprise Portal desktop client
- IBM Eclipse Help Server

For more information about installing and configuring the Tivoli Monitoring Services components, see the IBM Tivoli Monitoring *Installation and Setup Guide*.

Step 7. Install the Tivoli Enterprise Portal Server and client on a Windows workstation

---

> **Tips**
>
> Be aware of the following details as you perform the installation:
>
> 1. The initial user ID **sysadmin** cannot be changed. You can add other user IDs after installation. For details, see the Tivoli Enterprise Portal online help or *IBM Tivoli Monitoring: Administrator's Guide*.
>
> 2. To have one less password to remember, you can use the same password for the **db2admin** account and the Tivoli Enterprise Portal Server database user account (**TEPS**). If the Local Security Settings on the Windows system require complex passwords (passwords that require both alphabetic and numeric characters), use a password that fits the requirements.
>
>   For information about Local Security Settings and password complexity, see the Windows system help. See Part 4, "Problem determination," on page 187 for Tivoli Enterprise Portal troubleshooting information.
>
> 3. Remember to start the DB2 instance before you configure the Tivoli Enterprise Portal or you will see an **Error** window. Start the DB2 instance, click **OK** and in the next window click **Retry**.

Step 8. Install SA z/OS application support

Product-specific application support data is required by distributed IBM Tivoli Monitoring components and by the hub Tivoli Enterprise Monitoring Server (on any platform).

To install SA z/OS application support, follow this procedure:

1. Ensure that the hub Tivoli Enterprise Monitoring Server is running.
2. The application support data is supplied as a Web download. Download either the compressed (.zip) or ISO file.
   a. If you have downloaded the compressed file, extract it and run `setup.exe` from the resulting folder.
   b. If you have downloaded the ISO file, create a CD with it. Insert the CD into the CD-ROM drive of the Windows workstation that hosts the Tivoli Enterprise Portal Server and desktop client.

      Installation begins automatically. If the installer does not start, go to the CD drive and run `setup.exe`.

   If `setup.exe` initialization fails, you do not have enough disk space to extract the setup files.
3. Read the text that welcomes you to the installation, and click **Next** to continue.
4. Read the license agreement and click **Accept**.
5. If necessary, specify the path to the directory where you installed the IBM Tivoli Monitoring components, and the path to the location of the application support data files that are to be installed.
6. In the Select Features window, select System Automation for z/OS Support for these components:
   - Tivoli Enterprise Monitoring Server
   - Tivoli Enterprise Portal Server
   - Tivoli Enterprise Portal desktop client

7. Click **Next** to continue.
8. Read the list of actions to be performed, and click **Next**.

   Application support for SA z/OS is installed on the IBM Tivoli Monitoring components that you selected.
9. When you see **Installation completed successfully**, click **Finish** to exit the installation program.
10. Add application support to the hub Tivoli Enterprise Monitoring Server on z/OS.

    a. On the Windows workstation, select **Start > Programs** (or **All Programs**) > **IBM Tivoli Monitoring > Manage Tivoli Monitoring Services**.

    b. Select **Actions > Advanced > Add TEMS application support**.

    c. In the Add application support to the TEMS window, select **On a different computer** and click **OK**.

    d. When you are prompted to ensure that the Tivoli Enterprise Monitoring Server is configured and running, click **OK**.

    e. In the Non-Resident TEMS Connection window, provide the hub monitoring server node ID (TEMS name) and select the communication protocol to use in sending the application support to the hub monitoring server on z/OS.

       You can find the Node ID as the value of the CMS_NODEID variable in this location:

       `&rhilev.&rte.RKANPARU(KDSENV)`

    f. In the next window, provide any values required by the communication protocol. For example, if the protocol is IP.PIPE, you are prompted for the fully qualified TCP/IP host name and port number of the z/OS system where the hub Tivoli Enterprise Monitoring Server resides.

    g. On the **Select the application support to add to the TEMS** window, select IBM Tivoli System Automation for z/OS V3R3, and click **OK**.

    h. When the application support has been added to the monitoring server (this might take several minutes), a window gives you information about seeding status and seed data location. Click **Save As** if you want to save the information in a text file. Click **Close** to close the window.

    i. Stop and restart the hub Tivoli Enterprise Monitoring Server.

Step 9. Verify the configuration

Now that you have completed the configuration, you can verify that it is successful. Verification involves starting these components:

- Tivoli Enterprise Monitoring Server and monitoring agent started tasks on your z/OS system
- Tivoli Enterprise Portal Server through Manage Tivoli Monitoring Services on your workstation
- Tivoli Enterprise Portal desktop client through Manage Tivoli Monitoring Services on your workstation

To do this, complete the following procedure:

1. Start the started tasks for the hub Tivoli Enterprise Monitoring Server and the SA z/OS monitoring agent, /S *taskname*, and check both logs for any errors.
2. On your workstation, select **Start > Programs** (or **All Programs**) > **IBM Tivoli Monitoring > Manage Tivoli Monitoring Services**.

3. To start the Tivoli Enterprise Portal Server, right-click its entry in Manage Tivoli Monitoring Services and click **Start**.

4. To start the Tivoli Enterprise Portal desktop client, right-click its entry in Manage Tivoli Monitoring Services and click **Start**.

5. When prompted, supply the user ID sysadmin and the password you specified for initial access to the Tivoli Enterprise Portal Server

6. When the Tivoli Enterprise Portal opens, you can expand the navigator pane to see the SA z/OS monitoring agent workspaces.

   For information about using the SA z/OS monitoring agent workspaces and situations to monitor your sysplex resources and z/OS systems, see the online help and Part 3, "User's guide," on page 135 section.

Setting up security

Now you can set up security for the product components. See Chapter 7, "Setting up security," on page 109.

Expanding your configuration

After you configure the hub Tivoli Enterprise Monitoring Server and a SA z/OS monitoring agent in different address spaces of the same z/OS image, you can add agents in other z/OS images that you want to monitor. These additional agents are called *remote agents* because they are not on the same z/OS image as the hub Tivoli Enterprise Monitoring Server. To add remote monitoring agents, complete the following steps:

__ "Step 1. Define the runtime environment" on page 58

   In this step, answer N for **this RTE have a Tivoli Enterprise Monitoring Server** on the Add Runtime Environment panel.

__ "Step 2. Build the runtime libraries" on page 64

   You can skip Step 3 (Configure the hub Tivoli Enterprise Monitoring Server) because all the SA z/OS monitoring agent monitoring agents can communicate with the same hub Tivoli Enterprise Monitoring Server.

__ "Step 4. Configure the monitoring agent" on page 75

   1. Register the remote monitoring agents with the hub Tivoli Enterprise Monitoring Server on the z/OS image where the hub is installed, not on the z/OS image where the monitoring agent is installed.

   2. To configure a remote monitoring agent, follow the instructions in "Step 4. Configure the monitoring agent" on page 75.

__ "Step 5. Load the runtime libraries" on page 82

__ "Step 6. Complete the configuration of the Tivoli Enterprise Monitoring Server and the monitoring agent" on page 83

__ "Step 9. Verify the configuration" on page 87

Batch mode processing

The Configuration Tool offers batch mode processing for several configuration scenarios. You can use the batch mode processing utility to configure runtime environments and monitoring agents without going through the ISPF panels and filling in parameter values there. After you establish and configure a runtime environment in a z/OS image, you can use the batch mode processing utility to replicate your runtime environment in other z/OS images. See Chapter 9, "Using batch mode processing," on page 125.

Chapter 6. Configuring the hub monitoring server on a Windows system and the monitoring agent on a z/OS image

This procedure describes the steps to follow in configuring the hub Tivoli Enterprise Monitoring Server on Windows, and the SA z/OS monitoring agent in a z/OS image, as shown in Figure 37.
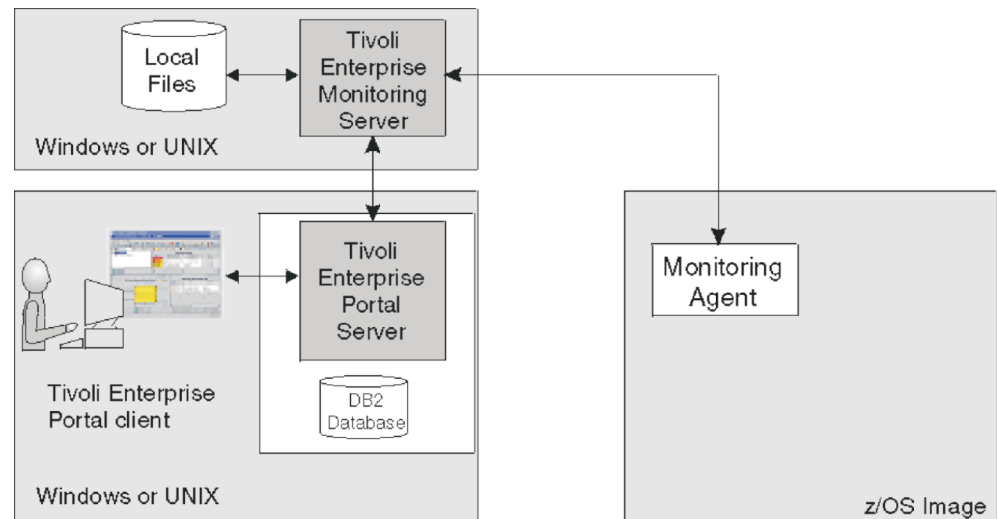
Figure 37. Hub Tivoli Enterprise Monitoring Server on a distributed system and monitoring agent on a z/OS system

For this deployment, you install and configure the hub Tivoli Enterprise Monitoring Server on a distributed system. You then configure a monitoring agent on each z/OS system that you want to monitor, with all monitoring agents defined to communicate with the hub Tivoli Enterprise Monitoring Server. Note that to monitor the automation resources in an sysplex, only one monitoring agent is required although others might be configured as optional secondary agents that are started if the primary agent fails. The configuration can be expanded by adding remote monitoring servers and monitoring agents.

Configuration steps

To configure the product, complete the following steps in order:
- "Step 1. Install the required Tivoli Monitoring Services components" on page 90
- "Step 2. Install SA z/OS application support" on page 91
- "Step 3. Define the runtime environment" on page 92
- "Step 4. Build the runtime libraries" on page 97
- "Step 5. Configure the monitoring agent" on page 98
- "Step 6. Load the runtime libraries" on page 105
- "Step 7. Complete the configuration of the monitoring agent" on page 105
- "Step 8. Verify the configuration" on page 107

Step 1. Install the required Tivoli Monitoring Services components

In this step, you install the hub Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal desktop client on a single Windows workstation. If you decide to install these components on different workstations, install them in this order:

1. Tivoli Enterprise Monitoring Server
2. Tivoli Enterprise Portal Server
3. Tivoli Enterprise Portal desktop client

These instructions assume that the operating system on the workstation is Windows XP Professional Edition with Service Pack 1. For complete information about hardware and software requirements for the Tivoli Monitoring Services components, and for instructions for installing and configuring the components on a Linux or UNIX system, see the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Installing the DB2 Universal Database software

Tivoli Enterprise Portal Server requires DB2 Universal Database (DB2 UDB) Workgroup Server Edition. DB2 UDB is provided in the Tivoli Monitoring Services installation package. If DB2 UDB is already installed on the workstation where you plan to install a Tivoli Enterprise Portal Server, you can skip this procedure and go directly to "Installing and configuring the Tivoli Monitoring Services components."

For more details about installing DB2 Workgroup Server Edition, see the relevant documentation in the DB2 Information Center for the version of DB2 that you are installing at:
http://www.ibm.com/support/docview.wss?rs=71&uid=swg27009474

> **Important**
>
> DB2 UDB requires the user name and password for all administrative tasks, including installation and configuration of the Tivoli Enterprise Portal Server.
>
> - If the Local Security Settings on the Windows system require complex or long passwords, use a password that fits the requirements. For information about Local Security Settings and password complexity, see the Windows system help.
>
> - If you change the **db2admin** password after DB2 UDB installation, you receive error messages when you try to install the Tivoli Enterprise Portal Server. If your Local Security Settings require you to change the password, wait to do so until you finish installing the Tivoli Enterprise Portal Server. See Part 4, "Problem determination," on page 187 for troubleshooting information.

Installing and configuring the Tivoli Monitoring Services components

You must install the following features on a Windows workstation where DB2 UDB is already installed and running:
- Tivoli Enterprise Monitoring Agent framework
- Tivoli Enterprise Monitoring Server
- Tivoli Enterprise Portal Server framework
- Tivoli Enterprise Portal desktop client
- IBM Eclipse Help Server

Step 1. Install the required Tivoli Monitoring Services components

| For more information about installing and configuring the Tivoli Monitoring
| Services components, see the IBM Tivoli Monitoring *Installation and Setup Guide*.

> **Tips**
>
> Be aware of the following details as you perform the installation:
>
> 1. The initial user ID **sysadmin** cannot be changed. You can add other user IDs after installation. For details, see the Tivoli Enterprise Portal online help or *IBM Tivoli Monitoring: Administrator's Guide*.
>
> 2. To have one less password to remember, you can use the same password for the **db2admin** account and the Tivoli Enterprise Portal Server database user account (**TEPS**). If the Local Security Settings on the Windows system require complex passwords (passwords that require both alphabetic and numeric characters), use a password that fits the requirements.
>
>   For information about Local Security Settings and password complexity, see the Windows system help. See Part 4, "Problem determination," on page 187 for Tivoli Enterprise Portal troubleshooting information.
>
> 3. Remember to start the DB2 instance before you configure the Tivoli Enterprise Portal or you will see an **Error** window. Start the DB2 instance, click **OK** and in the next window click **Retry**.

Step 2. Install SA z/OS application support

Product-specific application support data is required by distributed IBM Tivoli Monitoring components and by the hub Tivoli Enterprise Monitoring Server (on any platform).

To install SA z/OS application support, follow this procedure:

1. Ensure that the hub Tivoli Enterprise Monitoring Server is running.

2. The application support data is supplied as a Web download. Download either the compressed (.zip) or ISO file.

   a. If you have downloaded the compressed file, extract it and run `setup.exe` from the resulting folder.

   b. If you have downloaded the ISO file, create a CD with it. Insert the CD into the CD-ROM drive of the Windows workstation that hosts the Tivoli Enterprise Portal Server and desktop client.

      Installation begins automatically. If the installer does not start, go to the CD drive and run `setup.exe`.

   If `setup.exe` initialization fails, you do not have enough disk space to extract the setup files.

3. Read the text that welcomes you to the installation, and click **Next** to continue.

4. Read the license agreement and click **Accept**.

5. If necessary, specify the path to the directory where you installed the IBM Tivoli Monitoring components, and the path to the location of the application support data files that are to be installed.

6. In the Select Features window, select System Automation for z/OS Support for these components:

   • Tivoli Enterprise Monitoring Server
   • Tivoli Enterprise Portal Server

Step 2. Install SA z/OS application support

- Tivoli Enterprise Portal desktop client

7. Click **Next** to continue.

8. Read the list of actions to be performed, and click **Next**.

   Application support for SA z/OS is installed for the IBM Tivoli Monitoring components that you selected.

9. When you see **Installation completed successfully**, click **Finish** to exit the installation program.

Step 3. Define the runtime environment

In this step you define the runtime environment for configuring the SA z/OS monitoring agent.

> **Tip**
>
> Be sure you have completed the steps in "First steps: Installing the z/OS components and beginning the configuration" on page 47 before beginning this procedure.

- If you installed the SA z/OS monitoring agent on a z/OS image that contains no other OMEGAMON products, you must add the runtime environment and then build its libraries. This procedure is described below.

- If you installed the SA z/OS monitoring agent on a z/OS image that already contains another OMEGAMON product, and you want to use an existing runtime environment (rather than creating a new one) to configure the SA z/OS monitoring agent, you do not need to add a runtime environment. Go directly to "Step 4. Build the runtime libraries" on page 97 and continue from there.

- If you have installed preventive service planning (PSP) maintenance for the SA z/OS monitoring agent, browse the PSPHL*vvv* file to see whether it indicates changes to the configuration values for the product. If so, go directly to "Step 5. Configure the monitoring agent" on page 98 and continue from there. If not, go directly to "Step 6. Load the runtime libraries" on page 105 and continue from there.

To define the runtime environment for the SA z/OS monitoring agent, complete the following procedure:

1. On the Configure Products panel, enter 1 (Select product to configure).

```
---------------------------- CONFIGURE PRODUCTS ----------------------------
OPTION ===> 1

 Enter the number to select an option:

    1    Select product to configure

    I    Configuration information
    S    Services and utilities



 F1=Help  F3=Back
```

Figure 38. Configuration Tool: Configure Products panel

The Product Selection Menu is displayed, listing the products that are available for configuration.

```
--------------------------- PRODUCT SELECTION MENU --------------------------
COMMAND ===>

Actions: S Select product

_    IBM Tivoli Monitoring Services on z/OS V6.2.0
s    IBM Tivoli System Automation for z/OS V3.3.0

F1=Help   F3=Back   F5=Refresh   F7=Up   F8=Down
```

Figure 39. Configuration Tool: Product Selection Menu panel

2. Type S to the left of **IBM Tivoli System Automation for z/OS V3.3.0** and press Enter.

   The Runtime Environments (RTEs) panel is displayed. This panel lists all the runtime environments defined to the Configuration Tool, along with the actions you can perform to create and manage runtime environments.

```
----------------------- RUNTIME ENVIRONMENTS (RTEs) ------------------------
  COMMAND ===>

  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     SAT1     FULL             Full RTE for SYS1.INSTALL.V330.T02
-------------------------------------------------------------------------------
        SVTBASE1 BASE             Base RTE for the SVT environment
-------------------------------------------------------------------------------
Enter=Next  F1=Help  F3=Back  F7=Up  F8=Down
```

Figure 40. Configuration Tool: Runtime Environments (RTEs) panel

3. On the Runtime Environments (RTEs) panel, type A (Add RTE) in the **Action** field beside the first (empty) row and type a name for your new runtime environment in the **Name** field.

   The runtime environment name is a unique identifier of up to 8 characters. It is automatically used as the mid-level qualifier for full and sharing runtime environments. You can optionally specify a mid-level qualifier for base runtime environments.

4. In the **Type** field specify the type of runtime environment being created. If you intend to add sharing runtime environments later on, start by creating either a base or full type.

   Valid RTE types are:

   FULL Allocates both private and base libraries. Use this if only one RTE will be defined for your environment, or if you add an RTE for a unique set of products.

   BASE Allocates base libraries only, and does not execute alone. Use this only in conjunction with sharing RTEs populated with the same products.

   SHARING
           Allocates private libraries only. This type can share base libraries with a base or full RTE populated with the same products, or use SMP/E target libraries for its base libraries. Define one sharing RTE for each z/OS image if you have multiple images.

Step 3. Define the runtime environment

> **Tip**
>
> In most cases, when you are monitoring multiple z/OS images, you should get good results with a sharing-with-base or sharing-with-SMP/E type of runtime environment.
>
> A base runtime environment is not configurable. For information about the different types of runtime environments, see "Understanding runtime environments" on page 14.

5. (For *sharing* runtime environments only) In the **Sharing** field specify the name of the base or full runtime environment that this runtime environment obtains its base library information from. If SMP/E target libraries are to be shared, type SMP.

6. In the **Description** field type a description for this runtime environment.

   The description can be any information that is useful for you and others at your site.

7. When you have specified all required values on the Runtime Environments (RTEs) panel, press Enter.

8. This displays the first of two Add Runtime Environment panels (for base runtime environments, there is only one panel). This panel shows the defaults for your system.

> **Tip**
>
> If you enter this panel again after specifying values, the high-level qualifiers are locked and cannot be modified. If you need to modify these values, you can unlock them by selecting **Unlock runtime high-level qualifiers** on the Configuration Services and Utilities menu.

```
---------------------- ADD RUNTIME ENVIRONMENT (1 of 2) ----------------------
COMMAND ===>

RTE: RTEname       Type: SHARING Desc: RTE with TEMS

  Libraries  High-level Qualifier      Volser Unit     Storclas Mgmtclas PDSE
  Non-VSAM   hilev                     P2OMG1 3390                       N
  VSAM       hilev                     P2OMG1
  Mid-level qualifier ==> RTEname

  JCL suffix          ==> suffix
  STC prefix          ==> CANS
  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 41. Configuration Tool: Add Runtime Environment (1 of 2) panel

Use the information below to complete this panel.

Non-VSAM libraries
- Type the high-level qualifier.
- Type valid values for your enterprise for either the Volser Unit parameters or the Storclas/Mgmtclas parameters.
- Indicate whether PDSE libraries are to be used.
- PDSEs do not require compression, and are not limited by a predefined number of directory entries. The default of N signifies that PDS libraries are to be used.

   Note: Supply SMS values for libraries specified as PDSEs.

VSAM libraries
- Type the high-level qualifier.
- Type valid values for your enterprise for the Volser Unit or the Storclas/Mgmtclas parameters.

Mid-level qualifier
- For full and sharing RTEs, accept the mid-level qualifier default value (which is the RTE name you previously specified) or specify a unique mid-level qualifier.
- For base RTEs, specify a unique mid-level qualifier or optionally leave this field blank.

JCL suffix
   Type a suffix for the JCL. The suffix (up to four characters) is appended to all JCL that is generated in INSTJOBS. The JCL suffix uniquely identifies the batch job members created by the Configuration Tool for this RTE.

STC prefix
   For a full or sharing RTE, type a global STC Prefix (from 1–4 characters) to be used in building started task names for products in this RTE, or accept the default value of *CANS*.

SYSOUT class / Diagnostic SYSOUT class
   Specify values for the non-diagnostic and diagnostic output DDNAMES.

   Note: These values were previously hardcoded.

Load optimization
   Indicate whether you want to optimize loading of this RTE. The default is N. Refer to the online help (F1) for more details.

Will this RTE have a Tivoli Enterprise Monitoring Server
   This applies only to full or sharing RTEs. Specify whether a monitoring server will be configured within this runtime environment. The default of Y allocates Tivoli Enterprise Monitoring Server libraries.

   For this procedure, type N because no monitoring server will be configured for this runtime environment.

Copy configuration values from RTE
   This is optional and applies only to full or sharing RTEs. Type the name of an existing RTE that configuration values are copied from and used for this RTE.

Step 3. Define the runtime environment

This procedure makes an exact copy of the existing runtime environment. If you will not be using the same products in the new runtime environment, do not use this procedure.

For further details of the parameters, press F1 (Help).

9. From the Add Runtime Environment (1 of 2) panel, press Enter. This displays the Add Runtime Environment (2 of 2) panel (for full or sharing RTEs only).

```
-------------------- ADD RUNTIME ENVIRONMENT (2 of 2) -----------------------
 COMMAND ===>

 Use z/OS system variables? ==> Y (Y, N)    Use VTAM model applids? ==> N (Y, N)
    RTE name specification      ==> &SYSNAME.
    RTE base alias specification ==>                     n/a
    Applid prefix specification  ==>

 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     ==> CTD       Network ID     ==> Netid
    Logmode table     ==> KDSMTAB1  LU6.2 logmode  ==> CANCTDCS

 If you require TCP/IP communications for this RTE, complete these values:
   Hostname      ==>

   Started task ==>  *      (Recommended default = *)
   Port number  ==>
 Enter=Next  F1=Help  F3=Back
```

Figure 42. Configuration Tool: Add Runtime Environment (2 of 2) panel

Use the following information to complete this panel:

Use z/OS system variables?
Specify Y if this runtime environment will use z/OS system variables.

Security system
You can leave NONE as the value of this field, or specify the security system of your choice. You will return to the Configuration Tool later to enable security validation, and you can specify a security system at that time.

VTAM communication values
If you intend to use the SNA communication protocol, supply the name of your network ID in the VTAM section.

- Type a global VTAM applid prefix (of from 1–4 characters) to be used in building the VTAM applids for products in this runtime environment. The default is CTD.
- Identify your VTAM network.
- Type the Logmode table name for LU6.2 logmode entries. The default is KDSMTAB1.
- Type the LU6.2 logmode for this runtime environment. The default is CANCTDCS.

> **Important**
>
> If you do not intend to use SNA, clear the system defaults displayed in the **VTAM** section. Otherwise, you will be required to define SNA as one of your communication protocols during "Step 5. Configure the monitoring agent" on page 98.

TCP/IP communication values

For TCP/IP communications between the monitoring agent and the Tivoli Enterprise Monitoring Server, supply the following information:

Hostname

The TCP/IP host name of the z/OS system where this runtime environment is being added.

> **Tip**
>
> To obtain the host name and IP address values, enter TSO HOMETEST at the command line on the z/OS system where this runtime environment is being added.

Started task

The started task name of the TCP/IP server. The default value of * (asterisk) allows the IP stack to find the TCP/IP image dynamically, if it is available.

Port number

The address of the IP port. The default is 1918.

10. When you have finished defining your runtime environment, press Enter. This returns you to the Runtime Environments (RTEs) panel (Figure 40 on page 93).

> **Tip**
>
> Select **View Values** (**V**) to verify the runtime environment information and **Update** (**U**) to make any necessary changes.

11. You must define a runtime environment on each z/OS image where the SA z/OS monitoring agent might be running. Note that only one instance of the monitoring agent is required for monitoring an SA z/OS sysplex.

This completes the creation or addition of your runtime environment.

Step 4. Build the runtime libraries

Complete the following steps to allocate the required runtime libraries:

1. Type B next to the name of the runtime environment that you want to build the libraries for, and press Enter.

   The JCL is displayed for you to review, edit if necessary, and submit. Verify that the job completes successfully and that all return codes are zero.

2. Press F3 to return to the Runtime Environments (RTEs) panel (Figure 40 on page 93).

Step 5. Configure the monitoring agent

To configure the SA z/OS monitoring agent to communicate with a hub Tivoli Enterprise Monitoring Server, complete the following steps:

1. On the Runtime Environments (RTEs) panel (Figure 40 on page 93), type C (Configure) next to the runtime environment that you want to configure the SA z/OS monitoring agent in.

   This displays the Product Component Selection Menu.

```
---------------------- PRODUCT COMPONENT SELECTION MENU ----------------------
COMMAND ===>

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   System Automation Monitoring Agent
```

Figure 43. Configuration Tool: Product Component Selection Menu

2. From the Product Component Selection Menu, enter 2 to select the System Automation Monitoring Agent.

   The Configure IBM Tivoli System Automation for z/OS menu shown in Figure 44 is displayed.

```
------ CONFIGURE IBM Tivoli System Automation for z/OS / RTE: RTEname ----------
OPTION ===>

                                                    Last selected
Perform these configuration steps in order:          Date     Time

 I  Configuration information (What's New)

 1  Specify NetView PPI parameters

If you have defined a TEMS in this RTE that this Agent
will communicate with, select option 2.
   2  Register with local TEMS

 3  Specify Agent address space parameters
 4  Create runtime members

 5  Complete the configuration

Note: Press F5=Advanced to configure Agent to runin the TEMS address space.



 F1=Help  F3=Back  F5=Advanced
```

Figure 44. Configuration Tool: Configure IBM Tivoli System Automation for z/OS panel

Perform the following configuration steps in order:

   1. Specify NetView PPI parameters

   3. Specify Agent address space parameters

   4. Create runtime members

Note: You complete the configuration (option 5) later, after completing options 1, 3 and 4, and then loading the runtime libraries.

3. **Option 1, Specify NetView PPI parameters:**

   From the Configure IBM Tivoli System Automation for z/OS menu, enter 1 to display the Specify Configuration Parameters panel, as shown in Figure 45.

```
---------------------- SPECIFY CONFIGURATION PARAMETERS ----------------------
Command ===>

 Specify the following Program-To-Program Interface (PPI) information:

    NetView Agent PPI Receiver Name      ==> INGAHRCV
    Monitoring Agent PPI Listener Name   ==> KAHNVLIS
    NetView PPI Buffer Size              ==> 1024K
    NetView PPI Timeout                  ==> 60


 Specify the following communication monitoring information:

    Heartbeat Interval      ==> 60
    Check Active Interval    ==> 10


 Enter=Next  F1=Help  F3=Back
```

Figure 45. Configuration Tool: Specify Configuration Parameters panel

You can accept the defaults as shown, or provide the required information:

NetView Agent PPI Receiver Name
   Specify the name of the PPI receiver that processes requests from the SA z/OS monitoring agent within SA z/OS or NetView.

Monitoring Agent PPI Listener Name
   Specify the name of a listener that is used by the SA z/OS monitoring agent to listen for events, such as systems that join or leave the automation manager's XCF group.

NetView PPI Buffer Size
   Set the PPI buffer size that is used for communication between the SA z/OS monitoring agent and NetView.

NetView PPI Timeout
   The interval after which the monitoring agent stops waiting for data from SA z/OS. It is specified in seconds and can be between 1 and 3600. The default interval is 60 seconds.

Heartbeat Interval
   The interval used to periodically check for the availability of the SA z/OS automation agent on the local system. The heartbeat interval is specified in seconds and may be set to any value between 1 and 3600. The default interval is 60 seconds.

Check Active Interval
   Once a communication problem has been detected, this interval is used to periodically check for the SA z/OS automation agent being restarted for the communication to resume. The check active interval is specified in seconds and may be set to any value between 1 and 3600. The default interval is 10 seconds.

Complete this panel and press Enter to return to the Configure IBM Tivoli System Automation for z/OS panel.

4. **Option 3, Specify Agent address space parameters:**

   From the Configure IBM Tivoli System Automation for z/OS panel, enter 3 to display the Specify Agent Address Space Parameters panel, as shown in Figure 46.

```
------------------- SPECIFY AGENT ADDRESS SPACE PARAMETERS -------------------
COMMAND ===>

 The following information is needed to define the Agent address space.
  Agent started task             ==> agent_started_taskname
  Connect to TEMS in this RTE    ==> N          (Y, N)
     Name of Primary TEMS        ==>

  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.
            IP6.* and *.SPIPE protocols do not apply to this Agent.


 Enter=Next  F1=Help  F3=Back  F5=Advanced  F10=CMS List
```

Figure 46. Configuration Tool: Specify Agent Address Space Parameters panel

a. Provide the required information:

   Agent started task
   Supply the started task name for the agent. This started task must be copied to your system procedure library at a later time. The default is CANSAH.

   Connect to TEMS in this RTE
   Specify N for this procedure because no monitoring server was configured for this runtime environment.

   Name of Primary TEMS
   Leave the name of the primary Tivoli Enterprise Monitoring Server blank for now.

   Communication protocols
   Specify the communication protocols in priority sequence. When communication with the monitoring server is initiated, the monitoring agent tries Protocol 1 first and goes to Protocol 2 and then to Protocol 3, and so on, in case of failure. Be sure to specify the same protocols that you specified for the monitoring server (see "Installing and configuring the Tivoli Monitoring Services components" on page 90).

   Refer to the online help for a description of the protocols.

   Note: There is no need to specify the SNA protocol because this is not required when the monitoring server is on a distributed system.

   Press Enter to display a list of monitoring servers on z/OS systems. Because your Tivoli Enterprise Monitoring Server is on a distributed system, it is not included in the list.

b. Press F5 (Advanced) to display the Specify Agent Primary TEMS Values panel, as shown in Figure 47.

```
-------------------- SPECIFY AGENT PRIMARY TEMS VALUES ----------------------

 Primary TEMS name     ==> HUB_host_name                      (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)
   ==> host_name
            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 47. Configuration Tool: Specify Agent Primary TEMS Values panel

Enter the following information:

Primary TEMS name
> The name of the monitoring server, as defined in "Installing and configuring the Tivoli Monitoring Services components" on page 90.

Network address (Hostname of Primary TEMS)
> The host name for the monitoring server.

Primary TEMS port number
> The port numbers for the protocols that you specified in the Specify Agent Address Space Parameters panel.

Press Enter to return to Specify Agent Address Space Parameters panel.

Press F5 (Advanced) to display the Specify Advanced Agent Configuration Values panel, as shown in Figure 48 on page 102.

Step 5. Configure the monitoring agent

```
----------------- 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            ==> Y  (Y, N)
   Intervals (hh:mm):
     Storage detail logging: Hours ==> 0  (0-24)  Minutes ==> 60 (0-60)
     Flush VSAM buffers:     Hours ==> 0  (0-24)  Minutes ==> 30 (0-60)
   Virtual IP Address (VIPA) type ==> N  (S=Static, D=Dynamic, N=None)
   Minimum extended storage       ==> 150000  K
   Language locale ==> 1          (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 48. Configuration Tool: Specify Advanced Agent Configuration Values panel

Accept the defaults or specify other values.

Language locale
> This is a required field and has no default. Specify 1 for United States English.

The Program to Program Interface (PPI) information section is optional. If desired, specify the PPI values that enable forwarding of Take Action commands to NetView for z/OS for authorization and execution. If you enable forwarding, you must also enable NetView to authorize the commands. See "Setting up NetView authentication of Take Action commands" on page 114.

NetView PPI receiver:
> Specify the name of the PPI receiver on NetView for z/OS that will receive Take Action commands. This value is required if you specified Y in the **Forward Take Action commands to NetView for z/OS** field.

TEMS PPI sender:
> Specify the optional name of the PPI sender.

Press Enter twice.

c. The following panels are displayed where you can specify the configuration values for the communication protocols that you specified in the Specify Agent Address Space Parameters panel.

IP.PIPE, IP6.PIPE, IP.SPIPE
> Uses the TCP/IP protocol for underlying communications. IP.PIPE is the best choice for Protocol 1 in a firewall environment.

```
------------------ SPECIFY AGENT IP.PIPE CONFIGURATION VALUES -----------------
COMMAND ===>

 Specify the IP.PIPE communication values for this Agent.

 * Network address (Hostname)
        ==>
   Started task  ==> *          (Recommended default = *)
   Network interface list:              (If applicable)
        ==>


 Specify Agent IP.PIPE configuration.

   Address translation             ==> N        (Y, N)
      Partition name               ==>



 * Note: See F1=Help for TSO HOMETEST command instructions.

 Enter=Next  F1=Help  F3=Back
```

Figure 49. Configuration Tool: Specify Agent IP.PIPE Configuration Values panel

Use the information below to complete this panel, which also applies to the IP.PIPE for IPV6 and IP.SPIPE protocols.

Network address (Hostname)
> Specify the TCP ID of the z/OS system that the SA z/OS monitoring agent will connect to. To get this value, issue the TSO HOMETEST command and use the first qualifier of the TCP hostname.

Started task
> Specify the started task name of TCP that is running on the z/OS system, for example, TCPIP.

Network interface list
> A list of network interfaces for the monitoring agent to use. This parameter is required for sites that are running more than one TCP/IP interface or network adapter on the same z/OS image. Setting this parameter allows you to direct the monitoring agent to connect to a specific TCP/IP local interface.

> Specify each network adapter by the host name or IP address to be used for input and output. Use a blank space to separate the entries. If your site supports DNS, you can enter IP addresses or short host names. If your site does not support DNS, you must enter fully qualified host names. If you specify an interface address or a list of interface addresses, the Configuration Tool generates the KDEB_INTERFACELIST parameter in the KDSENV member of the *&rhilev.&rtename*.RKANPARU library.

Address translation
> Specify Y to configure IP.PIPE support for communication across firewalls using address translation.

> By default, Ephemeral Pipe Support (EPS) is enabled automatically to allow IP.PIPE connections to cross a (network address) translating firewall. This feature obviates

Step 5. Configure the monitoring agent

the need for a broker partition file
(KDC_PARTITIONFILE=KDCPART). If you specifically want to
disable EPS, specify Y for **Address translation**.

Complete this panel and press Enter to configure the next
communication protocol in your sequence.

IP.UDP
Uses the UDP protocol.

```
----------------- SPECIFY AGENT IP.UDP CONFIGURATION VALUES -----------------
COMMAND ===>

 Specify the IP.UDP communication values for this Agent.

 * Network address (Hostname)
       ==>
   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 50. Configuration Tool: Specify Agent IP.UDP Configuration Values panel

See the description of the "Specify Agent IP.PIPE Configuration
Values panel" on page 103 for details of these communication
values.

Complete this panel and press Enter to configure the next
communication protocol in your sequence.

When you have provided these values, press Enter to save them and return
to the Configure IBM Tivoli System Automation for z/OS panel.

5. **Option 4, Create runtime members:**

This step creates the runtime members that are required by the SA z/OS
monitoring agent. These members are created in the runtime libraries for this
RTE.

From the Configure IBM Tivoli System Automation for z/OS menu, enter 4
(Create runtime members).

A JCL job is generated and displayed. Review the sample JCL and submit the
job. Verify that the job completes successfully with a return code of 0.

6. After the job has completed, press F3 to return to the Configure IBM Tivoli
System Automation for z/OS menu.

> **Tip**
>
> Even though **5 Complete the configuration** is an option on the Configure
> IBM Tivoli System Automation for z/OS menu, you must load the runtime
> libraries from the SMP/E target libraries *before* you perform the tasks required
> to complete the configuration.
>
> If you select **Complete the configuration** (option 5 on the Configure IBM
> Tivoli System Automation for z/OS menu), the Configuration Tool displays a
> list of the steps you must take outside the Configuration Tool. You can
> examine and print the list now. Instructions for completing the configuration
> are in "Step 7. Complete the configuration of the monitoring agent."

Step 6. Load the runtime libraries

Before you complete the configuration of the product outside the Configuration
Tool, you must load the runtime libraries from the SMP/E target libraries. The load
job requires exclusive access to the runtime libraries.

You must load the runtime libraries after you have done any of the following:
- Installed and configured the products you want in a new RTE
- Installed and configured an additional product in an existing RTE
- Installed maintenance, whether or not you re-configured a product
- Changed the configuration of the SA z/OS monitoring agent

To load the runtime libraries from the SMP/E target libraries, complete the
following steps:
1. Go to the Runtime Environments (RTEs) panel (Figure 40 on page 93).
2. Type L in the **Action** field to the left of the runtime environment that you have
   just configured the SA z/OS monitoring agent in, and press Enter.

   Note: If you are sharing RTEs, you must perform this loading step on both the
   base RTE and the sharing RTE.
3. If you specified usage of system variables on the Add Runtime Environment (2
   of 2) panel (Figure 42 on page 96) you may receive a warning to run the
   CB#V*xxxx* system variable members job (see Creating the system variable
   members on page 106). Press Enter to continue with loading the runtime
   libraries job.
4. Review the JCL and submit the job. Verify that the job completes successfully
   and that the return code is 04 or less.
5. When you finish loading the libraries, press F3 to return to the Runtime
   Environments (RTEs) panel.

Step 7. Complete the configuration of the monitoring agent

To complete the configuration, perform the following steps in the order shown.
1. Copy the started task procedures to your procedure library.
   a. From the Runtime Environments (RTEs) panel (Figure 40 on page 93), enter
      Z (Utilities) next to your runtime definition to open the RTE Utility Menu,
      as shown in Figure 51 on page 106.

Step 7. Complete the configuration of the monitoring agent

```
 .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
----------------------- RTE UTILITY MENU / RTE: RTEname -------------------
OPTION ===>

 Specify the number of the desired utility.

   1  Create batch mode parameters
   2* Create System Variable parameter member
   3  Create System Variable VTAM major node rename job
   4  Create VTAM major node (one node for all products)
   5  Generate sample transport JCL
   6  Generate sample system procedure copy JCL
   7  Generate sample system VTAMLST copy JCL
   8  Analyze user modified elements
   9  Create consolidated complete the configuration and README reports
  10  Process Edit subcommands for INSTJOBS or RKANPARU members
  11  Verify configuration and generate parameter map
  12  Upgrade attribute and catalog members


 * Important: After the CB#VSA job runs, review/edit RKANPAR(midlvl)
   See F1=Help topic for more info.: Create System Variable parameter member

 F1=Help  F3=Back
```

Figure 51. Configuration Tool: RTE Utility Menu

   b. On the RTE Utility Menu, enter 6 to display the **Generate sample system procedure copy JCL** panel.

   c. Type the name of your procedure library (for example, USER.PROCLIB). Press Enter.

   d. The JCL is displayed for you to review, edit if necessary, and submit. Verify that the job completes successfully and that all return codes are zero.

   This job creates a member called KCISYPJB in the RKANSAMU library.

   e. Edit KCISYPJB and submit the job. Verify that the job completes successfully and that all return codes are zero.

   This job copies all the required started tasks from your RKANSAMU library to the specified procedure library. The code contains the names of all the started tasks that were created during configuration.

2. Create the system variable members.

   If you have enabled system variable support, you must run the CB#V*xxxx* system variable members job to create the system variable parameter member and other components.

   Note: If a new product is added to the RTE or an existing product is reconfigured to change any of the system variable values, rerun the CB#V*xxxx* job.

3. Vary the VTAM major node active. For example:

   V NET,ACT,ID=CTDDSN

4. APF-authorize the runtime load libraries.

   These are concatenated in the STEPLIB DDNAME and in the RKANMODL DDNAME of the CANSDSST started tasks. Ask your security administrator to grant the appropriate authorizations.

5. Verify successful installation and configuration.

   a. Start the started tasks for the Tivoli Enterprise Monitoring Server and the SA z/OS monitoring agent.

   b. Verify successful startup. In the RKLVLOG for the monitoring agent address space, look for the following message to indicate successful startup:

KAHM024I SYSTEM AUTOMATION MONITORING AGENT VERSION V310 (BUILD LEVEL *level*) HAS STARTED

If you do not find this message, review the steps performed and look for errors. If you need assistance, see Part 4, "Problem determination," on page 187.

Step 8. Verify the configuration

Now that you have completed the configuration, you can verify that it is successful. Verification involves starting these components:

- Tivoli Enterprise Monitoring Server:
- Tivoli Enterprise Portal Server
- Tivoli Enterprise Portal desktop client

To do this, complete the following procedure:

1. Start the started task for the SA z/OS monitoring agent, /S *taskname*, and check the log for any errors.
2. On your workstation, select **Start > Programs** (or **All Programs**) > **IBM Tivoli Monitoring > Manage Tivoli Monitoring Services**.
3. To start the Tivoli Enterprise Monitoring Server, right-click its entry in Manage Tivoli Monitoring Services and click **Start**.
4. To start the Tivoli Enterprise Portal Server, right-click its entry in Manage Tivoli Monitoring Services and click **Start**.
5. To start the Tivoli Enterprise Portal desktop client, right-click its entry in Manage Tivoli Monitoring Services and click **Start**.
6. When prompted, supply the user ID sysadmin and the password that you specified for initial access to the Tivoli Enterprise Portal Server
7. When Tivoli Enterprise Portal opens, you can expand the navigator pane to see the SA z/OS monitoring agent workspaces.

   For information about using the SA z/OS monitoring agent workspaces and situations to monitor your sysplex resources and z/OS systems, see the online help and Part 3, "User's guide," on page 135 section.

Setting up security

Now you can set up security for the product components. See Chapter 7, "Setting up security," on page 109.

Expanding your configuration

You can add monitoring agents to other z/OS images that you want to monitor, and configure them to communicate with the hub Tivoli Enterprise Monitoring Server or with a remote monitoring server that reports to the hub. To add a monitoring agent, repeat the following steps (these require that an RTE already exists, otherwise you must create and build the RTE beforehand):

__ "Step 5. Configure the monitoring agent" on page 98
__ "Step 6. Load the runtime libraries" on page 105
__ "Step 7. Complete the configuration of the monitoring agent" on page 105
__ "Step 8. Verify the configuration"

Batch mode processing

The Configuration Tool offers batch mode processing for several configuration scenarios. You can use the batch mode processing utility to configure runtime environments and monitoring agents without going through the ISPF panels and filling in parameter values there. After you establish and configure a runtime environment in a z/OS image, you can use the batch mode processing utility to replicate your runtime environment in other z/OS images. See Chapter 9, "Using batch mode processing," on page 125.

Chapter 7. Setting up security

This chapter explains two aspects of product security:

- Configuring user security
- "SA z/OS monitoring agent security considerations" on page 114

Configuring user security

You can control who has access to the Tivoli Enterprise Portal through authentication of user IDs and passwords. Initially, the Tivoli Enterprise Portal has only one valid user ID, sysadmin. You use this user ID to log on and create other users.

How you configure user security depends on the operating system where the hub Tivoli Enterprise Monitoring Server is installed.

Table 12. User security configuration methods

Operating system of the hub monitoring server	Method of Tivoli Enterprise Portal user authentication
z/OS	Security product specified in the Configuration Tool, for example, RACF®
Windows	User accounts
Linux and UNIX	Password files

For complete information about user security issues in the Tivoli Monitoring Services environment, see the Tivoli Enterprise Portal online help and the following IBM Tivoli Monitoring publications:

- *Installation and Setup Guide*
- *Configuring IBM Tivoli Enterprise Monitoring Server on z/OS*
- *Administrator's Guide*

Setting up user security if the hub Tivoli Enterprise Monitoring Server is running on a z/OS system

If your hub Tivoli Enterprise Monitoring Server is running on z/OS, you need to configure RACF or another supported security product to authenticate your Tivoli Enterprise Portal users. User IDs must also be defined on any Linux, UNIX, and Windows systems where distributed components are installed.

After you specify a security product and activate security validation by the hub monitoring server in the Configuration Tool, user access to the Tivoli Enterprise Portal is controlled by user ID and password validation at the monitoring server, using the selected security product.

> **Important**
>
> 1. The first time you configure the Tivoli Enterprise Monitoring Server, you can select a security system for the runtime environment if desired, but be sure to leave security turned off in the **Security validation** field of the Specify Configuration Values panel (Figure 21 on page 67) for the monitoring server.
>
>    ```
>    Security validation?  ==> N (Y, N)
>    ```
>
> 2. The Tivoli Enterprise Portal Server assumes that the Tivoli Enterprise Monitoring Server is using ICSF encryption. If you set the ICSF value to N, the Tivoli Enterprise Monitoring Server uses an alternative, less secure encryption scheme.
>
>   Perform the following steps so that the portal server can connect to a monitoring server without ICSF:
>
>   a. When you specify configuration values for the hub monitoring server on z/OS, answer N to the prompt **Integrated Cryptographic Service Facility (ICSF) installed?**
>
>   b. After the monitoring server has been configured and is running, modify the portal server configuration to use the older, less robust encoding algorithm used by the hub monitoring server in the absence of ICSF:
>
>   1) In a text editor, edit the **kfwenv** file in *drive*:\IBM\ITM\CNPS.
>   2) In a line by itself, type the text USE_EGG1_FLAG=1
>   3) Save the file and exit.
>   4) Stop and restart the portal server.

Steps to perform before turning on security validation

Before turning on security validation, perform the following steps:

1. Configure and start the Tivoli Enterprise Monitoring Server, the SA z/OS monitoring agent, and Tivoli Enterprise Portal Server, following the instructions in Chapter 5, "Configuring the hub monitoring server and the monitoring agent on z/OS," on page 57.

2. Use the sysadmin user ID to log on to the Tivoli Enterprise Portal, and create other user accounts with different levels of permissions. Be sure to create at least one Tivoli Enterprise Portal user account with administrator authority and with a valid TSO user ID, to enable you to log on to the Tivoli Enterprise Portal after security validation is turned on at the Tivoli Enterprise Monitoring Server.

   To create an administrator user account in the Tivoli Enterprise Portal, follow these steps:

   a. Click **Administer Users**.

   b. In the Administer Users window, select the sysadmin user account and click **Create Another User**.

   c. Create a user account with the same user ID as a valid TSO user ID. The new user account is based on the sysadmin account and therefore has administrator authority in the Tivoli Enterprise Portal.

   For further instructions on managing user accounts, see the Tivoli Enterprise Portal online help or the *IBM Tivoli Monitoring: Administrator's Guide*.

3. Verify that your security product is installed and configured correctly.

Activating user security

After you have performed all the steps listed above, you can turn on user security at the Tivoli Enterprise Monitoring Server.

1. If you have already specified a security system for the runtime environment where the hub Tivoli Enterprise Monitoring Server is installed and configured, skip to step 3. Otherwise, navigate in the Configuration Tool to the Runtime Environments (RTEs) panel (Figure 40 on page 93) and enter U (**Update**) in the **Action** field beside the name of the runtime environment where the hub Tivoli Enterprise Monitoring Server is installed and configured.

2. On the Update Runtime Environment panel, specify the security system you want to use, and press Enter. This example specifies RACF:

   ```
   Security system        ==> RACF  (RACF, ACF2, TSS, NAM, None)
   ```

   If you select ACF2, you must also specify the ACF2 macro library in the next field.

3. On the Product Component Selection Menu (Figure 18 on page 65), enter 1 to select Tivoli Enterprise Monitoring Server.

4. On the Configure the TEMS menu (Figure 19 on page 65), select option 2 (**Specify configuration values**).

5. On the Specify Configuration Values panel (Figure 21 on page 67), specify Y in the **Security validation?** field:

   ```
   Security validation?  ==> Y (Y, N)
   ```

6. Press Enter to return to the Configure the TEMS menu.

7. On the Configure the TEMS menu, select option 4 (**Create runtime members**) to open JCL that you can review, edit, and submit. Check to make sure the return code is zero.

8. After the job completes, press F3 (Back) repeatedly to exit the Configuration Tool.

9. Locate the section for the security system you are using and follow the instructions:
   - "Defining security for RACF"
   - "Defining security for Network Access Method (NAM)"
   - "Defining security for CA-ACF2" on page 112
   - "Defining security for CA-TOP SECRET" on page 112

10. Verify that the user account you created, using a TSO user ID, can log on to the Tivoli Enterprise Portal.

Defining security for RACF

To implement RACF security, recycle the Tivoli Enterprise Monitoring Server started task.

Defining security for Network Access Method (NAM)

You can use the product-provided security feature NAM (Network Access Method) to secure your Tivoli Enterprise Monitoring Server.

You enable NAM, an alternative to vendor software security packages, from the system console, using the MVS MODIFY command.

Complete the following steps to add users to NAM from the z/OS system console.

1. Access the z/OS system console.

2. Define a password for each user who accesses the Tivoli Enterprise Monitoring Server:

```
F cccccccc,NAM SET user_id PASSWORD=password
```

where *cccccccc* is the name of your Tivoli Enterprise Monitoring Server started task, *user_id* is the user ID, and *password* is the NAM password you want to define for that user.

Adding a user ID password file to NAM: If you are defining passwords for a large number of users, you might want to use the procedure below. It enables you to set up a file containing all your NAM SET statements and run the file to define all passwords.

1. Access *rhilev.rte*.RKANCMD and create member `userids`.
2. Edit `userids`, and populate it with a NAM SET command for each user who access your Tivoli Enterprise Monitoring Server.

   Example:

   ```
   NAM SET userid1 PASSWORD=password1
   NAM SET userid2 PASSWORD=password2
   NAM SET userid3 PASSWORD=password3
   ```

   Note: Make sure the RKANCMD library has sufficient security, as it now contains sensitive information.
3. To run member `userids`, enter this command from the z/OS system console:

   ```
   F cccccccc,userids
   ```

   where *cccccccc* is the name of your Tivoli Enterprise Monitoring Server started task.

Defining security for CA-ACF2

Complete the following steps to install an exit for CA-AF2 security validation.

1. Stop the Tivoli Enterprise Monitoring Server started task.
2. Follow the instructions in KLVA2NEV to assemble and link KLVA2NEV. Change the variables as directed. Member KLVA2NEV in *&hilev.&rte.*TKANSAM is the product-supplied interface to CA-ACF2. The product-supplied member KLV@ASM, in *&hilev.&rte.*RKANSAM, contains sample assembly JCL, which is assembled into the RKANMODU data set for the specific runtime environment..
3. Define the Tivoli Enterprise Monitoring Server started task as a MUSASS to CA-ACF2:
   - Log on to TSO. At the READY prompt, type `ACF` and press Enter.
   - At the ACF prompt, type `SET LID` and press Enter.
   - At the LID prompt, type

     CH *ctaskname* MUSASS

     where *taskname* is the name of the Tivoli Enterprise Monitoring Server started task. Press Enter.
   - At the LID prompt, type `END` and press Enter.
4. Start the Tivoli Enterprise Monitoring Server started task.

Defining security for CA-TOP SECRET

Complete the following steps to implement CA-TOP SECRET security.

1. Stop the Tivoli Enterprise Monitoring Server started task.
2. Define the Tivoli Enterprise Monitoring Server as a started task in the STC record and relate it to a master facility accessor identifier. For example:

```
TSS ADD(STC) PROC(taskname) ACID(master_facility_acid)
```

where *taskname* is the name of your Tivoli Enterprise Monitoring Server started task. The value for *master_facility_acid* might be the same as *taskname*.

3. Define the name of your Tivoli Enterprise Monitoring Server started task as a FACILITY in the CA-TOP SECRET Facility Matrix Table. Set the SIGN parameter as SIGN(M) and set MODE to MODE=FAIL. Make sure the name of your Tivoli Enterprise Monitoring Server started task and the FACILITY name match.

   Example: This example shows FACILITY statements for a site that uses CA-TOP SECRET. Some statements might not be relevant to your site or might need to be modified to fit the standards and configuration of your site.

```
FACILITY(USER3=NAME=task)                        &#SPACE
FACILITY(task=MODE=FAIL,ACTIVE,SHRPRF)           &#SPACE
FACILITY(task=PGM=KLV,NOASUBM,NOABEND,NOXDEF)&#SPACE
FACILITY(task=ID=3,MULTIUSER,RES,WARNPW,SIGN(M))&#SPACE
FACILITY(task=NOINSTDATA,NORNDPW,AUTHINIT,NOPROMPT,NOAUDIT,NOMRO)
FACILITY(task=NOTSOC,LOG(INIT,SMF,MSG,SEC9))          &#SPACE
```

4. Start the Tivoli Enterprise Monitoring Server started task.

Setting up security for a hub Tivoli Enterprise Monitoring Server running on a Windows, Linux, or UNIX system

When you install and configure the hub Tivoli Enterprise Monitoring Server on a Windows, Linux, or UNIX system, do not turn on security validation immediately. Make sure the **Security: Validate User** check box is deselected. To see this setting in **Manage Tivoli Monitoring Services**, right-click **Tivoli Enterprise Monitoring Server** and click **Reconfigure**.

Steps to perform before turning on security validation

Before turning on security validation, perform the following steps:

1. Configure and start the Tivoli Enterprise Monitoring Server, SA z/OS monitoring agent, and Tivoli Enterprise Portal Server, following the instructions in Chapter 6, "Configuring the hub monitoring server on a Windows system and the monitoring agent on a z/OS image," on page 89.

2. Use the sysadmin user ID to log on to the Tivoli Enterprise Portal, and create other user accounts with different levels of permissions. Be sure to create at least one Tivoli Enterprise Portal user account with administrator authority and with the same user ID as one already set up in your network domain user accounts or in the operating system where the hub Tivoli Enterprise Monitoring Server is installed.

   To create an administrator user account in the Tivoli Enterprise Portal, follow these steps:

   a. Click ⚮ **Administer Users**.

   b. In the Administer Users window, select the sysadmin user account and click ⚮ **Create Another User**.

   c. Create a user account with the same user ID as one already set up in your network domain user accounts or in the operating system where the hub Tivoli Enterprise Monitoring Server is installed. The new user account is based on the sysadmin account and therefore has administrator authority in the Tivoli Enterprise Portal.

For further instructions on managing user accounts, see the Tivoli Enterprise Portal online help or the *IBM Tivoli Monitoring: Administrator's Guide*.

Activating user security

After you have performed the steps listed above, you can activate user security validation by the hub Tivoli Enterprise Monitoring Server:

1. In **Manage Tivoli Monitoring Services**, right-click **Tivoli Enterprise Monitoring Server** and click **Reconfigure**.

2. Select **Security: Validate User**.

3. Click **OK** twice.

4. Recycle the **Tivoli Enterprise Monitoring Server**.

5. Verify that the user account you created can log on to the Tivoli Enterprise Portal.

SA z/OS monitoring agent security considerations

Access to the SA z/OS monitoring agent workspaces and authority to perform various functions with the product are controlled through password validation. Administrative users can set permissions for specific product features to each user. It is important to provide access to the product only to users who can be trusted with the information and capabilities the product provides. For information about user administration, see *IBM Tivoli Monitoring: Administrator's Guide*.

The SA z/OS monitoring agent does not provide user-based security with respect to z/OS information and command capability. All users of the product have access to the same SA z/OS reports and can issue the same SA z/OS commands.

OMVS segment

To use the TCP/IP communication protocols, both the Tivoli Enterprise Monitoring Server and the SA z/OS monitoring agent require a default OMVS segment. See the *z/OS Communications Server IP Configuration Guide* for an explanation of how to provide an OMVS segment.

Setting up NetView authentication of Take Action commands

You can configure a monitoring server or monitoring agent address space to redirect z/OS Take Action commands to NetView through the Program to Program Interface (PPI). Take Action commands issued in NetView make full System Authorization Facility (SAF) calls for authorization. NetView uses the Tivoli Enterprise Portal user ID to determine the NetView operator on which the command authorization is performed. If command authorization passes, the command is executed on the NetView operator. Messages are written to the NetView log to provide an audit trail of the commands and the users that issued them.

If you enable NetView command authorization on the monitoring server, you must also enable NetView to execute the commands.

Take Action forwarding requires NetView on z/OS V5.2 with APAR OA18449 applied.

To set up NetView authentication of Take Action commands, complete the steps below:

1. "Step 1. Configure NetView authentication in the Configuration Tool"
2. "Step 2. Add the NetView CNMLINK data set to the Tivoli Enterprise Monitoring Server started task" on page 116
3. "Step 3. Enable NetView to authorize Take Action commands" on page 116

Step 1. Configure NetView authentication in the Configuration Tool

You configure NetView authentication of Take Action commands on the following Configuration Tool panels:

- Tivoli Enterprise Monitoring Server: The Specify Configuration Values panel (Figure 21 on page 67)
- System Automation for z/OS monitoring agent: The Specify Advanced Agent Configuration Values panel (Figure 32 on page 79)

The parameters for the monitoring server and the monitoring agent are the same.

Forward Take Action commands to NetView for z/OS?
> Indicate whether you want z/OS console commands issued as Take Action commands to be forwarded to NetView for authorization and execution.

NetView PPI receiver
> Specify the name of the PPI receiver on NetView that is to receive Take Action commands. This name is required if you answer Y to **Forward Take Action commands to NetView for z/OS?** and must match the receiver name specified on the NetView APSERV command. (The default name is CNMPCMDR.) If the specified name is incorrect or the receiver is not active on NetView for z/OS, default (MGCR) command routing is performed. The Configuration Tool generates the KGLHC_PPI_RECEIVER parameter in the K*pp*ENV member of the *&rhilev.&rtename*.RKANPARU library (where *pp* is DS for the monitoring server or AH for the System Automation for z/OS monitoring agent).
>
> The receiver name must be a unique identifier, up to 8 characters in length. It can contain alphabetic characters A-Z or a-z, numeric characters 0-9, and the following special characters: dollar sign ($), percent sign (%), ampersand (&), at sign (@), and number sign (#). This value must match the value specified in the NetView DSIPARM initialization member, CNMSTYLE (see "Step 3. Enable NetView to authorize Take Action commands" on page 116).The value for the monitoring agent defaults to the value set for the monitoring server, if one is configured in the same runtime environment. Otherwise, the default is CNMPCMDR.

TEMS PPI sender
> Optionally, specify the name of the PPI sender. The value must be a unique identifier, up to 8 characters in length. It can contain alphabetic characters A-Z or a-z, numeric characters 0-9, and the following special characters: dollar sign ($), percent sign (%), ampersand (&), at sign (@), and number sign (#). This name must not conflict with any NetView for z/OS domain name, as it is used in logging the command and command response in the NetView log. If a value is specified, the Configuration Tool generates the KGLHC_PPI_SENDER parameter in the K*pp*ENV member of the *&rhilev.&rtename*.RKANPARU library (where *pp* is DS for the monitoring server or AH for the System Automation for z/OS monitoring agent).
>
> If you do not specify a value in this field, the default is the job name of the Tivoli Enterprise Monitoring Server that is the source of the command.

Step 2. Add the NetView CNMLINK data set to the Tivoli Enterprise Monitoring Server started task

To connect to NetView, the monitoring server must reference the NetView CNMLINK data set. Concatenate the NetView CNMLINK data set to the RKANMODL statement in the Tivoli Enterprise Monitoring Server started task.

To provide the location, uncomment the CNMLINK DD card in the Tivoli Enterprise Monitoring Server started task and specify the NetView CNMLINK data set. For example:

```
000350 //RKANMODL DD DISP=SHR,
000351 // DSN= &RHILEV.&SYS.RKANMODU
000352 // DD DISP=SHR,
000353 // DSN= &RHILEV.&SYS.RKANMODUL
000354 // DD DISP=SHR,
000355 // DSN= &RHILEV.&SYS.RKANMOD
000356 //*********************************************************************
000357 //* RKANMODL DD: CNMLINK
000358 //*********************************************************************
000359 //* Uncomment this DD card and specify the location of the CNMLINK
000360 //* load module for NetView for z/OS. This library is required for the
000361 //* "Forward Take Action commands to NetView for z/OS" support which
000362 //* is enabled for this Agent. The CNMLINK library must also be
000363 //* APF-authorized.
000364 //         DD DISP=SHR,
000365 //         DSN=NETVIEW.V5R2M0.CNMLINK
```

Contact your NetView for z/OS system programmer for the data set name, if necessary. The default NetView 5.2 CNMLINK data set is NETVIEW.V5R2M0.CNMLINK. The CNMLINK library must be APF-authorized.

Step 3. Enable NetView to authorize Take Action commands

If you have configured the monitoring server or monitoring agent address spaces to forward z/OS Take Action commands to NetView, you must also enable NetView to receive and execute the commands. NetView performs command authorization as part of the execution.

To enable execution of forwarded commands, complete the following steps:

1. Define Tivoli Enterprise Portal user IDs to NetView.

   For information on defining user IDs, see the section "Defining operators for the NetView for z/OS Tivoli Enterprise Portal agent" in *IBM Tivoli NetView on z/OS: Security Reference*. You can find the NetView documentation in the IBM Tivoli NetView for z/OS documentation information center at: http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?toc=/com.ibm.itnetviewforzos.doc/toc.xml

2. Optionally, define the NetView PPI receiver in the NetView DSIPARM member CNMSTYLE (see Figure 52 on page 117).

```
*************************************************************************
*            Tivoli Management Services infrastructure server          *
*                                                                      *
* Uncomment the following (and, optionally, supply preferred OPID) to  *
* initialize support for commands and messages from Tivoli Management  *
* Services infrastructure and/or other APF authorized clients. See     *
* command help for APSERV for information about the function and       *
* clients depending on it.                                             *
*                                                                      *
*************************************************************************
function.autotask.APSERV = AUTOTMSI
*
AUTOTASK.?APSERV.Console = *NONE* //
AUTOTASK.?APSERV.InitCmd = APSERV CNMPCMDR
```

Figure 52. CNMSTYLE member after editing

Follow the instructions in the member. The PPI receiver for APSERV will be started during NetView initialization.

3. If you do not customize CNMSTYLE to define the receiver, start the NetView PPI receiver manually by issuing the APSERV command.

SA z/OS monitoring agent security considerations

Chapter 8. Enabling system variable support

This chapter provides detailed instructions for enabling system variable support and using it to run your IBM Tivoli Monitoring products on any z/OS system. With system variables, the software becomes z/OS system-independent. It can then be ported and started on any z/OS system without extensive Configuration Tool reconfiguration.

Tip

For additional information, you can access the README file for system variable support by issuing the **README SYS** command from any Configuration Tool panel.

By using system variable support, the components inherit the system values for the system on which they are started (the host z/OS system). These system-specific values are then automatically loaded into dynamic in-memory parameter members that exist only while the component runs. The result is that the software runs correctly using the system-specific parameter values for the host z/OS system.

Following are some of the benefits of using system variable support:

- You can deploy the same software unit, consisting of any or all IBM Tivoli Monitoring products, on any system without modification. LPAR-specific values are automatically resolved and substituted at product startup.
- The number of unique runtime environments required is smaller. This feature saves storage space, CPU, and labor.
- The same started task JCL and the same VTAM node can be used on any system without modification.
- You can choose to use a single VTAM major node in place of the individual product major nodes. When generated, a single VTAM major node contains all VTAM applids for all IBM Tivoli Monitoring products you have configured in the runtime environment.

When using system variable support, consider the following:

- Product started tasks (STCs) contain a new preprocessing step (STEP1 in the STC JCL). This new step resolves all system variable specifications in the product parameter members.
- Product parameter members contain many variables, instead of values, that are resolved when the STC starts. For example, the members contain &SVXDSNV instead of the VSAM high-level qualifier value.

Sample usage scenario

The following steps describe the process for enabling and using system variable support.

1. Define and configure a runtime environment. During runtime environment configuration, specify the values to enable system variable support. See Chapter 5 for details on configuring a runtime environment.

> **Note:** Multiple runtime environments might be required depending on the runtime environment structure (full, sharing, base, or SMP/E), the TEMS type (hub or remote), and variations in product mixtures.

2. Create the system variable parameter member.

   After configuring a runtime environment, you can create the system variable parameter member. Each runtime environment contains one user system variable parameter member named RKANPARU(*rtename*), which contains all system-specific values.

   See "Creating the system variable parameter member" on page 122 for information on creating the *rtename* system variable parameter member in the RKANPARU library.

3. Create the VTAM major node rename job.

   After configuring a runtime environment, you can create the VTAM major node rename job. This job creates VTAM major nodes on remote systems with names that are resolved from your system variable specification.

   See "Creating the VTAM major node rename job" on page 123 for information on creating a VTAM major node rename job.

4. Create the runtime environment transport job by using the RTE Utility option **Generate sample transport JCL**.

5. Copy the runtime environment to a remote system by using the runtime environment transport job (or any other copy utility).

6. After the copy completes, edit the system variable parameter member RKANPARU (*rtename*). If necessary, set values for components running on other systems. For example, set values for a hub TEMS running on a different LPAR.

7. Perform other remote system setup tasks as required.
   - Copy the new started tasks to your system procedure library. These started tasks have been enabled for system variables.
   - If you are not using an existing system variable for the runtime environment name on the LPAR, set the &SYSNAME system variable to the name of the runtime environment. This is set in SYS1.PARMLIB(IEASYM*xx*).
   - If you are using VTAM system variable support, you must run the VTAM major node rename job. This job creates new major nodes that are named according to your system variable specifications. After the new nodes are created, copy them to SYS1.VTAMLST.
   - VSAM file allocation and seeding are required on every system.

8. Start the components.

Enabling system variable support

You enable system variable support from the Add Runtime Environment panel. In an existing runtime environment, use the **Update** (**U**) command to enable system variable support.

Some older versions of IBM Tivoli Monitoring products might not support the system variable feature. These products can exist in the same runtime environment, and you need not reconfigure them in the runtime environment.

Complete the following steps to enable system variable support.

1. From the Main Menu, select **Configure products > Select product to configure** and select the product you are configuring.

   The Configuration Tool displays the Runtime Environments (RTEs) panel.

2. Add a new runtime environment or update an existing runtime environment:
   a. If you are adding a new runtime environment, type A in the **Action** field and specify all other required information.
   b. If you are updating a runtime environment, type U in the **Action** field.
   c. Press Enter.
   d. On the first Add Runtime Environment panel, enter all of the required information.
   e. Press Enter to access the second Add Runtime Environment panel.
3. Specify the following values to enable system variable support:

   Table 13. System variable values

Field	Value
Use z/OS system variables?	Specify Y to enable support. The default is N.
RTE name specification	Specify the system variable name by which the runtime environment is identified in the SYS1.PARMLIB LPAR system definition member. The default is &SYSNAME. This value becomes the value of the SYS parameter in all started tasks (for example, SYS='&SYSNAME'). **Note:** Resolved system variable values cannot exceed the length of the variable name (maximum length of 8 characters).

   Important

   If you change the status of system variable support in an existing runtime environment (**on** to **off** or vice versa), you must reconfigure all IBM Tivoli Monitoring products in that runtime environment. This includes specifying VTAM values and creating runtime members.

   ---

4. (Optional) Specify the following values on the second Add Runtime Environment panel to enable other functions:

Enabling system variable support

Table 14. Add runtime environment values

Field	Value
RTE base alias specification	If this runtime environment is sharing with a base runtime environment, specify an optional system variable specification for the base runtime environment. This value is inserted into the base runtime environment library references in all started tasks. The resolved name must be a valid library name qualifier. This field is commonly used to switch between base runtime environments at different maintenance levels. You can use the runtime environment base alias as one of the following: • An easy way to switch runtime environment bases. • An alternative way to refer to an existing base. **Note:** A label of **n/a** might be next to this field if the current runtime environment is not sharing with a base runtime environment.
Applid prefix specification	Specify the VTAM applid prefix that contains system variables. Be sure to place a period after the last symbol in the specification. The resolved prefix can be a maximum of four characters. The default is K&SYSCLONE.
Use VTAM model applids?	If you want to use model applids (wild cards), specify Y. Using model applids generate VTAM nodes that contain applids with wildcard suffixes wherever possible. These wild cards allow you to use any applids that match the pattern within the VTAM node. The default is N.

5. When you have finished specifying the values to enable system variable support, press F3 until you return to the Main Menu.

Creating the system variable parameter member

After configuring a runtime environment, you can create the system variable parameter member.

Each runtime environment contains one user system variable parameter member named RKANPARU(*rtename*). All system-specific values are contained in this member.

Complete the following steps to create the system variable parameter member, *rtename*, in the RKANPARU library.

1. From the Configuration Tool Main Menu, select **Configure products > Select product to configure** and select the product you are configuring.

   Result: The Configuration Tool displays the Runtime Environments (RTEs) panel.

2. Create the system variable parameter member:
   a. Type Z next to the name of the runtime environment you have configured and press Enter.
   b. On the RTE Utility Menu, select **Create System Variable parameter member** and press Enter.

      Result: The JCL that creates the system variable parameter member (CB#V*xxxx*) job is displayed.
   c. Review the JCL and submit the job. Verify that the job completes successfully and that all return codes are zero.
   d. Edit the RKANPARU(*rtename*) parameter member. Follow the directions to ensure proper resolution of cross-system variables.
3. When you have finished creating the system variable parameter member, press F3 until you return to the Main Menu.

Creating the VTAM major node rename job

After configuring a runtime environment, you can create the VTAM major node rename job. This job creates VTAM major nodes on remote systems with names that are resolved from your system variable specification.

Complete the following steps to create a VTAM major node rename job in the INSTJOBS library.

1. From the Configuration Tool Main Menu, select **Configure products > Select product to configure** and select the product you are configuring.

   Result: The Configuration Tool displays the Runtime Environments (RTEs) panel.
2. Create the VTAM major node rename job:
   a. Type Z next to the name of the runtime environment you have configured and press Enter.
   b. On the RTE Utility Menu, select **Create System Variable VTAM major node rename job**, and then press Enter.

      Result: The JCL that renames the VTAM major node (CB#7*xxxx*) job is displayed.
   c. Review the JCL. Do not submit the job yet.

      Note: You submit this job on each remote system where the monitoring software is to run. The job is in the RKANSAM library.
3. When you have finished creating the VTAM major node rename job, press F3 until you return to the Main Menu.

Creating one VTAM major node for all IBM Tivoli Monitoring products in the runtime environment

A single VTAM major node can contain all the VTAM applids for all of the IBM Tivoli Monitoring products you have configured in the runtime environment. This single major node is then used in place of the individual product major nodes.

If you choose to use a single VTAM major node, you must create it after all IBM Tivoli Monitoring products have been configured in the runtime environment. After the node is created and copied to your system VTAM system library (SYS1.VTAMLST), you vary it active and then start all of the components (started tasks).

Creating one VTAM major node for all IBM Tivoli Monitoring products in the runtime environment

Complete the following steps to create a single VTAM major node in the RKANSAMU library.

1. From the Configuration Tool Main Menu, select **Configure products > Select product to configure** and select the product you are configuring.

   Result: The Configuration Tool displays the Runtime Environments (RTEs) panel.

2. Create the VTAM major node:

   a. Type Z next to the name of the runtime environment you have configured and press Enter.

   b. On the RTE Utility Menu, select **Create VTAM major node (one node for all products)** and press Enter.

   c. On the Create VTAM Major Node panel, type the name you want to use for the single node and press Enter.

      The JCL that creates the single node is displayed.

   d. Review the JCL and submit the job. Verify that the job completed successfully and that all return codes are zero.

3. When you have finished creating a single VTAM major node, press F3 until you return to the Configuration Tool Main Menu.

Chapter 9. Using batch mode processing

The Configuration Tool offers batch mode processing for several configuration scenarios. You can use the batch mode processing utility to configure runtime environments and monitoring agents without going through the ISPF panels and filling in the required parameter values. After you establish and configure a runtime environment in a z/OS image or address space, you can use the batch mode processing utility to replicate your runtime environment in other z/OS images or address spaces.

This chapter provides instructions on using batch mode processing to perform these tasks:

- Create a new runtime environment by running a single batch job
- Replicate an existing runtime environment
- Transport a replicated runtime environment to other z/OS images

Batch mode processing using the Configuration Tool is an alternative way of building and configuring a runtime environment. Instead of using the interactive Configuration Tool to build and configure a runtime environment, you can submit a single batch job that performs the same processing.

The components of batch mode processing in the Configuration Tool include the following:

Configuration Tool batch job (CICATB)
CICATB is a new job that is generated into the INSTJOBS library. You submit this job to build and configure a runtime environment.

Configuration Tool batch parameter member
This is a single member in INSTJOBS, containing all of the configuration values for all IBM Tivoli Monitoring products to be configured in the runtime environment.

RTE Utility to create Configuration Tool batch parameter member
This utility creates the batch parameter member for an existing runtime environment, which can then be used for running subsequent CICATB jobs. The name of the parameter member is the runtime environment name.

You create the Configuration Tool batch job only once on an image and then use it for all subsequent batch mode processing on that image.

> **Tips**
>
> - You must recreate the Configuration Tool batch job if your ISPF environment has changed.
> - When the SUBMIT parameter is set to **YES**, the generated runtime environment configuration jobs are submitted automatically if the job names do not currently exist in the INSTJOBS library. If the generated jobs already exist, then the jobs are regenerated but not automatically submitted.
> - The JCL suffix must be unique for each runtime environment, because when the Configuration Tool batch job runs, it is used in every member name that is generated in INSTJOBS. If the suffix is not unique, the jobs that are generated conflict with other runtime environment jobs that might already exist in INSTJOBS.

For more information about the Configuration Tool batch utilities, see Appendix B, "Configuration Tool batch utilities," on page 235.

Planning your runtime environment replication

The Configuration Tool batch mode process involves the following three broad steps:

- Creating batch mode parameters
- Adding and configuring parameter input decks
- Creating the new runtime environment on the appropriate z/OS image, using the appropriate runtime environment transportation method

> **Tip**
> After you create a runtime environment in batch mode, you can use Configuration Tool to configure it further.

1. Edit the newly created member and invoke Configuration Tool edit macros to add additional product parameter decks to it.
2. Configure the product by changing the default parameter values as required.
3. Create the new runtime environment on the appropriate z/OS image using one of the following transport methods.

Table 15. Runtime environment transport methods

Transport method	Mode used	Advantages and disadvantages
Define the runtime environment on the local z/OS image using shared storage.	Interactive and batch mode Configuration Tool on the local z/OS image, to create a runtime environment accessible to the target image.	Advantages of this method: • The interactive Configuration Tool, located on the local image, contains the configuration information for all images. • Only one copy of the runtime libraries is created. • Only one batch job is submitted. The disadvantage of this method is that it applies only to z/OS images with shared storage.

Table 15. Runtime environment transport methods (continued)

Transport method	Mode used	Advantages and disadvantages
Transport the runtime environment from the local z/OS image to the remote image.	Interactive and batch mode Configuration Tool on the local image to create a runtime environment. After the runtime environment is defined, you use sample transport jobs to distribute the runtime libraries and parameters to the remote image.	Advantages of this method: • The interactive Configuration Tool, located on the local image, contains the configuration information for all images. • Only one batch job is submitted. • The method applies to remote z/OS images that do not share storage. The disadvantage of this method is that two copies of the runtime libraries are created.
Transport runtime environment batch jobs from the local z/OS image to the remote image.	Interactive and batch mode Configuration Tool on the local image to create a set of batch jobs that can build a runtime environment. You use the sample transport jobs to distribute the batch jobs to the remote image. Then you submit the jobs on the remote image to create the runtime libraries and parameters.	Advantages of this method: • The interactive Configuration Tool, located on the local image, contains the configuration information for all images. • The method applies to remote z/OS images that do not share storage. • Only one copy of the runtime libraries is created. The disadvantage of this method is that you must submit a series of batch jobs, or use the Auto Submit CLIST to submit the jobs that create the runtime environment.
Transport runtime environment batch mode parameters from the local z/OS image to the remote image equipped with the Configuration Tool.	Interactive Configuration Tool on the local image to export an existing runtime environment. After the runtime environment parameters are collected, you use the sample transport jobs to distribute the batch mode parameters to the remote image. The batch mode Configuration Tool is run on the remote image to create the runtime libraries and parameters.	Advantages of this method: • The method applies to remote z/OS images that do not share storage. • Only one copy of the runtime libraries is created. • Only one batch job is submitted. The disadvantage of this method is that the interactive Configuration Tool located on the local image does not contain the configuration information for all images.

Creating batch mode parameters

Use the Create batch mode parameters processing option to export parameters from an existing runtime environment into a library member. You then copy the member and change the image-specific parameters, as required, to configure the runtime environment for its new environment.

You can generate parameter decks for all IBM Tivoli Monitoring products in an existing runtime environment, and then copy the information into a new library member to be used during batch mode processing.

Complete the following steps to generate the runtime environment parameters and copy the information into a new library member.

Creating batch mode parameters

1. From the Configuration Tool Main Menu, select **Configure products > Select product to configure** and select the product you are configuring.

   The Configuration Tool displays the Runtime Environments (RTEs) panel.

2. Create the new library member:

   a. Type Z next to the runtime environment you want to replicate and press Enter.

   b. From the RTE Utility Menu, select **Create batch mode parameters** and press Enter.

   c. Specify the library that receive the batch parameter member generated by the Configuration Tool.

   d. The INSTJOBS library is specified by default, and the member name be the same as that of the current runtime environment.

   e. Press Enter.

3. Exit the Configuration Tool.

4. Edit the INSTJOBS library and copy the exported library member to a new member name. This new member name also be used as the name of the new runtime environment.

5. Using ISPF Option 2, edit the new library member to reflect the settings specific to the z/OS image where the new runtime environment exist.

Example

The following example assumes that you have created a configuration similar to the one described for Chapter 6, "Configuring the hub monitoring server on a Windows system and the monitoring agent on a z/OS image," on page 89. The runtime environment that was created for this standalone monitoring agent is referred to as RTE1. This section explains the steps to configure the SA z/OS monitoring agent for another z/OS image. It assumes that you have already created the batch mode parameters for RTE1, as outlined in "Creating batch mode parameters" on page 127, as member RTE1 in INSTJOBS.

Step 1. Use KCISETUP to set up the environment

You use the KCISETUP utility to set up the environment that is required for using the Configuration Tool batch utilities. This utility must be run after starting your TSO ISPF session and can only be run from an ISPF session.

Before using the KCISETUP utility, you must generate the KCISETUP member in your INSTLIB. KCISETUP can only be run once per session. No confirmation message is issued to indicate successful completion of KCISETUP.

Complete the following steps to generate and run KCISETUP:

1. Start the Configuration Tool on your master image.

2. From the Main Menu, select **Configure products > Services and utilities > Create batch mode job**.

   The Configuration Tool generates member KCISETUP in your INSTLIB and member CICATB in your INSTJOBS library.

3. Press F3 until you return to the Main Menu.

   Note: KCISETUP must be created on an image and can be used for all subsequent parameter deck processing on that image. If your ISPF environment changes or you split your INSTLIB, you must recreate KCISETUP.

4. To run the KCISETUP environment setup utility, enter this command at the ISPF command line:

```
TSO EXEC '&shilev.INSTLIB(KCISETUP)'
```

where &shilev is the high-level qualifier of the INSTLIB.

Step 2. Customize the sample parameter deck

To create a new parameter deck from the &shilev.INSTJOBS(RTE1) parameter deck, complete the following steps:

1. In the &shilev.INSTJOBS library, rename the RTE1 batch member to the RTE that you want to create.

   For example, runtime environment names can be the same as the LPAR name (SYSA if you intend to configure the monitoring agent on SYSA LPAR). The new RTE is referred to as *&rte_new*.

2. Edit &shilev.INSTJOBS(*&rte_new*) and customize all parameter values where RTE1 should differ from *&rte_new*. Examine parameter for parameter and decide whether the value for *&rte_new* should be the same or different from the value in RTE1.

   For example, when you use shared storage, you can retain the specifications for runtime environment such as RTE_VOL and RTE_VSAM_VOL. But other parameters, such as the description (RTE_DESC) or the name and address of the host that the SA z/OS monitoring agent is installed on (RTE_TCP_HOST and RTE_TCP_ADDR), are changed to make *&rte_new* unique.

   > **Tip**
   >
   > Online help is available to explain each parameter in the sample deck. While editing the sample parameter member, type `KCICPGHP` on the ISPF command line, and then position your cursor on any of the parameters. Alternatively, you can use the KCICFKEY utility to setup a PF-key that when pressed issues the KCICPGHP-command.

Step 3. Create and submit the CICATB batch job

After you finish customizing the parameter member *&rte_new*, complete the following steps to create and submit the CICATB batch job:

1. On the Configuration Tool Main Menu, select **Configure products > Services and utilities > Create batch mode job**.

   The CICATB batch job is created in the &shilev.INSTJOBS library and the KCISETUP member is re-created in the &shilev.INSTLIB library.

2. Edit the &shilev.INSTJOBS(CICATB) job to use the &shilev.INSTJOBS(*&rte_new*) parameter member as input to the job.

   Specify BATCHMEM(*&rte_new*) to denote the name of the new RTE. To scan first for errors only, use the SUBMIT(SCAN) option. If you want to create the batch jobs to add, build, configure, and load the runtime environment *&rte_new*, use the SUBMIT(YES) option.

Transporting the runtime environment

Use any of the following methods to transport the new runtime environment to the appropriate z/OS image.

- "Define a runtime environment on a local z/OS image using shared storage" on page 130

- "Transport a runtime environment from a local z/OS image to a remote image"
- "Transport runtime environment batch jobs from a local z/OS image to a remote image equipped with the Configuration Tool" on page 131
- "Transport runtime environment batch mode parameters from a local z/OS image to a remote image" on page 132

Before using the transport methods within this section, make sure that sufficient space and library security authorizations exist.

For a list of the advantages and disadvantages for each transport method, see Table 15 on page 126.

Define a runtime environment on a local z/OS image using shared storage

Complete the following steps to define a runtime environment on a local z/OS image using shared storage.

1. Start the Configuration Tool on your local image.
2. Create the Configuration Tool batch mode job:

   Starting from the Main Menu, select **Configure products > Services and utilities > Create batch mode job**. Press Enter.
3. Exit the Configuration Tool.
4. Perform a scan on your runtime environment parameters:
   a. Edit CICATB, updating the BATCHLIB and BATCHMEM parameters as required, and setting the SUBMIT parameter to SCAN.
   b. Submit the CICATB job to scan your runtime environment parameters.
   c. Verify that the job completes successfully; review the parameter report in the job output (ddname KCIPMRPT); correct any errors in the parameter member; repeat the scan until a clean report is generated.
5. Create a new runtime environment that is accessible to the target image:
   a. Edit CICATB again, setting the SUBMIT parameter to YES. This submits the runtime environment configuration jobs that allocate and populate runtime libraries.
   b. Submit the CICATB job to create the runtime environment.
   c. Verify that the job completes successfully.
6. Perform any manual configuration steps on the target image, such as the following:
   - Copying procedures to PROCLIB.
   - Copying VTAM definitions to VTAMLST.
   - APF-authorizing libraries.

Transport a runtime environment from a local z/OS image to a remote image

Complete the following steps to transport a runtime environment from a local z/OS image to a remote image:

1. Start the Configuration Tool on your local image.
2. Create the Configuration Tool batch mode job:
   a. Starting from the Main Menu, select **Configure products > Services and utilities > Create batch mode job**.
   b. Press Enter.

3. Exit the Configuration Tool.
4. Perform a scan on your runtime environment parameters:
   a. Edit CICATB, updating the BATCHLIB and BATCHMEM parameters as required, and setting the SUBMIT parameter to SCAN.
   b. Submit the CICATB job to scan your runtime environment parameters.
   c. Verify that the job completes successfully; review the parameter report in the job output (DD name KCIPMRPT); correct any errors in the parameter member; repeat the scan until a clean report is generated.
5. Create a new runtime environment that is accessible to the target image runtime environment:
   a. Edit CICATB again, setting the SUBMIT parameter to YES. This submits the runtime environment configuration jobs that allocate and populate runtime libraries.
   b. Submit the CICATB job to create the runtime environment.
   c. Verify that the job completes successfully.
6. Start the Configuration Tool again.
7. Select the runtime environment you want to transport:
   a. Access the Runtime Environments (RTEs) panel. (From the Main Menu, select **Configure products > Select product to configure,** and then select a product.)
   b. Type Z next to the runtime environment you want to transport and press Enter.
8. On the RTE Utility Menu, select **Generate sample transport JCL** and press Enter. This action generates several sample transport jobs in the RKANSAM library. Member $XPRTNDX provides a description of all generated members.

   For example, to use DFDSS to transport the runtime libraries to the target image, use the following sample jobs:
   - XDFDMP01 on the master image to dump the runtime libraries.
   - XDFRST01 on the target image to restore the runtime libraries.
9. Perform any manual configuration steps on the target image, such as the following:
   - Copying procedures to PROCLIB.
   - Copying VTAM definitions to VTAMLST.
   - APF-authorizing libraries.

Transport runtime environment batch jobs from a local z/OS image to a remote image equipped with the Configuration Tool

Complete the following steps to transport runtime environment batch jobs from a local z/OS image to a remote image that is equipped with the Configuration Tool.

1. Start the Configuration Tool on your local image.
2. Create the Configuration Tool batch mode job:
   a. Starting from the Main Menu, select **Configure products > Services and utilities > Create batch mode job**.
   b. Press Enter.
3. Exit the Configuration Tool.
4. Perform a scan on your runtime environment parameters:
   a. Edit CICATB, updating the BATCHLIB and BATCHMEM parameters as required, and setting the SUBMIT parameter to SCAN.

     b. Submit the CICATB job to scan your runtime environment parameters.

     c. Verify that the job completes successfully; review the parameter report in the job output (DD name KCIPMRPT); correct any errors in the parameter member; repeat the scan until a clean report is generated.

5. Create the runtime environment generation jobs:

     a. Edit CICATB again, setting the SUBMIT parameter to NO. This creates the runtime environment configuration jobs that allocate and populate runtime libraries.

     b. Submit the CICATB job to create the runtime environment generation jobs.

     c. Verify that the job completes successfully.

6. Start the Configuration Tool again.

7. Select the runtime environment you want to transport:

     a. Access the Runtime Environments (RTEs) panel. (From the Main Menu, select **Configure products > Select product to configure,** and then select a product.)

     b. Type Z next to the runtime environment you want to transport and press Enter.

8. On the RTE Utility Menu, select **Generate sample transport JCL** and press Enter. This action generates several sample transport jobs in the RKANSAM library. Member $XPRTNDX provides a description of all generated members.

   For example, to use DFDSS to transport the targets, INSTLIB, INSTDATA, and INSTJOBS to the remote image, use the following sample jobs:

   • XDFDMP03 on the master image to dump the batch jobs.

   • XDFRST03 on the target image to restore the batch jobs.

9. Submit the batch jobs on the target image in the order listed in the **Jobs Sorted By Generation Sequence** section of the Configuration Tool Batch Mode job report.

   You can submit each job manually or use the Auto Submit CLIST to automatically submit the Configuration Tool jobs on the target image. To use the Auto Submit CLIST, complete the following steps:

     a. Verify that the SMP/E target libraries are available on the image where the CLIST run.

     b. Edit the member named SUB#*jclsuffix* in INSTJOBS, where *jclsuffix* identifies the JCL suffix for the new runtime environment.

     c. Run the CLIST to submit the Configuration Tool jobs that create the runtime environment.

10. Perform any manual configuration steps on the target image, such as the following:

   • Copying procedures to PROCLIB

   • Copying VTAM definitions to VTAMLST

   • APF-authorizing libraries

Transport runtime environment batch mode parameters from a local z/OS image to a remote image

Complete the following steps to transport runtime environment batch mode parameters from a local z/OS image to a remote image.

1. Start the Configuration Tool on your local image.

2. Select the runtime environment you want to transport:

    a. Access the Runtime Environments (RTEs) panel. (From the Main Menu, select **Configure products > Select product to configure**, and then select a product.)

    b. Type Z next to the runtime environment you want to transport and press Enter.

3. On the RTE Utility Menu, select **Generate sample transport JCL** and press Enter. This causes several sample transport jobs to be generated within the RKANSAM library. Member $XPRTNDX provides a description of all generated members.

   For example, to use DFDSS to transport the targets, INSTLIB, INSTDATA, and INSTJOBS to the remote image, use the following sample jobs:
   - XDFDMP03 on the master image to dump the batch jobs.
   - XDFRST03 on the target image to restore the batch jobs.

4. Create the Configuration Tool batch mode job:

    a. Starting from the Main Menu, select **Configure products > Services and utilities > Create batch mode job**.

    b. Press Enter.

5. Exit the Configuration Tool.

6. Perform a scan on your runtime environment parameters:

    a. Edit CICATB, updating the BATCHLIB and BATCHMEM parameters as required, and setting the SUBMIT parameter to SCAN.

    b. Submit the CICATB job to scan your runtime environment parameters.

    c. Verify that the job completes successfully; review the parameter report in the job output (DD name KCIPMRPT); correct any errors in the parameter member; repeat the scan until a clean report is generated.

7. Create the runtime environment on the target image:

    a. Edit CICATB again, setting the SUBMIT parameter to YES. This submits the runtime environment configuration jobs that allocate and populate runtime libraries.

    b. Submit the CICATB job to create the runtime environment.

    c. Verify that the job completes successfully.

8. Perform any manual configuration steps on the target image, such as the following:
   - Copying procedures to PROCLIB.
   - Copying VTAM definitions to VTAMLST.
   - APF-authorizing libraries.

Transporting the runtime environment

Part 3. User's guide

Chapter 10. The SA z/OS monitoring agent and its environment

The SA z/OS monitoring agent is one of a suite of Tivoli Monitoring Services products called Tivoli Enterprise Monitoring Agents. These products use common IBM Tivoli Monitoring components to monitor your mainframe and distributed systems on a variety of platforms, and to provide workstation-based reports you can use to track trends and understand and troubleshoot system problems.

The SA z/OS monitoring agent collects information about the status of automation on z/OS systems and z/OS sysplexes, and reports the information in the Tivoli Enterprise Portal (formerly named CandleNet Portal) graphical user interface. The product workspaces provide the following types of information about your enterprise:

- Resource overview and detail information
- Resource requests inserted into the automation
- The current automation environment, that is, the location and status of automation managers and automation agents within the sysplex
- System and application health information through monitor resources
- User-defined status items for installation-specific monitoring
- Exceptional messages that are captured by SA z/OS
- Gateway definitions and statuses for a system in the sysplex
- Outstanding WTORs in the SA z/OS subplex

The user interface contains expert advice on alerts and corrective actions.

Default workspaces and situations enable you to start monitoring your enterprise as soon as the SA z/OS monitoring agent is installed. The user interface supports several formats for viewing data, such as bar charts, and tables. Workspaces and situations can be customized to meet the needs of your enterprise.

> **Note:**
> The SA z/OS monitoring agent does not include historical reporting

The rest of this chapter describes the Tivoli Monitoring Services components and the Tivoli Enterprise Portal interface that the SA z/OS monitoring agent reports system information in. If you are already familiar with the components and operations of Tivoli Monitoring Services, you can skip to Chapter 11, "Workspaces," on page 145.

Tivoli Monitoring Services

The client-server-agent implementation of Tivoli Monitoring Services includes the following components:

- A Tivoli Enterprise Portal (formerly named CandleNet Portal) client with a graphical user interface for viewing and monitoring your enterprise. Tivoli Enterprise Portal offers two modes of operation: desktop and browser.

- A Tivoli Enterprise Portal Server (formerly named CandleNet Portal Server) that retrieves, manipulates, and analyzes data from the monitoring agents in your enterprise.
- A Tivoli Enterprise Monitoring Server (formerly named Candle Management Server), which acts as a collection and control point for alerts and data received from the monitoring agents.
- Tivoli Enterprise Monitoring Agents installed on the systems or subsystems you want to monitor. These monitoring agents collect and distribute data to a Tivoli Enterprise Monitoring Server.

Tivoli Enterprise Portal

The monitoring agents, including the SA z/OS monitoring agent, use the Tivoli Enterprise Portal to provide a view of your enterprise from which you can drill down to examine details about each system being monitored. Its application window consists of a Navigator that shows all the systems in your enterprise where monitoring agents are installed, and a workspace that includes table and chart views of system and application conditions. Each workspace is designed to help monitor a specific component of your system. A table of attributes is provided for each workspace.

Each attribute represents a particular kind of data about system resources being monitored and reported. Attributes can also be used to define situations to test for specific conditions. When the conditions for a situation are met, situation event indicators are displayed in the Navigator.

The Tivoli Enterprise Portal client has two modes of operation:

desktop
The application software is installed on your system.

browser
Access the Tivoli Enterprise Portal from a browser, using the Web address of the Tivoli Enterprise Portal Server. In browser mode, the software is downloaded to your system the first time you log on to Tivoli Enterprise Portal, and thereafter only when there are software updates.

You can find detailed instructions for using Tivoli Enterprise Portal in the Tivoli Enterprise Portal online help and in the IBM Tivoli Monitoring publications (see "IBM Tivoli Monitoring publications" on page xvi).

The Navigator

The physical Navigator view shows the hierarchy of your monitored enterprise, from the top level (Enterprise) down to individual groupings of information collected by the monitoring agents. When you click an item in the Navigator, its default workspace displays in the application window.
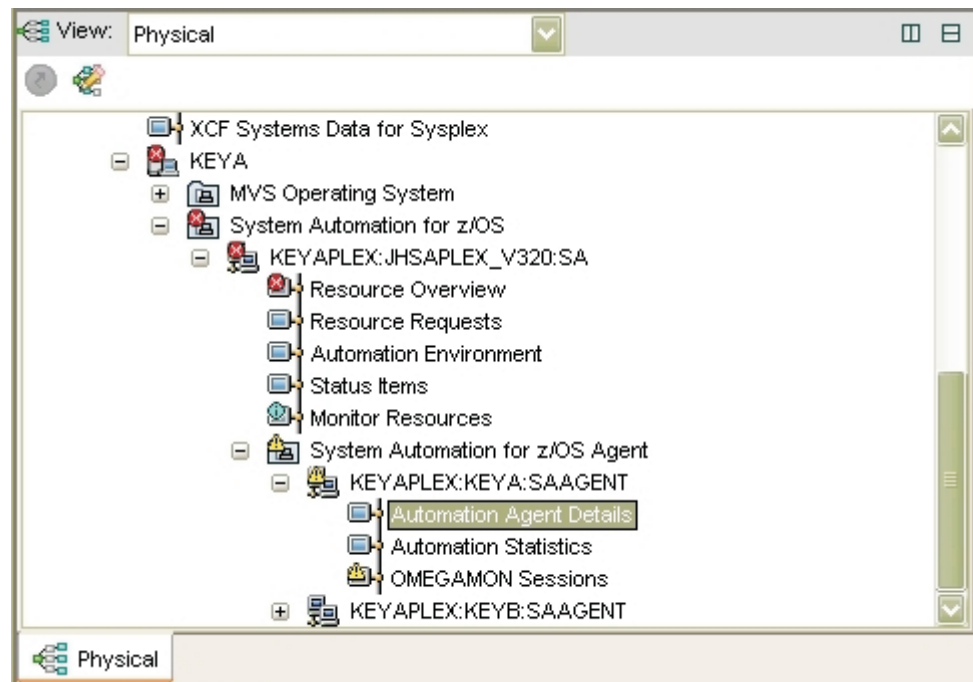
Figure 53. Tivoli Enterprise Portal Navigator

The Tivoli Enterprise Portal Navigator provides a physical view of your monitored enterprise. Under the nodes that represent the monitoring agents, you can find a list of workspaces for the data collected by each agent.

Workspaces

A *workspace* is the work area of the Tivoli Enterprise Portal application window and is made up of one or more views. A *view* is a pane in the workspace (typically a chart, graph, or table) showing data collected by a monitoring agent.
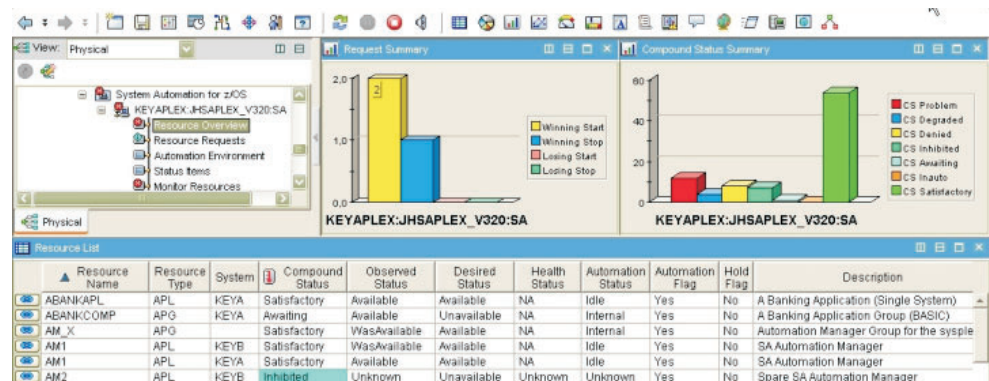
Figure 54. Tivoli Enterprise Portal workspace

As you select items in the Navigator, each workspace presents views relevant to your selection. Every workspace has at least one view, and every view has a set of properties associated with it. You can customize the workspace by working in the Properties Editor to change the style and content of each view. You can also change, add, and delete views on a workspace.

The Tivoli Enterprise Portal can present data in the following types of graphical views:
- Table view
- Pie chart view
- Bar chart view
- Plot chart view
- Circular gauge view
- Linear gauge view

Additional function is provided in the following Tivoli Enterprise Portal views:
- Notepad view
- Message log view, showing the status of the situations associated with the system
- Take Action view, used to send a command to the monitored system
- Terminal view, from which you can start a 3270 or 5250 work session
- Browser view, from which you can open a browser to see HTML pages and Websites

The SA z/OS monitoring agent provides a set of predefined workspaces that allow you to start monitoring your environment immediately. As you become more familiar with the product, you can modify the predefined workspaces or create new workspaces. For more information about the predefined workspaces provided by the SA z/OS monitoring agent, see Chapter 11, "Workspaces," on page 145.

Each table view in a workspace corresponds to an attribute group, and each column of the table corresponds to an individual attribute from the group. A workspace can be linked to other workspaces from its table and charts. A link can be context-sensitive, whereby right-clicking a row in a table or a graphic object in a chart allows you to link to related or more detailed information.

Attributes

The SA z/OS monitoring agent gathers automation resource information from the primary automation manager or the local and remote automation agents residing on the monitored z/OS systems, and stores the data in system elements called *attributes*. You can use these attributes to monitor the status of automation and of your automated applications, build custom workspaces, and create situations to alert you of pending problems.

Related attributes are grouped into attribute groups (also called attribute tables). Each table view contains information provided by a single attribute group.

For a complete description of the SA z/OS monitoring agent attributes, see Chapter 12, "Attributes," on page 153 or the online help.

Using attributes in queries

Graph and table views use queries to specify which attribute values and monitored resources to request from a Tivoli Enterprise Monitoring Agent. You can use the Query Editor to create a new query, modify an existing one, or apply filters and set styles to define the content and appearance of a view based on an existing query.

For instructions on using the Query Editor, see the Tivoli Enterprise Portal online help or *IBM Tivoli Monitoring: User's Guide*, SC32-9409.

Situations and situation events

A *situation* describes a condition or set of conditions that you set to determine whether a problem exists in one or more monitored systems and resources. A condition consists of an attribute, a value, and a comparison operator. The value of the attribute is compared with the value set for the condition to determine whether the condition is met. For example, the `Kah_Rsrc_Not_Satisfactory_Crit` situation is true when the value of the `Compound Status` attribute is `Problem`.

You can create complex situations that contain more than one condition, allowing you to compare attributes and values that represent characteristics of specific problems. When all the conditions of a situation are met (the situation is triggered), a *situation event* is registered. The operator is alerted to situation events by indicator icons that are displayed in the Navigator. Operators can also be alerted by sound. As you move up the Navigator hierarchy, situation events are consolidated to show only the indicator with the highest severity level (Critical, followed by Warning, then Informational).
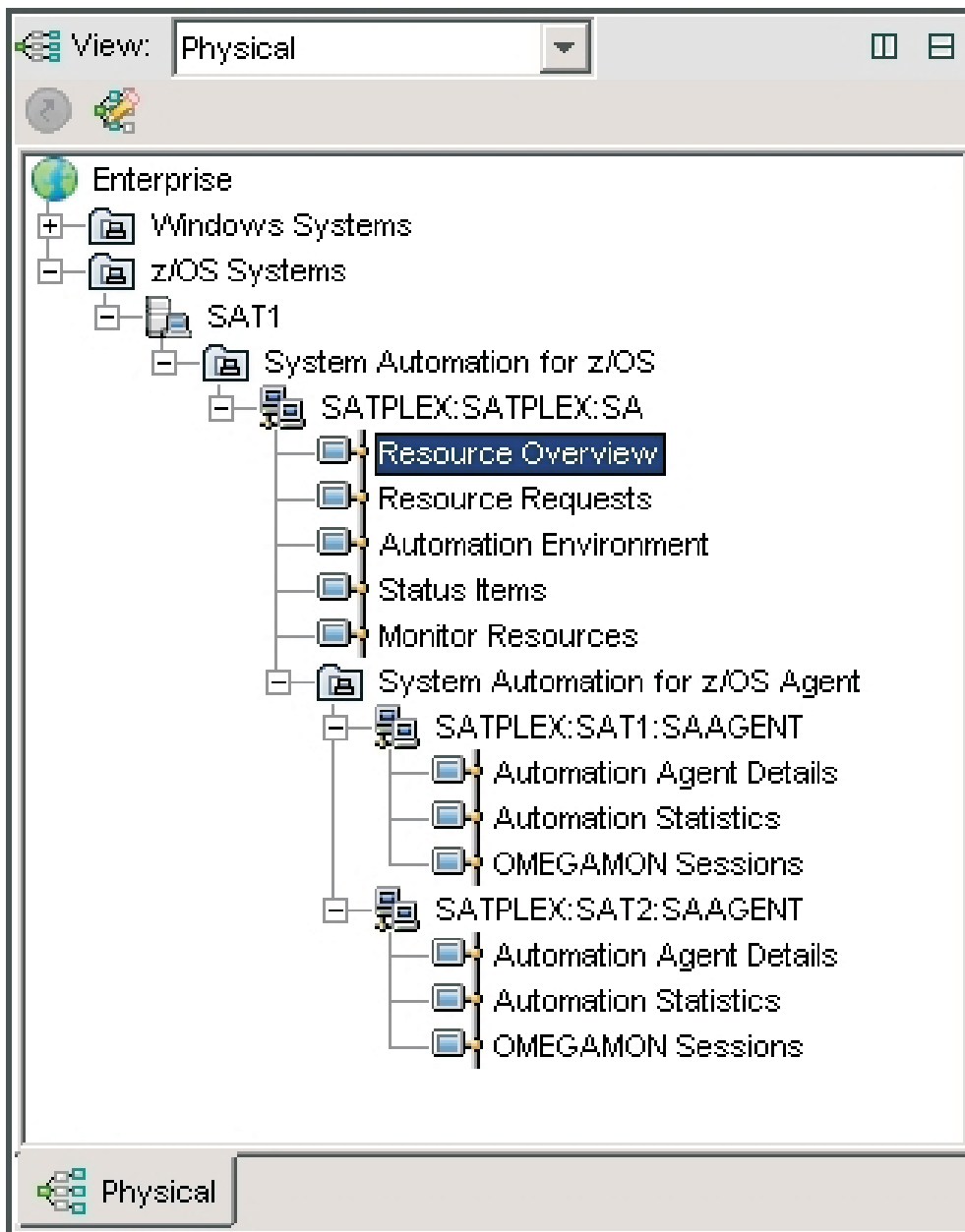
Figure 55. Tivoli Enterprise Portal Navigator with critical situation event indicators

A situation can include a Take Action command that runs when the situation is triggered. This allows you to automate a response to a specific system condition. In addition, each situation can include text describing the probable cause and expert advice allowing you to address and resolve problems quickly.

You can create or modify situations from the Tivoli Enterprise Portal user interface by using the Situation Editor. From the Situation Editor, you can specify situations to run at startup or you can start and stop situations manually. SA z/OS monitoring agent provides a set of default situations to enable you to start monitoring your enterprise as soon as the product is installed. You can also use the Situation Editor to create new situations to meet the needs of your enterprise.

For information about the predefined situations provided with SA z/OS
monitoring agent, see the product online help or Chapter 13, "Situations and
situation events," on page 179. For instructions on using the Situation Editor, see
the Tivoli Enterprise Portal online help or *IBM Tivoli Monitoring: User's Guide*,
SC32-9409.

Tivoli Monitoring Services

Chapter 11. Workspaces

The SA z/OS monitoring agent provides predefined workspaces, which you can access from the Navigator in the Tivoli Enterprise Portal. The product workspaces enable you to monitor the status of automation of your z/OS systems and sysplex resources. You access these workspaces from nodes at two levels of the Navigator tree: the System Automation for z/OS level and the System Automation for z/OS Agent level.

Figure 56 on page 146 shows the Navigator expanded to display the nodes for the SA z/OS monitoring agent predefined workspaces.
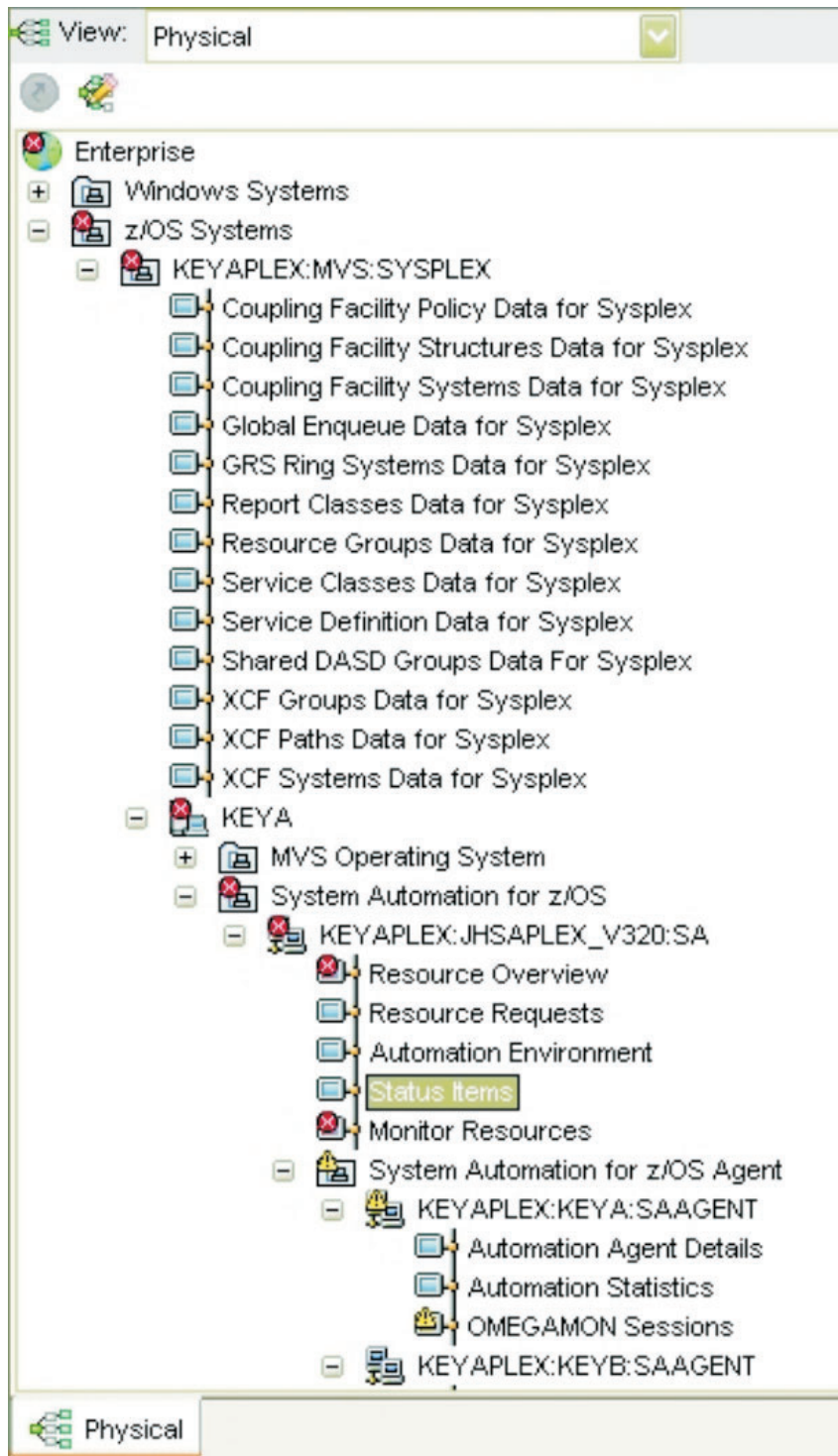
Figure 56. SA z/OS monitoring agent nodes in the Navigator

As you select items in the Navigator, the workspace presents views pertinent to
your selection. Each workspace has at least one view with a set of associated
properties. You can customize the workspace by working in the Properties Editor
to change the style and content of each view. You can resize views, add them to
and remove them from workspaces, and change the types of view in a workspace.

> **Tip**
>
> If a view in a workspace is not fully visible, use your cursor to drag the borders of the view and increase its size as needed.

For more information about customizing views and navigating workspaces, see the Tivoli Enterprise Portal online help or *IBM Tivoli Monitoring: User's Guide*, SC32-9409.

The rest of this chapter provides basic information about using workspaces in the Tivoli Enterprise Portal interface and describes the predefined workspaces provided with the SA z/OS monitoring agent.

Workspace basics

This section explains how to access workspaces in the Tivoli Enterprise Portal interface and how to define workspace properties.

Accessing workspaces

When accessing workspaces in the Navigator, you can select a node to display a workspace. You can navigate to alternative workspaces for some of the nodes by right-clicking the node to see the other selections.

The subsidiary workspaces for each primary workspace are accessible by one or more of these methods:

- From the Navigator:
  1. Select the primary workspace node.
  2. Right-click the name of the selected workspace in the Navigator.
  3. Select **Workspaces** from the context menu.
  4. Select the subsidiary workspace.
- From the **View** menu:
  1. Select the primary workspace node in the Navigator.
  2. In the menu bar at the top of the Tivoli Enterprise Portal, select **View > Workspaces**.
  3. Select the subsidiary workspace.
- From the table view:
  1. Select the primary workspace node in the Navigator.
  2. If the workspace's table view contains a link icon to the left of each row, you can click the icon to navigate to the default subsidiary workspace pertaining to the selected row, or right-click the icon and select a subsidiary workspace from the context menu. If the subsidiary workspace is unavailable (for example, if no pertinent information is available), the ☜ link icon is dimmed ☜ .
- From a chart view:

The information displayed in some bar charts and plot charts is linked to subsidiary workspaces. To find a link, right-click a bar or data point in the chart. If **Link to >** is one of the items in the context menu, you can select a subsidiary workspace pertaining to the data in the chart.

For specific information on working with views (for example, splitting, closing, or expanding views), see the Tivoli Enterprise Portal online help or *IBM Tivoli Monitoring: User's Guide*, SC32-9409.

Defining view properties

Every view in a workspace has a set of properties, which you can customize. Predefined workspaces are read-only. To change a workspace, copy it or perform a Save As operation and rename it. Changes you make to workspace properties, such as adding or editing a view, are temporary. They are lost when you exit Tivoli Enterprise Portal unless you save the workspace.

Adding a workspace to your favorites

Each workspace has a unique web address. When using Tivoli Enterprise Portal in browser mode, you can display any workspace by entering the unique web address. You can save the workspace to your Favorites list or specify it as your home page.

Predefined workspaces for the SA z/OS monitoring agent

This section summarizes the views and types of information displayed in each predefined workspace provided with the SA z/OS monitoring agent. The list below shows the order and hierarchy of the predefined workspaces.

The rest of the chapter describes the predefined workspaces in alphabetical order.

Automation Agent Details workspace

The **Automation Agent Details** workspace reports detailed information about the NetView environment of a particular automation agent running on a z/OS system. This workspace displays data provided by the Automation Agent Detail Information attribute group (see "Automation Agent Detail Information attribute group" on page 154).

The predefined workspace contains the following views:
- The **Automation Agents** table lists all automation agents in the same SA z/OS subplex. A recursive link is provided to navigate the Automation Agent Details workspace for detailed information about the NetView environment of the selected agent.
- The **Automation Agent Details** table provides information about the NetView environment of an automation agent. In particular, it shows:
  – What automation configuration is currently being used
  – The status of global automation flags
  – Configuration information for the Status Display Facility (SDF) and UNIX System Services (USS)
  – Captured messages for non-application related resources, that is, MVSESA resources

Automation Environment workspace

The **Automation Environment** workspace provides an overview of the automation agents and automation managers configured in the SA z/OS subplex. This workspace displays data provided by the SA z/OS Sysplex Automation Manager Detail attribute group (see "Automation Manager Detail Information attribute group" on page 157) and the SA z/OS Sysplex Nodes List attribute group (see "Automation Environment attribute group" on page 155).

The predefined workspace contains the following views:

- The **Automation Environment Members** table shows the automation managers and automation agents that are configured within the same SA z/OS subplex, together with their states.
- The **Automation Manager Details** table shows detailed information about the status of the primary automation manager, in particular, the name and status of the takeover file and the automation configuration that was most recently loaded. Links are provided to navigate to:
  - The Automation Agent Details workspace for detailed information about the NetView environment of a particular automation agent
  - The OMEGAMON Sessions workspace for detailed information about OMEGAMON classic activity of a particular z/OS system
  - The Automation Statistics workspace for statistical information about the automation workload on a particular z/OS system.

Automation Statistics workspace

The **Automation Statistics** workspace reports various statistical information about a system in the sysplex. This workspace displays data provided by the Automation Statistics attribute group (see "Automation Statistics attribute group" on page 157).

The predefined workspace contains the following views:

- The **Automation Agent Activity** bar chart shows the absolute number of commands, messages, and startup and shutdown commands that the automation agent has handled since the last reset.
- The **Autom. Manager Activity** bar chart shows the hourly rate of work items and orders since the data was last reset.
- The **Messages and Commands** bar chart shows the hourly rate of commands and messages since the data was last reset.
- The **Automation Statistics** and **More Statistics** tables present detailed metrics for both the automation manager and the automation agent, as well as the number of resources automated in this environment.

Critical Messages Display workspace

The **Critical Messages Display** workspace displays exceptional messages that are captured by SA z/OS. An exceptional message has a severity of either UNUSUAL, IMPORTANT or CRITICAL.

The predefined workspace contains the following views:

- The **Critical Messages** table shows a tokenized output of the INGMSGS command.
- The **Critical Messages Severity Summary** bar chart shows the distribution of the message severity.

Gateway Connections workspace

The **Gateway Connections** workspace displays gateway definitions and statuses for a system in the sysplex. The predefined workspace contains the following views:

- The **Gateway Connections** overview. The contents of this table are the output of the DISPGW command.
- The **Gateway Connections Status Summary** bar chart shows the distribution of the various gateway connection statuses.

Monitor Resources workspace

The **Monitor Resources** workspace shows all monitor resources configured in the SA z/OS subplex (or the agent node itself) and a colored display of the status. This workspace displays data provided by the Monitor Resource List attribute group (see "Monitor Resources attribute group" on page 161).

The predefined workspace contains the following views:

- The **Health Status Summary** bar chart shows the distribution of the various health states across the monitor resources in the SA z/OS subplex.
- The **Monitor Resources** table shows detailed information about each monitor resource, the monitoring status, the health status, and the last status message captured for the monitor resource. A link is provided to navigate to the Resource Details workspace for further information about the monitor resource's status or health status history.

OMEGAMON Sessions workspace

The **OMEGAMON Sessions** workspace reports information for OMEGAMON sessions on a particular z/OS system. This workspace displays data provided by the OMEGAMON Sessions attribute group (see "OMEGAMON Sessions attribute group" on page 162).

The predefined workspace contains the following views:

- The **Session Activity** bar chart shows the command and exception activity of each session with an OMEGAMON classic monitor.
- The **OMEGAMON Sessions** table shows detailed information about each OMEGAMON session, in particular the status of the connection and security information.

Outstanding WTOR Replies workspace

The **WTOR Replies** workspace lists all outstanding WTORs in the SA z/OS subplex. The table that is presented lists all the WTORs that are defined in an SA z/OS policy, enriched with attributes such as ASID and others.

The predefined workspace contains the following views:

- The **Outstanding WTOR Replies** table lists all outstanding WTORs with all available attributes. Whenever a resource is known for the WTOR, links are provided to navigate to the **Resource Details** workspace for further details about that resource.
- The **Severity Summary** bar chart shows the distribution of the message severity across all WTORs in the SA z/OS subplex.
- The **Message Flag Summary** bar chart shows the distribution of the message flag type.

Resource Details workspace

The **Resource Details** workspace reports detailed information about a resource. This workspace does not appear in the Navigator view and can only be accessed from the Resource Overview workspace or the Resource Request workspace. The Resource Details workspace displays data provided by the following attribute groups:

- Resource Votes (see "Resource Votes attribute group" on page 175)
- Resource Agent Information (see "Resource Agent Information attribute group" on page 165)
- Resource Manager Information (see "Resource Manager Information attribute group" on page 171)

The predefined workspace contains the following views:

- The **Resource Votes** table shows all requests that have been incorporated into the automation for this resource and the votes that result from propagation of requests along the resource dependency graphs.
- The **Manager Information** table shows detailed resource information from the automation manager's perspective. This includes the history of decisions made by the automation manager based on the change of resource states that affect this resource either directly or indirectly.
- The **Agent Information** table shows detailed resource information from the automation agent's perspective. This includes the history of messages that caused this resource's status to change. For a monitor resource, a detailed history of health status messages is shown.

Resource Overview workspace

The **Resource Overview** workspace provides an overview of resources in the sysplex, their state and requests to them. This workspace displays data provided by the Resource List attribute group (see "Resource List attribute group" on page 166) and the Resource Requests attribute group (see "Resource Requests attribute group" on page 172).

The predefined workspace contains the following views:

- The **Request Summary** bar chart shows the distribution of request types (start vs. stop, winning vs. losing) across all requests in the SA z/OS subplex. A link is provided to navigate to the Resource Requests workspace for detailed information about the requests in the SA z/OS subplex.
- The **Compound Status Summary** bar chart shows the distribution of compound states across all resources in the SA z/OS subplex.
- The **Resource List** table lists all resources, the various automation states, and other descriptive information in the SA z/OS subplex. Links are provided to navigate to the Resource Details workspace for further details about a particular resource or to navigate to the Resource Requests workspace for detailed information about the requests in the SA z/OS subplex.

Filter support

Special filter support exists for the Resource Overview workspace because this list can be extremely large. Although all filtering is done on the Tivoli Enterprise Portal (TEP) side, some filters for this workspace are also implemented on the NetView side. This can help reduce the amount of data that must be transferred from the automation manager. The following filters are supported:

- Operand may be equal to or contained in the resource name.

- Operand may be equal to or contained in the resource type.
- Operand may be equal to or contained in the resource system.
- Status may be equal to the compound, observed, or health status *and* a multiple of such expressions are logically ORed.
- Status may be not equal to the compound, observed, or health status *and* a multiple of such expressions are logically ANDed.
- Combinations of different attributes are *only* allowed within a single filter row, that is, the attributes are logically ANDed.

Examples: Supported and unsupported filters include, for example:

- Supported resource name, type, and system filters:

  ```
  '*/APL/*'
  '*IMS*/APL/KEY*'
  '*ABC*/*/*KEY*'
  ```

- Supported filters, for example (read Compound_Status for CS, Health_Status for HS):

  ```
  (CS=Problem) | (CS=Denied)
  (CS<>Satisfactory) & (HS<>Problem)
  ```

- Unsupported filters, for example:

  ```
  (CS=Problem) | ( (CS=Critical) & (HS=Fatal) )
  ( (ResourceName='*IMS") & (CS=Problem) ) | (CS=Denied)
  ```

You can check for successful filtering on the NetView side by setting Debug on for INGRAHCP or setting global Debug. Supported Tivoli Enterprise Portal (TEP) query filters are translated to INGRAHCP parameters of the following form:

```
resource-pattern [ C compountFlags ] [ O observedFlags ] [ H  healthFlags ]
```

Where the Flags are strings of readable hexadecimal values.

Resource Requests workspace

The **Resource Requests** workspace reports detailed information about requests in the SA z/OS subplex. This workspace displays data provided by the Resource Requests attribute group (see "Resource Requests attribute group" on page 172).

The predefined workspace contains the following views:

- The **Request Summary** bar chart shows the distribution of request types (start vs. stop, winning vs. losing) over all requests in the SA z/OS subplex.
- The **Resource Requests** table shows all requests in the SA z/OS subplex. A link is provided to navigate to the Resource Details workspace for further details about a particular resource, especially information about votes that affect this resource.

Status Items workspace

The **Status Items** workspace displays any active user-defined status items in the SA z/OS subplex. This data is provided by the Status Items attribute group (see "Status Items attribute group" on page 176).

The predefined workspace contains only one view:

- The **Status Items** table lists the status items in the SA z/OS subplex together with descriptive text, the status value and optional transient text and other status item attributes. The object that is represented by a status item is defined entirely by the installation.

Chapter 12. Attributes

Attributes are characteristics or properties of the objects monitored by the SA z/OS monitoring agent. Related attributes are organized into attribute groups (also called attribute tables). The attributes are used to define the queries that collect the information displayed in tables and charts in the SA z/OS monitoring agent workspaces and to create situations that trigger alerts in response to specified conditions.

The table view in each workspace displays data collected for a single attribute group. See Table 16 for a tabular representation of the relationships between the predefined workspaces and the attribute groups.

Attribute names

Every attribute is identified by a unique name composed of the attribute group name followed by a period and the name of the attribute item. For example, the attribute Compound_Status, a member of the Resource_List group, stores a value representing the compound automation status of a resource at the time of the data collection:

`Resource_List.Compound_Status`

Attribute groups used by predefined workspaces

In most cases, a workspace contains graphical data or table columns that are reported by related attributes in an attribute group. The table identifies the attribute group related to each predefined workspace provided by the SA z/OS monitoring agent. The workspaces are listed in alphabetical order. For more information about the product workspaces, see Chapter 11, "Workspaces," on page 145.

Table 16. Attribute groups and workspaces

Workspace	Attribute group
Automation Agent Details workspace	Automation Agent Detail Information attribute group
Automation Environment workspace	Automation Environment attribute group, Automation Manager Detail Information attribute group
Automation Statistics workspace	Automation Statistics attribute group
Critical Messages Display workspace	Critical Messages attribute group
Gateway Connections workspace	Gateway Connections attribute group
Monitor Resources workspace	Monitor Resources attribute group
OMEGAMON Sessions workspace	OMEGAMON Sessions attribute group
Outstanding WTOR Replies workspace	Outstanding WTOR Replies attribute group
Resource Details workspace	Resource Agent Information attribute group, Resource Manager Information attribute group, Resource Votes attribute group
Resource Overview workspace	Resource List attribute group, Resource Requests attribute group

Table 16. Attribute groups and workspaces (continued)

Workspace	Attribute group
Resource Requests workspace	Resource Requests attribute group
Status Items workspace	Status Items attribute group

Attributes by attribute group

The rest of this chapter lists the attributes (in alphabetical order by attribute group) for the SA z/OS monitoring agent. You can use these attributes to monitor the status of automation and of your automated applications, build custom workspaces, and create situations to alert you of pending problems.

Automation Agent Detail Information attribute group

Use the Automation Agent Detail Information attributes to display a report about the details known about a particular automated system, that is, a NetView domain. In contrast to other attribute groups, the information provided here is intended only for reference and not for monitoring.

Managed System
> The name of the node that the SA z/OS agent is running on. The valid format is a character string with a maximum length of 32 bytes and the following syntax:

> `sysplex:smfid:SAAGENT`

Text   This table shows detailed information about the NetView automation agent.

- The first section identifies the system by its name, the name of the sysplex it belongs to, the domain ID and the sysplex group as defined in the policy database. The XCF group name specifies the XCF group that the system is a member of.
- The "Software" section shows the z/OS release level, the NetView release level including the active Tower (or Towers) and the SA z/OS release level.
- The "Configuration" section shows the name of the currently active Automation Control File (ACF), when it was built and who built it. It also shows the timestamp when the ACF was activated and the configuration token.
- The next section shows the names of the currently active NetView Automation Tables.
- The "Flags" section shows the current settings for system automation.
- The "Scheduling Subsystem" section identifies the name and type of the primary scheduling subsystem. The type is either JES2, JES3, or ? if unknown.
- The Root for SDF updates is used to differentiate between systems when performing status updates.
- USS path shows the path where the SA z/OS USS automation programs (for example, INGCCMD) are installed.
- Sysplex Timing modes show any differences between the defined and actual sysplex configuration. The defined mode may be NONE, ONE, or TWO. SA z/OS determines the current mode: LOCAL, SIMULATED, SINGLE, or DOUBLE. A current mode of unknown means that the

detection routines have not yet run. The IDs of any Sysplex Timers that SA z/OS has found are also displayed.

- The "Heartbeat Interval" specifies the time interval in minutes at which SA z/OS will send a generic alert from this system to the NMC focal point. SA z/OS on the focal point uses Heartbeat alerts to verify the status forwarding path from each remote system.
- The "Missing Heartbeat Delay" specifies the time in seconds that SA z/OS on the NMC focal point will wait for a heartbeat. If this time expires without receiving the heartbeat, SA z/OS will begin its missing heartbeat processing for the remote system. For more information see *IBM Tivoli System Automation for z/OS Defining Automation Policy*.
- The next section shows the messages captured for the system components. This section is only displayed when the captured message limit is greater than zero.
- The "WLM Data" section shows the WLM capacity information that SA z/OS uses to place the members of MOVE and SERVER groups on the systems. This section is displayed only when the WLM querying process is active.
- The timestamp indicates when WLM was queried.
- SUs Total shows the number of SUs that were available in the last 10 minutes.
- SUs Used shows the number of SUs that were used in the last 10 minutes.
- Res. DS=AVAILABLE shows the number of SU-consuming resources with a desired state of AVAILABLE.
- SUs expected free shows the number of free SUs taking into account the resources that SA z/OS is about to start or stop.

Automation Environment attribute group

Use the Automation Environment attributes to display those systems running a SA z/OS agent or a SA z/OS manager connected to the SA z/OS sysplex XCF group. The SA z/OS sysplex is denoted by the managed system name.

Managed System
> The name of the SA z/OS subplex, that is, the group of systems controlled by a single primary automation manager and configured to the same XCF group. The valid format is a character string with a maximum length of 32 bytes and the following syntax:
>
> ```
> sysplex:saplex:SA
> ```

System Name
> The name of the system the automation agent or automation manager is running on. The system name can be up to 8 characters long.

Member Name
> The name given to the automation manager or automation agent. The member names are automatically assigned by SA z/OS.

Role The role that the instance plays:

> **AGENT**
> > The instance is an automation agent.
>
> **PAM** The instance is the primary automation manager.
>
> **SAM** The instance is a secondary automation manager.

Automation Environment attribute group

AM The instance is an automation manager that initializes.

Status The member's status. It can be one of the following:

NOT READY
Indicates that the automation manager is initializing. For an automation agent it means one of the following:

- The automation agent is initializing but has not yet received the ACF_LOAD order from the automation manager.
- The automation agent could not load the ACF as requested by the automation manager, this is most likely due to token mismatch.

READY
Indicates that the automation manager or automation agent has completely initialized.

PENDING
Indicates that the automation manager is in the process of initializing as a primary automation manager. For an automation agent it means that the automation agent is in the process of loading the ACF as requested by the automation manager or with the ACF LOAD command.

SELECTED
Indicates that the automation manager has been selected to become the next primary automation manager (PAM).

STOPPING
Indicates that the automation manager is terminating.

REFRESH
Indicates that the automation agent will perform a configuration refresh. After the configuration refresh is completed the status shows READY again.

Sysplex Name
The name of the sysplex.

XCF Group Name
The name of the associated XCF group.

Product Release
The release level of the automation agent or automation manager. The syntax of this field is V*v*R*r*M*m*, where

- *v* denotes the product version
- *r* denotes the product release
- *m* denotes the modification level

Comm Method
The type of communication being used between the automation manager and the automation agent. It can be one of the following:

XCF Communication is handled by means of XCF.

MQ Communication is handled by means of MQSeries® messages.

E2E Focal Point™
The end-to-end focal point indicator. The end-to-end focal point is the interface that the automation adapter with the z/OS plug-in is running for end-to-end automation. The value can be one of the following:

> **No**   This z/OS system is not the focal point for connecting the SA z/OS subplex to an end-to-end automation environment.
>
> **Yes**   This z/OS system is the focal point that connects the SA z/OS subplex to an end-to-end automation environment.

SID   The 4-character SMF system ID the member is running on.

Automation Manager Detail Information attribute group

Use the Automation Manager Detail Information attributes to display reference information about the environment the SA z/OS automation manager is running in. In contrast to other attribute groups, the information provided here is intended only for reference and not for monitoring.

Managed System
> The name of the SA z/OS subplex, that is, the group of systems controlled by a single primary automation manager and configured to the same XCF group. The valid format is a character string with a maximum length of 32 bytes and the following syntax:
>
> `sysplex:saplex:SA`

Text   This table shows detailed information about the specified primary automation manager.

> - The **Workitem Statistics** section shows the number of work items received from the various automation agents (external) as well as internally generated work items.
> - The **CPU Time** shows the processor time (in seconds) used by the automation manager.
> - The **Logic deck** section shows the date and time when the logic deck was built and the last APAR number of the logic deck.
> - The **Configuration** section displays the data set name that the configuration is loaded from, the main configuration member name, and the include members with their timestamps.
> - The **Diagnostic Info** section shows details about the size of the state image and other useful information. This can be used when allocating the data set that will hold snapshot data.
> - The **Queue** section shows MQ statistics about the various queues used by SA z/OS.

Automation Statistics attribute group

Use the Automation Statistics attributes to display statistical information about the automation agent and some basic information about the automation manager.

Managed System
> The name of the node that the SA z/OS agent is running on. The valid format is a character string with a maximum length of 32 bytes and the following syntax:
>
> `sysplex:smfid:SAAGENT`

Statistics Begin
> Local time that statistics reporting started at.

Statistics End
> Local time that statistics reporting ended at. This is the current time that the statistics were requested at.

Automation Statistics attribute group

Statistics Interval
Report interval as the difference between Statistics End and Statistics Begin in the format hhhh:mm.

CPU Time
The CPU time in seconds consumed by the NetView address space.

Resource Count
Total number of resources defined.

Managed Resource Count
Total number of resources managed.

Monitor Count
Total number of monitors defined.

Messages Count
Total number of messages automated.

Command Count
Total number of commands resulting from message automation.

Startup Command Count
Total number of startup commands.

Shutdown Command Count
Total number of shutdown commands.

Workitem Count
Total number of work items.

Timeout Count
Total number of timeouts.

Order Count
Total number of orders.

Messages Per Hour
Average number of messages per hour.

Commands Per Hour
Average number of commands per hour.

Workitems Per Hour
Average number of work items per hour.

Average Waittime
Average wait time for work item to be processed.

Maximum Waittime
Maximum wait time for work item to be processed.

Orders Per Hour
Average number of orders per hour.

System Count
Number of systems in the SA z/OS subplex.

SAplex Resource Count
Total number of resources known by the automation manager.

SAplex Application Count
Total number of application resources (type APL).

SAplex Application Group Count
Total number of application group resources (type APG).

> **SAplex Monitor Resource Count**
> Total number of monitor resources (type MTR).

Critical Messages attribute group

Use the Exceptional Messages attributes to display all important messages that currently exist for a given System.

Managed System
The name of the node that the SA z/OS agent is running on. The valid format is a character string with a maximum length of 32 bytes and the following syntax:

```
sysplex:smfid:SAAGENT
```

System Message ID
The system message identifier that is used to DOM the message.

Resource Name
The resource name that is associated with the message.

Resource Type
The resource type that is associated with the message.

Resource System
The resource system that is associated with the message.

Severity
The message severity, which can be IMPORTANT, UNUSUAL, or CRITICAL. For details see the chapter "Captured Message Status Definitions" in *IBM Tivoli System Automation for z/OS User's Guide*.

Timestamp
The timestamp in ITM format when the message was captured.

Store Clock Time
The timestamp in STCK format when the message was captured.

Message
The message text.

Job ID
The JES ID of the originating job.

Reply ID
The reply ID if the message is a WTOR.

CM Severity Important
The message severity is IMPORTANT.

CM Severity Unusual
The message severity is UNUSUAL.

CM Severity Critical
The message severity is CRITICAL.

Gateway Connections attribute group

Use the Gateway Connections attributes to display gateway connections and their connection status.

Managed System
The name of the node that the SA z/OS agent is running on. The valid format is a character string with a maximum length of 32 bytes and the following syntax:

Gateway Connections attribute group

Domain Name
    The name of the NetView domain that the gateway has been defined to.

SDF Root Name
    The system name of the domain.

Status The gateway session status at the time of the query. The status can be:
- ACTIVE
- BADDOMAIN
- INACTIVE
- INVOPID
- NOTSTARTED
- SESSFAIL

Communication Method
    The communication method, which can be XCF, IP, SNA, RPC, or empty (N/A).

Description
    Descriptive information about the gateway.

Inbound Status
    The current inbound status of the gateway. The status can be:
- ACTIVE
- BADDOMAIN
- INACTIVE
- INVOPID
- NODIRECT
- NOTSTARTED
- SESSFAIL

Outbound Status
    The current outbound status of the gateway. The status can be:
- ACTIVE
- BADDOMAIN
- INACTIVE
- INVOPID
- NODIRECT
- NOTSTARTED
- SESSFAIL

Last InRequest
    The last gateway request from the gateway domain to this domain. It can be: CHECK, CONNECT, DISCONN, or empty (N/A).

Last OutRequest
    The last gateway request from this domain to the gateway domain. It can be: CHECK, CONNECT, DISCONN, or empty (N/A).

Release Level
    The SA z/OS release level on the gateway domain.

GW Status Active
    The gateway session status is ACTIVE.

GW Status BadDomain
    The gateway session status is BADDOMAIN.

GW Status InActive
    The gateway session status is INACTIVE.

GW Status InvOpid
> The gateway session status is INVOPID.

GW Status NotStarted
> The gateway session status is NOTSTARTED.

GW Status Sessfail
> The gateway session status is SESSFAIL.

Monitor Resources attribute group

Use the Monitor Resources attributes to display information about SA z/OS Monitor Resources that are defined in the SA z/OS subplex.

Managed System
> The name of the SA z/OS subplex, that is, the group of systems controlled by a single primary automation manager and configured to the same XCF group. The valid format is a character string with a maximum length of 32 bytes and the following syntax:
>
> ```
> sysplex:saplex:SA
> ```

Monitor Name
> The name of the monitor resource.

System Name
> The name of the system where the monitor resource runs.

Status The status of the monitor resource. The monitor resource status can be any of the following:

> **Active** The monitor resource is active.
>
> **Inactive**
> > The monitor resource is inactive.
>
> **Failed** The monitor resource failed. Recovery might be in progress. No acceptable health status is provided.
>
> **Broken**
> > The monitor resource and its recovery failed. This is a permanent condition. The monitor resource is no longer invoked.

Health
> The health state of the objects that the monitor resource is watching. This implies that the monitor resource is active. It can have the following value:

> **Unknown**
> > The health status has not been determined yet.
>
> **Normal**
> > The health is OK.
>
> **Warning**
> > The health is degraded.
>
> **Minor** Similar to Warning but more severe.
>
> **Critical**
> > Similar to Minor but more severe.
>
> **Fatal** Similar to Critical but more severe.

Last Monitored
> The time stamp when the monitor resource status was last recorded.

Status Message
> The message that is associated with the status.

Description
> Descriptive information about the monitor resource.

HS Unknown
> The health status is Unknown.

HS Normal
> The health status is Normal.

HS Warning
> The health status is Warning.

HS Minor
> The health status is Minor.

HS Critical
> The health status is Critical.

HS Fatal
> The health status is Fatal.

OMEGAMON Sessions attribute group

Use the OMEGAMON Sessions attributes to display information about the OMEGAMON sessions that exist between SA z/OS and any of the classic OMEGAMON monitors for MVS, CICS, DB2, and IMS™.

Managed System
> The name of the node that the SA z/OS agent is running on. The valid format is a character string with a maximum length of 32 bytes and the following syntax:
>
> `sysplex:smfid:SAAGENT`

Session Name
> The OMEGAMON session name.

Session Type
> Type of OMEGAMON classic monitor that is represented by this session.

Session Status
> The session status at the time of the query.
>
> **Inactive**
> > The session is inactive.
>
> **Active** The session is active.
>
> **Maintenance**
> > The session was explicitly stopped by operations.
>
> **SessFail**
> > The session could not be established due to a communication error or invalid application ID.
>
> **AuthFail**
> > The session could not be established because OMEGAMON product security is enabled and the user that is defined to log on to the session is not authorized to do so.
>
> **Terminated**
> > The session has terminated (internal status only).

Starting
> The session is about to be established (internal status only).

Attached
> The session is attached and about to be fully initialized (internal status only).

Application ID
> Application ID (VTAM minor node) of the OMEGAMON monitor that is connected to.

Source LU Name
> Source LU name of the Terminal Access Facility (TAF) session that is connected to the OMEGAMON monitor.

Session Data
> Session data used to establish a connection.

User ID
> Name of user that logged on to the OMEGAMON session.

Managed Password
> Indicates whether the password is managed by SA z/OS using the NetView password data set.
>
> **No**   The password is defined directly in the OMEGAMON session definition policy.
>
> **Yes**   The password is kept in the NetView password data set.

Authentication Group
> The 5-character group name used to manage a set of OMEGAMON sessions having the same userid and password. The authentication group is only relevant in combination with passwords managed by SA z/OS.

Session Operator
> Name of the SA z/OS automated function that is processing the requests for this session.

Timeout
> Timeout after which a request is thrown away.

Request Count
> Total number of requests, that is, commands and traps issued since the session became active.

Command Count
> Total number of commands issued since the session became active.

Trap Count
> Total number of exception traps issued since the session became active.

Exception Count
> Total number of exceptions found since the session became active.

Users   List of NetView operators using the session since it became ACTIVE. If the actual number of operators exceeds the space reserved for this attribute, the list is truncated and ends with "...".

Session Profile
> Suffix of the OMEGAMON session profile that is used for this session.

OMEGAMON Version
> The version of the OMEGAMON Classic product that is being used.

Target System
The SMF ID of the system that the OMEGAMON Classic product is running on.

Fixed LU Name
The fixed LU name of the Terminal Access Facility (TAF) session as defined in the automation policy.

Outstanding WTOR Replies attribute group

Use the Outstanding WTOR Replies attributes to display the Sysplex WTORs and their severity.

Managed System
The name of the SA z/OS subplex, that is, the group of systems controlled by a single primary automation manager and configured to the same XCF group. The valid format is a character string with a maximum length of 32 bytes and the following syntax:

`sysplex:saplex:SA`

Resource Name
The name of the subsystem that issued the WTOR.

Resource Type
The resource type of the subsystem that issued the WTOR. The only valid type is APL.

Resource System
The name of the system where WTOR is issued

Severity
The message severity, which can be any of the following: IGNORE, NORMAL, IMPORTANT, UNUSUAL, CRITICAL. For details see the chapter "WTOR Processing" in *IBM Tivoli System Automation for z/OS Customizing and Programming*.

Reply ID
The reply ID.

Message ID
The message ID.

Message Text
The message text.

Timestamp
The time stamp when the WTOR was issued, in the format hh.mm.ss.

Jobname
The job name, if applicable.

Job ID
The JES ID of the originating job.

User ID
The user ID that issued the WTOR.

Asid The address space ID.

Message Flag
The message flag that indicates the status of the message. It can be (the parentheses containing the z/OS message flag character):
  • DELETED (|)
  • INFO (-)

- WTOR (*)
- PROGRAM(@)
- WTO (+)
- NOACTION (Blank)

In this context the default is WTOR.

WT Sev Ignore
The WTOR severity is IGNORE.

WT Sev Normal
The WTOR severity is NORMAL.

WT Sev Important
The WTOR severity is IMPORTANT.

WT Sev Unusual
The WTOR severity is UNUSUAL.

WT Sev Critical
The WTOR severity is CRITICAL.

WT MsgFlag Deleted
The WTOR Message Flag is DELETED.

WT MsgFlag Info
The WTOR message flag is INFO.

WT MsgFlag WTOR
The WTOR message flag is WTOR.

WT MsgFlag Program
The WTOR message flag is PROGRAM.

WT MsgFlag WTO
The WTOR message flag is WTO.

WT MsgFlag Noaction
The WTOR message flag is NOACTION.

Resource Agent Information attribute group

Use the Resource Agent Information attributes to display report about the details known about a particular resource from the automation agent's view. In contrast to other attribute groups, the information provided here is intended only for reference and not for monitoring.

Managed System
The name of the node that the SA z/OS agent is running on. The valid format is a character string with a maximum length of 32 bytes and the following syntax:
```
sysplex:smfid:SAAGENT
```

Text This table shows detailed information about the specified subsystem or Monitor Resource.

- For *subsystems*, the following is shown:
  - Description
  - Job name and type
  - Current® status
  - Monitoring information
  - Automation flag settings
  - Restart information

- Threshold values
- Start commands
- Shutdown commands
- Timer commands associated with the subsystem
- Captured messages

Note: For details of what most of the fields mean, refer to the SA z/OS customization dialogs, or *IBM Tivoli System Automation for z/OS Defining Automation Policy*.

- For *Monitor Resources*, the following information is shown:
  - Monitor name
  - Monitor description
  - Activate and deactivate command
  - Monitor command and monitor interval
  - Monitor status and time stamp when monitor information was last recorded
  - Health status
  - Status message, if present
  - Policy definitions
  - History data provided by the monitor. This consists of
    - The monitor status
    - Time stamp when the monitor information was recorded
    - A message that explains the status.

Resource List attribute group

Use the Resource List attributes to display the System Automation Manager's view of resources and their different types of states in the SA z/OS subplex denoted by the managed system name.

Managed System
　　The name of the SA z/OS subplex, that is, the group of systems controlled by a single primary automation manager and configured to the same XCF group. The valid format is a character string with a maximum length of 32 bytes and the following syntax:

```
sysplex:saplex:SA
```

Resource Name
　　The name of an automation resource, that is, the first qualifier of the resource name in automation manager notation.

Resource Type
　　The type of an automation resource, that is, the second qualifier of the resource name in automation manager notation. The valid types are:

APL　　The resource is an application, for example, a job.

APG　　The resource is an application group.

SYS　　The resource is a z/OS system.

SYG　　The container resource that contains all the resources in the z/OS system.

GRP A group representing a physical sysplex (systems with the same XCF group ID) or a logical sysplex (systems with different XCF group IDs).

IMG The resource is an application whose sole purpose is to represent a system image.

MTR The resource is a monitor resource.

System

The name of the system where the resource resides. Blank for sysplex resources.

Observed Status

The current status of the resource as observed by the automation agent.

Unknown

The automation manager does not have any observed status information about the resource. The automation manager will assume that the resource is unavailable and will try to make it available if this is the desired status.

SysGone

The system that the resource resides on is no longer an active member of the sysplex.

SoftDown

The resource is not available (is unavailable), but automation may make it available if a request is made to do so.

HardDown

The resource is not available and automation will not make it available.

Starting

The automation agent that is in charge of the resource is either in the process of making the resource available, or has detected that the resource is being started by another source.

Available

The resource is ready for use.

Degraded

The resource is available but has some performance or capacity problems.

Problem

The resource is available but has a serious problem, most likely making it unusable.

Stopping

The automation agent that is in charge of the resource is in the process of stopping the resource, or has detected that the resource is being shut down by another source.

WasAvailable

The automation manager has lost contact with the automation agent that is responsible for the resource. However, the resource was active (available) when contact was lost and the system that the resource resides on appears to be running. The resource will be treated as being available. This is primarily to prevent inappropriate recovery actions from being initiated whenever an SA z/OS NetView is recycled.

Resource List attribute group

Standby
> The resource has a primary or secondary system association defined. The automation agent posts this status when setting the agent status to MOVED or FALLBACK.
>
> **Note:** The automation manager treats STANDBY like a HARDDOWN status except that it is not considered to indicate an error condition.

Desired Status
> The status that the automation manager is trying to move the resource to.

Available
> The resource should be started (made available).

Unavailable
> The resource should be stopped (made unavailable).

Automation Status
> The status representing the automation agent's automation for the resource.

Unknown
> The automation manager does not have a connection to the automation agent that is responsible for the resource. No automation will be done.

Sysgone
> The system that the resource resides on is no longer an active member of the sysplex.

Idle
> The automation agent that is responsible for the resource is not doing anything for the resource. No orders have been sent by the automation manager that the agent is working on. The automation manager may send the automation agent new orders.
>
> The automation agent posts this status when setting the agent status to DOWN, RESTART, UP, ENDED, AUTODOWN, CTLDOWN, STOPPED, BROKEN, INACTIVE, MOVED, or FALLBACK.

Ordered
> The automation manager has sent an order to the automation agent that is responsible for the resource to either start or stop the resource. The agent is working on the order.

Busy
> The automation agent that is responsible for the resource is processing the orders that were sent by the automation manager, or observing or assisting a start or stop process that was initiated by another source. This status is set when the resource's observed status becomes STARTING or STOPPING, and the previous automation status was IDLE or ORDERED. This status is changed to IDLE if the resource reaches an observed status other than STARTING or STOPPING.
>
> The automation agent posts this status when setting the agent status to STARTED, EXTSTART, ACTIVE, RUNNING, ENDING, AUTOTERM, STOPPING, ABENDING or BREAKING.

Denied
> The automation agent was not allowed to process the last order

that it received. The status is changed to IDLE if the resource reaches an observed status of HARDDOWN, SOFTDOWN or AVAILABLE.

The automation agent posts this status if the agent automation flags do not permit the action.

Problem
The automation agent encountered a problem while processing for the resource. This status is changed to IDLE if the resource achieves an observed status of HARDDOWN, SOFTDOWN or AVAILABLE.

Note: This status is posted by the automation agent when setting the agent status to STARTED2, HALFDOWN, STUCK or ZOMBIE.

Internal
This means that the automation of the resource is being handled internally. The resource does not have an automation agent that is responsible for it.

Automation Flag
Shows the automation flag that is maintained by the automation manager. No automation is done for the resource by the automation manager when the flag is off.

Yes   Automation is allowed.

No   Automation is not allowed.

Hold Flag
Shows the hold flag that is maintained by the automation manager.

No   Start the resource at IPL.

Yes   Hold the resource at IPL until it is released by operations.

Description
Descriptive information about the resource.

Start Type
The preset start type that will be used the next time the resource is made available (started). This value is set by INGSET and will override any TYPE value that is specified (or defaulted to) in the next INGREQ start request.

Stop Type
The preset stop type that will be used the next time the resource is made unavailable (shut down). This value is set by INGSET and will override any TYPE value specified (or defaulted to) in the next INGREQ stop request. However, a stop type of FORCE, wherever specified, will always be honored.

Schedule
The schedule (service period) that the resource is linked to.

Trigger
The trigger that is associated with the resource.

Compound Status
The compound status of the resource. This is a summary of all statuses of

Resource List attribute group

the resource and provides a single value that tells you if the resource is OK or if it has a problem. It can have one of the following values:

Problem
There is a problem with this resource that automation cannot solve. Operator intervention is required.

Denied
The resource is not in its desired state but automation is unable to process it. This can be caused, for example, by an automation flag that has been turned off, a resource that has been put on hold, or if the automation agent was not allowed to process the last order. Another cause is that the system hosting the resource is in a suspended state.

Inhibited
The resource is not in its desired state and automation is unable to proceed because of a problem with its supporting resource or resources. In most cases this is caused by a supporting resource that has a compound status of PROBLEM or DENIED.

Awaiting
The resource is not in its desired state and the automation manager is waiting for its supporting resources to reach the appropriate state.

InAuto
The automation manager is in the process of starting or stopping the resource.

Degraded
The resource is either starting or stopping, or it is suffering from a performance or throughput problem (corresponding to the automation agent status HALTED).

For a group resource this means that it is partially running, but not at full capacity (not all of the members necessary to meet the availability target are active).

Satisfactory
The resource's desired and observed status are synchronized; no further automation or operator activity is required.

Startability Status
Indicates whether or not it is possible to start the resource if the automation manager is asked to do so at this point in time. It can have one of the following values:

Unknown
The startability status is not available for this resource.

Yes The resource can be started.

No The resource cannot be started.

Inhibited
The resource cannot be started because of either a problem with one of its supporting resources (start dependency), or because automation has been prohibited.

Denied
> The resource is not startable because automation for this resource is denied. For example, this might be the case when the system is suspended.

Group Nature
> Applies to group resources only and defines the type of the group.

> **BASIC**
>> Indicates that the group contains a number of different resources, all of which perform different roles to make a complete application.

> **MOVE**
>> Indicates that the group contains alternate instances of the same resource.

> **SERVER**
>> Indicates that the group contains a number of readily interchangeable resources. The group has a target that tells the automation manager how many of them should be made available for the group to be available.

Category
> Shows the category of the resource, such as CICS, DB2 or IMS.

Subtype
> The subtype of the resource. Applies to resources of category CICS, DB2, IMS and TWS.

Health Status
> The health status of the resource.

> **Unknown**
>> The health status has not yet been determined.

> **Normal**
>> The health is OK.

> **Warning**
>> The health is degraded.

> **Minor** Similar to Warning but more severe.

> **Critical**
>> Similar to Minor but more severe.

> **Fatal** Similar to Critical but more severe.

> **Ignore** The health status is ignored.

> **SysGone**
>> The system that this monitor resource is running on is no longer available.

> **NA** No health status is available.

Resource Manager Information attribute group

Use the Resource Manager Information attributes to display a report about the details known about a particular resource from the automation manager's view. In contrast to other attribute groups, the information provided here is intended only for reference and not for monitoring.

Managed System

The name of the SA z/OS subplex, that is, the group of systems controlled by a single primary automation manager and configured to the same XCF group. The valid format is a character string with a maximum length of 32 bytes and the following syntax:

```
sysplex:saplex:SA
```

Text This table shows detailed information about the specified resource.

- Resource statuses and dependencies
- Resource settings
- Relationships that have been defined for the resource
- Requests that have been issued against the resource
- Votes that are pending for the resource
- History data that has been collected for the resource

Resource Requests attribute group

Use the Resource Requests attributes to display the System Automation Manager's view of requests for resources in the SA z/OS subplex denoted by the managed system name.

Managed System

The name of the SA z/OS subplex, that is, the group of systems controlled by a single primary automation manager and configured to the same XCF group. The valid format is a character string with a maximum length of 32 bytes and the following syntax:

```
sysplex:saplex:SA
```

Resource Name

The name of the resource that the request was made against.

Resource Type

The type of an automation resource, that is, the second qualifier of the resource name in automation manager notation. The valid types are:

APL The resource is an application, for example, a job.

APG The resource is an application group.

SYS The resource is a z/OS system.

SYG The container resource that contains all the resources in the z/OS system.

GRP A group representing a physical sysplex (systems with the same XCF group ID) or a logical sysplex (systems with different XCF group IDs).

IMG The resource is an application whose sole purpose is to represent a system image.

MTR The resource is a monitor resource.

System

The name of the system where the resource resides. Blank for sysplex resources.

Action

The action requested for this resource and the scope of this action. The scope specifies whether the action affects the resource itself or its descendants, or both. The list of possible actions are:

- Unknown
- MakeAvailable
- MakeAvailable_Only
- MakeAvailable_All
- MakeUnAvailable
- MakeUnAvailable_Only
- MakeUnAvailable_All
- MakeUnAvailable_Children

Creation Time

The date and time when the request was made.

Source

Indicates who made the request. It is normally OPERATOR or AUTOOPS, but can also be anything else. If the request was made by an operator it also shows the operator ID. Note that each source can have only one active request of each type against each resource. While votes relating to other requests are propagated to the resource, if the source makes a second request directly against the resource, it will replace the first request.

Priority

The hexadecimal priority of the request. It determines the importance of this request relative to other requests within the resource structure. The higher this value, the higher is the request's priority.

Status The status of the request. A request can be pending (P), winning (W), or losing (L). Requests can furthermore be satisfied (S), unsatisfied (U), or timed out (T). The status is a combination of these attributes, for example W/S/T represents a satisfied winning request that timed out.

Timeout Option

An optional request modifier that can be specified in combination with the timeout:

- When 'Message' is shown, a message is sent to the notify operator stating that the request has not been satisfied within the expected time interval.

- When 'Cancel' is shown, the request will be cancelled automatically after expiration of the timeout.

The default behavior is 'Message'. Only set when a timeout has been specified.

Overrides

Possible override options passed with the request. The override options can be used to bypass the conditions and settings that would otherwise prevent a resource from starting or shutting down. It can be 'NO', 'ALL', or a combination of the following options:

TRG Ignores the current trigger setting.

FLG Ignore automation flags.

DPY Ignores the start and stop dependencies that have been defined for the resource.

STS Ignores an observed status of HARDDOWN. However, a resource will only be started until it is placed in SOFTDOWN status.

UOW Ignores the current outstanding Unit Of Work status for a CICS subsystem.

Resource Requests attribute group

INIT Ignores the results of the INITIAL start tests for a CICS subsystem.

User The operator ID that issued the request, if applicable.

Comment
A comment that is associated with the request.

Appl Parms
Optional application parameters that can be specified with the request. If the text is longer than 32 characters, it is truncated and ends with "...".

Auto Remove
Optional specification of observed states that, when seen, cause the automatic removal of this request. The observed states that can be specified are a combination of AVAILABLE, DEGRADED, SYSGONE, and UNKNOWN.

Restart
Specifies whether the resource should be restarted automatically after it has been shut down completely.

No The resource is stopped and left in Softdown status.

Yes The resource is stopped and after completion of the shutdown of the resource, it is started again.

Children
The children of the resource are stopped and after completion of the shutdown, they are started again.

Request Type
An optional start or stop type for the request. Start types can be NORM or any other customer-defined start types. The standard stop types are NORM, IMMED, and FORCE.

Timeout Time
Optional time when the request will time out (GMT).

Expiration Time
Optional time when the request will expire (GMT).

Winning Start
Count is set to 1 if this request is a winning start request.

Winning Stop
Count is set to 1 if this request is a winning stop request.

Losing Start
Count is set to 1 if this request is a losing start request.

Losing Stop
Count is set to 1 if this request is a losing stop request.

Operator Request
Count is set to 1 if this request is an operator request.

Priority Class
The priority class is set according to the hexadecimal priority string denoted by the Priority attribute. It can have the following values: NA, Low, High, and Force.

Resource Votes attribute group

Use the Resource Votes attributes to display all requests and votes that are queued for the resource. A vote is a request that has been entered for another resource but propagated along the dependency graph to the resource.

Managed System
> The name of the SA z/OS subplex, that is, the group of systems controlled by a single primary automation manager and configured to the same XCF group. The valid format is a character string with a maximum length of 32 bytes and the following syntax:
>
> sysplex:saplex:SA

Action
> The action resulting from the request. This is either to START or STOP the resource as determined by the automation manager for the resource.

Win   Indicates whether or not this is the winning vote.

> **Y**   This is the winning vote.
>
> **P**   This is a vote that is propagated along the dependency graph.
>
> **N**   This is a vote, referred to as the losing vote, that is *not* propagated along the dependency graph to other resources.
>
> **N/A**   This is a vote that is currently not relevant for the decision making process.

> The vote with the highest priority is the winning one.

Type   The type of activity. It can be Request or Vote.

> **Request**
> > Indicates that the entry represents a request. It shows the requested action that has been asked for in the INGREQ command or the associated service period definitions.
>
> **Vote**   Indicates that the entry represents a vote. It shows the proposed action for the resource. A vote is a request that has been entered for another resource but propagated along the dependency graph to this resource.

From Action
> The original request that was propagated to the resource. Refer to the From_Resource attribute to see the resource that the request was made against.

From Resource
> For votes only, the resource that this vote was propagated from.

Creation Time
> The time that this request or vote was created.

Usage   The number of times that the vote has been propagated to the resource. This is the case when more than one path exists from the entry resource to this resource in the dependency web. It is only shown when greater than one.

Source
> Indicates who made the request. It is normally OPERATOR or AUTOOPS, but can also be something else. If the request was made by an operator it also shows the operator ID.

Priority

The priority that is assigned to the request. The value is the hexadecimal representation of the priority.

The priority determines how important the request is with regard to other requests within the resource structure. Low priority requests may be ignored if the resources that they target are already affected by a higher priority request.

Status The status of the request or vote. It can be pending (P), winning (W), or losing (L). Requests can furthermore be satisfied (S), unsatisfied (U), or timed out (T). The status is a combination of these attributes, for example W/S/T represents a satisfied winning request that timed out.

Comment

A comment that is associated with the request.

Priority Class

The priority class is set according to the hexadecimal priority string denoted by the Priority attribute. It can have the following values: NA, Low, High, and Force.

Status Items attribute group

Use the Status Items attributes to display all user defined status items within the SA z/OS subplex.

Managed System

The name of the SA z/OS subplex, that is, the group of systems controlled by a single primary automation manager and configured to the same XCF group. The valid format is a character string with a maximum length of 32 bytes and the following syntax:

```
sysplex:saplex:SA
```

System

Status item originator. This field contains the name of the system that the status item is collected on.

The ATOMIZE flag is set for this attribute, making it a selectable display item.

Group Status item group. If the status item was defined in form of two subfields separated by a period, this is the first subfield. Otherwise, the field is empty.

The ATOMIZE flag is set for this attribute, making it a selectable display item.

Name Status item name. If the status item was defined in form of two subfields separated by a period, this is the second subfield. Otherwise, this is the complete name that was specified when the status item was created.

The ATOMIZE flag is set for this attribute, making it a selectable display item.

Value The current value of the status item. This is a positive integer value or zero that can be used to represent the status item's current condition.

The ATOMIZE flag is set for this attribute, making it a selectable display item.

Description

A textual description of the status item.

Transient Text

Status item text that can be set by the user to store transient text information.

The ATOMIZE flag is set for this attribute, making it a selectable display item.

Change Time

Time that the status item was changed most recently.

Persistence

Attribute that indicates whether or not the status item is persistent across NetView recycle or IPL.

Status Items attribute group

Chapter 13. Situations and situation events

The SA z/OS monitoring agent provides a set of predefined situations that monitor the status and health of automation resources within the SA z/OS subplex. These situations check for specified conditions and can trigger ❌ Critical, ⚠ Warning, or ⓘ Informational situation event indicators (also called alerts) in the Navigator. When a situation triggers an alert, you can investigate the situation event by opening its workspace. If both a warning and a critical condition occur for the same workspace, the indicator always shows the highest-level situation event (the critical one).

You can use the Situation Editor to examine the conditions or values being monitored and, if necessary, change them to ones better suited to your environment. You can also use the predefined situations as models for creating your own situations, using SA z/OS monitoring agent attributes. Before your new situations can take effect, you must distribute them to the systems you want to monitor. For instructions, see the Tivoli Enterprise Portal online help or *IBM Tivoli Monitoring: User's Guide*, SC32-9409.

> **Tip**
>
> Rather than editing a predefined situation, copy it with **Create Another** and then edit the copy. This practice prevents your edited situations from being overwritten during installation and configuration of future versions of the product.

Using the Situation Editor

You can use the Situation Editor in the Tivoli Enterprise Portal to perform the following operations:

- Create, edit, delete, or view a situation.
- Start and stop a situation.
- Associate a situation with the current Navigator item.

When you right-click a Navigator node and select **Situations** from the context menu, the Situation Editor opens with a list of the situations associated with the selected Navigator node. When you select the **Situation Editor** icon ( ) on the toolbar, the Situation Editor opens with a list of all SA z/OS monitoring agent situations.

See the Tivoli Enterprise Portal online help or *IBM Tivoli Monitoring: User's Guide*, SC32-9409 for more detailed information about using the Situation Editor.

Investigating a situation event

When the conditions of a situation have been met, the situation evaluates True, causing a situation event indicator to be displayed in the Navigator. You can investigate the cause of a situation event by opening its workspace. The situation event workspace shows two table views: one with the values of the attributes when the situation evaluated True, and the other with the current values of the

attributes. The event workspace also displays any expert advice written by the author of the situation, as well as a Take Action view that enables you to send a command to the z/OS system. (See the Tivoli Enterprise Portal online help or *IBM Tivoli Monitoring: User's Guide*, SC32-9409 for instructions.)

Situation formulas

Situations are expressions embedded in IF-TRUE statements of system conditions that you want to monitor. This means that if the specified condition exists, then the situation is true and triggers an alert.

A condition consists of an attribute, a value, and a comparison operator. When a situation is activated, the value of the attribute is compared with the value set for the condition to determine whether the condition is met. For example, the Kah_Rsrc_Not_Satisfactory_Crit situation is true when the value of the Compound_Status attribute is Problem. This is the formula:

```
If
Resource_List.Compound_Status equals Problem
then
the situation Kah_Rsrc_Not_Satisfactory_Crit is true.
```

For information about the attributes you can use in situations, see Chapter 12, "Attributes," on page 153.

Avoid using negative values

If you define situations that use a counter or a range of numbers, always provide positive values. For example, use a greater-than-or-equal-to-zero expression, as shown in some of the predefined situations described below. This practice prevents a situation from falsely tripping when the monitoring agent encounters an undefined attribute value. Undefined attribute values are interpreted as negative numbers and might erroneously raise alerts for a situation that specifies a negative number.

Predefined situations provided by the SA z/OS monitoring agent

The predefined situations packaged with the SA z/OS monitoring agent are distributed when the Tivoli Enterprise Monitoring Server is seeded (that is, initialized with application data).

In SA z/OS 3.3 the predefined situations are no longer started automatically, which means that the 'run at startup' flag is set to inactive.

The rest of this section describes the predefined situations and gives their formulas.

Kah_Rsrc_Not_Satisfactory_Crit

Kah_Rsrc_Not_Satisfactory_Crit raises an alert if the compound status of a resource is Problem. The formula is:

```
If
Resource_List.Compound_Status equals Problem
then
the situation Kah_Rsrc_Not_Satisfactory_Crit is true.
```

Kah_Rsrc_Not_Satisfactory_Warn

Kah_Rsrc_Not_Satisfactory_Warn raises an alert if the compound status of a resource is Degraded. The formula is:

```
If
Resource_List.Compound_Status equals Degraded
then
the situation Kah_Rsrc_Not_Satisfactory_Warn is true.
```

Kah_Rsrc_Not_Satisfactory_Info

Kah_Rsrc_Not_Satisfactory_Info raises an alert if the compound status of a resource is either Inhibited, Denied, Awaiting, or InAuto. The formula is:

```
If
Resource_List.Compound_Status equals Inhibited
or
Resource_List.Compound_Status equals Denied
or
Resource_List.Compound_Status equals Awaiting
or
Resource_List.Compound_Status equals InAuto
then
the situation Kah_Rsrc_Not_Satisfactory_Info is true.
```

Kah_Oper_Requests_Exist_Info

Kah_Oper_Requests_Exist_Info raises an alert for requests that originated from an operator. The formula is:

```
If
Resource_Requests.Operator_Request is greater than 0
then
the situation Kah_Oper_Requests_Exist_Info is true.
```

Kah_Resource_Health_Crit

Kah_Resource_Health_Crit raises an alert if the health status of a resource is Fatal. The formula is:

```
If
Resource_List.Health_Status equals Fatal
then
the situation Kah_Resource_Health_Crit is true.
```

Kah_Resource_Health_Warn

Kah_Resource_Health_Warn raises an alert if the health status of a resource is either Critical, Minor, or Warning. The formula is:

```
If
Resource_List.Health_Status equals Critical
or
Resource_List.Health_Status equals Minor
or
Resource_List.Health_Status equals Warning
then
the situation Kah_Resource_Health_Warn is true.
```

Kah_Agent_Not_Ready_Warn

Kah_Agent_Not_Ready_Warn raises an alert if the automation agent status is either Unknown or Not Ready. The formula is:

```
If
Automation_Environment.Status equals Unknown
or
```

```
Automation_Environment.Status equals NotReady
then
the situation Kah_Agent_Not_Ready_Warn is true.
```

Kah_Mtr_Resource_Status_Crit

Kah_Mtr_Resource_Status_Crit raises an alert if the monitor resource status is Broken. The formula is:

```
If
Monitor_Resources.Status equals Broken
then
the situation Kah_Mtr_Resource_Status_Crit is true.
```

Kah_Mtr_Resource_Status_Warn

Kah_Mtr_Resource_Status_Warn raises an alert if the monitor resource status is Failed. The formula is:

```
If
Monitor_Resources.Status equals Failed
then
the situation Kah_Mtr_Resource_Status_Warn is true.
```

Kah_Mtr_Health_Status_Crit

Kah_Mtr_Health_Status_Crit raises an alert if the monitor resource health status is Fatal. The formula is:

```
If
Monitor_Resources.Health equals Fatal
then
the situation Kah_Mtr_Health_Status_Crit is true.
```

Kah_Mtr_Health_Status_Warn

Kah_Mtr_Health_Status_Warn raises an alert if the monitor resource health status is either Critical, Minor, or Warning. The formula is:

```
If
Monitor_Resources.Health equals Critical
or
Monitor_Resources.Health equals Minor
or
Monitor_Resources.Health equals Warning
then
the situation Kah_Mtr_Health_Status_Warn is true.
```

Kah_Mtr_Health_Status_Info

Kah_Mtr_Health_Status_Info raises an alert if the monitor resource health status is either Unknown, or SysGone, or Ignore, or NA. The formula is:

```
If
Monitor_Resources.Health equals Unknown
or
Monitor_Resources.Health equals SysGone
or
Monitor_Resources.Health equals NA
or
Monitor_Resources.Health equals Ignore
then
the situation Kah_Mtr_Health_Status_Info is true.
```

Kah_OM_Session_Failure_Warn

Kah_OM_Session_Failure_Warn raises an alert if the OMEGAMON session status is SessFail. The formula is:

```
If
OMEGAMON_Sessions.Session_Status equals SessFail
then
the situation Kah_OM_Session_Failure_Warn is true.
```

Kah_OM_Authorization_Warn

Kah_OM_Authorization_Warn raises an alert if the OMEGAMON session status is AuthFail. The formula is:

```
If
OMEGAMON_Sessions.Session_Status equals AuthFail
then
the situation Kah_OM_Authorization_Warn is true.
```

Kah_GW_Bad_Status_Warn

Kah_GW_Bad_Status_Warn raises an alert if a gateway connection status is BadDomain, InvalidOpid, or Sessfail.

A BadDomain status indicates that the logon to the target domain failed. You should check the SA z/OS customization dialog GATEWAY policy and verify that the target domain is defined correctly.

An InvalidOpid status indicates that the automation operator that is used for GATOPER automated function does not exist on the target domain. It is recommended that you use identical DSIOPF definitions for all systems that communicate though gateways. See AOFOPFGW for an example.

A SessFail status indicates a network problem that prevented creating or maintaining a gateway connection with the target domain. You should check your SNA and TCP/IP connectivity.

The formula is:

```
If
Gateway_Connections.Status equals BadDomain
or
Gateway_Connections.Status equals InvOpid
or
Gateway_Connections.Status equals SessFail
then
the situation Kah_GW_Bad_Status_Warn is true.
```

Kah_WTOR_SevMsg_Crit

Kah_WTOR_SevMsg_Crit raises an alert if a WTOR that is defined as IMPORTANT or CRITICAL in the automation policy was issued on a system. You should consult the message description and installation guidelines to take appropriate action. The formula is:

```
If
Outstanding_WTORs.Severity equals Important
or
Outstanding_WTORs.Severity equals Critical
then
the situation Kah_WTOR_SevMsg_Crit is true.
```

Kah_WTOR_SevMsg_Info

Kah_WTOR_SevMsg_Info raises an alert if a WTOR was issued on a system that is undefined to automation. You should consider adding this message to the SA z/OS customization policy and assigning a proper value. The formula is:

```
If
Outstanding_WTORs.Severity equals Unusual
then
the situation Kah_WTOR_SevMsg_Info is true.
```

Kah_CM_SevMsg_Crit

Kah_CM_SevMsg_Crit raises an alert if a message that is defined as IMPORTANT or CRITICAL by the automation policy was issued on a system. You should consult the message description and installation guidelines to take appropriate action. The formula is:

```
If
Critical_Messages.Severity equals Important
or
Critical_Messages.Severity equals Critical
then
the situation Kah_CM_SevMsg_Crit is true.
```

Kah_CM_SevMsg_Info

Kah_CM_SevMsg_Info raises an alert if a message was issued on a system that is undefined to automation. You should consider adding this message to the SA z/OS customization policy and assigning a proper value. The formula is:

```
If
Critical_Messages.Severity equals Unusual
then
the situation Kah_CM_SevMsg_Info is true.
```

Chapter 14. Usage scenarios

The SA z/OS monitoring agent provides predefined workspaces and situations to help you start monitoring your z/OS systems and sysplex resources immediately. As you become more familiar with the product, you can modify the workspaces and situations to meet the specific needs of your enterprise.

This chapter contains scenarios that illustrate how the SA z/OS monitoring agent alerts you to potential or actual problems, and how you can use the product to isolate and resolve these problems.

Scenario 1: Monitoring the compound status of resources

In this scenario, you monitor the compound status of resources.

1. When a resource's compound state changes from SATISFACTORY to some other status, depending on the actual compound status, any of the predefined situations Kah_Rsrc_Not_Satisfactory_Crit, Kah_Rsrc_Not_Satisfactory_Warn, or Kah_Rsrc_Not_Satisfactory_Info becomes true and trigger a Critical, Warning, or Informational situation event indicator in the navigator view.

2. You view the event data by clicking on the colored icon on the navigator to see what resources are showing non-satisfactory states.

3. You click on the link icon in the event data panel to obtain additional details about this situation. The situation data that is presented tells you the resource name and the sysplex where the resource was found.

4. You return to the navigator view and select the node that represents the affected sysplex. The default workspace that is shown is the Resource Overview workspace that contains information similar to the SA z/OS NCCF INGLIST command. This workspace presents the overall automation status. You can see at a glance what other resources are defined, the number of non-satisfactory states in general, and an overview of requests that are currently being handled by the automation manager.

5. For further details about the resource, you select the resource that is in trouble from the list of all resources. This resource should be easier to locate if you first sort the list by compound status. When you click once on the attribute header, the table is sorted in ascending order, click once more and the table is sorted in descending order, and click a third time to displays the table in the original row order.

   Double click on the link icon to take you to the resource detail view where you find additional information related to the issue.

6. Once you have found the cause of the problem, you might open a 3270 NCCF terminal session on the Tivoli Enterprise Portal or delegate the problem to someone who is responsible for fixing it.

   Alternatively, you can use Take Action and issue the SA z/OS NCCF command of choice as a console command that must be directed to the z/OS system that the SA z/OS monitoring agent is running on.

Scenario 2: Identifying temporary operator requests

In this scenario, you identify at regular intervals requests whose source is OPER* to make sure that requests that are intended to be temporary in nature are removed after the expiration of the temporary time interval.

1. When resource start or stop requests exist that were inserted by an operator, the predefined situation Kah_Oper_Requests_Exist_Info becomes true and triggers an Informational situation event indicator in the navigator view.
2. When an event indicator has been triggered in the navigator view, you view the event data by clicking on the colored icon on the navigator to see all events that are associated with this node.
3. You click on the link icon for situation Kah_Oper_Requests_Exist_Info in the event data panel to obtain additional details about this situation. The situation data that is presented tells you the resource (or resources) that requests are made against that stem from an operator.

Similar information, which also includes requests from sources other than operators, is available on the Resource Overview workspace that provides a graphical overview of all requests that are currently injected into the automation.

1. When there are resource requests as indicated by the colored bar in the Request Summary view on the Resource Overview workspace you know that the automation has been overruled by operations.
2. The summary of requests is linked to the Resource Requests workspace that shows additional request details for all resources. If you sort the table by the columns Source or User, you can easily identify those requests that stem from operators only.
3. If you want to know even more detail about requests that affect a particular resource, you can click on the link icon that leads you to the Resource Details workspace for that resource.
4. On the Resource Details workspace, votes that stem from requests issued directly against this resource or that stem from requests to other supporting resources are displayed along with their status, their source, and their priority.

Once you have identified a request that should no longer exist, you can either remove the request yourself or delegate this to another person, by issuing the corresponding INGREQ CANCEL command from a 3270 NCCF screen.

Alternatively, you can use Take Action and issue the SA z/OS NCCF INGREQ command as a console command that must be directed to the z/OS system that the SA z/OS monitoring agent is running on.

Part 4. Problem determination

Chapter 15. Introduction to problem determination

This chapter helps you decide where to look for causes when you have a problem with the SA z/OS monitoring agent. Some of the problems you encounter might involve Tivoli Monitoring Services common components (such as the Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal client) rather than the SA z/OS monitoring agent. See the *IBM Tivoli Monitoring: Problem Determination Guide* for problems related to the common components.

Typically, you start with a symptom, or set of symptoms, and trace them back to their cause. This process is called *problem determination*. Problem determination is not the same as problem solving, although during the process of problem determination, you can often obtain enough information to solve a problem. Sometimes, however, you might encounter a problem that you cannot solve by yourself, even after determining its cause. For example, a performance problem might be caused by a limitation of your hardware. If you are unable to solve a problem on your own, contact IBM Software Support for a solution.

Problem determination flow

When you encounter a problem with any component, the primary troubleshooting feature is logging. *Logging* refers to the writing of text messages and trace data generated by the software to an output destination, such as a console screen or a file. A monitoring agent does not display messages at the Tivoli Enterprise Portal. Instead, the messages are sent to more typical z/OS output locations, such as sysout data sets or spool files or, more rarely, to the z/OS system console.

Tracing creates a record of the processing of a computer program or transaction. Trace logs capture information about the operating environment to help you diagnose problems when components fail to operate as intended. The principal trace log type is the reliability, availability, and serviceability (RAS1) trace log. You can set up RAS tracing for the monitoring agents, Tivoli Enterprise Monitoring Server, and Tivoli Enterprise Portal Server. The default level of tracing depends on the component and operating system. For the monitoring agents on z/OS, the default level is KBB_RAS1=ERROR, which means that only error messages are captured. This is the setting for minimal tracing.

> **Tips**
> - The Log and Trace Analyzer is a useful tool that can help you collect, view, analyze, and correlate log and trace information. See "Using the Log and Trace Analyzer tool" on page 196.
> - Overhead (CPU and I/O) associated with detailed RAS1 tracing might degrade performance of the monitoring agent. Restore RAS1 tracing for the monitoring agent to the default level KBB_RAS1=ERROR after you complete problem diagnosis.

Figure 57 on page 190 shows the flow of problem determination procedures for a monitoring agent on z/OS.

Problem determination flow

See "Determining whether the problem is caused by the monitoring agent"

Is the problem caused by the monitoring agent? — NO → Refer to the *IBM Tivoli Monitoring Problem Determination Guide*

For the monitoring agent:
- Check the program directory for required PTFs
- Check the PSP bucket for new information

YES

For Tivoli Management Services Components:
- Check Tech Notes
- Determine whether fix packs are available for any distributed components
- Consult IBM Support Assistant

Has required maintenance for all components been applied? — NO → Apply maintenance and see whether the problem persists

YES

Set up RAS1 tracing for the affected component.

See the instructions in this chapter and in "Setting up a trace on a z/OS system"

Analyze the logs.

Define a different type of trace

Would a more focused type of trace be helpful? — YES → (Define a different type of trace)

NO

Check the following:
- Problem Determination Guide for the monitoring agent
- *IBM Tivoli Monitoring Problem Determination Guide*
- RETAIN database

Am I experiencing a known problem? — YES → Use the documented solution or workaround

NO

Have I solved my problem or do I need help from IBM? — Solved → No further action required

Need help

See "Capturing z/OS logs to send to IBM Software Support"

Contact IBM Software Support.

Figure 57. Problem determination flow for a monitoring agent on z/OS

Determining whether the problem is caused by the monitoring agent

One of the most difficult troubleshooting issues in a client-server environment such as Tivoli Monitoring Services is determining which component is the origin of the problem. In most cases, the problem might seem to be a Tivoli Enterprise Portal client problem because this is what you can see. But this can be misleading, because the client can display data only if it receives data from the Tivoli Enterprise Monitoring Server.

In any problem scenario, try to gather documentation at the time of the error. What appears to be a client problem might well be a server problem, especially if data is not showing up at the client.

As you collect logs, create an exact description of the problem. For reproducible problems, document the exact navigation path that produced the error. Screen prints might also help with problem determination. For locations of log files for all the components of Tivoli Monitoring Services and for information about enabling tracing for distributed components, refer to *IBM Tivoli Monitoring: Problem Determination Guide*.

The sections that follow discuss types of problems that you might see and methods of capturing the information needed to diagnose those problems.

Reproducible problems reported as Tivoli Enterprise Portal client problems

If the problem is reproducible and is reported as a Tivoli Enterprise Portal client problem, you need the client log. The location of the log depends on the type of client and the operating system the client is running on. You might be asked to set a trace in the client and then collect the log.

Log files are created automatically when you start the Tivoli Enterprise Portal. You can view the logs with any text editor. Logon prompts, progress messages, and error messages are also displayed in the status bar of the Tivoli Enterprise Portal logon window. You can change the level of tracing by either of two methods:

* In the Tivoli Enterprise Portal, select **File > Trace Options...**. See the Tivoli Enterprise Portal online help for instructions.
* In Manage Tivoli Monitoring Services, right-click **Tivoli Enterprise Portal** and select **Advanced > Edit Trace Parms...**.

If the Tivoli Enterprise Portal desktop client is being used, collect the logs shown in Table 17 on page 192.

Determining whether the problem is caused by the monitoring agent

Table 17. Log locations for Tivoli Enterprise Portal desktop client

Windows system	Linux system

`install_dir\CNP\logs`
 	
Where **install_dir** is the directory where the Tivoli Monitoring Services components are installed (usually, `C:\IBM\ITM`).
 	
You can find three types of log files in the portal client log location:
 	
• `kcjerror.log` contains environment variables and command strings for starting the Tivoli Enterprise Portal.
 	
  Tivoli Enterprise Portal keeps the last five error logs (kcjerror_1.log, kcjerror_2.log, and so on) in addition to the current one. Every time the Tivoli Enterprise Portal starts, it purges the oldest error log and renames the rest.
 	
• `kcjras1.log` contains the RAS1 tracing for the portal client.
 	
• `KCJ.LOG` contains any errors in the Java libraries used by the portal client.
 	
  Every time the Tivoli Enterprise Portal starts, it purges the kcjras1.log and KCJ.LOG files and writes new ones. If you want to preserve these log files, you must rename them or copy them to another directory before restarting the Tivoli Enterprise Portal.
	`install_dir/logs/hostname_cj_timestamp.log`
	
	Where:
	
	install_dir
	    Is the directory where the Tivoli Monitoring Services components are installed.
	
	hostname
	    Is the host name of the system.
	
	cj Is the component code for the portal client.
	
	timestamp
	    Is a decimal representation of the time when the process started.

If the Tivoli Enterprise Portal browser client is being used, collect the following trace log:

`C:\Documents and Settings\Administrator\Application Data\IBM\Java\Deployment\log\plugin1.4.2.trace`

The plugin1.4.2.trace file contains the RAS1 tracing for the Tivoli Enterprise Portal browser client and any Java exceptions. You might need to edit your Internet Explorer browser options to enable tracing on your local system. When tracing is enabled, you can change the level of tracing by selecting **File > Trace Options...** in the Tivoli Enterprise Portal.

The Tivoli Enterprise Portal Server log is found in the locations shown in Table 18 on page 193.

Table 18. Log locations for Tivoli Enterprise Portal Server

Windows system	Linux or AIX system

`install_dir\logs\hostname_cq_hex_timestamp-nn.log`
 	
Where:
 	
install_dir
      Is the directory where the Tivoli Monitoring Services components are installed.
 	
hostname
      Is the host name of the system.
 	
cq   Is the component code for the portal server.
 	
hex_timestamp
      Is a hexadecimal representation of the time when the process started.
 	
nn   Represents the circular sequence in which logs are rotated. Ranges from 01 to 05, by default, though the first is always retained, since it includes configuration parameters.
	`install_dir/logs/hostname_cq_timestamp.log`
	
	Where:
	
	install_dir
	      Is the directory where the Tivoli Monitoring Services components are installed.
	
	hostname
	      Is the host name of the system.
	
	cq Is the component code for the portal server.
	
	timestamp
	      Is a decimal representation of the time when the process started.

The log files are created automatically when you start the portal server. You can view the logs with any text editor.

When you investigate portal server problems on Windows systems, use the Windows Event Viewer to check that the portal server started correctly and to look for errors. You can also use the service console, accessible from the portal server with an Internet Explorer browser, to read logs and turn on traces for remote product diagnostics and configuration information. See *IBM Tivoli Monitoring: Problem Determination Guide* for instructions on using the service console.

You can change trace settings in Manage Tivoli Monitoring Services. Right-click **Tivoli Enterprise Portal Server** and select **Advanced > Edit Trace Parms...**.

In addition, you can set the portal server to display messages in a command prompt window on a Windows system.
1. Right-click **Tivoli Enterprise Portal Server** in the **Manage Tivoli Monitoring Services** window.
2. Select **Change startup**.
3. Select **Allow service to interact with desktop**.

Collect the Tivoli Enterprise Monitoring Server logs, too. Even when a problem appears to be a Tivoli Enterprise Portal problem, the real problem might be a monitoring server failure.
- Table 20 on page 195 shows the location of logs for a Tivoli Enterprise Monitoring Server on a z/OS system.
- Table 19 on page 194 shows the location of logs for a Tivoli Enterprise Monitoring Server on distributed systems.

Determining whether the problem is caused by the monitoring agent

Table 19. Log locations for Tivoli Enterprise Monitoring Server on distributed systems

Windows system	Linux or UNIX system
`install_dir\logs\hostname_cms_hex_timestamp-nn.log` Where: *install_dir* Is the directory where the Tivoli Monitoring Services components are installed. *hostname* Is the host name of the system. **cms** Is the component code for the monitoring server. *hex_timestamp* Is a hexadecimal representation of the time when the process started. *nn* Represents the circular sequence in which logs are rotated. Ranges from 01 to 05, by default, though the first is always retained, since it includes configuration parameters.	`install_dir/logs/hostname_ms_timestamp.log` Where: *install_dir* Is the directory where the Tivoli Monitoring Services components are installed. *hostname* Is the host name of the system. **ms** Is the component code for the monitoring server. *timestamp* Is a decimal representation of the time when the process started.

The log files are created automatically when you start the monitoring server on a Windows, Linux, or UNIX system. You can view the log files with any text editor.

When you investigate monitoring server problems on Windows systems, use the Windows Event Viewer to check that the monitoring server started correctly and to look for errors. You can also use the service console, accessible from the portal server with an Internet Explorer browser, to read logs and turn on traces for remote product diagnostics and configuration information. See *IBM Tivoli Monitoring: Problem Determination Guide* for instructions on using the service console.

You can change trace settings in Manage Tivoli Monitoring Services. Select **Action > Advanced > Edit Trace Parms...**.

In addition, you can set the monitoring server to display messages in a command prompt window on a Windows system.

1. Right-click **Tivoli Enterprise Monitoring Server** in the **Manage Tivoli Monitoring Services** window.
2. Select **Change startup**.
3. Select **Allow service to interact with desktop**.

Irreproducible problems reported as Tivoli Enterprise Portal client problems

If a problem reported as a Tivoli Enterprise Portal client problem is not reproducible, collect the portal client and portal server logs. The logs might be the only indication of the real problem. Always try to get the logs at the time of the error.

Problems reported as Tivoli Enterprise Portal Server problems

If the problem is reported as a Tivoli Enterprise Portal Server problem, collect the portal server logs. If the problem is reproducible, you might be asked to set unit traces for the portal server and gather the logs. The location for the portal server logs is found in Table 18 on page 193. Also collect the portal client log at the time of the error, if it is available.

Problems affecting the monitoring agent

After you have ruled out problems with Tivoli Monitoring Services components, treat the problem as a monitoring agent problem. A data collection problem with a monitoring agent manifests itself as the display of no data or incorrect data in the Tivoli Enterprise Portal.

Log files and trace information are provided in a common fashion across all monitoring agents on z/OS and the z/OS components of Tivoli Monitoring Services. The Log and Trace Analyzer is a useful tool that can help you collect, view, analyze, and correlate log and trace information. See "Using the Log and Trace Analyzer tool" on page 196.

Table 20 explains the location of log and trace files for the monitoring agent and the Tivoli Monitoring Services z/OS components.

Table 20. Locations of log and trace information for z/OS components

Component	Locations of log and trace information
Monitoring agent	RKLVLOG for the monitoring agent started task is the single most helpful piece of service information for a monitoring agent on z/OS. The RKLVLOG is the sysout data set or spool file that contains log and trace messages. Instructions on how to save the contents of this log to a data set are provided under "Capturing z/OS logs to send to IBM Software Support" on page 225. These additional log files (if available) are also useful: • The RKLVSNAP sysout data set or spool file contains formatted dump output. • The RKPDLOG sysout data set or spool file contains information and error messages related to the handling of persistent data stores. Refer to your started procedures for the locations of these serviceability log files.
Tivoli Enterprise Monitoring Server on z/OS	Because the Tivoli Enterprise Monitoring Server on z/OS runs under ITMS:Engine just as a monitoring agent on z/OS does, all logging under ITMS:Engine is handled the same way: log and trace data is written to RKLVLOGs and RKPDLOGs.

Determining whether the problem is caused by the monitoring agent

Table 20. Locations of log and trace information for z/OS components (continued)

Component	Locations of log and trace information
ITMS:Engine	ITMS:Engine is a collection of basic operating system and communication service routines built specifically for z/OS. All address spaces used by monitoring agents load and use the services of ITMS:Engine. The following message indicates successful initialization of ITMS:Engine: `KLVIN408 IBM OMEGAMON PLATFORM ENGINE VERSION 400 READY` For troubleshooting information about ITMS:Engine problems, refer to the z/OS initialization section of *IBM Tivoli Monitoring: Problem Determination Guide*. ITMS:Engine writes messages to the same RKLVLOG as the product it is running. For the SA z/OS monitoring agent, product-specific messages begin with the product code KAH. Messages for the ITMS:Engine begin with the product code KLV. Tivoli Enterprise Monitoring Server messages begin with the product code KDS.
Persistent data store	The RKPDLOG sysout data set or spool file contains the information and error messages related to the handling of persistent data stores. **Note:** SA z/OS does not exploit the persistent data store.

See Chapter 20, "Setting up a trace on a z/OS system," on page 217 for detailed instructions on using traces and logs to debug the monitoring agent and the monitoring server on z/OS systems.

Using the Log and Trace Analyzer tool

Tivoli Monitoring Services includes a Log and Trace Analyzer tool that helps you view, analyze, and correlate log files. You can evaluate event and error logs with time synchronization.

Launch the Log and Trace Analyzer tool from the Tivoli Enterprise Portal Event Tools view. You can then use the tool to view logs from the Tivoli Enterprise Portal Server or Tivoli Enterprise Monitoring Server on a distributed system, or the RKLVLOG from a monitoring agent or monitoring server on z/OS.

In addition to the Log and Trace Analyzer, specialized OMEGAMON adapters are provided to aid in problem determination for some of the more common problems that you might experience when using Tivoli Monitoring Services (Tivoli Enterprise Portal, Tivoli Enterprise Portal Server, and Tivoli Enterprise Monitoring Server). The OMEGAMON adapters process application log files and transform their contents into a common format for logging, management, and problem determination.

Note: SA z/OS does not currently provide such a specialized adapter.

You can find more information about the Log and Trace Analyzer at http://www.ibm.com/developerworks/autonomic/probdet.html. OMEGAMON adapters and associated documentation are available for download from http://www.ibm.com/software/tivoli/opal?NavCode=1TW10TM2U. The Website is updated as additional adapters become available.

Submitting problems to IBM Software Support

For information about submitting problems to IBM Software Support, see Appendix C, "Support," on page 239.

Summary: Collecting problem information

If you have a problem that you are unable to solve by referring to this guide and to *IBM Tivoli Monitoring: Problem Determination Guide*, gather the following information about the problem and contact IBM Software Support for further assistance.

- Monitored application file.
- Appropriate RAS1 trace output.
- Description of the operation scenario that led to the problem.
- Incorrect output, such as Tivoli Enterprise Portal screen prints or a description of what you observed, if applicable.
- Log files from failing systems. You can collect all logs or logs of a certain type, such as RAS trace logs or message logs.
- Application information, such as version number and patch level.
- Operating system version number and patch level.
- Messages and other information displayed on the screen.
- Version number of the following components of the monitoring environment:
  - Tivoli Enterprise Portal client. Select **About Tivoli Enterprise Portal ...** from the **Help** menu.
  - Tivoli Enterprise Portal Server and Tivoli Enterprise Monitoring Server on distributed systems. Also provide the IBM Tivoli Monitoring patch level, if available.
    - On Windows and Linux systems, you can find the version number and patch level in the **Version** column of Manage Tivoli Monitoring Services.
    - On UNIX systems, you can find the version number and patch level in the KBBENV file located in the *install_dir*/tables subdirectory.
  - Tivoli Enterprise Monitoring Server on z/OS. You can find the version number and patch level in the KDSENV member of the RKANPARU data set.

For more information about collecting problem information, see *IBM Tivoli Monitoring: Problem Determination Guide* for distributed components and Chapter 20, "Setting up a trace on a z/OS system," on page 217 for z/OS components.

Summary: Collecting problem information

Chapter 16. Messages

This appendix documents messages generated by SA z/OS and the SA z/OS monitoring agent. In the course of running and administering the product, you might see messages not listed here. Those messages are probably issued by other components of Tivoli Monitoring Services and documented in the *IBM Tivoli Monitoring: Problem Determination Guide*, GC32-9458.

SA z/OS messages

Message format

SA z/OS messages related to the SA z/OS monitoring agent have the following format:

- INGnnnI

Where:

ING   is the SA z/OS system program identifier.

nnn   is the message number.

I   is the message type: Information. This usually requires no action. The message is issued only for advisory purposes.

ING087I   *task_name*: **PPI RECEIVER** *receiver_name* **READY**

Explanation: The task *task_name* has initialized completely and the PPI receiver named *receiver_name* is ready for processing requests.

System action: Processing continues

Operator response: None

System programmer response: None

ING088I   *task_name*: **PPI RECEIVER** *receiver_name* **TERMINATED**

Explanation: The task *task_name* has deleted the PPI receiver named *receiver_name*. No more requests can be processed.

System action: Processing terminates

Operator response: None

System programmer response: None

ING089I   *task_name*: **INVALID BUFFER RECEIVED, DATA DROPPED. RELATED INFO:** *request_data*

Explanation: The PPI receiver owned by the task *task_name* received an invalid request buffer. The first 64 bytes are dumped with the message in the variable *request_data*.

System action: Processing continues

Operator response: None

System programmer response: Ensure that only the SA z/OS monitoring agent is sending requests to the PPI receiver that is owned by the task *task_name*.

Message Class: 43

ING090I   **TASK** *task_name* **IS NOW ACTIVE**

Explanation: The task *task_name* has been activated.

System action: Processing continues

Operator response: None

System programmer response: None

ING091I   *task_name* **ALREADY ACTIVE OR IN PROCESS OF BECOMING ACTIVE**

Explanation: You started the task *task_name* but the task is already active or in the process of becoming active.

System action: Processing terminates

Operator response: None

System programmer response: None

ING092I   *task_name*: *service_name* **SERVICE FAILED, RC=***rc*. **ERROR**

INFORMATION: *error_info*

Explanation: During the execution of the service *service_name*, an error occurred. The variable *error_info* indicates in what context the service was invoked by the task *task_name*.

For detailed error information, refer to *NetView: Customization – Using Assembler*. In case of NetView Program-to-Program Interface (PPI) errors refer to *NetView: Application Programming Guide* for more information related to the service return code *rc*.

System action: Processing terminates

Operator response: None

System programmer response: Determine why the service routine failed and correct the problem. Examine the NETLOG for additional information. If necessary, contact your local IBM Support Center for further assistance.

ING093I   *task_name*: **INVALID KEYWORD OR SYNTAX ERROR. RELATED INFORMATION:** *error_info*

Explanation: An invalid keyword or value was specified in the initialization member for task *task_name*. Related error information is provided in variable *error_info*.

System action: Processing terminates

Operator response: None

System programmer response: Refer to "Step 2. Configure SA z/OS and NetView" on page 47 for a list of valid keywords and values and correct the problem.

ING094I   **TASK** *task_name* **HAS TERMINATED**

Explanation: The task *task_name* has terminated.

System action: Processing terminates

Operator response: None

System programmer response: None

ING095I   *task_name*: **NO ACTIVE OPERATOR FOUND**

Explanation: The PPI receiver owned by task *task_name* received a request for monitoring data but could not find an active automation operator to process the request.

System action: The message is sent back to the requestor and processing continues.

Operator response: None

System programmer response: Refer to "Step 2. Configure SA z/OS and NetView" on page 47 for instructions how to setup automation operators for this function and correct the problem.

ING096I   **function :** *text*

Explanation: During processing the function request for monitoring data any of the following errors as indicated by *text* occurred. Examples for *text* are:

- NetView RC *rc* from: *command*
- Timeout occurred
- ING008I ...

System action: The message is sent back to the requestor and processing continues.

Operator response: None

System programmer response: If *text* contains an existing SA z/OS message ID, refer to the message help for problem resolution.

In case of a timeout, increase the time allotted for the longest request.

For return codes returned by SA z/OS or NetView services refer to related documentation or contact your local IBM Support Center for further assistance.

SA z/OS monitoring agent messages

Message formats

SA z/OS monitoring agent messages take one of the following forms:

- KAH*xnnnt* (for messages written to the SA z/OS monitoring agent log)

Where:

KAH   Is the SA z/OS monitoring agent identifier.

x   Identifies the product component:
  A   The SA z/OS monitoring agent
  M   System Automation for z/OS
  X   NetView PPI

nnn   Is the message number.

t   Is the message type. I is for informational messages and E is for messages that eventually require an action.

Message types

All monitoring agent messages are written to the monitoring agent log. In addition the following messages are also written to the syslog and are available for the automation purposes of the agent:

- KAHM020I
- KAHM021I
- KAHM022I
- KAHM034E
- KAHM035E

KAHM001I   Data buffer error line *num* **=** *msg*

Explanation: A request was sent to the automation agent but during processing of the request an error occurred. One or more error lines may be returned.
    The variable *num* shows the line # beginning with 0. The variable *msg* contains the actual error message.

System action: Processing continues.

System programmer response: Contact your local IBM support center for further assistance.

KAHM002I   Service *service_name* **rc(***num***)**

Explanation: The SA z/OS monitoring agent Program-to-Program Interface (PPI) service routine *service_name* was unable to process the PPI request. The return code *num* contains the decimal return code that was returned by the service.

service_name	PPI Request
kahppdel	Type 10 (Delete Receiver)
kahppini	Type 1 (Query Status) Type 4 (Initialize Receiver)
kahpplis	Type 22 (Receive Buffer)
kahppprg	Type 23 (Purge Buffer)
kahppreq	Type 14 (Send Buffer) Type 22 (Receive Buffer)

Refer to *NetView: Application Programming Guide* for a detailed explanation of the return code from any of the PPI request types.

System action: Processing continues.

System programmer response: Correct the error and restart the SA z/OS monitoring agent. If the error still remains, contact your local IBM support center for further assistance.

KAHM005I   Added new node *node_name*

Explanation: A new system represented by node *node_name* was added to the list of systems that are being monitored by the SA z/OS monitoring agent.

System action: Processing continues.

System programmer response: None.

KAHM007I   Register subnode *node_name*

Explanation: The node *node_name* was registered as a subnode from the SA z/OS monitoring agent. The subnode becomes active on the Navigator view of the Tivoli Enterprise Portal.

System action: Processing continues.

System programmer response: None.

KAHM008I   De-register subnode *node_name*

Explanation: The node *node_name* was de-registered as a subnode from the SA z/OS monitoring agent. The subnode becomes inactive on the Navigator view of the Tivoli Enterprise Portal.

System action: Processing continues.

System programmer response: None.

KAHM009I   Module *module_name* **could not be loaded, completion code=***cc*

Explanation: The SA z/OS monitoring agent failed to load module *module_name*. The z/OS, LOAD-service completed with completion code *cc*.

System action: Processing terminates.

System programmer response: Make sure that the module requested is available in the STEPLIB or any other program library that is searched by the SA z/OS monitoring agent's started task and restart the SA z/OS monitoring agent.

KAHM010I   Could not obtain storage for PPI-buffer *num*, **size=***size*

Explanation: The SA z/OS monitoring agent failed to obtain the response buffer for the PPI receiver that is indicated by number *num*. The size of the response buffer was specified in KAH_PPI_BUFFER_SIZE.

System action: Processing terminates.

System programmer response: Ensure that the address space hosting the SA z/OS monitoring agent has sufficient region size so that the storage request can be satisfied. Otherwise decrease the buffer size as denoted by KAH_PPI_BUFFER_SIZE so that the region limit for all PPI buffers is not exceeded.

KAHM011I   Heartbeat lost

Explanation: The heartbeat to SA z/OS was lost. PPI communication is not possible.

System action: The SA z/OS monitoring agent attempts periodically to get back the heartbeat in intervals denoted by KAH_PPI_CHECK_UP_INTVL. All active subnodes are de-registered and the subnodes remain inactive until the heartbeat comes back.

System programmer response: Ensure that the SA z/OS agent on NetView is active. Also ensure that the PPI receiver on the NetView side is active. Use the DISPPI command to obtain a list of registered PPI receivers and their current status.

KAHM012I   Heartbeat still not available

Explanation: The heartbeat to SA z/OS was lost and is still not available. PPI communication remains impossible.

System action: The SA z/OS monitoring agent continues to periodically get back the heartbeat.

System programmer response: Refer to KAHM011I for details.

KAHM013I   Heartbeat OK

Explanation: The heartbeat to SA z/OS is available. PPI communication is possible.

System action: Processing continues.

System programmer response: None.

**KAHM020I   SYSTEM AUTOMATION
                 MONITORING AGENT STARTED**

Explanation: Initialization of the SA z/OS monitoring agent has started.

System action: Processing continues.

System programmer response: None.

**KAHM021I   SYSTEM AUTOMATION
                 MONITORING AGENT STARTUP
                 COMPLETE**

Explanation: Initialization of the SA z/OS monitoring agent has completed.

System action: Processing continues.

System programmer response: None.

**KAHM022I   SYSTEM AUTOMATION
                 MONITORING AGENT ENDED**

Explanation: The SA z/OS monitoring agent was terminated in response to an MVS STOP command.

System action: Processing continues.

System programmer response: None.

**KAHM024I   SYSTEM AUTOMATION
                 MONITORING AGENT VERSION
                 version (BUILD LEVEL *level*) HAS
                 STARTED**

Explanation: The SA z/OS monitoring agent has started. The message indicates the version and the build level of the monitoring agent.

System action: Processing continues.

System programmer response: None.

If you contact the local IBM support center, you may be asked for the version and build level of the product, which can be found here.

**KAHM034E   SYSTEM AUTOMATION
                 MONITORING AGENT
                 INITIALIZATION FAILED. REASON:
                 *text***

Explanation: Initialization of the SA z/OS monitoring agent could not be completed due to any of the following reasons indicated by variable text:

CNMNETV NOT LOADED
The NetView Program-to-Program Interface (PPI) routine, CNMNETV, was not found in any of the program libraries that were searched by the SA z/OS monitoring agent's started task

PARAMETER ERROR
One or more of the parameters that are configured through the Configuration Tool or modified in the K*xx*ENV member within *&hilev*.RKANPARU is unknown or specifies an invalid value. Refer to the "Step 5. Configure the monitoring agent" on page 98 for details on the parameters that may be specified.

PPI INITIALIZATION ERROR
The PPI receivers could not be initialized completely. Check the RKLVLOG for KAHM002I messages that were issued earlier that report the return code from NetView while attempting to initialize the PPI receivers.

Refer to the *NetView: Application Programming Guide* for a description of the Type 1 (Query Status) or Type 4 (Initialize Receiver) PPI requests.

NO HEARTBEAT

The SA z/OS monitoring agent was unable to connect to the SA z/OS agent that is running on NetView.

The heartbeat will fail if the PPI receiver task running in NetView for z/OS is not active or the wrong PPI receiver is used.

Ensure that you have started the task as described in "Step 2. Configure SA z/OS and NetView" on page 47 and that the PPI receiver name matches the name reported by message KAHM117I KAH_PPI_RECEIVER.

The NetView DISPPI command shows the current status of the PPI receivers that have registered once.

NODES INFO MISSING

The SA z/OS monitoring agent connected to the SA z/OS agent running on NetView but no system was found that is properly initialized and in the READY status. Possible causes are:
- The automation agent is still in the progress of being initialized
- An automation configuration (ACF) data mismatch between automation manager and automation agent

SYSPLEX NAME MISSING

The name of the sysplex is not available. The minimum prerequisite configuration is a z/OS monoplex with a valid sysplex name and an SA z/OS policy containing a corresponding sysplex group.

NO SUBNODES AVAILABLE

The SA z/OS monitoring agent was unable to register the sub nodes with the Tivoli Monitoring Services infrastructure.

This message is also written to the console.

System action: Processing terminates but the monitoring agent address space remains up.

System programmer response: Correct the problem and restart the SA z/OS monitoring agent.

KAHM035E   SYSTEM AUTOMATION MONITORING AGENT INITIALIZATION FAILED. REASON: *text*, *rc*: *description*

Explanation: Initialization of the SA z/OS monitoring agent could not be completed due to any of the following reasons indicated by variable text:

PTHREAD ERROR

The SA z/OS monitoring agent was unable to create the heartbeat or listener thread or was unable to create the mutexes or condition variables to communicate with the threads.

The return code rc indicates the type of error and the variable description provides a descriptive information about this error.

This message is also written to the console.

System action: Processing terminates but the monitoring agent address space remains up.

System programmer response: Correct the problem and restart the SA z/OS monitoring agent.

KAHM107I   Too many nodes

Explanation: The internal nodes table already has 32 entries with a status of either 'current' or 'added' and an attempt was made to add another node. The limit for systems in a sysplex is 32 systems.

System action: Processing terminates.

System programmer response: Contact your local IBM support center for further assistance.

KAHM114I   PPI name *value* **specified for** *name* **is invalid**

Explanation: The current value for the PPI *name* contains invalid characters. A valid name can be up to 8 characters long. It can contain alphabetic characters A–Z, numeric characters 0–9, and the following special characters: dollar sign ('$'), percent sign ('%'), ampersand ('&'), at sign ('@'), and number sign ('#'). It may not start with a digit.

System action: Processing terminates.

System programmer response: Correct the value and recycle the SA z/OS monitoring agent.

KAHM115I   PPI name *value* **specified for** *name* **is too long**

Explanation: The current value for the PPI *name* is more than 8 characters long. A valid name can be up to 8 characters long. It can contain alphabetic characters A–Z, numeric characters 0–9, and the following special characters: dollar sign ('$'), percent sign ('%'), ampersand ('&'), at sign ('@'), and number sign ('#'). It may not start with a digit.

System action: Processing terminates.

System programmer response: Correct the value and recycle the SA z/OS monitoring agent.

KAHM116I   PPI name for *name* **not specified. Default** *value* **is used**

Explanation: No value was specified for the required PPI name *name*, therefore the default *value* is used.

System action: Processing continues.

System programmer response: None.

KAHM117I   *name* **set to specified <***value***>**

Explanation: The *name* parameter is set to the value specified in the K*pp*ENV parmlib member found in &hilev.RKANPARU.

System action: Processing continues.

System programmer response: None.

KAHM118I   **Value** *value* **specified for** *name* **is invalid**

Explanation: The current value for the *name* parameter contains invalid characters. A valid value contains numeric digits only. For the KAH_PPI_BUFFER_SIZE parameter, the size value may optionally be followed by a multiplier of 1024 'K' or 1048576 'M' resulting in Kilo-Bytes or Mega-Bytes, respectively.

System action: Processing terminates.

System programmer response: Correct the value and recycle the SA z/OS monitoring agent.

KAHM119I   **Value** *value* **specified for name is too big**

Explanation: The current value for the *name* parameter is too big. Upon conversion into a number format, an underflow or overflow may occur. For time intervals, the maximum value is 3600 seconds.

System action: Processing terminates.

System programmer response: Correct the value and recycle the SA z/OS monitoring agent.

KAHM120I   **Value** *value* **specified for** *name* **is too small**

Explanation: The current value for the *name* parameter is too small. For PPI buffers, a minimum of one page (4096 Bytes) is required. The minimum time interval can be 1 second.

System action: Processing terminates.

System programmer response: Correct the value and recycle the SA z/OS monitoring agent.

KAHM121I   **Value for** *name* **not specified. Default (***value***) is used**

Explanation: No value was specified for the required *name* parameter, therefore the default value is used.

System action: Processing continues.

System programmer response: None.

KAHM122I   *name* **set to specified <***value***>, decimal=***num*

Explanation: The *name* parameter is set to the value specified in the K*pp*ENV parmlib member found in &hilev.RKANPARU. For storage sizes, the value that

was specified, including the optional multiplier character and its decimal representation *num*, is shown.

System action: Processing continues.

System programmer response: None.

KAHM123I   **Module** *module_name* **entry point=***entry_point*

Explanation: The *module_name* module was loaded at the *entry_point* entry point.

System action: Processing continues.

System programmer response: None.

KAHA002I   **Service** *service_name* **rc(***num***)**

Explanation: The SA z/OS monitoring agent Program-to-Program Interface (PPI) service routine, *service_name*, was unable to process the PPI request. The return code *num* contains the decimal return code returned by the service.

service_name	PPI Request
kahppdel	Type 10 (Delete Receiver)
kahppini	Type 1 (Query Status) Type 4 (Initialize Receiver)
kahpplis	Type 22 (Receive Buffer)
kahppprg	Type 23 (Purge Buffer)
kahppreq	Type 14 (Send Buffer) Type 22 (Receive Buffer)

Refer to *NetView: Application Programming Guide* for a detailed explanation of the return code from any of the PPI request types.

System action: Processing continues.

System programmer response: Correct the error and restart the SA z/OS monitoring agent. If the error still remains, contact your local IBM support center for further assistance.

KAHA101I   *agent* **- No connection. Exit TakeSample**

Explanation: The agent *agent* attempted to issue a request to the SA z/OS agent but no connection was available. No data was returned.

System action: Processing continues. No data is returned to the Tivoli Monitoring Server and further on.

System programmer response: Correct the problem.

KAHX016I   **RCV=**_requestor_ **OUT OF SEQUENCE**
                BUFFER IS IGNORED

Explanation: Indicates that the named PPI _requestor_
has received a response buffer whose correlator does
not match the correlator supplied with the request. This
can happen if a request is canceled due to a timeout
condition in the monitoring agent while the System
Automation agent has almost completed collecting data
and sending the response back to the requestor.

System action: Processing continues.

System programmer response: Review the timeout
settings of the monitoring agent and increase the
timeout, if possible.

KAHX018I   **RCV=**_requestor_ **TIMEOUT OCCURRED**

Explanation: Indicates that the named PPI _requestor_
was unable to receive a data buffer within the allotted
time interval specified by the KAH_PPI_TIMEOUT
environment variable.

System action: Processing continues. The current
request is completed. Any response data that arrives
until a new request is issued by the same requestor will
be ignored. PPI buffers for such response data will be
purged upon the next request.

System programmer response: Review the timeout
settings of the monitoring agent and increase the
timeout, if possible.

Chapter 17. Troubleshooting installation and configuration problems

This chapter provides information about problems that might be caused by installation or configuration errors. Some of these problems show up during initialization of the SA z/OS monitoring agent or of one of the components of Tivoli Monitoring Services. Other problems show up in the Tivoli Enterprise Portal, either in the Navigator or in the product workspaces.

Tivoli Enterprise Portal Server installation or initialization fails on Windows

Many problems with installation and initialization of the Tivoli Enterprise Portal Server on Windows result from DB2 Universal Database (UDB) initialization or password errors.

Tivoli Enterprise Portal Server cannot start because DB2 UDB is not running

If DB2 UDB is not running, the Tivoli Enterprise Portal Server cannot start, and users attempting to log on to the Tivoli Enterprise Portal receive this message:

```
KFWITM392E Internal error occurred during logon.
```

On a Windows workstation, you can check the status of DB2 UDB by looking at the system tray. If the DB2 button is green, DB2 is running. If the button is red, start DB2 by right-clicking the button and selecting **Start**.

User account password errors prevent installation or initialization of the Tivoli Enterprise Portal Server

DB2 UDB requires the following Windows user accounts:

- **db2admin**, added when you install DB2 UDB and required by the OMEGAMON Platform installer when you configure the Tivoli Enterprise Portal Server (**TEPS**) data source.
- **TEPS**, added during Tivoli Enterprise Portal Server installation for creating the Tivoli Enterprise Portal Server data source.

Problems can result from password errors in the two user accounts:

- If you change the **db2admin** password after DB2 UDB installation, you might receive error messages when you try to install the Tivoli Enterprise Portal Server. If your Local Security Settings require you to change the password, wait to do so until you finish installing the Tivoli Enterprise Portal Server.
- If you change the **db2admin** password after you install and configure Tivoli Enterprise Portal Server, the Tivoli Enterprise Portal Server might not initialize correctly the next time it is started. Even if the **Manage Tivoli Monitoring Services** window indicates that the Tivoli Enterprise Portal Server status is **Started**, a user logging on to Tivoli Enterprise Portal client cannot connect. Check for SQL exceptions in the Tivoli Enterprise Portal Server log.

Changing the Tivoli Enterprise Portal Server database user account password

If your Windows environment requires you to change passwords after you install and configure Tivoli Enterprise Portal Server, complete the following steps to change the Tivoli Enterprise Portal Server database user account password:

1. On the Windows workstation where the Tivoli Enterprise Portal Server is installed, be sure you are logged on with an ID that has local Administrator authority.
2. Select **Start > Programs > IBM Tivoli Monitoring > Manage Tivoli Monitoring Services**.
3. Right-click **Tivoli Enterprise Portal Server** and select **Advanced > Utilities > Build TEPS Database** from the context menu.
4. Click **DB2** to open the **TEPS Data Source Config Parameters** window.
5. Enter the **db2admin** account password.
6. Specify a new password for the Tivoli Enterprise Portal Server database user account.

> **Tip**
>
> To have one less password to remember, you can use the same password for the **db2admin** account and the Tivoli Enterprise Portal Server database user account (**TEPS**). If the Local Security Settings on the Windows system require complex passwords, you must use a password that fits the system requirements:
> - Not containing the user's account name.
> - Being at least six characters in length.
> - Containing characters from three of the following categories:
>   - English uppercase characters (A through Z)
>   - English lowercase characters (a through z)
>   - Base 10 digits (0 through 9)
>   - Non-alphanumeric characters (Examples: !, $, #, %)

Installation of SA z/OS application support fails on Windows: Empty selection list

If you attempt to install SA z/OS application support on a Windows system and find an empty selection list on the Select Features window of the InstallShield, make sure that the Tivoli Enterprise Portal Server is already installed on the workstation. This is the required order for installing distributed components:

1. DB2 Universal Database (DB2 UDB) Workgroup Server Edition

   You can install DB2 UDB from the installation CDs included in the Tivoli Monitoring Services on z/OS product package.

2. Tivoli Enterprise Portal Server

   You can install the Tivoli Enterprise Portal Server from the *IBM Tivoli Monitoring Services on z/OS* CDs. If you want to install the Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal desktop client on the same system as the Tivoli Enterprise Portal Server, you can install them at the same time.

3. SA z/OS application support

You can install SA z/OS application support either from downloaded files or from the *IBM Tivoli System Automation for z/OS Workspace Enablement, Version 3.3.0* CD that is included in the product package.

Linux and UNIX installation and configuration problems

This section discusses problems specific to the installation and configuration of components on Linux and UNIX systems.

Preventing configuration problems on Linux and UNIX systems

To prevent problems on Linux and UNIX systems, perform installation and configuration steps in this order:

1. Install and configure the Tivoli Monitoring Services (IBM Tivoli Monitoring) components:
   - Tivoli Enterprise Monitoring Server (if you want a monitoring server on the local Linux or UNIX system)
   - Tivoli Enterprise Portal Server
   - Tivoli Enterprise Portal client

   Follow the instructions in the *IBM Tivoli Monitoring: Installation and Setup Guide*.

2. Stop all components.
3. Install SA z/OS application support.

> **Tip**
>
> Installing application support on a Linux or UNIX system is a looped procedure, with four iterations:
>
> - Installing application support on the browser client
> - Installing application support on the desktop client
> - Installing application support on the portal server
> - Installing application support on the monitoring server (if the monitoring server is on the local Linux or UNIX system)
>
> Application support can be installed on only one component at a time.

   a. In the SA z/OS monitoring agent installation program, select a product package from the numbered list, for example, Tivoli Enterprise Portal Browser Client support.

   ```
   Product packages are available for the following operating systems and component support categories
    1) Tivoli Enterprise Portal Browser Client support
    2) Tivoli Enterprise Portal Desktop Client support
    3) Tivoli Enterprise Portal Server support
    4) Tivoli Enterprise Monitoring Server support

   Type the number for the OS you want, or type "q" to quit selection: 1

   You selected number "1" or "Tivoli Enterprise Portal Browser Client support"

   Is the operating system or component support correct [ y or n; "y" is default ]?
   ```

   b. At the prompt for products to install, select and confirm either **IBM Tivoli System Automation for z/OS** or **all of the above**.

   c. Enter **y** at the next prompt:

   ```
   Do you want to install additional products or product support packages [ y or n; "n" is default ]?
   ```

   d. Repeat the procedure to install items 2, 3, and 4 from the numbered list:

```
2) Tivoli Enterprise Portal Desktop Client support
3) Tivoli Enterprise Portal Server support
4) Tivoli Enterprise Monitoring Server support
```

Only one item can be installed at a time. For each item, select **IBM Tivoli System Automation for z/OS** as the product to install.

e. When you have selected and installed **IBM Tivoli System Automation for z/OS** application support on the browser client (item 1), desktop client (item 2), portal server (item 3), and monitoring server (item 4), enter **n** at this prompt:

```
Do you want to install additional products or product support packages [ y or n; "n" is default ]?
```

f. Exit the installation program.

4. Start the monitoring server on Linux and UNIX:

   `./itmcmd server start tems_name`

   where *tems_name* is the node ID of the monitoring server. On Linux and UNIX systems, you can find the value of CMS_NODEID in the KBBENV file located in the *install_dir*/tables subdirectory.

5. Activate application support on the monitoring server on Linux and UNIX:

   `./itmcmd support -t tems_name ah`

   The two-character product code **ah** indicates the System Automation for z/OS product.

6. Stop and restart the monitoring server on Linux and UNIX:

   `./itmcmd server stop tems_name`
   `./itmcmd server start tems_name`

7. Reconfigure the portal server with the new agent information:

   `./itmcmd config -A cq`

8. Reconfigure the portal client with the new agent information:

   `./itmcmd config -A cj`

Hover (flyover) help is not displayed in the Tivoli Enterprise Portal on a Linux system

If the System Automation for z/OS help system does not function properly on a Linux system, make sure you have completed all the steps of installing and configuring SA z/OS application support. See "Preventing configuration problems on Linux and UNIX systems" on page 209.

No sysplex-level workspaces are displayed in the Tivoli Enterprise Portal

If the Navigator in the Tivoli Enterprise Portal does not include any sysplex-level System Automation for z/OS workspaces, you might have forgotten to add application support to the Tivoli Monitoring Services components. For instructions, see "Step 1. Install the required Tivoli Monitoring Services components" on page 90 and "Step 2. Install SA z/OS application support" on page 91, and *IBM Tivoli Monitoring: Installation and Setup Guide*. For the required order of steps on Linux and UNIX systems, see "Preventing configuration problems on Linux and UNIX systems" on page 209.

No SA z/OS predefined situations are listed in the Situation Editor

If the list of predefined situations in the Situation Editor does not include any SA z/OS situations, you might have forgotten to add application support to the Tivoli Monitoring Services components. For instructions, see:

- For the hub monitoring server and the monitoring agent on z/OS, "Step 7. Install the Tivoli Enterprise Portal Server and client on a Windows workstation" on page 84
- For the hub monitoring server on a Windows system and the monitoring agent on a z/OS image, "Installing and configuring the Tivoli Monitoring Services components" on page 90

and *IBM Tivoli Monitoring: Installation and Setup Guide*. For the required order of steps on Linux and UNIX systems, see "Preventing configuration problems on Linux and UNIX systems" on page 209.

U200 Port in use message found in RKLVLOG, indicating an incorrect default port

After you complete all installation and configuration tasks for the SA z/OS monitoring agent and try to start the monitoring agent, you might find the following abend message in RKLVLOG, indicating a connection failure:

```
U200 Port in use
```

One possible cause of this problem is that the port defined for communication among the Tivoli Monitoring Services components is already reserved for a different application in the PORT statement of the TCP/IP profile. In that case, complete the following steps to correct the problem:

1. Verify that the existing port reservation is no longer needed, or choose a different port for communication among the Tivoli Monitoring Services components.
2. Edit your TCP/IP profile to reserve the port for the Tivoli Enterprise Monitoring Server started procedure, or change the configuration settings for the portal server (on a Windows, Linux, or UNIX system) and monitoring agent (on a z/OS system) to communicate with the Tivoli Enterprise Monitoring Server on a different port.
3. Stop and restart the monitoring server, monitoring agent, and portal server.

U200 Port in use message found in RKLVLOG, indicating an incorrect default port

Chapter 18. Troubleshooting security problems

This chapter provides information about problems that might be caused by security system or password incompatibilities, or by insufficient levels of authority.

Tivoli Enterprise Monitoring Server and Tivoli Enterprise Portal Server start normally but cannot communicate

The IBM Integrated Cryptographic Service Facility (ICSF, called Global Security Kit or GSKit on distributed systems) provides a robust encryption and decryption scheme for stored passwords in the portal server and monitoring server components. If ICSF is not installed on a z/OS system where a hub monitoring server is configured, the monitoring server uses an alternative, less secure encryption scheme. However, communication with the portal server requires ICSF.

The following messages are displayed when the portal server cannot connect to the monitoring server because ICSF is not installed:

```
Call to KLE_CryptoGetFP failed with exit code 8.
Cannot get CSNBXAE function pointer
Logon validation did not complete - system error.
```

Users attempting to log on to the portal client see this message:

```
KFWITM215E Unable to Process Logon Request
```

Perform the following steps so that the portal server can connect to a monitoring server on a z/OS system without ICSF:

1. When you specify configuration values for the hub monitoring server on z/OS, answer N to the prompt **Integrated Cryptographic Service Facility (ICSF) installed?**

2. After the monitoring server has been configured and is running, modify the portal server configuration to use the older, less robust encoding algorithm used by the hub monitoring server in the absence of ICSF:

    a. In a text editor, edit the **kfwenv** file in *drive*:\IBM\ITM\CNPS.
    b. In a line by itself, type the text USE_EGG1_FLAG=1.
    c. Save the file and exit.
    d. Stop and restart the portal server.

Problems with Tivoli Enterprise Portal Server and DB2 UDB passwords

See "Tivoli Enterprise Portal Server installation or initialization fails on Windows" on page 207.

Chapter 19. Troubleshooting usage problems

This chapter provides information about problems that might arise while you are using the Tivoli Enterprise Portal user interface to monitor your z/OS systems and to issue Take Action commands.

Information in a workspace is inconsistent or a table in a workspace has no rows

It is important to keep in mind that the workspaces displayed in the Tivoli Enterprise Portal are static, while the z/OS data is dynamic. When you view a workspace, you see data values from the most recent data collection. Data can change between the time it is collected and the time it is displayed on the workstation, and you might see inconsistencies caused by different times of data collection for different data items in the workspace.

For example, in the **Resource Overview** workspace, you might see a resource with a component status of SATISFACTORY but when you look at detailed information, the compound status might be different. Inconsistencies of data are more likely when you use links, because data in a workspace might have been collected seconds or even minutes before you click the link.

Problems with the TEP Navigator View

The managed system name representing an SA z/OS LPAR node normally consists of the sysplex name, a colon (':'), the system ID, another colon (':'), and eventually terminated by 'SAAGENT'. For example:

```
KEYAPLEX:KEYA:SAAGENT
```

You may see managed system names without the middle qualifier if you have not installed IBM Tivoli Monitoring 6.1 FixPack 4 or higher. As a circumvention, perform the following steps:

1. In a text editor, edit the **kfwenv** file in *install_dir*\CNPS (where *install_dir* is the directory where the Tivoli Enterprise Monitoring Server component is installed).
2. In a line by itself, type the text:

```
#               ----+----1----+----2----+----3----+----4----+----5----+----6----+----7----+----8----+--
KFW_TOPOLOGY_MVS_PROBE_AFFINITIES=000000000000000000008000000000000000000000 000000000000000000008000000000000000000000
```

> **Note:** The comment line is just to help ensure proper string sizes and bit positions (the number 8 is at positions 21 and 64).

3. Save the file and exit.
4. Stop and restart the portal server.

Take Action commands show return code 0 but are unsuccessful

When you submit a Take Action command from the Tivoli Enterprise Portal (which is always on a distributed system) to a z/OS system, a return code of zero displayed in the portal interface indicates successful submission of the command but gives no indication of the result. You can find the command output in the z/OS SYSLOG.

No heartbeat after SSI recycle

After shutting down the SSI, the connection between KAHAGENT and NetView is irrecoverably lost. A restart of the monitoring agent and INGAHPPI task is required.

Chapter 20. Setting up a trace on a z/OS system

Trace logs capture information about the operating environment to help you diagnose problems when components fail to operate as intended. The principal log type is the reliability, availability, and serviceability (RAS1) trace log. When the monitoring agents and Tivoli Monitoring Services components are initialized, RAS1 is one of the first processes started. RAS logs are in the English language only. You can set up RAS tracing for the monitoring agents, Tivoli Enterprise Monitoring Server, and Tivoli Enterprise Portal Server.

The default level of tracing depends on the component and operating system. For the monitoring agents on z/OS, the default level is KBB_RAS1=ERROR, which means that only error messages are captured. This is the setting for minimal tracing. When you report a problem, IBM Software Support might ask you to enable a more in-depth and detailed form of tracing, such as one of those discussed under "Syntax for RAS1 traces" on page 218.

IBM Software Support uses the information captured by trace logging to trace a problem to its source or to determine why an error occurred. The default configuration for trace logging, such as the level of trace logging, depends on the source of the trace logging. Trace logging is always enabled.

Tip

Overhead (CPU and I/O) associated with detailed RAS1 tracing might degrade performance of the monitoring agent. Restore RAS1 tracing for the monitoring agent to the default level KBB_RAS1=ERROR after you complete problem diagnosis.

You can also use communications traces during TCP/IP initialization to help diagnose problems in connections between the monitoring agent and the monitoring server. See "Setting up communications tracing."

This section provides instructions for setting up traces on z/OS components for your own use and to forward to IBM Software Support.

Setting up communications tracing

Communications tracing during TCP/IP initialization is controlled by the KDC_DEBUG environment variable. To obtain the level of tracing required for the TCP/IP initialization messages to be recorded in the RAS1 log, add the string KDC_DEBUG=Y to member KAHENV for the SA z/OS monitoring agent or to member KDSENV of RKANPARU for the Tivoli Enterprise Monitoring Server.

Possible values for KDC_DEBUG are:

Y The data flow between the monitoring agent and monitoring server during TCP/IP initialization is recorded, including data packages sent and received. When **KDC_DEBUG=Y** is active in the environment during initialization of TCP/IP services for this address space, you can confirm successful initialization of TCP/IP by looking for one of the following messages in RKLVLOG:

```
"KDE1I_OpenTransportProvider") Transport opened: socket/ip.tcp
"KDE1I_OpenTransportProvider") Transport opened: socket/ip.pipe
"KDE1I_OpenTransportProvider") Transport opened: socket/ip.udp
```

N The data flow between the monitoring agent and monitoring server during TCP/IP initialization is not recorded. This is the default and the recommended setting for normal operation.

Refer to the environment variables appendix in *IBM Tivoli Monitoring: Problem Determination Guide* for a list of environment variables associated with other components.

Setting up RAS1 tracing

RAS1 tracing is the primary diagnostic tool for product components. It is provided by the KBB library service and is set either in the IBM Tivoli Monitoring Service Console interface or by a more direct method of modifying the KBB_RAS1 parameter. RAS1 messages are sent to STDOUT and redirected to the files shown in Table 20 on page 195.

RAS1 trace log files can grow very large with the wrong amount of filtering. Be careful with the levels of tracing that you specify.

Syntax for RAS1 traces

This syntax is used to specify a RAS1 trace in the K*pp*ENV file (where *pp* is the product code: **AH** for the SA z/OS monitoring agent or **DS** for the Tivoli Enterprise Monitoring Server). After you add this command to the K*pp*ENV file, you must stop and restart the address space for the command to take effect. After that, it remains in effect for the life of the address space. To end the trace, you must edit the K*pp*ENV file again to reset the trace level, and stop and restart the address space.

An IBM Software Support representative can tell you the values to set for the RAS1 trace parameters.

The basic syntax of the RAS1 trace command is:

```
►►──KBB_RAS1=global_class─────────────────────────────────────────────────────►
                          └─(COMP:component_type)─┘  └─(ENTRY:entry_point)─┘

►──────────────────────────────────────────────────────────────────────────►◄
   └─(UNIT:unit_name,class)─┘
```

where:

global_class
> Indicates the level of tracing that you want. This is a global setting that applies to all RAS1 filters in the process. If you set this global class by itself, it is global in scope and the trace cannot filter on any of the other keywords. Separate combined classes with a space. The following values are possible. Valid abbreviations are in parentheses.
> - **ERROR (ER):** returns severe error messages only (this is the default for most applications).
> - **STATE (ST):** records the condition or current setting of flags and variables in the process. If state tracing is enabled, you can see the current state of particular variables or flags as the process is running.

- **FLOW (FL):** causes a message to be generated at an entry or exit point of a function.
- **DETAIL (DE):** produces a detailed level of tracing.
- **INPUT (IN):** records data created by a particular API, function, or process.
- **ALL:** causes all available messages to be recorded. This setting combines all the other forms of tracing.

COMP

Indicates that the trace includes a component type. The COMP keyword is used to trace groups of routines related by function (or component). Use this keyword only at the explicit request of an IBM Software Support representative.

component_type

Identifies a component type. An IBM Software Support representative can tell you what value to specify.

ENTRY

Narrows a filtering routine to specify a specific ENTRY POINT. Since multiple entry points for a single routine are rare, use this keyword only at the explicit request of an IBM Software Support representative.

entry_point

Represents the name of the entry point. An IBM Software Support representative can tell you what value to specify.

UNIT Indicates that the trace is to look for a match between the compilation unit dispatched and the fully or partially qualified compilation unit specified on the RAS1 statement. A match results in a trace entry.

unit_name

Represents the name of the compilation unit. In most instances, this name defines the component that is being traced. The value is likely to be the three-character component identifier for the monitoring agent (**KAH** for the SA z/OS monitoring agent).

class   One of the same values specified for *global_class* but, because of its position inside the parentheses, narrowed in scope to apply only to the *unit_name* specified.

Note: The default setting for monitoring agents on z/OS is KBB_RAS1=ERROR, meaning that only error tracing is enabled. You can specify any combination of UNIT, COMP, and ENTRY keywords. No keyword is required. However, the RAS1 value you set with the global class applies to all components.

Example: Tracing monitoring agent requests to and answers from the monitoring server

To show monitoring agent requests to and answers from the Tivoli Enterprise Monitoring Server, specify this trace:

```
KBB_RAS1=ERROR (UNIT:KRA ST ERR)
```

The unit values ST and ERR indicate collection of state and error information for a monitoring agent infrastructure component (KRA).

Note: Use this type of trace only for debugging a specific problem, because the settings greatly increase the number of messages generated by the monitoring agent. With this type of trace, messages include a detailed dump of all rows of data that pass filtering: attribute names and values, request

names, table names, and collection intervals. Be sure to disable this
resource-intensive form of tracing immediately after you complete the trace.

Setting RAS1 trace levels by editing RKANPARU

One of the simplest ways to set trace levels for a monitoring agent on z/OS is to
edit the RKANPARU(K*pp*ENV) member, where *pp* is the product code (AH for the
SA z/OS monitoring agent). The text in bold is an example of what an IBM
service representative might ask you to add to this member.

```
  EDIT       RKANPARU(KAHENV)
 Command ===>
 ****** ***************************** Top of Data *****************************
 000001 KDE_TRANSPORT=\
 000002    SNA.PIPE PORT:135 USE:N\
 000003    IP6.PIPE PORT:19184 USE:N\
 000004    IP6.UDP PORT:19184 USE:N\
 000005    IP.SPIPE PORT:3660 USE:N\
 000006    IP6.SPIPE PORT:3660 USE:N\
 000007    IP.PIPE PORT:1918 EPHEMERAL:Y\
 000008    IP.UDP PORT:1918
 000009 KBB_RAS1=ERROR (UNIT:KAH ALL)
 000010 CT_CMSLIST=\
 000011    IP.PIPE:n.nn.nnn.nn;\
 000012    IP.UDP:n.nn.nnn.nn;
 000013 CTIRA_STANDALONE=N
 000014 CTIRA_IP_PORT=0
 000015 LANG=en_US.ibm-037
 ****** **************************** Bottom of Data ****************************
```

Setting RAS1 trace levels dynamically from the IBM Tivoli Monitoring Service Console

You can also use the IBM Tivoli Monitoring Service Console to set trace levels for
monitoring agents on z/OS, as well as for a Tivoli Enterprise Monitoring Server on
z/OS or for distributed components. Using the service console, you can read logs
and turn on traces for remote product diagnostics and configuration.

The service console is uniquely identified by its service point name. All service
consoles for a host are linked and presented on the IBM Tivoli Monitoring Service
Index for that host. You can perform operations on a specific component process
by selecting the service console associated with the service point name of the
component.

Starting the service console

Use the following procedure to start the service console.

1. Start Internet Explorer (version 5 or higher).
2. In the **Address** field, type the URL for the Tivoli Enterprise Portal browser
   client:

   http://*hostname*:1920

   where *hostname* specifies the system where the Tivoli Enterprise Portal Server is
   installed. If the service console is not displayed, a system administrator might
   have blocked access to it. Refer to the *IBM Tivoli Monitoring: Problem
   Determination Guide* for information about blocking access to the service
   console.
3. On the **IBM Tivoli Monitoring Service Console** window, select the desired
   component process (service point name).
4. Click **OK**.

In secure environments, you need a valid user ID and password to proceed.

You can issue service console commands in the command input area. For a list of available commands, type a question mark (?) and click **Submit**.

Service console commands

The service console supports the following commands, most of them useful for problem determination:

bss1 Manages BSS1 (Basic System Services). This command is paired with one of the following sub-commands:

- **dumpcvt**: Display KBBSS_cvt_t
- **listenv**: Display the resident ITMS:Engine variables
- **getenv**: Display environment variables
- **setenv**: Assign an environment variable
- **info**: Display BSS1_Info() data
- **config**: Manage configuration variables

config Modifies the settings of the ITMS: Engine debug environment variables: RES1_DEBUG, KDH_DEBUG, KDC_DEBUG, and KDE_DEBUG . For example, the following **config** command alters the setting of KDC_DEBUG:

```
CONFIG KDC_DEBUG=Y
```

ctbld Determines the maintenance level of the product.

http Displays HTTP server management.

kdcstat
Displays the status of the KDC remote procedure call (RPC) service component.

kdestat
Displays the status of the KDE Transport Service component.

ras1 Manages RAS1 (Reliability, Availability, and Servicability). This command is paired with one of the following sub-commands:

- **dumpcvt**: Display KBBRA_cvt_t
- **log**: Display RAS1 log capture buffer
- **list**: List the RAS1 filters
- **set**: Set the RAS1 filters
- **ctbld**: Display the resident CTBLD data
- **units**: Display the registered compilation units

You can use the RAS1 command without operands to view the current ITMS:Engine log capture buffer. When you supply operands with the RAS1 command, the operands are assumed to be keywords applicable to the KBB_RAS1 environment variable.

The RAS1 command is especially useful for dynamically enabling and disabling RAS1 traces. Often the documentation requests of IBM Software Support conflict with your availability requirements. The RAS1 command can be used to alter KBB_RAS1 tracing parameters dynamically without the need to recycle the product. For example, to enable the standard IRA traces, you can issue the following service console command:

```
RAS1 set error (unit:kpx all) (unit:kra all)
```

The string is passed to RAS1 as operands of the KBB_RAS1 environment variable.

After you capture this trace, you can disable it with the following service console command:

```
RAS1 set error (unit:kpx error) (unit:kra error)
```

This command restores the RAS1 logging level from ALL to ERROR for units KPX and KRA.

res1   Displays the status of RES1 Logical Resource Manager

Commands for dynamic RAS1 tracing

You can send commands to the monitoring agent or monitoring server on z/OS to alter its RAS1 tracing dynamically while a process is running. You cannot issue these commands if RAS1 monitoring agent tracing is not enabled. Enable the RAS1 tracing first.

If desired, you can send these commands as Tivoli Enterprise Portal Take Action commands.

Dynamic RAS1 monitoring agent tracing uses syntax similar to RAS1 monitoring agent tracing:

```
►►─action─FILTER ID=id─[UNIT=ras1_unit]──────────────────────────►◄
                                      └[CLASS=(ras1_class)]┘
```

where:

action   Can be one of the following:
ADD   Enables a specific filter,
REMOVE   Disables a specific filter.
ENABLE   Enables a global class.
DISABLE   Disables a global class.

FILTER ID
          Identifies the filter.

id   Is a unique key for each filter specified. The ID is usually a three-letter component identifier for the component that the filter is being added to, removed from, enabled, or disabled.

UNIT   Indicates that the trace is specific to a product or component. Use this keyword only at the explicit request of an IBM Software Support representative. Only one unit ID can be specified at a time.

ras1_unit
          Represents the name of the filter. In most instances, the value is the three-character component identifier for the monitoring agent (**KAH** for the SA z/OS monitoring agent).

CLASS
          Specifies the type of trace.

ras1_class
          One of the same values specified for *global_class* but, because of its position inside the parentheses, narrowed in scope to apply only to the specified unit.

Using the Configuration Tool to set trace levels

When you use the Configuration Tool to configure a Tivoli Enterprise Monitoring Server or a monitoring agent on z/OS, you can specify the level of trace information collected. For the monitoring server, you specify trace levels on the Specify Advanced Configuration Values panel. For the monitoring agent, you specify trace levels on the Specify Advanced Agent Configuration Values panel.

Setting trace levels for the monitoring server in the Configuration Tool

The Specify Advanced Configuration Values panel for the monitoring server provides several parameters for setting up logging and tracing.

Enable startup console messages
> Set this parameter to Y if you want a SYSLOG message on the console to indicate when the monitoring server finishes initializing. The default is Y.

Enable communications trace
> Set this parameter to Y if you want KDC_DEBUG=Y as the override setting in the KDSENV member of RKANPARU. Otherwise, the default setting of KDC_DEBUG=N is used. This default parameter instructs the data communications layer to report communications problems using a minimal, summary format. This parameter is intended for stable applications in production. Note that the default KDC_DEBUG=N generates standard RAS1 trace data in the monitoring server RKLVLOG, in addition to the summary information diagnosing possible timeout conditions.
>
> The following settings report on data communications problems:
> - KDC_DEBUG=N: minimal tracing (default)
> - KDC_DEBUG=Y: full-packet tracing
> - KDC_DEBUG=D: KDC_DEBUG=Y plus STATE & FLOW tracing
> - KDC_DEBUG=M: KDC_DEBUG=D plus INPUT & OUTPUT HELP tracing
> - KDC_DEBUG=A: KDC_DEBUG=M plus all format tracing
>
> Do not set KDC_DEBUG=A unless directed by an IBM Software Support representative.

Enable storage detail logging
> Set this parameter to Y to enable storage allocation detail logging. You can use the storage detail command output to analyze storage use in the monitoring server address space. Specifying Y generates the second EVERY command in the KDSSTART member of RKANCMDU.
>
> To disable storage detail logging, set this parameter to N, which generates the second EVERY command as a comment. To control storage detail logging further, you can also dynamically issue the following modify command to the Tivoli Enterprise Monitoring Server started task:
>
> ```
>   ==> F taskname,STORAGE D
> ```
>
> where *taskname* is the name of the Tivoli Enterprise Monitoring Server started task (the default is CANSDSST)
>
> This modify command is useful if the monitoring server is already running with storage detail logging disabled. Issuing the modify command activates storage detail logging without recycling the monitoring server. The default is Y.

If you set this parameter to Y, you must also define the times for storage detail logging and flushing the VSAM buffers.

- For **Storage detail logging**, set the interval to monitor storage. The interval values are written as part of the second EVERY command in the KDSSTART member of RKANCMDU. The default is 0 hours (hh) and 60 minutes (mm).
- For **Flush VSAM buffers**, set the interval to force all deferred VSAM writes to DASD. The interval values are written as part of the command in the KDSSTART member of RKANCMDU. The default is 0 hours (*hh*) and 30 minutes (*mm*).

Setting trace levels for a monitoring agent in the Configuration Tool

The Specify Advanced Agent Configuration Values panel provides several parameters for setting up logging and tracing.

Enable startup console messages
Set this parameter to Y if you want a SYSLOG message on the console to indicate when the monitoring agent finishes initializing. The default is Y.

Enable WTO messages
Set this parameter to Y if you want write-to-operator (WTO) messages logged. The default is N.

Storage detail logging interval
Set the interval (hh:mm) to monitor storage. The interval values are written as part of the second EVERY command in the KAHSTART member of RKANCMDU. The default is 0 (no storage detail logging).

Flush VSAM buffers interval
Set the interval (*hh:mm*) to force all deferred VSAM writes to DASD. The interval values are written as part of the command in the KAHSTART member of RKANCMDU. The default is 0 (no writes to DASD).

Redirecting output of RAS1 tracing

Nearly all diagnostic information for the z/OS components is delivered by the RAS1 component. This component is configured by the KBB_RAS1 environment variable in member KBBENV of RKANPARU. Often, Tivoli customers redirect the initialization member using the ITMS:Engine INITLIST processing. INITLIST processing is always echoed to the RKLVLOG with the KLVIN411 message.

This example shows a typical KBBENV override to a different member, KDSENV:

```
KLVIN410 INITLIST MEMBER KDSINIT BEING PROCESSED
  KLVIN411 KLVINNAM=KDSINNAM
  KLVIN411 KLVINTB=KDSINTB
  KLVIN411 KLVINVLG=KDSINVLG
  KLVIN411 KLVINNAF=KDSINNAF
  KLVIN411 KLVINVPO=KDSINVPO
  KLVIN411 KLVINSTG=KDSINSTG
  KLVIN411 KLVINVAM=KDSINVAM
  KLVIN411 KBBENV=KDSENV
```

In this example, configuration of KBB_RAS1 is recorded in member KDSENV of RKANPARU.

Capturing z/OS logs to send to IBM Software Support

You can view the RKLVLOG for a monitoring agent or monitoring server on z/OS online, or you can save the log to a file. To save a log to a file rather than viewing the log online, you need to know how to do the following:

- "Saving the contents of an RKLVLOG"
- "Ending one RKLVLOG and starting another" on page 226
- "Submitting problems to IBM Software Support" on page 197

Saving the contents of an RKLVLOG

To save the information in your z/OS logs (such as RKLVLOG), use the System Display and Search Facility (SDSF). Follow these instructions to use SDSF to capture (in this example) the RKLVLOG associated with any running task in your monitoring agent.

1. From ISPF, select the SDSF option.
2. Enter the following on the command line:

   ```
   st taskname
   ```

   where *taskname* is the name of the procedure whose log you are trying to display and capture. For example, entering st cansah on the command line results in display of the SA z/OS monitoring agent job.

3. From the SDSF screen, enter ? next to the name of the started task to display a list of the output files. For example, the output files for the SA z/OS monitoring agent task look like this:

   ```
   JESMSGLG JES2
   JESJCL   JES2
   JESYSMSG JES2
   SYSTSPRT CANSAH
   SYSPRINT CANSAH
   RKLVLOG  CANSAH
   RKLVSNAP CANSAH
   ```

4. To print the RKLVLOG for this job to a data set, type s next to the RKLVLOG output file. Then, on the command line of SDSF, type:

   ```
   print d
   ```

   Press Enter. The d means that you want the file printed to a data set.

   The SDSF Print to Data Set panel is displayed.

```
 COMMAND INPUT ===>

Data set name  ===> 'data_set_name'
Member to use  ===>
Disposition    ===> NEW        (OLD, NEW, SHR, MOD)

If the data set is to be created, specify the following.
Volume serial will be used to locate existing data sets if specified.

Management class     ===>           (Blank for default management class)
Storage class        ===>           (Blank for default storage class)
  Volume serial      ===>           (Blank for authorized default volume)  *
  Device type        ===>           (Generic unit or device address)       *
  Data class         ===>           (Blank for default data class)
  Space units        ===> TRKS      (BLKS, TRKS, CYLS, BY, KB, or MB)
  Primary quantity   ===> 5         (In above units)
  Secondary quantity ===> 5         (In above units)
  Directory blocks   ===> 0         (Zero for sequential data set)
  Record format      ===> VBA
  Record length      ===> 240
  Block size         ===> 3120
  * Only one of these fields may be specified
```

Figure 58. SDSF Print to Data Set panel

5. On this panel, type the data set name and characteristics for the file you want to print, and press Enter.
6. You are returned to the RKLVLOG output file. On the command line, specify the number of lines you want to print by entering a range large enough to include the entire file, such as:

   `print 1 99999999`

   Then press Enter. A message in the upper right corner of the panel tells you how many lines are printed.
7. Type `print close` on the SDSF command line to close the file. The log is now saved in the data set that was specified in Step 5.

For more information about SDSF commands, see *z/OS SDSF Operation and Customization* (SA22-7670).

Ending one RKLVLOG and starting another

When you want to recreate a problem to send it to IBM Software Support, you can use a z/OS MODIFY command to close the current RKLVLOG spool data set and open a new one. This command is issued from a z/OS console or from the Tivoli Enterprise Portal (with a Take Action command). The TLVLOG command manages the recording of information to RKLVLOG. The syntax and usage of this command are as follows:

```
►►──MODIFY──stcname──,──TLVLOG──SWITCH──────────────────────────────────►
                                     └─,CLASS=class─┘   └─,COPIES=copies─┘


►───────────────────────────────────────────────────────────────────────►
   └─,DEST=dest─┘  └─,FCB=fcb─┘  └─,FORM=form─┘          ┌─NO──┐
                                              └─HOLD=────┼─────┤─┘
                                                        └─YES─┘


►──────────────────────────────────────────────────────────────────►◄
   └─,MAXLINES=maxlines─┘  └─,UCS=ucs─┘  └─,USER=user─┘  └─,WTRNAME=wtrname─┘
```
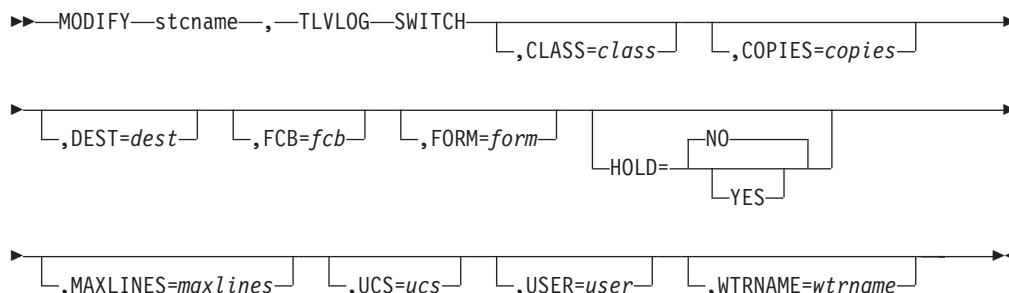
where:

SWITCH
> Dynamically allocates a new RKLVLOG file using the current values, begins recording on the new file, and closes the current RKLVLOG file, releasing it for processing by JES.

class Is the one-character JES SYSOUT class. **CLASS=A** is the ITMS:Engine startup value.

copies Is the copy count. The valid range is 1-254. **COPIES=1** is the startup value.

dest Is the 1-8 character JES SYSOUT destination. **DEST=()** is the startup value.

fcb Is the 1-4 character FCB name to be used. **FCB=()** is the startup value.

form Is the 1-4 character form name to be used. **FORM=()** is the startup value.

hold Determines whether the SYSOUT is to be placed in a JES operator hold when spun off. Specify **YES** (operator hold is requested) or **NO**. **HOLD=NO** is the startup value.

> **Note:** If **HOLD=YES** is specified, you must issue the appropriate JES release command for the SYSOUT data set to be processed.

maxlines
> Is the maximum number of lines to be written to RKLVLOG, in thousands (for example, MAXLINES=2 means a maximum of 2000 lines). The valid range is 0 through 16000 (16 million lines). When this number is reached, an automatic TLVLOG SWITCH is performed, closing the current RKLVLOG and allocating a new one If the specified value is 0, there is no maximum; you must manually enter TLVLOG SWITCH to switch log files. **MAXLINES=0** is the startup value.

> **Note:** Unlike the other values, MAXLINES takes effect immediately. If the new MAXLINES value is less than the number of lines that have already been written to the current RKLVLOG, a switch is performed immediately.

ucs Specifies the 1-4 character z/OS UCS name to be used. **UCS=()** is the startup value.

user Is the 1-8 character user ID to which the SYSOUT is to be spooled. Ignored if **DEST** is blank. **USER=()** is the startup value.

wtrname
> Is the 1-8 character external writer name to be used. **WTRNAME=()** is the startup value.

Notes:

1. The `TLVLOG` command performs up to three functions, depending on the keywords specified. Assuming that you select all three functions, they are performed in the following order:

   a. Updates the dynamic allocation values. With the exception of MAXLINES, these values are used when the next dynamic allocation is performed. Values are updated whenever they are coded on the command.

   b. Lists the current dynamic allocation values. This is always done.

   c. Switches RKLVLOGs. This is done only when SWITCH is specified on the command.

   You can update values and request a switch with the same command. The values are updated first, and then the switch is performed.

2. RKLVLOGs can be closed automatically after a certain number of records have been written to them. Refer to the MAXLINES keyword for more information.
3. To set up an automatic RKLVLOG switch whenever the ITMS:Engine address space is started, add the following command to your RKANCMD startup CLIST:

   TLVLOG MAXLINES=*nnn*

   This command causes RKLVLOG to be closed and released to JES whenever *nnn* thousands of lines have been written. If needed, you can add other values (for example, CLASS) to this command.
4. Many diagnostic messages are recorded in RKLVLOG. If you set RKLVLOG to spin off automatically, or if you explicitly switch RKLVLOG, you must ensure that the SYSOUT files are kept at least for the life of the ITMS:Engine run, in case they are required for problem solving.
5. You might want to issue a `TLVLOG SWITCH` command after a problem occurs. This spins off the RKLVLOG data related to the problem into a separate spool data set, which can be included in the problem documentation. Be sure to include all previously spun-off RKLVLOG files.
6. Because RKLVLOG is managed with standard IBM data management routines, records are buffered before being written. If you are viewing the currently active RKLVLOG with a product such as SDSF, you do not see the latest messages. Issue the command `FLUSH TLVLOG` to force the current data management buffer to be written. Do not use the `TLVLOG SWITCH` to spin off the current RKLVLOG for this purpose, as it fragments the messages recorded in RKLVLOG.
7. Unless you explicitly set a non-zero MAXLINES value, RKLVLOG never switches automatically.
8. If an error occurs when writing to RKLVLOG, ITMS:Engine issues a message and disables RKLVLOG recording. However, messages are still written to VIEWLOG and to all active operator interfaces. Depending on the error, you might be able to restart RKLVLOG by issuing a switch request.

Examples

Here are some examples of ways to use this command:

- To list the current RKLVLOG destination and values:

  tlvlog

- To establish class X and destination SYSPROG as default SYSOUT attributes, and the maximum number of lines as 20,000:

  tlvlog class=x dest=sysprog maxlines=20

- To switch to a new RKLVLOG:

  tlvlog switch

Flushing the log buffers

After a TLVLOG is switched, issuing an echo command can flush the log buffers and ensure that new messages are written to the new RKLVLOG. The ECHO command echoes any text entered back to the screen. The syntax of the ECHO command is shown below:

```
►►──ECHO──────────────────────────────────────────────►◄
        └─string─┘
```

where *string* is a character string to be echoed back to the operator screen where the ECHO command was entered.

Notes:

1. Use ECHO to verify that the ITMS:Engine operator facility is functioning properly and to force all buffered messages to the log.

2. Even after an ECHO, log output might not be visible in JES3 systems, because of the way JES3 manages spool buffers.

3. Enclosing *string* in single quotes is necessary only if you want to preserve leading blanks.

Understanding and using the trace logs

When you open a trace log, you find a mix of status lines and numbered product messages. Most messages with IDs are documented in the problem determination guides for each monitoring agent. You can also determine the meaning of a message by entering the message number into an Internet search engine such as Google. The information that follows helps you interpret the messages and status lines in a z/OS log.

Format of messages in a RAS1 log

A RAS1 log for a monitoring agent on z/OS includes the following information:

- Environmental information
  - Operating system and CPU data. This information is prefaced with the following string:

    pppxxmmm

    where:

    ppp   Is the component prefix.

    xx   Is the component code.

    mmm   Is the module name.
  - Initial command line settings
- Component summary:
  - Name of the module
  - Information about where the library was loaded from
  - Date and time the module was compiled
  - Version (if this detail was specified)
- Formatted output, including entry and exit points and text strings. Entry and exit points show flow into and out of a given function. The exit shows the return code, if applicable. The text depends on the kind of trace specified. Here is an example:

```
(00D41 F9C-1{99%}:KppMAIN.CPP,953,"MainWnd::MainWnd") Entry
(00D41 FD3-1{99%}:KppMAIN.CPP,959,"MainWnd::MainWnd") Exit
Time,Thread,{%stack avail},pgm_name,Line#,function,text
```

As noted earlier, not all functions are RAS1-enabled, and trace level might exclude some paths.

Understanding and using the trace logs

Appendix A. Configuration services and utilities

You can use the configuration services and utilities to perform various services on the runtime environment and specify diagnostic information. Some of the services can modify the Configuration Tool values stored in ISPF tables.

Note: Do not modify any values unless you are told to do so in the documentation or by IBM Software Support personnel. If the Configuration Tool values are modified incorrectly, the Configuration Tool can stop functioning or produce unpredictable results.

To access the configuration services and utilities,
1. From the Configuration Tool Main Menu, select **Configure products**.
2. Select **Services and utilities**.

Services: Unlocking runtime high-level qualifiers

You can use this option to unlock the high-level qualifier values that you specified when you set up your configuration environment. If you need to modify these values, you must first unlock them.

Warning: If you unlock and change the high-level qualifiers, the Configuration Tool does not automatically delete and reallocate the existing libraries. The jobs generated by the Configuration Tool fail if they are pointing at incorrect libraries.

Complete the following steps to unlock and modify runtime high-level qualifiers.
1. From the Main Menu, select **Configure products > Services and utilities > Unlock runtime high-level qualifiers**.
2. Unlock and modify the high-level qualifiers:
   a. On the Unlock Runtime High-Level Qualifiers panel, specify **Y.**
   b. On the Set Up Configuration Environment panel, make your modifications to the high-level qualifiers and press Enter
3. Press F3 until you return to the Main Menu.

Services: Creating the Configuration Tool batch mode job

You can use this option to generate the JCL that runs the Configuration Tool steps under batch.

This option also creates the KCISETUP REXX exec. Invoking KCISETUP enables your ISPF environment to use the ISPF macros provided with the Configuration Tool. You can use these macros to compose and manage the parameter members used for the Configuration Tool batch mode process.

Complete the following steps to create the Configuration Tool batch mode job.
1. From the Main Menu, select **Configure products > Services and utilities >Create batch mode job**.
   Result: The Configuration Tool displays a message at the top of the panel indicating the job has been created.

To view additional information about this job press F1.

2. Press F3 until you return to the Main Menu.

Utilities: Specifying DEBUG options

Complete the following steps to specify or modify DEBUG parameter values.

1. From the Configuration Tool Main Menu, select **Configure products > Services and utilities > DEBUG options**.

   Result: The Configuration Tool displays the Debug Options panel with all of the existing DEBUG values that you entered when invoking the Configuration Tool.

2. Contact IBM Software Support.

   Note: IBM Software Support personnel direct you in specifying or modifying the DEBUG parameter values.

3. Press F3 until you return to the Main Menu.

Utilities: Displaying an ISPF table

You can use this option to specify the contents of an ISPF table located in the data library.

Complete the following steps to display an ISPF table.

1. From the Configuration Tool Main Menu, select **Configure products > Services and utilities > Display an ISPF table**.

2. Specify and view an ISPF table:

   a. Specify the name of the ISPF table you want to display. You can limit the information displayed for an ISPF table by specifying one to three sets of display criteria under **Optional section parameters**. For each set you must specify the variable name and matching value.

   b. Press Enter to view the ISPF table you specified. You can take the following actions:

Action	Result
END (PF3)	Go to the previous record.
ENTER	Go to the next record.
CANCEL	Go back to the previous panel.
UP/DOWN	Use scroll variables.

3. Press F3 until you return to the Main Menu.

Utilities: Running a CLIST in the TKANCUS library

Complete the following steps to run a specific CLIST/REXX exec in the TKANCUS library.

1. From the Configuration Tool Main Menu, select **Configure products > Services and utilities > Execute a CLIST in the TKANCUS library**.

2. Contact IBM Software Support.

   Note: Software Support personnel direct you in selecting and running a CLIST in the TKANCUS library.

3. Press F3 until you return to the Main Menu.

Utilities: Preparing user libraries

The Configuration Tool supports the allocation of the following user libraries required for product operation:

- *&rhilev.&rte.*RKANCMDU
- *&rhilev.&rte.*RKANMODU
- *&rhilev.&rte.*RKANPARU
- *&rhilev.&rte.*RKANSAMU
- *&rhilev.&rte.*RKANSQLU (applicable to the Tivoli Enterprise Monitoring Server only)

The **Prepare user libraries** utility generates a batch job to create, from the existing target libraries, the necessary user libraries.

1. From the Configuration Tool Main Menu, select **Configure products > Services and utilities > Prepare user libraries**.

   The Runtime Environments (RTEs) for Conversion panel lists all the runtime environments whose libraries are eligible for conversion to user libraries.

2. On the Runtime Environments (RTEs) for Conversion panel, you can accept the default (all runtime environments listed) or delete from the list any runtime environments you want to exclude from conversion.

3. When you finish reviewing the list, press Enter to generate the KCIJSP01 batch job.

4. Edit the job as needed, then submit it.

Utilities: Preparing user libraries

Appendix B. Configuration Tool batch utilities

Several Configuration Tool utilities are available for batch mode processing. These utilities are designed to run outside the Configuration Tool, but can also be used while in the Configuration Tool.

KCISETUP

> Sets up the environment that is required to use the Configuration Tool batch utilities.

KCICFKEY

> Manages the PF keys that are used for the Configuration Tool batch utilities.

KCICPGHP

> Displays help information for parameters in a batch parameter deck member.

KCISETUP: Setting up the environment

You use the KCISETUP utility to set up the environment that is required for using the other Configuration Tool batch utilities. This utility must be run after starting your TSO ISPF session and can only be run from an ISPF session.

Before using the KCISETUP utility, you must generate the KCISETUP member in your INSTLIB. KCISETUP can only be run once per session. There is no confirmation message issued to indicate successful completion of KCISETUP.

Complete the following steps to generate KCISETUP.

1. Start the Configuration Tool on your master image.
2. From the Main Menu, select **Configure products > Services and utilities > Create batch mode job**.

   Result: The Configuration Tool generates member KCISETUP in your INSTLIB.
3. Press F3 until you return to the Main Menu.

   Note: KCISETUP must be created on an image and can be used for all subsequent parameter deck processing on that image. If your ISPF environment changes or you split your INSTLIB, you must recreate KCISETUP.

You can invoke the environment setup utility, using either of the following methods.

Location	Command
ISPF command line	`TSO EXEC '`*shilev*`.INSTLIB(KCISETUP)'`
ISPF Primary Option Menu > Enter TSO or Workstation commands	`EXEC '`*shilev*`.INSTLIB(KCISETUP)'` where *shilev* is the high-level qualifier of the INSTLIB.

KCICFKEY: Managing PF keys

You use the KCICFKEY utility to manage ISPF session PF keys that are used for batch utilities. This includes turning the PF keys on and off, and toggling which set of keys display. This utility can *only* be run under an ISPF session.

Note: If you are using KCICFKEY to manage the ISPF session PF keys for the batch utilities, you must turn on the predefined function keys. To do this, issue the PFSHOW command from either the ISPF command line or any of the Configuration Tool panel command lines.

Before using this Configuration Tool batch utility, you must use the KCISETUP utility to set up the environment.

To use the KCICFKEY utility, the ISPF session must support 24 PF keys. Complete the following steps to set up the ISPF session to support 24 PF keys.

1. From the ISPF Primary Option Menu, select **Terminal and user parameters > Function keys > Non-Keylist PF Key settings**.
2. Type 24 for **Number of PF Keys**.
3. Press F3 to return to the ISPF Primary Option Menu.

If the ISPF session is not set up to support 24 PF keys, the KCICFKEY utility runs but issues the following ISPF dialogue warning message:

```
"PFKEYS COUNT ERROR", "Number
of PF Keys must be 24.  See ISPF Settings."
```

When setting PF keys, the Configuration Tool PF Key Manager owns PF keys 13–24. On keyboards that do not support 24 PF keys, PF keys 13–24 are enabled by holding the Shift key and pressing a function key. While the Shift key is pressed, function keys 1–12 become 13–24.

When the Configuration Tool PF keys are active, any change in the PF Key Show State is preserved. If you have set the PF Key Show State to **Show All** and then turned off the PF keys, when you turn the PF keys back on, the PF Key Show State is restored to **Show All**.

While using the Configuration Tool PF Key Manager, all of your original PF key and Show State settings are preserved. After exiting the PF Key Manager, all of your original PF key and Show State settings are restored.

You invoke the PF Key Manager utility using one of the following methods.

Method	Command
ISPF edit	From the Edit command line, enter KCICFKEY state **Note:** To use this method you must be running under an ISPF session, editing a member or data set.
TSO command	From the ISPF command line, enter TSO KCICFKEY state where *shilev* is the high-level qualifier of the INSTLIB.

The *state* is the desired state of the Configuration Tool PF keys. Valid states are:

ON   Turn on the PF keys.

OFF   Turn off the PF keys.

SHOW
>If the PF keys are active, then toggle the PF keys between All (1–24), Alternate (13–24), and Primary (1–12).

HELP   Display the PF Key Manager help information.

If *state* is not specified, the Configuration Tool PF keys toggle between **ON** and **OFF**.

KCICPGHP: Displaying help for batch parameters

You use the KCICPGHP utility to display help information for parameters in a batch parameter deck member. The detailed help information for each of the batch parameters is provided to help you modify or construct a batch parameter deck.

This utility must be run from an ISPF Edit session.

Before using this batch utility, you must use the KCISETUP utility to set up the environment.

You invoke the Batch Parameter Deck Help utility using either of the following methods:
* From an ISPF Edit command line, enter the command `KCICPGHP`, position the cursor on the row that contains a batch parameter, and then press Enter.
* Position your cursor on the row that contains a batch parameter and then select the PF key assigned by the Configuration Tool PF Key Manager.

>**Note:** This is the preferred method for invoking Batch Parameter Deck Help. The PF Key Manager assigns a PF key to invoke this function.

With either method, you must position the cursor on the row that contains the batch parameter. The utility then isolates the parameter, looks it up, and displays detailed help information.

The batch parameter online help contains the following four sections:

Description Area
>The detailed help information for the parameter. This area is scrollable, as indicated by the (+) indicator on the bottom right. PF7 and PF8 are assigned to scroll this area.

Attribute Area
>The attributes of the parameter. This information can help you determine what type of data is expected for this parameter.

PF Key Area
>The PF key assignments that apply only to the dialog box.

>**Note:** PF5 (Show All) displays the help information for all parameters that make up this product.

Following is an example of a batch parameter help:

KCICPGHP: Displaying help for batch parameters

```
KMV_CMS_NAME   -   CMS Name
Description:
    This is the nodeid of the CMS to which you are connecting the agent.
    This name must match the domain name of a non-z/OS CMS, or the nodeid
    parameter in the KDSCNFG member of the RKANPAR library for a z/OS
    CMS. If the NODEID parameter contains the literal "*SMFID", the CMS Name
    definition must use the actual z/OS SMFID in place of this literal value.

    The value of this field is case sensitive for both z/OS and
Attributes:
    Required:Yes
    Maximum Length:32
    Type of Data:Character (Mixed Case)
    Default value:

F1=Help   F3=End   F5=Show All   **=Backward   F8=Forward
```

Figure 59. Batch parameter help example

Appendix C. Support

If you have a problem with your IBM software, you want to resolve it quickly. This section describes the following options for obtaining support for IBM software products:

- "Obtaining fixes"
- "Receiving weekly support updates"
- "Contacting IBM Software Support" on page 240

> **Tip**
>
> Before using the resources listed below, look for troubleshooting information in this guide and in the *IBM Tivoli Monitoring: Problem Determination Guide*.

Obtaining fixes

A product fix might be available to resolve your problem. To determine what fixes are available for the OMEGAMON z/OS Management Console product, complete the following steps:

1. Go to the IBM Software Support Website at http://www.ibm.com/software/support.
2. Under **Find product support**, click **All IBM software (A-Z)**. This opens the software product list.
3. In the software product list, click **IBM Tivoli System Automation for z/OS**. This opens the IBM Tivoli System Automation for z/OS support site.
4. Under **Solve a problem**, click **APARs** to go to a list of fixes, fix packs, and other service updates for IBM Tivoli System Automation for z/OS.
5. Click the name of a fix to read the description and optionally download the fix. You can also search for a specific fix; for tips on refining your search, click **Search tips**.
6. In the **Find downloads and drivers by product** section, select one software category from the **Category** list.
7. Select one product from the **Sub-category** list.
8. Type more search terms in the **Search within results** if you want to refine your search.
9. Click **Search**.
10. From the list of downloads returned by your search, click the name of a fix to read the description of the fix and to optionally download the fix.

For more information about the types of fixes that are available, see the *IBM Software Support Handbook* at http://techsupport.services.ibm.com/guides/handbook.html.

Receiving weekly support updates

To receive weekly e-mail notifications about fixes and other software support news, complete the following steps:

Receiving weekly support updates

1. Go to the IBM Software Support Website at http://www.ibm.com/software/
   support.
2. Click **My support** in the upper right corner of the page.
3. If you have already registered for **My support**, sign in and skip to the next
   step. If you have not registered, click **register now**. Complete the registration
   form using your e-mail address as your IBM ID and click **Submit**.
4. Click **Edit profile**.
5. In the **Products** list, select **Software**. A second list is displayed.
6. In the second list, select the product segment **Systems Management**. A third
   list is displayed.
7. In the third list, select **Other Systems Management**. A list of applicable
   products is displayed.
8. Select the products for which you want to receive updates.
9. Click **Add products**.
10. After selecting all products that are of interest to you, click **Subscribe to
    e-mail** on the **Edit profile** tab.
11. Select **Please send these documents by weekly e-mail**.
12. Update your e-mail address as needed.
13. In the **Documents** list, select **Software**.
14. Select the types of documents that you want to receive information about.
15. Click **Update**.

If you experience problems with the **My support** feature, you can obtain help in
one of the following ways:

Online
> Send an e-mail message to erchelp@ca.ibm.com, describing your problem.

By phone
> Call 1-800-IBM-4You (1-800-426-4968).

Contacting IBM Software Support

IBM Software Support provides assistance with product defects.

Before contacting IBM Software Support, your company must have an active IBM
software maintenance contract, and you must be authorized to submit problems to
IBM. The type of software maintenance contract that you need depends on the
type of product you have:

- For IBM distributed software products (including, but not limited to, Tivoli,
  Lotus®, and Rational® products, as well as DB2 and WebSphere® products that
  run on Windows, or UNIX operating systems), enroll in Passport Advantage in
  one of the following ways:

  Online
  > Go to the Passport Advantage Website at http://www-306.ibm.com/
  > software/howtobuy/passportadvantage/pao_customers.htm and click
  > **How to Enroll**.

  By phone
  > For the phone number to call in your country, go to the IBM Software
  > Support Website at http://techsupport.services.ibm.com/guides/
  > contacts.html and click the name of your geographic region.

- For customers with Subscription and Support (S & S) contracts, go to the Software Service Request Website at https://techsupport.services.ibm.com/ssr/login.
- For customers with IBMLink, CATIA, Linux, S/390®, iSeries®, pSeries®, zSeries, and other support agreements, go to the IBM Support Line Website at http://www.ibm.com/services/us/index.wss/so/its/a1000030/dt006.
- For IBM eServer™ software products (including, but not limited to, DB2 and WebSphere products that run in zSeries, pSeries, and iSeries environments), you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for eServer software products, go to the IBM Technical Support Advantage Website at http://www.ibm.com/servers/eserver/techsupport.html.

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States. From other countries, go to the contacts page of the *IBM Software Support Handbook* on the Web at http://techsupport.services.ibm.com/guides/contacts.html and click the name of your geographic region for phone numbers of people who provide support for your location.

To contact IBM Software support, complete the following steps:
1. "Determining the business impact"
2. "Describing problems and gathering information"
3. "Submitting problems" on page 242

Determining the business impact

When you report a problem to IBM, you are asked to supply a severity level. Therefore, you need to understand and assess the business impact of the problem that you are reporting. Use the following criteria:

Severity 1
> The problem has a *critical* business impact. You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.

Severity 2
> The problem has a *significant* business impact. The program is usable, but it is severely limited.

Severity 3
> The problem has *some* business impact. The program is usable, but less significant features (not critical to operations) are unavailable.

Severity 4
> The problem has *minimal* business impact. The problem causes little impact on operations, or a reasonable circumvention to the problem was implemented.

Describing problems and gathering information

When describing a problem to IBM, be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently. To save time, know the answers to these questions:
- What software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information. See

Chapter 15, "Introduction to problem determination," on page 189 and Chapter 20, "Setting up a trace on a z/OS system," on page 217.

- Can you re-create the problem? If so, what steps were performed to re-create the problem?
- Did you make any changes to the system? For example, did you make changes to the hardware, operating system, networking software, and so on.
- Are you currently using a workaround for the problem? If so, be prepared to explain the workaround when you report the problem.

Submitting problems

You can submit your problem to IBM Software Support in one of two ways:

Online

Click **Submit and track problems** on the IBM Software Support site at http://www.ibm.com/software/support/probsub.html. Type your information into the appropriate problem submission form.

By phone

For the phone number to call in your country, go to the contacts page of the *IBM Software Support Handbook* at http://techsupport.services.ibm.com/guides/contacts.html and click the name of your geographic region.

If the problem you submit is for a software defect or for missing or inaccurate documentation, IBM Software Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Software Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the Software Support Website daily, so that other users who experience the same problem can benefit from the same resolution.

Appendix D. 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 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
USA

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 may 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 Websites are provided for convenience only and do not in any manner serve as an endorsement of those Websites. The materials at those Websites are not part of the materials for this IBM product and use of those Websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who 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 Deutschland Research & Development GmbH
Department 3248
Schoenaicher Strasse 220
D-71032 Boeblingen
Federal Republic of Germany

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.

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.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

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 www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Intel is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Index

A

abbreviations
  Configuration Tool xx
  qualifiers xx
abend 211
accessibility xix
Action attribute 172, 175
Add Runtime Environment panel,
  Configuration Tool 61, 94
Address Space Information table 148,
  149, 150, 151, 152
Administrator authority, Windows 85,
  90
agent, monitoring
  permissions for product features 114
  security considerations 114
  started task 78, 84, 100, 106
  starting 87, 107
agents, monitoring 137
alerts 179
APF authorization 84, 106
Appl Parms attribute 174
Application ID attribute 163
application support 86, 91, 208, 209
Asid attribute 164
attribute groups
  and workspaces 153
  Automation Agent Detail
    Information 154
  Automation Environment 155
  Automation Manager Detail
    Information 157
  Automation Statistics 157
  Critical Messages 159
  Gateway Connections 159
  Monitor Resources 161
  OMEGAMON Sessions 162
  Outstanding WTOR Replies 164
  Resource Agent Information 165
  Resource List 166
  Resource Manager Information 171
  Resource Requests 172
  Resource Votes 175
  SA z/OS monitoring agent 153
  Status Items 176
attributes
  defined 140
  naming 153
  SA z/OS monitoring agent 153
  using in queries 140
Authentication Group attribute 163
Auto Remove attribute 174
Automation Agent Detail Information
  attribute group 154
Automation Agent Details
  workspace 148
automation agent problems 181
Automation Environment attribute
  group 155
Automation Environment
  workspace 149

Automation Flag attribute 169
Automation Manager Detail Information
  attribute group 157
Automation Statistics attribute
  group 157
Automation Statistics workspace 149
Automation Status attribute 168
Average Waittime attribute 158

B

base libraries 15
base runtime environment 15, 17
Basic System Services (BSS1) 221
batch mode
  Configuration Tool 125, 231
  example 128
  parameters 128
  services 231
  utilities 235
Batch Parameter Deck Help utility 237
books
  see publications xvii
browser client 13, 138, 192
browser view 5
buffers, log 228

C

case studies 185
Category attribute 171
CB#Vxxxx system variable members
  job 106
Change Time attribute 177
chart views 5
CICAT
  See Configuration Tool
client 138
CM Severity Critical attribute 159
CM Severity Important attribute 159
CM Severity Unusual attribute 159
code, product
  See product code
Comm Method attribute 156
Command Count attribute 158, 163
commands
  dynamic tracing 222
  ECHO 228
  RAS1 221, 222
  service console 221, 222
  Take Action 216
  TLVLOG 226
Commands Per Hour attribute 158
Comment attribute 174, 176
communication failure 213
Communication Method attribute 160
communication protocols
  IP 70, 81, 104
  IP.PIPE 70, 79, 102
  IP.SPIPE 79, 102

communication protocols *(continued)*
  IP6.PIPE 79, 102
  SNA 70, 81
  specifying 69
  TCP/IP 70, 79, 102
  UDP 70, 81, 104
communication tracing 217, 223
complex passwords 208
component code
  See product code
components, product 5, 9
Compound Status attribute 169
conditions, situation 180
configuration
  adding monitoring agents 88, 107
  batch mode processing 88, 108
  Configuration Tool environment 51
  expanding 88, 107
  monitoring agent security 114
  NetView 47
  overall 22
  planning 9
  roadmap 38
  runtime environments 16
  SA z/OS 47
  SA z/OS monitoring agent
    security 114
  SA z/OS monitoring agent,
    communication 75, 98
  security
    monitoring agent 114
    runtime environment 63, 96
    Tivoli Enterprise Monitoring
      Server 67, 109
  setting up Configuration Tool 49
  Tivoli Enterprise Monitoring Server on
    Windows 84, 85, 90
  Tivoli Enterprise Monitoring Server on
    z/OS 64
  Tivoli Enterprise Monitoring Server
    security 67, 109
  Tivoli Enterprise Portal Server and
    client 84, 85, 90
  verifying 87, 107
configuration scenarios
  hub Tivoli Enterprise Monitoring
    Server on Windows 89
  separate address spaces on z/OS 57
Configuration Tool
  abbreviations xx
  batch mode 42, 125, 128, 231, 235
  commands 43
  defined 40, 42
  display requirements 43
  errors 42
  example 128
  interactive mode 42
  online help 43
  requirements 43
  services 231
  setting trace levels 223, 224

X

IBM ®

Program Number: 5698-SA3

Printed in USA