IBM Z OMEGAMON Monitor for z/OS
5.6

# *Planning and Configuration Guide*

IBM

**Note**

Before using this information and the product it supports, read the information in "Notices" on page 97.

**Edition notice**

This edition applies to Version 5 Release 6 of IBM Z OMEGAMON Monitor for z/OS for z/OS and to all subsequent releases and modifications until otherwise indicated in new editions.

**© Copyright International Business Machines Corporation 2022.**
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

# Contents

# Figures

# Tables

# Chapter 1. Preparation and planning

This guide provides information specific to configuration of IBM Z OMEGAMON Monitor for z/OS. The *OMEGAMON XE Products: Preinstallation Requirements and Instructions* technote and the *Planning* and *Configuring* sections of the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Shared documentation* contain planning information that is common to the deployment and configuration of all OMEGAMON® XE monitoring agents and Tivoli® Management Services components on z/OS®. You should be familiar with the information in those documents before you read the information in this book.

The chapters in this section contain introductory and planning information:

- "Introducing IBM Z OMEGAMON Monitor for z/OS" on page 1 provides an overview of the monitoring product and the infrastructure on which it runs. It also introduces new features of the product that may affect deployment and configuration.
- "Planning for configuration" on page 4 discusses prerequisites for product installation and the monitoring of certain types of data and provides information to help you plan the configuration of IBM Z OMEGAMON Monitor for z/OS monitoring agents.
- "Upgrading to the new release" on page 13 discusses the product-specific requirements and sequence of steps for upgrading to this release.

A Tivoli Enterprise Monitoring Server must be configured in each runtime environment in which IBM Z OMEGAMON Monitor for z/OS is configured. Before you continue to Chapter 2, "Configuration," on page 15, use *IBM Tivoli Monitoring: Configuring the Tivoli Enterprise Monitoring Server on z/OS* to configure a monitoring server in each runtime environment.

## Introducing IBM Z OMEGAMON Monitor for z/OS

IBM Z OMEGAMON Monitor for z/OS is a member of the IBM Z Monitoring Suite. IBM Z OMEGAMON Monitor for z/OS enables you to monitor and manage the performance and availability of individual z/OS systems, as well as the workload performance and resource utilization of the Parallel Sysplex in which they participate.

IBM Z OMEGAMON Monitor for z/OS monitoring agents installed on monitored z/OS LPARs (logical partitions) provide comprehensive usage information for Sysplex-level resources such as coupling facilities, global enqueues, global resource serialization (GRS) ring systems, shared DASD groups, and cross-system coupling facilities (XCFs), as well as performance information for the service classes, report classes, and resource groups that use those resources.

IBM Z OMEGAMON Monitor for z/OS monitoring agents also provide extensive system-level performance and usage information for individual z/OS images. In addition, they monitor the status and configuration of IBM cryptographic coprocessors installed in zSeries servers, provide data on UNIX System Services hosted on your z/OS systems, and allow system-level and sysplex-wide reporting of actual and potential special processor resource usage.

The data collected by the monitoring agents and alerts triggered by monitored conditions can be displayed in a graphical, Java-based interface, shared with other OMEGAMON and IBM Tivoli Monitoring products. In addition, IBM Z OMEGAMON Monitor for z/OS offers continued access to the OMEGAMON for MVS 3270 interface, as well as a new, OMEGAMON enhanced 3270 user interface with specially-designed workspaces that can provide plex-wide and even cross-product data.

Used in conjunction with other OMEGAMON monitoring products, the data, analyses, and alerts presented by IBM Z OMEGAMON Monitor for z/OS help you develop a holistic view of your entire computing enterprise from a single console.

### Tivoli Management Services

IBM Z OMEGAMON Monitor for z/OS takes advantage of the Tivoli Management Services on z/OS infrastructure.

© Copyright IBM Corp. 2022

Tivoli Management Services on z/OS provide security, data transfer and storage, notification mechanisms, user interface presentation, and communication services for a number of products, including IBM Tivoli Monitoring and OMEGAMON XE monitoring agents, in an agent-server-client implementation (Figure 1 on page 2).

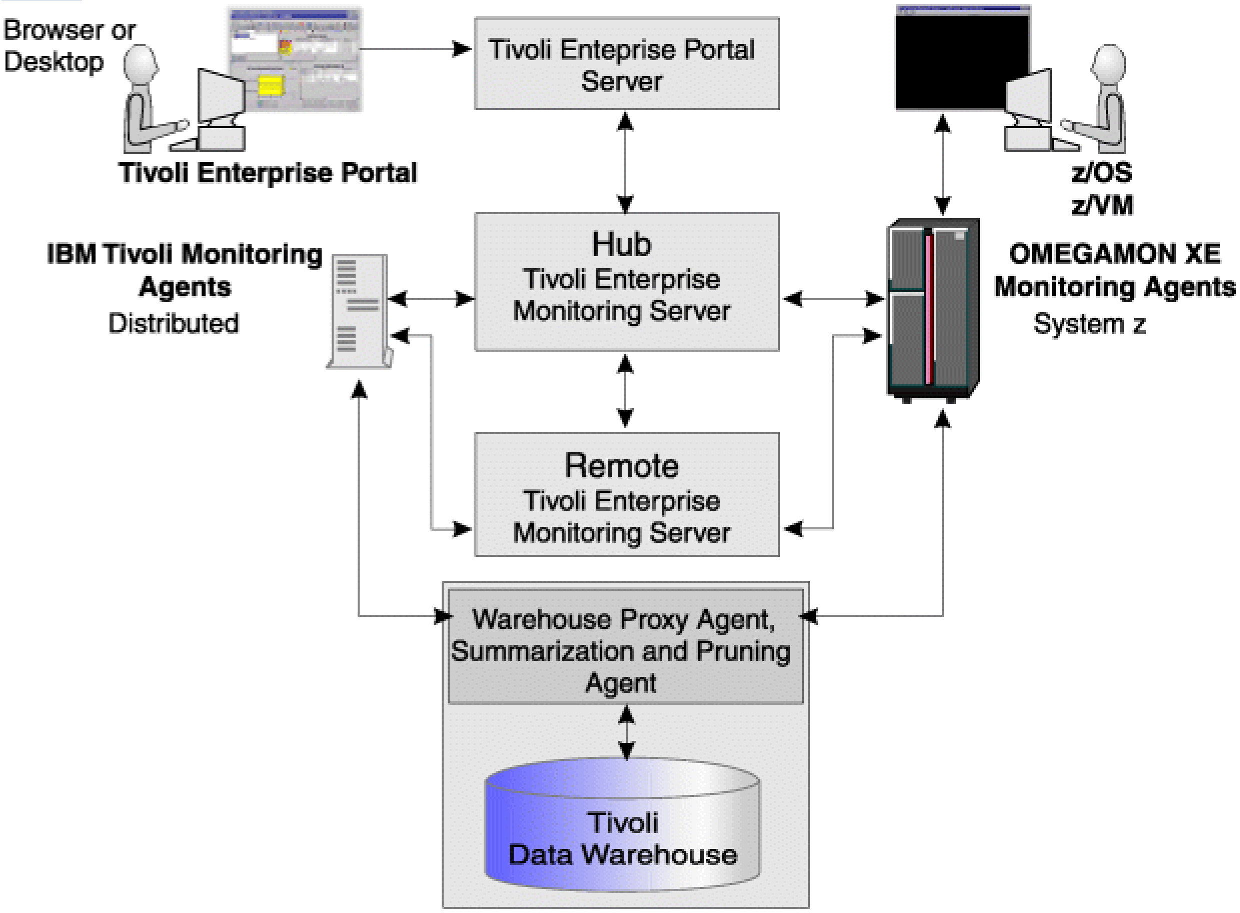

Browser or Desktop
Tivoli Enterprise Portal
Tivoli Enteprise Portal Server
z/OS
z/VM
IBM Tivoli Monitoring Agents
Distributed
Hub
Tivoli Enterprise Monitoring Server
OMEGAMON XE Monitoring Agents
System z
Remote
Tivoli Enterprise Monitoring Server
Warehouse Proxy Agent, Summarization and Pruning Agent
Tivoli Data Warehouse

*Figure 1. Agent-server-client architecture*

Some components of Tivoli Management Services on z/OS, such as Tivoli Enterprise Portal and the Warehouse Proxy and Summarization and Pruning agents, run only on distributed systems (Windows, AIX, and Linux). The Tivoli Enterprise Monitoring Server and the Tivoli Data Warehouse can run on either distributed or mainframe systems. The Tivoli Management Services:Engine runs only on mainframe systems. The components of Tivoli Management Services on z/OS are described in detail in the *Planning* and *Configuring* sections of the *OMEGAMON XE and Tivoli Management Services on z/OS: Shared documentation*.

The required versions of all Tivoli Management Services on z/OS components are included in the IBM Z OMEGAMON Monitor for z/OS package. For detailed information about installing, configuring, and using Tivoli Management Services, see the documents in the IBM® Tivoli Monitoring Library.

## OMEGAMON XE common components

IBM Z OMEGAMON Monitor for z/OS monitoring agents on z/OS share several components (referred to as *common components*: see Table 1 on page 3). These common components, along with the monitoring agent software, are included on the IBM Z OMEGAMON Monitor for z/OSproduct tape.

*Table 1. z/OS common components*

| Component | Description |
|---|---|
| OMNIMON base V7.3.0 | A set of common code used by OMEGAMON Classic (real-time collectors) components and the OMEGAMON Enhanced 3270 user interface to control initialization, security, and I/O for all sessions. OMNIMON Base has two components:<br>• **OMEGAMON Subsystem (formerly Candle Subsystem)**<br>A z/OS subsystem, running in its own address space to monitor dynamic device activity. The OMEGAMON Subsystem also collects coupling facility data for IBM Z OMEGAMON Monitor for z/OS. Not all OMEGAMON XE monitoring products require the OMEGAMON Subsystem. In addition, the OMEGAMON Subsystem caches some RMF near-term history data for theIBM Z OMEGAMON Monitor for z/OS product.<br>• **OMEGAMON Enhanced 3270 user interface**<br>An enhanced 3270-based user interface that collects and displays data from the Tivoli Enterprise Monitoring Server and the supporting IBM Z OMEGAMON Monitor for z/OS monitoring agents. One instance of the interface must be installed in each Sysplex for use by all supporting agents. |
| Shared probes | Data probes shared by several OMEGAMON XE products. |

**Note:** If you install IBM Z OMEGAMON Monitor for z/OS into an existing environment, in which the components are already at the required level (for example, if you have already installed another OMEGAMON XE agent), you may need to delete the FMIDs for these components from the SMP/E install jobs to avoid errors because they are already installed. See the *IBM Z OMEGAMON Monitor for z/OS: Program Directory* for more information.

## Interoperability and integration

IBM Z OMEGAMON Monitor for z/OS is designed to integrate with all products that use Tivoli Management Services on z/OS. These products exploit the ability of the Tivoli Enterprise Portal to integrate and correlate performance and availability information from a variety of sources.

For example, with OMEGAMON DE, the Tivoli Enterprise Portal allows you to create custom workspaces composed of data from a range of Tivoli monitoring solutions (IBM Tivoli Monitoring, IBM Tivoli Composite Application Manager, and IBM Tivoli NetView® for z/OS, as well as OMEGAMON XE monitoring agents). You can also create context-sensitive links between product workspaces to obtain additional information about systems, subsystems, resources or network components that are being monitored by other monitoring agents, or links that access related screens in TN3270-based applications.

OMEGAMON XE products are being integrated with an increasing number of other Tivoli and IBM products. Situation events reported by IBM Z OMEGAMON Monitor for z/OS can be forwarded to Tivoli Event Console or Tivoli Netcool/OMNIbus for event correlation and management. You can view historical reports using Tivoli Common Reporting. From the Tivoli Enterprise Portal you can launch "in context" into other Web-based or web-enabled Tivoli applications without having to re-enter user credentials, and you can launch in context into Tivoli Enterprise Portal workspaces from applications such as IBM Tivoli Business Services Management.

**Restriction:** IBM Z OMEGAMON Monitor for z/OS V5.6 is not compatible with IBM OMEGAMON z/OS Management Console.

# Planning for configuration

The information in this section is intended to help you plan the configuration of IBM Z OMEGAMON Monitor for z/OS.

This information assumes that you have met the relevant installation requirements discussed in the *OMEGAMON XE Products: Preinstallation Requirements and Instructions* technote and read the planning information in the *Planning* section of the *OMEGAMON XE and Tivoli Management Services on z/OS: Shared documentation*.

The following topics are covered in this section:

- "Configuration prerequisites" on page 4
- "Planning configuration of IBM Z OMEGAMON Monitor for z/OS" on page 9
- "Planning historical data collection" on page 11
- "Before you begin configuration" on page 13

If you are installing the IBM Z OMEGAMON Monitor for z/OS product for the first time, read the entire chapter. If you are upgrading from a prior version, you can proceed to "Upgrading to the new release" on page 13 after you have reviewed the configuration requirements for this release.

## Configuration prerequisites

The topics in this section cover the hardware and software requirements for IBM Z OMEGAMON Monitor for z/OS, as well as the prerequisites for the collection and display of certain types of data.

- "Software and hardware requirements" on page 4 summarizes the prerequisite software and the supported operating systems and hardware.
- "Prerequisites for data collection and display" on page 5 summarizes the conditions that must be in effect for certain types of data to be available.
- "Using RMF data collection" on page 7 provides an overview of the configuration tasks required to enable use of data collected by z/OS Resource Measurement Facility.

### Software and hardware requirements

A complete list of the software and hardware prerequisites is provided in the *IBM Z Monitoring Suite: Program Directory*.

The following sections provide an overview of these prerequisites:

- "Required software" on page 4
- "Supported operating systems" on page 5
- "Supported hardware" on page 5

#### *Required software*

IBM Z OMEGAMON Monitor for z/OS requires Tivoli Management Services on z/OS on z/OS version 6.2.3 Fix Pack 1 or later. The suggested minimum requirement is version 6.3.0 Fix Pack 1.

You can download Tivoli Management Services on z/OS on z/OS version 6.2.3 Fix Packs, by using your IBM customer number and ibm.com® ID from (https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=swg-tiv-acasf). You can also obtain information about ordering Tivoli Management Services on z/OS on z/OS from CBPDO and ServerPac (http://www-01.ibm.com/common/ssi/rep_ca/9/897/ENUS209-409/index.html).

If you are installing application support files from a DVD image or a fix pack, consult the `readme.txt` file that is provided with the DVD or fix pack. This file details the minimum Tivoli Management Services on z/OS requirements that are associated with the installation media. If you are installing application support files by using the self-describing agent feature your Tivoli Management Services on z/OS server components must be at version 6.2.3 Fix Pack 1 or later.

The hardware and software prerequisites for the distributed components of Tivoli Management Services on z/OS can be found in *IBM Tivoli Monitoring: Installation and Setup Guide*. The software and hardware requirements for a monitoring server on z/OS are detailed in *IBM Tivoli Management Services on z/OS: Configuring the Tivoli Enterprise Monitoring Server on z/OS*.

To make sure that you have the latest version of all components, check for any fix packs that might be available, go to the technote, *Recommended Maintenance Service Levels* (http://www-01.ibm.com/support/docview.wss?uid=swg21290883). For more information about answering your questions before you upgrade, see the technote, *Feature documents* (http://www-01.ibm.com/support/docview.wss?uid=swg21626495).

### Supported operating systems

LPARs on which IBM Z OMEGAMON Monitor for z/OS monitoring agents are installed must be running z/OS version 1 release 12 or later.

For information about APARs (authorized program analysis reports) required, see the *OMEGAMON XE shared documentation Version 6.3.0 Fix Pack 2 and above*. For late-breaking information, see the Preventive Service Planning (PSP) bucket for this monitoring agent.

### Supported hardware

IBM Z OMEGAMON Monitor for z/OS monitoring agents can be deployed on any hardware environment that supports z/OS 1.12 or later.

Ensure that you have adequate disk space to accommodate the products you are installing. Before installing your IBM Z Monitoring Suite products, review the disk space requirements and considerations for an SMP/E installed environment, as documented in the *IBM Z OMEGAMON Monitor for z/OS: Program Directory*, to make sure that sufficient storage is available.

**Tip:** During normal SMP/E processing, VSAM control interval and control area splits can occur. This causes fragmentation, which can degrade SMP/E performance and space utilization. To reorganize the CSI, use your site's approved utility and method for managing VSAM files.

## Prerequisites for data collection and display

For an IBM Z OMEGAMON Monitor for z/OS monitoring agent to collect certain types of data, the Tivoli Enterprise Monitoring Server address space in which it is configured must be assigned a user ID and given the appropriate authorization. In addition, some attributes or attribute groups collect and display data only if specific conditions are met.

To monitor UNIX System Services, the Tivoli Enterprise Monitoring Server must be identified to your security authorization facility as a UNIX System Services user as described in "Authorizing address spaces for UNIX System Services" on page 25).

To monitor coupling facility, cross-system coupling facility, or lock data collected by RMF, the Tivoli Enterprise Monitoring Server must have an RACF® ID and the ID must be authorized to generate PassTickets, as described in "Enabling RMF data collection" on page 25.

To collect RMF near-term history data, the Tivoli Enterprise Monitoring Server and OMEGAMON Subsystem must have an RACF ID and the ID must be authorized to generate PassTickets, as described in "Enabling RMF data collection" on page 25.

Table 2 on page 5 describes the additional prerequisites for collection and display of certain types of data.

*Table 2. Data prerequisites*

| Data is available for | Only if |
|---|---|
| 4 Hour MSUs attribute in the System CPU Utilization attributes group | A defined capacity is used as a basis for pricing and the z/OS system is *not* running as a guest on z/VM®. |
| Channel Path attributes | The IBM Resource Measurement Facility (RMF) has been started. |

*Table 2. Data prerequisites (continued)*

| **Data is available for** | **Only if** |
|---|---|
| Common Storage attributes | The Common Storage Area Analyzer (CSA Analyzer) is started.<br>**Note:** The CSA Analyzer is shipped and installed with IBM Z OMEGAMON Monitor for z/OS. It is started as a separate started task. |
| Coupling facility and cross-system coupling facility (XCF) data collected by the IBM Resource Measurement Facility (RMF) Distributed Data Server (DDS) | • The following RMF components are activated:<br>– RMF Control Task (RMF)–one instance on each system<br>– RMF Monitor III Gatherer (RMFGAT)–one instance on each system<br>– RMF Distributed Data Server (GPMSERVE)–one instance per sysplex<br>• You have enabled RMF data collection as described in "Using RMF data collection" on page 7. |
| Cryptographic attributes | 1. At least one IBM cryptographic coprocessor must be installed.<br>2. KM5EXIT3 and KMEXIT4 exits must be installed in the Integrated Cryptographic Service Facility (ICSF).<br>**Note:** The KM5EXIT3 and KM5EXIT4 exits are shipped and installed with IBM Z OMEGAMON Monitor for z/OS. See "Adding the KM5EXIT3 and KM5EXIT4 to the ICSF Configuration" on page 24 for more information.<br>3. The USERID for the IBM Z OMEGAMON Monitor for z/OS TEMS STC (typically xxxxDS) has access to the required ICSF Callable Services. See "Granting authorization to use ICSF Callable Services" on page 25 for more information. |
| DASD MVS™ workspace and DASD MVS Devices attributes | RMF has been started. |
| GRS Ring Systems attributes | The global resource serialization (GRS) complex is in ring mode. (If the complex is in star mode, only the name, status, and ring acceleration of each system are available.) |
| Health Check attributes | IBM Health Checker for z/OS software be installed, configured, and running. |
| HiperDispatch Management and HiperDispatch Logical Processors attributes | HiperDispatch Management mode is On. |
| Integrated Facility for Applications (IFA) on CP resource times at the address space and service class period level | Either<br>• z/Series Application Assist Processors are configured on the systems, or<br>• Java™ applications are started using a switch (-Xifa:force) |
| LPAR cluster attributes | The z/OS system is not running as a guest on z/VM. |
| Model Permanent Capacity ID and Rating and Model Temporary ID and Rating | System hardware is z10 or later. |

*Table 2. Data prerequisites (continued)*

| **Data is available for** | **Only if** |
|---|---|
| Near-term history data collected by the Resource Measurement Facility (RMF) Distributed Data Server. | • The following components are activated:<br>– OMEGAMON Subsystem - at least one instance per sysplex (two for redundancy), up to one instance on each monitored system<br>– RMF Control Task (RMF) - one instance on each monitored system<br>– RMF Monitor III Gatherer (RMFGAT) - one instance on each monitored system<br>– RMF Distributed Data Server (GPMSERVE) - one instance per sysplex<br>• You have enabled RMF data collection as described in "Using RMF data collection" on page 7 |
| Promoted Percent | The z/OS Workload Manager blocked workload capability is enabled. |
| Sysplex DASD attributes (Sysplex DASD Device, Sysplex DASD Group, Sysplex DASD) | A DASD filter situation is enabled. |
| Suspend lock and spin lock data | • The following RMF components activated:<br>– RMF Control Task (RMF)–one instance on each system<br>– RMF Monitor III Gatherer (RMFGAT)–one instance on each system<br>– RMF Distributed Data Server (GPMSERVE)–one instance per sysplex<br>• You have enabled RMF data collection (see "Using RMF data collection" on page 7).<br>• Lock data collection is enabled on RMF. |
| zAware data | The Integrated Cryptographic Service Facility (ICSF) must be active on the LPARs where IBM Z OMEGAMON Monitor for z/OS agents run. This does not require the Tivoli Enterprise Monitoring Server to be configured for ICSF usage. |
| zFS attributes | zFS is specified as the file system on the monitored system (FILESYSTEM TYPE(ZFS) is specified in SYS1.PARMLIB(BPXPRM*xx*)).<br>**Note:** For z/OS 1.10, IBM Z OMEGAMON Monitor for z/OS uses an address space name of ZFS, unless the parameter KM3KZFSASNM=*xxxxxxxx* (where *xxxxxxxx* is the started task (STC) name of the zFS address space) has been added to the &*rhilev*.&*rte*.RKANPARU(KDSENV). |
| z/OS UNIX System Services attributes | The address space where the IBM Z OMEGAMON Monitor for z/OS product is running has SUPER USER authority. This level of authority is equivalent to root (UID=0). |

## Using RMF data collection

IBM Z OMEGAMON Monitor for z/OS provides the capability to collect some real-time data and near-term history data from the IBM Resource Measurement Facility (RMF) Distributed Data Server (DDS). IBM Z OMEGAMON Monitor for z/OS can be configured to obtain real-time coupling facility (CF), cross-system coupling facility (XCF), and system lock data from the RMF Distributed Data Server instead of collecting its own data. Using RMF data can eliminate duplicate data collection and provide you with consistent metrics. It can also result in some processor usage savings. RMF data is collected at a shorter monitoring interval than the corresponding IBM Z OMEGAMON Monitor for z/OS data.

Use of RMF for real-time data collection can be enabled as part of Sysplex configuration. There are four options:

**NO**
The default. Disables RMF data collection. CF and XCF data is collected from the OMEGAMON Subsystem.

**ALL**
CF, XCF, and lock data is collected from RMF.

**CF/XCF**
CF and XCF data is collected from RMF.

**LOCK**
Spin and suspend lock data is collected from RMF.

Use of RMF to collect near-term history data is enabled by default. You can disable near-term history data collection from RMF by setting a parameter in the PARMGEN configuration profile. The IBM Z OMEGAMON Monitor for z/OS agents will discover the OMEGAMON Subsystem that has registered with a configured group name using the z/OS Sysplex Routing Services.

Use of RMF data collection for both real-time data and near-term history data requires that the following RMF components be activated:

- RMF Control Task (RMF)—one instance on each monitored system.
- RMF Monitor III Gatherer (RMFGAT)—one instance on each monitored system.
- RMF Distributed Data Server (GPMSERVE)—one instance per sysplex.

**Note:** The RMF Distributed Data Server migrates to the system running the highest level of z/OS.

For near-term history data, an additional requirement is that at least one instance (two for redundancy and up to one instance on each monitored system) of the OMEGAMON Subsystem must be active per sysplex

In addition, the following tasks must be completed:

- RACF IDs must be defined for the address spaces that are collecting RMF data.

  Activation of the RMF Distributed Data Server API requires a RACF user ID and password. As its user ID, IBM Z OMEGAMON Monitor for z/OS agents and the OMEGAMON Subsystem use the name shown in the SDSF Display Active screen as the OWNER of the address space. This is often the started task name but does not have to be. The user IDs of these address spaces must be defined to RACF. You will probably want to add those IDs to a group to simplify PassTicket authorization (see later in this section).
- RACF secured signon PassTicket function for the DDS must be enabled.

  Passwords specified during configuration would have to be held in a secure, encrypted format, and many sites have default time limits on how long passwords are viable. Instead, IBM Z OMEGAMON Monitor for z/OS agents and the OMEGAMON Subsystem use the RACF secured signon function. The secured signon function provides an alternative to the RACF password called a PassTicket. PassTicket is a one-time-only password that is generated by a requesting product or function. IBM Z OMEGAMON Monitor for z/OS agents and the OMEGAMON Subsystem generate a PassTicket for a specific address space ID when it accesses the RMF Distributed Data Server to obtain RMF data.

  To enable IBM Z OMEGAMON Monitor for z/OS agents and the OMEGAMON subsystem to use PassTicket, a RACF administrator must enable the PTKTDATA class and authorize the address spaces.

Detailed instructions for completing these tasks are provided in "Enabling RMF data collection" on page 25. See the *z/OS Security Server RACF Security Administrator's Guide* for a full discussion of PassTicket function and setup.

**Note:** You can choose to bypass user ID and password authentication for the RMF Distributed Data server API for all or selected users using initialization parameters. For further information, refer to discussion of the HTTP_NOAUTH in the RMF documentation.

### *Management of near-term history data collection*

In a sysplex, one OMEGAMON Subsystem per group runs an RMF cache. Other OMEGAMON Subsystems in the group are ready to start an RMF cache if the active RMF cache is stopped. The group contains all the OMEGAMON Subsystems that are configured with the same group name.

**Note:** After APAR OA63270 is installed, the OMEGAMON Subsystem RMF cache is disabled and the instructions in this section regarding the usage of the OMEGAMON Subsystem RMF cache can be ignored.

You can identify the OMEGAMON Subsystem in a group that is running an RMF cache by issuing a MODIFY command to any OMEGAMON Subsystem in the same group:

```
F stcname,NTHCACHE LOCATE
```

where `stcname` is the OMEGAMON Subsystem started task name

You can stop the OMEGAMON Subsystem address space with a STOP command:

```
P stcname
```

When you stop the OMEGAMON Subsystem that is running an RMF cache, another OMEGAMON Subsystem in the group obtains an ENQ using the group name and starts a new RMF cache.

You might want to suspend near-term history data collection by the OMEGAMON Subsystem that is running an RMF cache. One reason would be when you need to restart one of the RMF components. You can suspend near-term history data collection by issuing a MODIFY command to the OMEGAMON Subsystem running the RMF cache:

```
F stcname,NTHCACHE SUSPEND
```

After the RMF component or components are restarted, you resume near-term history collection by issuing a MODIFY command to the OMEGAMON Subsystem running the RMF cache:

```
F stcname,NTHCACHE RESUME
```

The OMEGAMON Subsystem will restart near-term history data collection with the next time period after data collection was suspended. If data collection was suspended longer than the configured range in hours (parameter RTE_KCN_CACHE_KM5_NTH_RANGE), data collection is resumed to retrieve the data for the configured range in hours (for example, the last 24 hours).

# Planning configuration of IBM Z OMEGAMON Monitor for z/OS

The topics in this section describe the Sysplex-level entities you will be defining during the configuration process.

## Defining Sysplexes

A *Sysplex* is a set of z/OS LPARS that share a common cross-system coupling facility (XCF) environment and a single Sysplex clock. You define Sysplexes to IBM Z OMEGAMON Monitor for z/OS and assign runtime environments to them during the configuration process.

When you configure each monitoring agent, you have the option of defining its runtime environment as single LPAR environment or as a Sysplex environment. If you define it as a Sysplex environment, you must assign it to a defined Sysplex. Data from each runtime environment in a Sysplex is pooled at the primary Sysplex proxy (see “Designating the Sysplex proxy” on page 10).

## Designating the Sysplex proxy

The *Sysplex proxy* is a Tivoli Enterprise Monitoring Server that serves as a data consolidation point for Sysplex monitoring. Sysplex situations are evaluated at the Sysplex proxy, and historical data for a Sysplex is collected there.

Figure 2 on page 10 shows the deployment of IBM Z OMEGAMON Monitor for z/OS in a multi-sysplex environment.

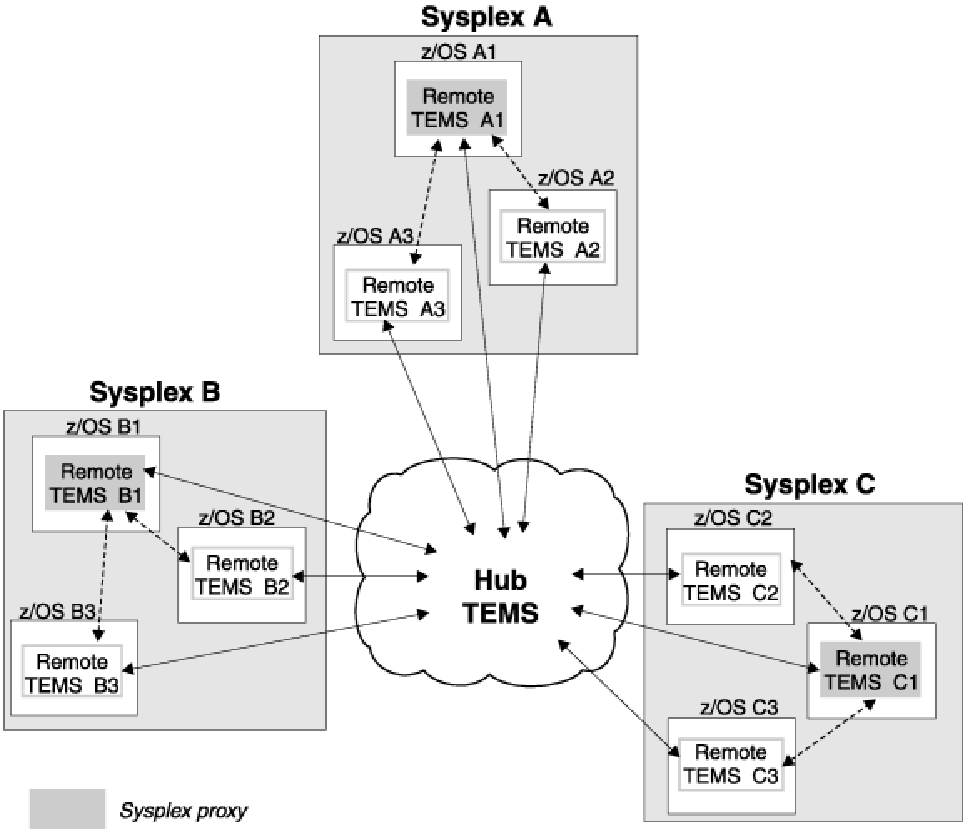


*Figure 2. Deployment of IBM Z OMEGAMON Monitor for z/OS in a multiplex environment*

Each Sysplex has a primary proxy and several backup proxies to which the function migrates when the primary proxy goes down or is taken offline. During the configuration of each runtime environment, assign each to a Sysplex and specify whether or not the runtime environment should be eligible to act as the Sysplex proxy. The first runtime environment to be assigned to the Sysplex is marked as the primary proxy. Subsequent runtime environments are defined as backups, unless you exclude them from proxy eligibility. The primary runtime environment is the only runtime environment that can define the persistent data store files that contain Sysplex-level data.

The hub Tivoli Enterprise Monitoring Server should not be the primary Sysplex proxy candidate. Like a hub, the proxy is a busy server, so it may be a good idea to exclude the hub from proxy eligibility entirely.

## Excluding a TEMS from becoming the KM5PLEX agent

The KM5PLEX agent will only run in a TEMS acting as the Sysplex proxy. The KM5_PLEXVIEW parameter, configured in PARMGEN, allows you to exclude a particular TEMS in a sysplex from becoming the KM5PLEX agent.

### About this task

Setting the KM5_PLEXVIEW parameter to N will prevent the TEMS from becoming the KM5PLEX (SYSPLEX:SYSPLEX:PLEXVIEW) agent. Setting the KM5_PLEXVIEW parameter to Y, or omitting the parameter, allows a TEMS to become the KM5PLEX agent.

### Procedure

1. Update the KDS$PENV PARMGEN override member:
   a) Select **Customize PARMGEN configuration profiles** from the PARMGEN Primary Option Menu.
   b) Select **WCONFIG** from the Customize Parmgen Configuration Profile Members panel.
   c) Select and edit the KDS$PENV member.
   d) Add or update the KM5_PLEXVIEW parameter as either KM5_PLEXVIEW=NO (to exclude the TEMS from being the KM5PLEX agent) or KM5_PLEXVIEW=YES (to allow it).
2. Update HLQ.rtename.WKANPARU library
   a) Select **Create this RTE's runtime members and jobs** from the PARMGEN Primary Option Menu.
   b) Select **Create runtime members/jobs in all WK* libs** and submit the generated $PARSE job.
3. Update HLQ.rtename.RKANPARU library
   a) Select **Submit batch jobs to complete PARMGEN setup** from the PARMGEN Primary Option Menu.
   b) Select **Copy runtime mbrs from WK*->RK* RW libs**
   c) Select and submit one of the jobs to populate the runtime libraries

### What to do next

Changes will not take effect until the TEMS for the newly configured RTE has been recycled.

## Defining an enqplex

In configurations where enqueue management (using CA-Multi-Image Manager, or MIM) spans two or more Sysplexes, IBM Z OMEGAMON Monitor for z/OS provides data on conflicts between Sysplexes, using the concept of an *enqplex*. An enqplex is a group of z/OS images under common enqueue management. Defining an enqplex allows IBM Z OMEGAMON Monitor for z/OS to correlate enqueue information for multiple Sysplexes and identify conflicts.

During the process of configuring IBM Z OMEGAMON Monitor for z/OS, you will be asked to perform the following tasks:

- Specify one or more enqplex names
- Assign each Sysplex to an enqplex
- Assign each runtime environment to a Sysplex
- List the MIM task names in the z/OS image in which you are configuring IBM Z OMEGAMON Monitor for z/OS

If you do not specify an enqplex name, or do not assign a system (that is, a z/OS image) to an enqplex, it is assigned to the $DEFAULT enqplex and is assumed to share resources and enqueue management.

# Planning historical data collection

The *Planning* section of the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Shared documentation* details the planning decisions that you make when you configure historical data collection. The information in this section is intended to help you understand the configuration options that you are presented with during the configuration of IBM Z OMEGAMON Monitor for z/OS.

During the configuration process you are given the option of configuring the historical data stores in four sections of the configuration profile member:

1. Run-Time Environment (parameters that start with "RTE_PDS_"): This profile section configures persistent data store control member options, high-level qualifier, and default maintenance procedure name.
2. Tivoli Enterprise Monitoring Server (parameters that start with "KDS_PD_"): This section configures the generic persistent data store (RPDSGRP). You must configure the persistent data store when you

configure the Tivoli Enterprise Monitoring Server if you intend to collect historical data for IBM Z OMEGAMON Monitor for z/OS.

3. IBM Z OMEGAMON Monitor for z/OS (parameters that start with "KM5_PDS_" and "KM5_PD"): This section configures the dedicated, or private, data sets for IBM Z OMEGAMON Monitor for z/OS RKM5LPR* and RKM5PLX* for the groups LPARDATA and PLEXDATA. The PLEXDATA data sets are allocated only on the Tivoli Enterprise Monitoring Server that is acting as the sysplex proxy. The LPARDATA data sets are allocated on every Tivoli Enterprise Monitoring Server.

   **Note:** If you want the IBM Z OMEGAMON Monitor for z/OS monitoring agent to use RMF data instead of collecting its own data, you must modify the KM5_RMF_DDS_COLLECTION parameter. For more information about enabling RMF data collection, see “Configuring the IBM Z OMEGAMON Monitor for z/OS agent to use RMF data” on page 17.

If you want to collect historical data for IBM Z OMEGAMON Monitor for z/OS, you must configure the data store parameters for the Run-Time Environment, Tivoli Enterprise Monitoring Server, and IBM Z OMEGAMON Monitor for z/OS.

**Note:** To collect historical data, you must configure and start historical data collection using the Tivoli Enterprise Portal, or the Enhanced 3270 user interface. See "Using Historical Data Collection and Reporting" in *IBM Z OMEGAMON Monitor for z/OS: User's Guide* for more information.

## Configuring the historical data stores for IBM Z OMEGAMON Monitor for z/OS

All OMEGAMON XE products use dedicated, or *private*, data sets. In addition, some OMEGAMON XE products use general, or *generic*, data sets, that is, data sets that can be shared by many products.

If you want to configure IBM Z OMEGAMON Monitor for z/OS to collect historical data for display in the Tivoli Enterprise Portal, you must configure both generic and private data stores. When you configure the persistent data store during configuration of a Tivoli Enterprise Monitoring Server, you are configuring the generic data sets. When you configure the persistent data store during configuration of IBM Z OMEGAMON Monitor for z/OS, you are configuring the private data sets.

IBM Z OMEGAMON Monitor for z/OS uses two groups of private data sets for historical data: LPARDATA (the RKM5LPR* data sets) and PLEXDATA (RKM5PLX*). The PLEXDATA data sets are allocated only on the Tivoli Enterprise Monitoring Server that is currently acting as the Sysplex proxy. The LPARDATA data sets are allocated on every Tivoli Enterprise Monitoring Server.

For Sysplex-level data, the Tivoli Enterprise Monitoring Servers that are acting as the primary proxy and the backup proxies share the same private data set (RKM5PLX*). During the configuration process, one set of files is created and initialized on shared DASD for the sysplex. At runtime, the Tivoli Enterprise Monitoring Server that becomes the Sysplex proxy allocates these files to itself. If the Sysplex proxy function migrates to a backup proxy system, that system dynamically allocates these same files. This way, all the Sysplex level history data is collected in a single set of persistent data store files.

Only the runtime environment that acts as the primary proxy is allowed to configure these files in the persistent data store.

For system-level data, each runtime environment allocates files in its own persistent data store.

## Determining DASD requirements for storing historical data

The *IBM Z OMEGAMON Monitor for z/OS: Program Directory* provides the basic space requirements for the Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal, the Tivoli Enterprise Portal Server, and the monitoring agents themselves. These basic space requirements do *not* include additional space that is required for maintaining historical data files.

Because of the variations in client distributed systems, system size, number of managed systems, and so on, it is difficult to provide actual additional disk space requirements necessary for historical data collection. You need to experiment to determine how much space you need.

Use the default amounts to configure the data store initially, then observe how quickly space gets used. Eventually, you want to allocate enough space so that maintenance procedures only need to run once a day. Use the information in Chapter 3, “Disk space requirements for IBM Z OMEGAMON Monitor for z/OS historical data tables,” on page 45 to help determine how much space you need to allocate.

## Before you begin configuration

Before you begin to configure IBM Z OMEGAMON Monitor for z/OS, complete the tasks listed in Table 3 on page 13:

*Table 3. Preconfiguration tasks*

| Task | Location of information |
|---|---|
| Complete any preinstallation requirements. | *OMEGAMON XE Products: Preinstallation Requirements and Instructions* |
| Verify that you have the required software and DASD<br>Install the product. | *IBM Z OMEGAMON Monitor for z/OS: Program Directory* |
| Read the planning information and make any necessary planning decisions.<br>Review information on batch processing and system symbolics, so your first runtime environment is appropriate for replication.<br>Set up the runtime environment and allocate the runtime libraries. | *Planning section of the IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Shared documentation* |
| Configure the Tivoli Enterprise Monitoring Server in the runtime environment. | *IBM Tivoli Management Services on z/OS: Configuring the Tivoli Enterprise Monitoring Server on z/OS* |
| Verify that no user-defined ICSF service call exits have been set up. | See note. |

**Note:** IBM Z OMEGAMON Monitor for z/OS monitors Integrated Cryptographic Service Facility (ICSF) subsystems by hooking the standard service call exits defined by IBM. If those exits are customized, data collection cannot occur.

If you need to define your own exits, use the ICSF security exits as alternatives to the two service call exits, CSFEXIT3 and CSFEXIT4. If the monitoring agent discovers a user-defined exit that conflicts with a IBM Z OMEGAMON Monitor for z/OS performance-monitoring exit, it replaces the user-defined exit, issues a warning message, and proceeds with data collection.

The OIBM Z OMEGAMON Monitor for z/OS exits use installation word 2 (CCVTINW2) in the Cryptographic Communications Vector (CCVT) control block. Your exits must not change this value, or fatal errors will occur in the monitoring agent. As an alternative, you can use installation word 1 (CCVTINW1), which is not used by the IBM Z OMEGAMON Monitor for z/OS exits and can be changed without affecting the monitoring agent.

# Upgrading to the new release

In addition to the common upgrade requirements documented in the *OMEGAMON XE and Tivoli Management Services on z/OS: Upgrade Guide*, there are several requirements specific to IBM Z OMEGAMON Monitor for z/OS.

- “Configuring a high availability hub and converting a static hub to a remote” on page 14
- “Performing a staged upgrade” on page 14
- “Persistence of zAware credentials” on page 14

## Configuring a high availability hub and converting a static hub to a remote

If you intend to enable the self describing agent (SDA) feature, and you have an agent configured in the hub monitoring server address space, configure a high availability (HA) hub on the LPAR and convert the static hub to a static remote monitoring server that connects to the new HA hub. In addition, you must reconfigure all the remote monitoring servers that connected to the previous hub to connect to the new HA hub.

For instructions on configuring an HA hub, see the *IBM Tivoli Monitoring: Configuring Tivoli Enterprise Monitoring Server on z/OS*.

To convert a static hub to a remote, you must make the following changes:

- Change TCP communication values for the monitoring server:
  - The name or IP address of the hub
  - The port of the HA hub
- Change the type of the local monitoring server type from hub to remote.
- Change the hub type that the remote connects to to HA.
- If the static hub was excluded from proxy eligibility, change it to proxy eligible.
- Set to virtual IP address type for connecting to the hub.
- Add TEMS network interface list support.

Complete scenario PGN04, Clone an existing environment and convert its hub monitoring server to a remote, in the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: PARMGEN Reference*.

## Performing a staged upgrade

To make product upgrades easier, IBM Z OMEGAMON Monitor for z/OS supports upgrading agents gradually, by allowing a mixture of monitoring agents of the current version and the previous version in the same environment. You can deploy new monitoring agents to your z/OS systems and Sysplexes along with older monitoring agents of the same product, during an upgrade transition period. If you are upgrading from a release before V4.2.0, you must upgrade to V4.2.0 or later before you upgrade to V5.6.

If you want to do a staged upgrade, Sysplex proxy and any monitoring servers eligible to serve as backups to the Sysplex proxy must be at V5.3.0. (See "Designating the Sysplex proxy" on page 10 for a discussion of the Sysplex proxy). This means that no address space at V4.2.0 or V5.1.0 can be eligible to be the Sysplex proxy.

## Persistence of zAware credentials

If you plan to configure IBM Z OMEGAMON Monitor for z/OS to connect to an IBM zAware server, you must consider persistence of the zAware credentials.

For more information about zAware integration, see the *IBM Z OMEGAMON Monitor for z/OS: User's Guide*.

The IBM Z OMEGAMON Monitor for z/OS zAware credentials are stored in the `RKCPDEFW` file that is allocated to the hub Tivoli Enterprise Monitoring Server.

### Hot Standby for distributed hub configurations

If your IBM Z OMEGAMON Monitor for z/OS agent is reporting to a hub server on a distributed platform and you configured Hot Standby with your distributed hub server, you must keep the `RKCPDEFW.db/idx` files defined at the hub in sync with the Standby Hub copy of the `RKCPDEFW.db/idx` files. If you modify your zAware credentials, you must copy the `RKCPDEFW.db/idx` files from your active or primary hub tables directory to your standby hub tables directory, then recycle the Hot Standby hub. This procedure ensures that whenever a failover to the Hot Standby hub is performed, that your latest zAware credentials are available after the failover switch completes. For more information, see *IBM Tivoli Monitoring High Availability Guide for Distributed Systems Version 6.2.3* or later.

# Chapter 2. Configuration

Configuration of IBM Z OMEGAMON Monitor for z/OS involves setting values for a set of configuration parameters using your preferred configuration tool (either PARMGEN or Configuration Manager).

You must take additional steps outside of the configuration tool to complete the configuration.

The instructions in this information make the following assumptions:

- A Tivoli Enterprise Monitoring Server has been configured in the runtime environment, as described in *IBM Tivoli Monitoring: Configuring the Tivoli Enterprise Monitoring Server on z/OS*.
- You have read "Planning for configuration" on page 4 and understand the decisions you will need to make during configuration.

"Completing the configuration - IBM Z OMEGAMON Monitor for z/OS" on page 19 describes the tasks you must perform outside the configuration tool to complete the configuration of IBM Z OMEGAMON Monitor for z/OS. This chapter consolidates the tasks for the OMEGAMON Subsystem and the IBM Z OMEGAMON Monitor for z/OS monitoring agent.

"Verifying the configuration" on page 42 contains instructions for validating the configuration of IBM Z OMEGAMON Monitor for z/OS.

## Configuring IBM Z OMEGAMON Monitor for z/OS

You configure IBM Z OMEGAMON Monitor for z/OS by accepting or customizing the values of parameters that begin with KM2 and KM5.

For guidance on setting parameter values, see the following sources of information:

- Comments in the configuration profiles
- Online help for the configuration profile

  If the supplied KCIRPLBS macro has been copied to your SYSPROC concatenation, you can enter TSO KCIRPLBS at the ISPF command line to run the help macro. Place the cursor anywhere on the line containing the parameter for which you want help text displayed, and press PF14.
- *IBM Tivoli OMEGAMON XE and IBM Tivoli Management Services on z/OS: PARMGEN Reference*
- The *Reference* section of the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Shared documentation*
- *IBM Z OMEGAMON Monitor for z/OS : Parameter Reference.*

Before you configure the IBM Z OMEGAMON Monitor for z/OS agent using your preferred configuration tool (either PARMGEN or Configuration Manager), you should have completed the tasks listed in "Completing the configuration - IBM Z OMEGAMON Monitor for z/OS" on page 19:

*Table 4. Tasks to complete before configuring IBM Z OMEGAMON Monitor for z/OS*

| Configuration task | Location of instructions |
|---|---|
| Set up PARMGEN work libraries for the runtime environment | *Configuring* section of the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Shared documentation* |
| Set up the PARMGEN configuration profile for the runtime environment | *Configuring* section of the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Shared documentation* |

© Copyright IBM Corp. 2022

*Table 4. Tasks to complete before configuring IBM Z OMEGAMON Monitor for z/OS (continued)*

| Configuration task | Location of instructions |
|---|---|
| Configure a Tivoli Enterprise Monitoring Server | *IBM Tivoli Management Services on z/OS: Configuring the Tivoli Enterprise Monitoring Server on z/OS* and the *Reference* section of the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Shared documentation*<br>**Note:** Because IBM Z OMEGAMON Monitor for z/OS runs in the monitoring server address space, you must install a monitoring server in every runtime environment in which you configure the monitoring agent. |
| Configure an OMEGAMON Subsystem | *Configuring* section of the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Shared documentation*<br>**Note:** Configure only one OMEGAMON Subsystem for each LPAR. |
| (Optional) Configure the OMEGAMON Enhanced 3270 user interface address space | *Configuring* section of the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Shared documentation*<br>**Note:** You only need to configure one OMEGAMON Enhanced 3270 user interface address space in a hub. |

**Tip:** If you are enabling self describing agents, configure a stand-alone high-availability hub monitoring server. Installing a high-availability hub lets you apply maintenance or upgrades without recycling the hub. If you have an existing static hub to which agents report, convert the hub to a remote and configure all the remotes to report to the new high-availability hub.

After you have configured IBM Z OMEGAMON Monitor for z/OS (and any other agents you want to configure) using the runtime environment profile, you must complete several configuration tasks outside of the profile. See "Completing the configuration - IBM Z OMEGAMON Monitor for z/OS" on page 19.

## Configuring IBM Z OMEGAMON Monitor for z/OS

You configure the IBM Z OMEGAMON Monitor for z/OS component of the monitoring product to define Sysplex-level entities, assign the current runtime environment to a Sysplex, install product-specific data on the Tivoli Enterprise Monitoring Server, and register the IBM Z OMEGAMON Monitor for z/OS monitoring agent in the Tivoli Enterprise Monitoring Server address space. You also configure the persistent data store for the product historical data and allocate the data sets to store the Sysplex-level and system-level data. These parameters are specified in the KM5 section of the configuration tool.

You configure RMF near-term history data collection in the global (RTE_) section of the configuration tool.

Default values are provided for all required parameters and some optional ones. If you do not want to customize these parameters, and you do not want to enable optional features, you can complete the configuration by accepting these defaults. Alternatively, you can specify custom values. You can also specify custom values for optional parameters that have no defaults. You must specify values for these parameters in order to activate those features. You can supply custom values for the following required and optional features:

- Security class and command-level control for Take Action commands

The security for Take Action commands provided with the IBM Z OMEGAMON Monitor for z/OS is implemented through direct System Authorization Facility (SAF) calls and is based on profiles and resource names. These commands cannot be run unless security is configured.

- RMF real time and near-term history data

  Optionally, the IBM Z OMEGAMON Monitor for z/OS monitoring agent can be configured to use RMF data instead of collecting its own. You can configure the agent to use all RMF-supplied real-time data, spin lock data only, or coupling facility and cross-coupling facility data only.

  The IBM Z OMEGAMON Monitor for z/OS monitoring agents and the OMEGAMON Subsystem will collect near-term history data from the RMF Distributed Data Server by default. You can disable near-term history data collection or you can specify a group name.

- Messages for proxy switch

  By default, messages reporting that the location of the Sysplex proxy has changed are sent to the log. You can configure the monitoring agent to send these messages to the operator console.

- Override zIIP offload

  By default, a portion of the IBM Z OMEGAMON Monitor for z/OS DASD data collection processing is redirected to IBM System z Integrated Information Processors (zIIPs), where these are available. This frees up the standard processors for other work.

- MIM started task names

  Optionally, you can specify names for MIM started tasks.

- ICSF load library for zAware

  Optionally, you can specify the ICSF load library in PARMGEN.

## Configuring security for Take Action commands

IBM Z OMEGAMON Monitor for z/OS agent Take Action commands cannot be issued unless a security class is defined to the SAF security manager and the security class name configured in each runtime environment in which an IBM Z OMEGAMON Monitor for z/OS monitoring agent is configured.

To secure Take Action commands, you must configure the global security parameter (RTE_SECURITY_CLASS). Optionally, you can use the SAF class name override parameter (KM5_SECURITY_ACTION_CLASS) to specify a separate class for securing individual Take Action commands. After each security class has been defined, profiles must be created to control access to individual commands and user IDs must be given UPDATE access to those profiles. See “Authorizing users to issue Prefixed Take Action commands” on page 39.

## Configuring the IBM Z OMEGAMON Monitor for z/OS agent to use RMF data

The use of RMF for real-time data collection is controlled by the KM5_RMF_DDS_COLLECTION parameter. By default, this parameter is set to *NO*.

If you want the IBM Z OMEGAMON Monitor for z/OS monitoring agent to use RMF data instead of collecting its own data, specify one of the following values:

**ALL**
RMF data collection is used for CF, XCF, and spin lock data.

**CF/XCF**
RMF data collection is used for CF and XCF data.

**LOCK**
RMF data collection is used for spin lock data.

**Note:** IBM Z OMEGAMON Monitor for z/OS does not collect lock data. If you want lock data, you must use RMF data.

The use of RMF for near-term history data collection is controlled by the RTE_KM5_NTH, RTE_KCN_CACHE_KM5_NTH, and RTE_KCN_CACHE_KM5_NTH_RANGE parameters. By default, the

RTE_KM5_NTH parameter is set to Y to enable RMF near-term history data collection. Both IBM Z OMEGAMON Monitor for z/OS monitoring agents and the OMEGAMON Subsystem participate in RMF near-term history data collection.

**RTE_KM5_NTH**

Default value is *Y*. Set this parameter to *N* or *NO* to disable RMF near-term history data collection.

**Note:** When APAR OA63270 is installed, the RMF cache is disabled so this variable only affects whether the z/OS agent is eligible to retrieve near-term-history data.

**RTE_KCN_CACHE_KM5_NTH**

**Note:** After APAR OA63270 is installed, this cache-related parameter is not necessary because the RMF cache is disabled.

Default value is KM5WMSRS. One OMEGAMON subsystem per group in a sysplex runs an RMF cache. Others in the group are ready to start an RMF cache if the active RMF cache is stopped. This parameter specifies the group name that is used by the OMEGAMON Subsystems and IBM Z OMEGAMON Monitor for z/OS agents. The IBM Z OMEGAMON Monitor for z/OS agents discover the OMEGAMON Subsystem that uses the z/OS Sysplex Routing Services to register with this group name.

**Note:** Specify the same value for RTE_KCN_CACHE_KM5_NTH in all RTEs in a sysplex. Setting different values results in caching data in more than one OMEGAMON Subsystem per sysplex, an agent not finding an OMEGAMON Subsystem to retrieve data from, or both.

**RTE_KCN_CACHE_KM5_NTH_RANGE**

**Note:** After APAR OA63270 is installed, this cache-related parameter is not necessary because the RMF cache is disabled.

Default value is *24*. The number of hours of near-term history data that the OMEGAMON Subsystem loads during initialization of the RMF cache.

For more information, see the *IBM Z OMEGAMON Monitor for z/OS: Parameter Reference*.

## Turning off zIIP offload

A portion of the IBM Z OMEGAMON Monitor for z/OS DASD data collection processing is redirected to IBM System z® Integrated Information Processors (zIIPs), where available. This frees up the standard processors for other work and can reduce software licensing costs. You can disable the offloading by adding `KM5ZIIPOFFLOAD=NO` to the &*rhilev*.&*rte*.WCONFIG(KDS$PENV) file.

The contents of the KDS$PENV file are dynamically embedded in the KDSENV file. This prevents the parameter from being overwritten when updates or maintenance is applied.

## Sending messages for proxy switch to the console

If the Tivoli Enterprise Monitoring Server designated as the Sysplex proxy goes down, the Sysplex proxy migrates to a backup monitoring server. You can configure the product to send a message to the operator console when the location of the proxy changes.

To configure IBM Z OMEGAMON Monitor for z/OS to send a message regarding the change of location of the proxy, set the value of KM5_KDS_KOSWTO_FLAG in the following section to Y:

```
** Write Sysplex proxy message to the MVS console:
KM5_KDS_KOSWTO_FLAG              N
```

## Specifying MIM names

CA-Multi-Image Manager (MIM) is used to control an enqueue environment across multiple Sysplexes. For systems that use MIM, you can define up to three MIM started task names.

Use the parameters in the following section to specify names for MIM started tasks:

```
** (Optional) Started task names for MIM support:
**KM5_MIM_STC1                     MIMPROC1
**KM5_MIM_STC2                     MIMPROC2
**KM5_MIM_STC3                     MIMPROC3
```

### Specifying the ICSF load library for zAware

ICSF must be enabled to support zAware user ID and password encryption.

The ICSF data set must be concatenated in the RKANMODL DD statement for each Tivoli Enterprise Monitoring Server where zAware is enabled. For more information, see "Enabling Integrated Cryptographic Service Facility (ICSF) to support zAware" on page 34.

You can specify the ICSF load library in the configuration tool without requiring the KAES256 key. To specify the ICSF load library, uncomment the ICSF parameter, GBL_DSN_CSF_SCSFMOD0 in the WCONFIG($GBL$USR) file.

```
** -----------------------------------------------------------------
** (Conditional) GBL_DSN_CSF_* ICSF system libraries:
** Note: The ICSF load library is required in the RKANMODL DDNAME
**       of the TEMS and Agent started tasks for several TMS-related
**       security encryption functions such as:
**       - if you are enabling the ITM Password Encryption (KAES256
**         key) across the ITM enterprise
**       - if you are enabling the SOAP server for a TEMS
**       - if you are enabling IBM Z OMEGAMON Monitor for z/OS zAware exploitation
** Tip:  It is ideal to customize this library as part of initial RTE
**       deployment prior to enabling any of the product features
**       that will require the ICSF load library. It ensures that the
**       product started tasks are already set-up to avoid recycling
**       the TEMS and/or Agent started tasks.
**       Related PARMGEN CONFIG profile parameters:
**       - RTE_SECURITY_KAES256_KEY
**       - KDS_KMS_SECURITY_COMPATMD (applicable to ITM6.3.0+ only)
**       - KDS_TEMS_SOAP_SERVER_FLAG
**       - KDS_TEMS_HTTP_PORT_NUM
** ---------------------------------------------------------------
*GBL_DSN_CSF_SCSFMOD0         "CSF.SCSFMOD0"
```

After $PARSE* job run, the ICSF load library is concatenated in the RKANMODL DD of the Tivoli Enterprise Monitoring Server started task.

## Completing the configuration - IBM Z OMEGAMON Monitor for z/OS

After you configure IBM Z OMEGAMON Monitor for z/OS using your preferred configuration tool (either PARMGEN or Configuration Manager), you must complete several post-configuration steps. The post-configuration steps that you must complete are a combination of required steps and optional steps that depend on your particular configuration and monitoring objectives.

*Table 5. Post-configuration steps*

| Step | Context |
|---|---|
| "Updating the IEFSSNxx member of SYS1.PARMLIB" on page 21 | Required for agent-specific security configuration |
| "Updating the LINKLIST" on page 21 | Required for agent-specific security configuration |
| "Adding support for the SYSTCPD DDNAME in the started tasks" on page 21 | Required for all configurations |
| "Copying started task procedures to your procedure library" on page 22 | Required for all configurations |
| "Copying the VTAM definitions to your system VTAMLST" on page 22 | Required for all configurations |
| "Varying the VTAM major node active" on page 22 | Required for all configurations |
| "Granting APF authorization for the runtime load libraries" on page 22 | Required for all configurations |
| "Enabling historical data store maintenance" on page 23 | Required to enable historical data collection |

*Table 5. Post-configuration steps (continued)*

| Step | Context |
|---|---|
| "Providing access to the persistent data store files" on page 23 | Required to enable historical data collection |
| "Authorizing the KPDDSCO module" on page 23 | Required to enable historical data collection |
| "Verifying persistent data store configuration" on page 23 | Required to enable historical data collection |
| "Copying CSFPRM00 into SYS1.PARMLIB" on page 24 | Required to collect ICSF data |
| "Adding the KM5EXIT3 and KM5EXIT4 to the ICSF Configuration" on page 24 | Required to collect ICSF data |
| "Modifying the ICSF subsystem JCL" on page 24 | Required to collect ICSF data |
| "Granting authorization to use ICSF Callable Services" on page 25 | Required to collect ICSF data |
| "Authorizing address spaces for UNIX System Services" on page 25 | Required to collect UNIX System Services information |
| "Enabling RMF data collection" on page 25 | Required to use RMF data collection for real-time or near-term history data collection |
| "Defining RACF IDs for IBM Z OMEGAMON Monitor for z/OS and OMEGAMON Subsystem address spaces" on page 26 | Required to use RMF data collection for real-time or near-term history data collection |
| "Enabling the RACF secured signon function (PassTicket)" on page 26 | Required to use RMF data collection for real-time or near-term history data collection |
| "Turning on RMF collection of coupling facility and lock data." on page 27 | Required to use RMF data collection for real-time or near-term history data collection |
| "Configuring a connection to an IBM zAware server" on page 28 | Required to connect to an IBM zAware server to monitor zAware data |
| "Configuring AT-TLS " on page 28 | Required to connect to an IBM zAware server to monitor zAware data |
| "Enabling Integrated Cryptographic Service Facility (ICSF) to support zAware" on page 34 | Required to connect to an IBM zAware server to monitor zAware data |
| "Configuring an ID and password for connection to zAware" on page 34 | Required to connect to an IBM zAware server to monitor zAware data |
| "Configuring historical data collection" on page 35 | Required for historical data collection |
| "Enabling the System Programmer's Toolkit" on page 35 | Required to use the System Programmer's Toolkit |
| "Enabling Warehouse agents on a z/OS hub monitoring server" on page 36 | Required to warehouse historical data in the Tivoli Data Warehouse but the hub monitoring server is not located on the same computer as the Tivoli Enterprise Portal Server |
| "Creating situations to filter DASD device collection" on page 37 | Required to enable monitoring of Sysplex DASD device data |

*Table 5. Post-configuration steps (continued)*

| Step | Context |
|---|---|
| "Setting the PROJECTCPU control in the SYS1.PARMLIB IEAOPTxx member" on page 37 | Required to use IBM Z OMEGAMON Monitor for z/OS to help you plan special processor resources |
| "Installing application and language support" on page 37 | Required for all configurations |
| "Enabling security for Tivoli Enterprise Portal" on page 38 | Required for all configurations |
| "Authorizing users to issue Take Action commands" on page 38 | Required to issue Take Action commands from the Tivoli Enterprise Portal and OMEGAMON Enhanced 3270 user interface user interfaces |
| "Recreating or replacing z/OS Management Console situations" on page 41 | If you previously ran z/OS Management Console situations, you can start corresponding situations for IBM Z OMEGAMON Monitor for z/OS or recreate comparable situations using IBM Z OMEGAMON Monitor for z/OS attributes |
| "Authorizing users to access IBM Z OMEGAMON Monitor for z/OS managed systems on the enhanced 3270 user interface" on page 41 | Required for all configurations |
| "Enabling z/OS Container Extensions (zCX) monitoring" on page 42 | Required for zCX monitoring. |

## Updating the IEFSSN*xx* member of SYS1.PARMLIB

The appropriate IEFSSN*xx* member of SYS1.PARMLIB must be updated to identify the OMEGAMON Subsystem to z/OS.

Member KCNDLSSI (created in the Create runtime members step) in the *&rhilev.&rte*.RKANSAMU data set contains a sample IEFSSN*xx* update. In addition to identifying the OMEGAMON Subsystem to z/OS, this sample causes an automatic start of the subsystem address space.

## Updating the LINKLIST

Load module KCNDLINT must be placed in an APF-authorized, link-listed library so that it is available during system IPL.

Copy the module to an appropriate library in the linklist. Follow your installation standards in making this decision.

**Note:** All runtime libraries concatenated in the STEPLIB DDNAME of the IBMCN started task must be APF-authorized.

## Adding support for the SYSTCPD DDNAME in the started tasks

If the monitoring server is using any of the IP.UDP-related or IP.PIPE-related communication protocols for connection, but the IP domain name resolution is not fully configured on this z/OS system, you must specify the SYSTCPD DDNAME in the IBMDSST started task.

The configuration tool generates the IBMDSST started task with the following commented out lines. Customize the SYSTCPD DDNAME accordingly if this scenario fits your environment:

```
//*SYSTCPD explicitly identifies which dataset to use to obtain
//*the parameters defined by TCPIP.DATA when no GLOBALTCPIPDATA
//*statement is configured. Refer to the IP Configuration Guide
//*for information on the TCPIP.DATA search order. The dataset
//*can be any sequential dataset or a member of a partitioned
```

```
//*dataset. TCPIP.SEZAINST(TCPDATA) is the default sample file.
//*TCPIVP.TCPPARMS(TCPDATA) is another sample and is created as
//*part of the Installation Verification Program for TCP/IP.
//*Note: Uncomment out this DDNAME and point to appropriate
//*      TCPDATA library name supported at your site if domain
//*      name resolution is not fully configured.
//*SYSTCPD DD DISP=SHR,
//*       DSN=TCPIP.SEZAINST(TCPDATA)
```

When you are finished, copy the procedures to PROCLIB.

## Copying started task procedures to your procedure library

During the configuration, a number of started task procedures are created in the *&rhilev.&rte.*RKANSAMU data set. If you have not already done so, you must copy these procedures to your procedure library. You can copy the procedures as part of the configuration process.

See the *Configuring* section of the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Shared documentation* for more information about parameter configuration.

## Copying the VTAM definitions to your system VTAMLST

The configuration process creates VTAM definitions in the RKANSAMU library. You must copy the VTAM major node (default: IBMDSN) to your system VTAMLST. You can copy the procedures as part of the configuration process.

See the *Configuring* section of the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Shared documentation* for more information about parameter configuration.

## Varying the VTAM major node active

The VTAM major node (default: IBMDSN) is created in the RKANSAMU library and copied to your system VTAMLST. It must be VARY'd active.

To vary VTAM major node active, enter:

```
V NET,ACT,ID=nodeid
```

There is code in the IBMM2 procedure that will vary the node (see "Copying started task procedures to your procedure library" on page 22).

## Granting APF authorization for the runtime load libraries

The runtime load libraries created during configuration must be added to the list of APF-authorized libraries

If you have not already done so, add the following runtime load libraries to your list of APF-authorized libraries.

- *&rhilev.&rte*.RKANMOD
- *&rhilev.&rte*.RKANMODU
- *&rhilev.&rte*.RKANMODL

If the runtime environment shares with SMP/E targets, you will also need to add:

- *&thilev*.TKANMOD
- *&thilev*.TKANMODL

**Note:** All runtime libraries concatenated in the STEPLIB DDNAME and in the RKANMODL DDNAME of any started tasks must be APF-authorized.

# Enabling historical data store maintenance

If you intend to enable historical data collection and have allocated and configured maintenance of the historical data set, you must perform three additional tasks to enable the maintenance.

Perform the following tasks:

- "Providing access to the persistent data store files" on page 23.
- "Authorizing the KPDDSCO module" on page 23.
- "Verifying persistent data store configuration" on page 23.

If you are upgrading an existing monitoring server or monitoring agent, you must also refresh the KPDPROC1 maintenance procedure in your system procedure library. See *OMEGAMON XE and Tivoli Management Services on z/OS: Upgrade Guide*.

## Providing access to the persistent data store files

The KPDPROC1 procedure is used to maintain the physical files that constitute the persistent data store. Ensure that KPDPROC1 procedure has the necessary authority to read, write, and update the persistent data store files.

Data store files are archived, exported or recycled according to the maintenance strategy that you specified for persistent data store file groups for the product. The persistent data store subsystem automatically submits maintenance jobs whenever a data store file becomes full. The maintenance procedure must be available in a system procedure library for the procedure to operate. The procedure is generic so it may be used by all runtime environment using this version of the persistent data store.

## Authorizing the KPDDSCO module

The KPDPROCC REXX procedure runs in a TSO environment and must be enabled to run as an authorized program under TSO.

Authorize the KPDDSCO module by adding KPDDSCO to the system PARMLIB(IKJTSOnn) under the AUTHPGM section and refresh the IKJTSO*nn* member by issuing the set command (**`T IKJTSO=nn`**). You might also request that authorized system programmers perform this step so it can be scheduled with the LPAR change control processes.

## Verifying persistent data store configuration

You can perform several steps to verify that the configuration and authorization of the procedures have been successful.

Perform the following steps:

1. Bring up the started task (for monitoring server or monitoring agent) that will collect historical data into the product's persistent data store libraries. In the RKPDLOG DDNAME started task, find any persistent data store libraries in a non-Offline status (for example, Partial or Full status).
2. From a z/OS operator console, issue the following z/OS MODIFY command:

   ```
   /F &stcname,KPDCMD RECOVER FILE=DSN:&pds_dataset
   ```

   (where &*stcname* is the name of the started task performing the persistent data store collection, and &*pds_dataset* is the persistent data store data set).

   For example, issue the following MODIFY command for the monitoring server:

   ```
   /F CIDSST,KPDCMD RECOVER FILE=+
    DSN:&rhilev.&rte.RGENHIS1
   ```
3. Wait 5 minutes.

4. In the RKPDLOG DDNAME started task, find the following `Command:` and `KPDDSTR:` references as shown in the following monitoring server RKPDLOG DDNAME example:

```
Command: RESUME FILE=DSN:&rhilev.&rte.RGENHIS1
KPDDSTR: CONNECT processing started for DataStore file
DSN:&rhilev.&rte.RGENHIS1
KPDDSTR: CONNECT processing ended for DataStore file
DSN:&rhilev.&rte.RGENHIS1
```

5. If these references are not found, view the KPDPROC1 started task in SDSF and look for any obvious errors.

## Copying CSFPRM00 into SYS1.PARMLIB

The file *&rhilev*.*&rte*.RKANSAMU(CSFPRM00) is created with the modifications necessary to successfully run this product.

If the CSFPRM00 file in your SYS1.PARMLIB does not include the necessary EXIT parameters, *EXIT(CSFEXIT3,KM5EXIT3,FAIL(EXIT))* and *EXIT(CSFEXIT4,KM5EXIT4,FAIL(EXIT))*, copy *&rhilev*.*&rte*.RKANSAMU(CSFPRM00) into SYS1.PARMLIB.

## Adding the KM5EXIT3 and KM5EXIT4 to the ICSF Configuration

To set up ICSF data collection, you must make KM5EXIT3 and KM5EXIT4 accessible at subsystem and agent startup. The RKANMOD runtime data set contains KM5EXIT3. You can choose between two methods of adding the exit to the ICSF configuration.

- "Method 1: Add RKANMOD to the ICSF STEPLIB" on page 24
- "Method 2: Copy RKANMOD(KM5EXIT3) to a new data set" on page 24

### Method 1: Add RKANMOD to the ICSF STEPLIB

To use this method, modify the ICSF subsystem JCL to include the *&rhilev.&rte*.RKANMOD data set in the STEPLIB DD concatenation (where *&rhilev* is the high-level qualifier and *&rte* is the runtime environment).

The data set must be APF-authorized. If KM5EXIT3 is then updated by a runtime environment load operation, you must recycle the ICSF subsystem to use the updated exit.

**Advantage of Method 1**: When maintenance is applied to the RKANMOD(KM5EXIT3) load module, you do not have to copy the module to another load library.

**Drawback of Method 1**: All load modules in the RKANMOD data set are exposed to the ICSF address space.

### Method 2: Copy RKANMOD(KM5EXIT3) to a new data set

To use this method, copy RKANMOD(KM5EXIT3) and RKANMOD(KM5EXIT4) into either a new APF-authorized LOADLIB data set or a data set defined to the LINKLIST. If you copy to a LOADLIB data set, you must concatenate the new data set to the STEPLIB of ICSF. If you copy to a LINKLIST data set, you need not adjust the STEPLIB of ICSF.

**Advantage of Method 2**: Only the KM5EXIT3 module is exposed to the ICSF address space.

**Drawback of Method 2**: When maintenance is applied to the RKANMOD(KM5EXIT3) load module, you will have to copy the updated load module to the separate LOADLIB or LINKLIST data set and then recycle the ICSF subsystem to use the updated exit. Additionally, if you have used a LINKLIST data set, you will have to perform a LINKLIST lookaside (LLA) refresh.

## Modifying the ICSF subsystem JCL

To provide sufficient storage to allow the monitoring exit to run, modify the ICSF subsystem JCL to increase the REGION limit to REGION=0M.

## Granting authorization to use ICSF Callable Services

IBM Z OMEGAMON Monitor for z/OS uses the ICSF callable services CSFIQF and CSFIQA to collect data.

The USERID assigned to the IBM Z OMEGAMON Monitor for z/OS TEMS STC (typically xxxxDS) requires access to use these callable services. Consult your Security Administrator to determine if action is required. See the *Cryptographic Services Integrated Cryptographic Service Facility Administrator's Guide*, Chapter 5, "Controlling who can use cryptographic keys and services" for additional information.

## Authorizing address spaces for UNIX System Services

If you intend to use IBM Z OMEGAMON Monitor for z/OS to monitor UNIX System Services data, you must grant superuser authority to the address space in which IBM Z OMEGAMON Monitor for z/OS is defined. This level of authority is equivalent to root authority (UID=0). (Alternatively, privileged or trusted attributes can be associated with the started task, or it may be given read access to BPX.SUPERUSER. See the documentation for your security system for details on how to associate attributes or give read access.)

The user ID of the Tivoli Enterprise Monitoring Server address space is the name shown in the SDSF Display Active screen as the OWNER of the address space, which is often the started task name but does not have to be. An administrator must define this ID to RACF or some other security system.

Users are defined to z/OS UNIX using RACF commands. The z/OS UNIX attributes are kept in the OMVS segment of the RACF user’s profile. This means that to enable IBM Z OMEGAMON Monitor for z/OS to collect UNIX System Services data and issue UNIX commands:

- The user ID of the Tivoli Enterprise Monitoring Server address space must be defined in RACF.
- The profile associated with the RACF user ID must contain an OMVS segment.
- In the OMVS segment, the z/OS UNIX user identifier (UID) must have a value of 0 (superuser).
- The user default group must be an UNIX System Services group.

If you recently migrated to z/OS v2.1, you might find OMVS errors in the system log when you launch the IBM Z OMEGAMON Monitor for z/OS monitoring agent. Be aware that as of z/OS V2R1, the ability to use default OMVS segments has been removed. All z/OS UNIX users or groups must now have OMVS segments defined for user and group profiles with unique user IDs (UIDs) and group IDs (GIDs). For more information about this error and solutions, see the section OMVS and SNAMGMT errors found in system log on z/OS v2.1 systems in the *IBM Z OMEGAMON Monitor for z/OS: Troubleshooting Guide*.

## Enabling RMF data collection

If you have configured IBM Z OMEGAMON Monitor for z/OS to use RMF data collection for real-time or near-term history data collection, you need to perform the steps described in this section.

Ensure that the following RMF components are activated:

- RMF Control Task (RMF)--one instance on each monitored system.
- RMF Monitor III Gatherer (RMFGAT)--one instance on each monitored system.
- RMF Distributed Data Server (GPMSERVE)--one instance per sysplex.

For near-term history data collection, an additional requirement is that at least one instance (two for redundancy and up to one instance on each monitored system) of the OMEGAMON Subsystem must be active per sysplex.

If RMF Collection has been configured, you must ensure that the RMF Distributed Data Server (DDS) is started and RMF Monitor III tasks are started in all LPARs in this sysplex so that the DDS can consolidate data from each LPAR. IBM Z OMEGAMON Monitor for z/OS and, for near-term history, the OMEGAMON subsystem (OB730 or higher) must also be enabled to connect to the DDS. This is done by enabling RACF's PassTicket service.

If IBM Z OMEGAMON Monitor for z/OS is configured to use coupling facility data collected by RMF, RMF Monitor III collection for coupling facility details (CFDETAIL) must be turned on. In RMF, collection is turned on by ensuring the Monitor III parameters in SYS1.PARMLIB(ERBRMF*nn*) have CFDETAIL set. Collection can also be turned on dynamically by issuing the following operator command:

```
ROUTE *ALL,MODIFY RMF,MODIFY III,CFDETAIL
```

See the RMF *z/OS V1R12.0 RMF User's Guide* for more details, in particular the section on Defining Parameters for RMF Monitor III and the section on CFDETAIL.

If IBM Z OMEGAMON Monitor for z/OS is configured to use lock data collected by RMF, RMF Monitor III collection for LOCK must be turned on. LOCK can be set as the default in SYS1.PARMLIB(ERBRMF*nn*) or by using the dynamic command:

```
/MODIFY RMF,MODIFY III,LOCK
```

**Note:** It is suggested that SYS1.PARMLIB(GPMSRV00) specify CACHESLOTS(10) and that SYS1.PARMLIB(ERBRMF*nn*) specify DATASET(WHOLD(50)) for RMF III fixed pages (in MB) and WSTOR(128) for RMF III size in storage buffer (in MB)

The following topics describe the additional steps you must take to enable use of RMF data:

- "Defining RACF IDs for IBM Z OMEGAMON Monitor for z/OS and OMEGAMON Subsystem address spaces" on page 26.
- "Enabling the RACF secured signon function (PassTicket)" on page 26.
- "Turning on RMF collection of coupling facility and lock data." on page 27.

## Defining RACF IDs for IBM Z OMEGAMON Monitor for z/OS and OMEGAMON Subsystem address spaces

Activation of the RMF DDS API requires a RACF user ID and password. An administrator must define the IDs of these address spaces to RACF.

For the user ID, IBM Z OMEGAMON Monitor for z/OS and OMEGAMON Subsystem use the name shown in the SDSF Display Active screen as the OWNER of the address space. This is often the started task name, but it does not have to be. You will probably also want those IDs added to a group to simplify PassTicket authorization.

## Enabling the RACF secured signon function (PassTicket)

Enabling the secured signon function requires a series of coordinated RACF commands.

To enable the function, a RACF administrator must complete the following steps:

1. Activate the PTKTDATA class (if not already activated). For example:

   ```
   SETROPTS CLASSACT(PTKTDATA)
   SETROPTS RACLIST(PTKTDATA)
   ```

   The PassTicket key class enables the security administrator to associate a RACF secured signon secret key with a particular mainframe application that uses RACF for user authentication. All profiles that contain PassTicket information are defined to the PTKTDATA class.
2. Define a profile in the PTKTDATA class for the Distributed Data Server (GPMSERVE).

   The name of the profile must be the name of the DDS application. For example,

   ```
   RDEF PTKTDATA GPMSERVE SSIGNON([KEYENCRYPTED|KEYMASKED](key))
   ```

   The profile associates a secret secured signon application key with a particular application on a particular system. The key is a 16-digit hexadecimal user-supplied value.

   **Note:** The default application name for PassTicket generation is GPMSERVE. If the RACF user exit ICHRIX01 redefines this name, the OMEGMON XE client must use the ID provided by the user exit. If you need to use an alternative name, contact IBM Software Support.

3. Create a RACF profile for PassTicket generation.

   This determines who can create PassTickets for GPMSERVE.

   ```
   RDEF PTKTDATA IRRPTAUTH.GPMSERVE.* UACC(NONE)
   ```

4. Authorize monitoring server and OMEGAMON Subsystem address spaces to use PassTicket services

   Use of R_ticketserv service to use PassTicket services (function code 3) is authorized by the resources in the PTKTDATA class that correspond to the application ID and target userid used in the PassTicket operation. The application server must be running with a RACF user or group that has the following authority specified:

   ```
   PERMIT IRRPTAUTH.GPMSERVE.* ID(STCUSER) ACCESS(UPDATE)  CLASS(PTKTDATA)
   ```

   where *STCUSER* is the group ID used for the monitoring server and OMEGAMON Subsystem address spaces.

   ```
    SETR RACLIST(PTKTDATA) REFRESH
   ```

   **Note:** If PassTicket authentication is used, the user ID for the monitoring server and OMEGAMON Subsystem address space cannot be defined as PROTECTED. Using PassTicket authentication is the equivalent to using a password, and a PROTECTED RACF user ID can not have a password specified in its definition.

   **Note:** KEYENCRYPTED requires that the CSNBENC module reside in the link pack area (LPA) if not already there. The CSNBENC module can be dynamically loaded, or added to PLPA or MLPA with the respective PARMLIB members. The following modules must reside in APF-authorized link-listed data sets: CSNBCKI, CSNBKRC, CSNBKRD, CSNBKRW.

### Tip

Depending on your RACF options, the user ID of the person who enters the **RDEF** command might also be on the access list for **IRRPTAUTH.GPMSERVE.***. You can check to see whether the ID is included by issuing the following command and then checking the access list:

```
RLIST PTKTDATA IRRPTAUTH.GPMSERVE.*
```

To delete an unwanted user ID, issue the following command:

```
PERMIT IRRPTAUTH.GPMSERVE.* id(userid) DELETE class(PTKTDATA)
```

**Note:** You can choose to bypass user ID and password authentication for all or selected users through initialization parameters. See the RMF documentation for a discussion of HTTP_NOAUTH.

## Turning on RMF collection of coupling facility and lock data.

If IBM Z OMEGAMON Monitor for z/OS has been configured to use RMF coupling facility data (RMF `Collection = CF/XCF`), you must ensure that collection of coupling facility details is turned on in every RMF Monitor III in the Sysplex. If IBM Z OMEGAMON Monitor for z/OS has been configured to use RMF lock data (RMF `Collection = LOCK`), ensure that collection of LOCK data is turned on in every RMF Monitor III in the Sysplex.

In RMF, collection of coupling facility details is enabled by setting CFDETAIL in the Monitor III parameters in SYS1.PARMLIB(ERBRMF*nn*). Collection can also be enabled dynamically by issuing the following operator command:

```
ROUTE *ALL,MODIFY RMF,MODIFY III,CFDETAIL
```

See the section on Defining Parameters for RMF Monitor III and the section on CFDETAIL in the RMF User's Guide for details.

You can enable collection of lock data by setting LOCK as the default in SYS1.PARMLIB(ERBRMF*nn*) or use the dynamic command

```
/MODIFY RMF,MODIFY III,LOCK
```

to turn on collection.

If IBM Z OMEGAMON Monitor for z/OS has been configured to use RMF data for both coupling facility and lock data (`RMF Collection = ALL`), both CFDETAIL and LOCK must be set.

# Configuring a connection to an IBM zAware server

You can configure IBM Z OMEGAMON Monitor for z/OS to connect to an IBM zAware server to monitor zAware data.

1. “Configuring AT-TLS ” on page 28
2. “Enabling Integrated Cryptographic Service Facility (ICSF) to support zAware” on page 34
3. “Configuring an ID and password for connection to zAware” on page 34

## Configuring AT-TLS

You must configure every LPAR that drives the zAware agent as enabled for AT-TLS encryption.

### About this task

Every LPAR that drives the zAware agent must be configured as enabled for *Application Transparent Transport Layer Security (AT-TLS)* encryption.

### Procedure

**RACF Settings**

1. Obtain the certificate that is provided by zAware to be used in the RACF settings.

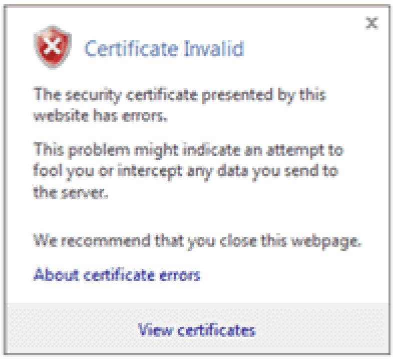
   To complete, this step requires that zAware is installed and operational and available from a browser session. The steps to obtain the certificate are dependent on the browser version used.

   The following example is for the Microsoft Internet Explorer browser:

   a. Start the logon process to zAware (https://zaware.url/zAware/). Use the appropriate URL address for your local zAware server. The IBM zAware login screen opens.

      **Note:** If you are running Windows 7, you must run Internet Explorer as ADMINISTRATOR so that you can save the certificate to a local file.

   b. Select **View** > **Security Report**. You might see a message such as this:



Certificate Invalid

The security certificate presented by this website has errors.

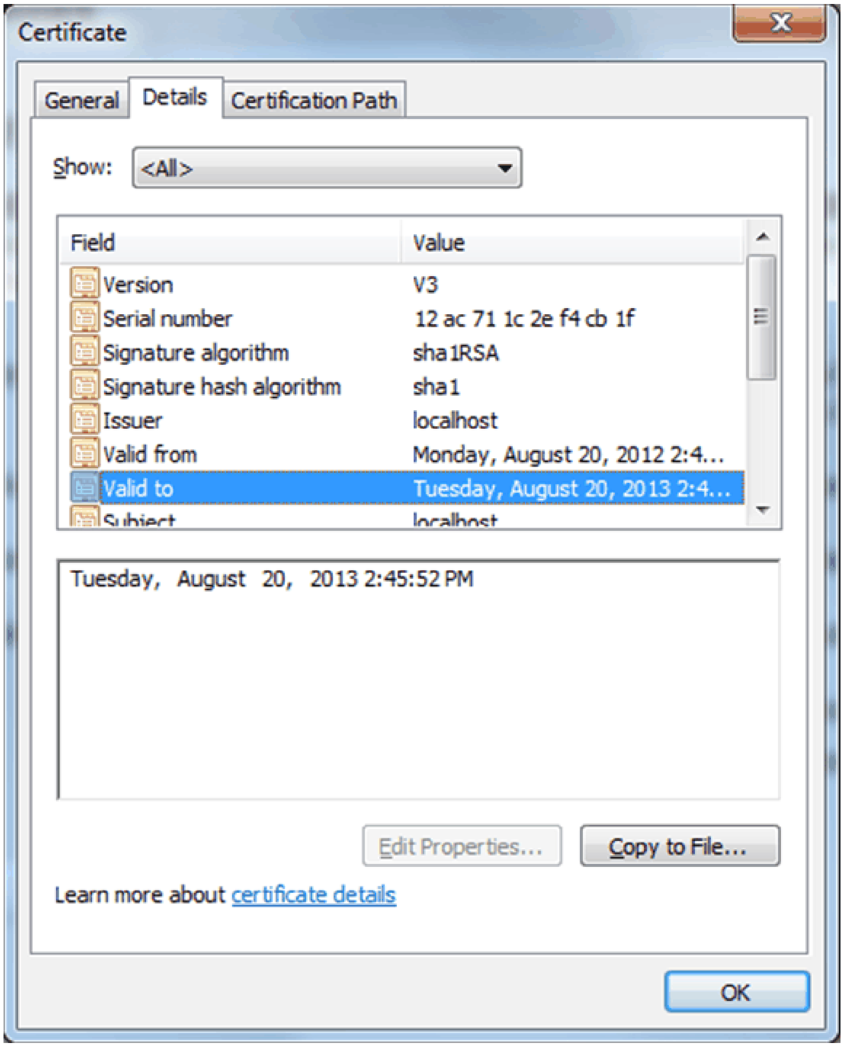
This problem might indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

*Figure 3. Certificate Invalid message.*

   c. Click **View certificates**. The **Certificate** window opens.

   d. Select the **Details** tab.



| Field | Value |
|---|---|
| Version | V3 |
| Serial number | 12 ac 71 1c 2e f4 cb 1f |
| Signature algorithm | sha1RSA |
| Signature hash algorithm | sha1 |
| Issuer | localhost |
| Valid from | Monday, August 20, 2012 2:4... |
| Valid to | Tuesday, August 20, 2013 2:4... |
| Subject | localhost |

Tuesday, August 20, 2013 2:45:52 PM

*Figure 4. Certificate Window.*

e. Note the **Valid to** date value that is shown. You might have to update your zAware certificate before this date to avoid service interruption.

f. Click **Copy To File** and follow the wizard prompts to save the certificate locally.

**Tip:** Use base-64 encoding.

g. Upload this certificate, as text, to your z/OS LPAR where you configure the RACF and save it in a sequential file with these characteristics:

```
Organization  . . . : PS
 Record format . . . : VB
 Record length . . . : 80
 Block size  . . . . : 27920
 1st extent tracks . : 1
 Secondary tracks  . : 0
 Data set name type  :
 SMS Compressible. . : NO
```

For this example the file is named `ZAWARE.CERTX509.D130820`. The last part of the file name reminds you that the certificate expires on `2013/08/20`.

h. RACF commands for AT-TLS:

The following RACF commands create a certificate specifically for the userid that the Tivoli Enterprise Monitoring Server (TEMS) runs under. A site certificate could also be used instead.

- **`SETROPTS CLASSACT(FACILITY)`**
- **`SETROPTS CLASSACT(SERVAUTH)`**

- **RDEF FACILITY IRR.DIGTCERT.LISTRING UACC(NONE)**
- **PE IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(***TEMS_userid***) ACC(READ)**

  The value for *TEMS_userid* is the user ID that your Tivoli Enterprise Monitoring Server started tasks runs under. It can be found by looking at your Tivoli Enterprise Monitoring Server started task, `JESMSGLG message ID IEF695I` as shown in the following example:

  ```
  IEF695I START jobname WITH JOBNAME jobname IS ASSIGNED TO USER TEMS_userid, GROUP
  grpname
  ```

- **SETROPTS RACLIST(FACILITY) REFRESH**
- **RDEF SERVAUTH EZB.INITSTACK.system_name.TCPIP UACC(NONE)**
- **PE EZB.INITSTACK.system_name.TCPIP CLASS(SERVAUTH) ID(OMVSKERN) ACC(READ)**
- **SETROPTS RACLIST(SERVAUTH) REFRESH**
- **RACDCERT ADDRING(***keyring***) ID(***TEMS_userid***)**

  The value that you use for *keyring* is carried forward to your Communications Manager settings as seen in the example `ttls.policy` file under the AT-TLS configuration, in step "3" on page 32.

- **RACDCERT ADD('ZAWARE.CERTX509.D130820') TRUST WITHLABEL('***trustlbl***') ID(***TEMS_userid***)**

  This command defines the certificate that is contained in the data set `ZAWARE.CERTX509.D130820` to RACF. This certificate expires periodically. Replacing this file with the new certificate allows communications to flow again.

- **RACDCERT CONNECT(ID(***TEMS_userid***) LABEL('***trustlbl***') RING(***keyring***) DEFAULT USAGE(PERSONAL)) ID(***TEMS_userid***)**

  This command grants permission to use the certificate to your Tivoli Enterprise Monitoring Server started task.

- **SETROPTS RACLIST(DIGTCERT,DIGTRING) REFRESH**

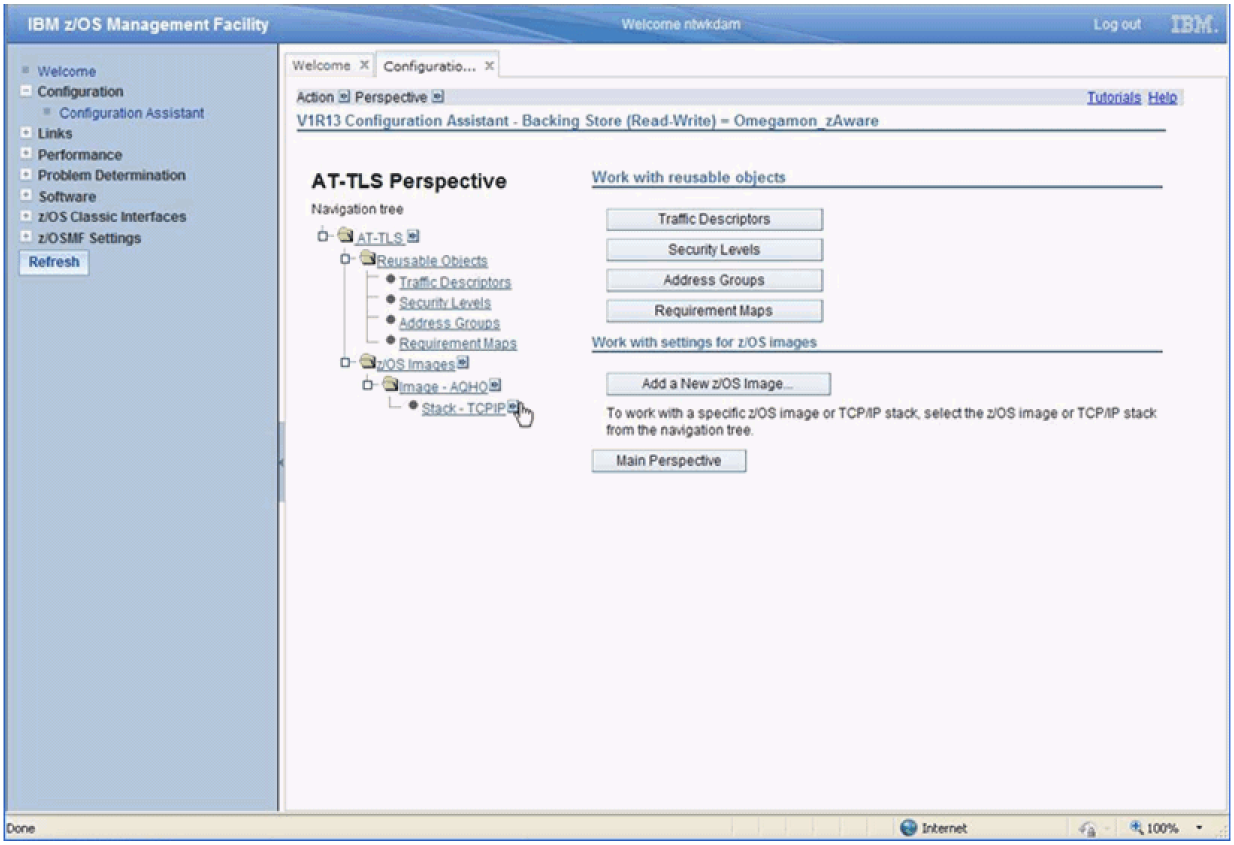
  This command activates the **ADDRING** change, assuming the `DIGTRING CLASS` is present in the `RACLIST` list in your environment.

### AT-TLS configuration

Policy configuration settings for AT-TLS must be entered by an authorized system programmer.

2. Optional: If you have the IBM z/OS Management Facility (z/OSMF), you can use it to specify your AT-TLS policy.
   Use z/OSMF to define your policy and the result is similar to the example definitions described in step "3" on page 32.

   The following is an example z/OSMF screen capture for the Configuration Assistant:



V1R13 Configuration Assistant - Backing Store (Read-Write) = Omegamon_zAware

To work with a specific z/OS image or TCP/IP stack, select the z/OS image or TCP/IP stack from the navigation tree.

*Figure 5. IBM z/OS Management Facility.*

Follow these steps when you use z/OSMF:

- Specify the zOS Image that has the AT-TLS policy
  - Specify the TCP/IP stack name that uses the AT-TLS policy
- Under **AT-TLS Perspective** specify the following settings:

**Reusable Objects**

**Traffic Descriptors**

Select Action **ADD**

Give this descriptor a name and description.

Under **List of traffic types in this traffic descriptor**, select Action **ADD**

**Details Tab**

Specify all local and remote ports. Indicate the **TCP connect direction** is **Outbound only**, and **TLS handshake role** is **Client**.

**Key Ring Tab**

Use simple name to specify the key ring that is created in the RACF settings.

**Advanced Tab**

Specify **Application Controlled** as **On**.

**Requirement Maps**

Select Action **ADD**

Give this requirement map a name and description.

**Traffic Descriptor**

Select the traffic descriptor name that you created earlier in this procedure.

**Security Level**

The suggested setting is **Default_Ciphers**.

**z/OS Images**

**Stack Connectivity Rules**

Select Action **ADD**

Click **Next**

Give this connectivity rule a name.

**Local data endpoint**

Select **Address group** as **All_IP_Addresses** or **IPv4 address** or **IPv6 address** or **subnet range**.

**Remote data endpoint**

Select **IPv4 address** or **IPv6 address** and specify the IP address for your zAware appliance.

**Requirements Map**

Use **Select an existing requirements map** and name the map that you created.

Click **Select** next to **Traffic Descriptor** and **Security Level**

Click **Next** tab

Click **Finish** tab

**Install Configure Files**

Select the row that you created, click **Show Configuration File**.

The resulting file is similar to the example `ttls.policy` file in step "3" on page 32 with the addition of a `TTLSCipherParms` segment.

3. Configure the policy definitions.

As an example, assume that the TCPIP started task is named `TCPIP`. `TCPIP` has a `PROFILES DD` statement that points to the stack 's settings. The Communications Server provides for invocation of System SSL in the TCP transport layer of the stack. *Application Transparent Transport Layer Security* (AT-TLS) support is controlled by the TTLS or `NOTTLS` parameter on the `TCPCONFIG` statement in the TCP/IP profile. Ensure TTLS is specified.

The Policy Agent address space is likely called `PAGENT`. If this address space is not already running, copy `EZA.SEZAINST(PAGENT)` to a `PROCLIB` library and set it for automatic start at each IPL. Do this step by adding the following statement:

```
PAGENT to SYS1.PARMLIB(COMMNDxx)
COM='S PAGENT                                PAGENT'
```

The JCL for PAGENT has a single step that runs program PAGENT, `(//PAGENT EXEC PGM=PAGENT)`. It has a DD statement like:

```
//STDENV   DD PATH=
```

This statement defines where the policy statements begin. If this statement is not already set, then set it as follows:

```
//STDENV DD PATH='/systemdir/etc/pagent/pagent.env',PATHOPTS=(ORDONLY)
```

*systemdir* is the directory for the LPAR being configured. In this example, it is named SYSA. Ensure that the file contains `PAGENT_CONFIG_FILE=//'sys1.tcpparms(PAGENT)'`. You can choose whatever file name is appropriate for your installation 's naming conventions. In this example, it is named `SYS1.TCPPARMS`. Edit the file `SYS1.TCPPARMS (PAGENT)` and find or enter the statement:

```
TcpImage TCPIP  /SYSA/etc/pagent/TCPIP.policy FLUSH PURGE
```

The TcpImage statement identifies the z/OS UNIX file or MVS data set that contains policy for that stack. In /SYSA/etc/pagent/TCPIP.policy you either see or insert the statement:

```
TTLSConfig /SYSA/etc/pagent/ttls.policy
```

The TTLSConfig statement identifies the z/OS UNIX file or MVS data set that contains the local AT-TLS policy. The TTLSConfig statement is required for each stack that receives AT-TLS policy. In this example, the UNIX System Services directory is /SYSA/etc/pagent/ttls.policy.

Example entries for the file ttls.policy:

```
TTLSGroupAction    KDEBEGRPACT
{
  TTLSEnabled  On
  TRACE 15
}

TTLSEnvironmentAdvancedParms      KDEBEADV
{
 ApplicationControlled  On
 ClientAuthType         PassThru
}

TTLSEnvironmentAction    ZAWAREENV
{
   TTLSKeyringParms
   {
      Keyring   keyring        <== same Keyring name used with RACF
   }
   HandShakeRole   Client
   TTLSEnvironmentAdvancedParmsRef    KDEBEADV
}

TTLSConnectionAction          KDEBECONNOUT
{
  HandShakeRole   Client
}

TTLSRule                    ZAWARE
{
  RemoteAddr   n.nn.nn.nnn                    <== the IP address used on your z/OS LPAR
                                                  to communicate with the zAware server
  Direction    Outbound
  TTLSGroupActionRef         KDEBEGRPACT
  TTLSEnvironmentActionRef   ZAWAREENV
  TTLSConnectionActionRef    KDEBECONNOUT
}
```

4. Refresh the Policy Agent to incorporate any changes by using operator commands.

   a) Optional: Bring your TCPIP stack down and back up.

   Do this step only the first time you enable TCPIP to use AT-TLS or if you previously did not have a policy agent setup.

   For example, use the following commands:

   **P TCPIP**

   **S TCPIP**

   **Tip:** If you normally start other tasks when you start TCPIP, you might want to stop those tasks also when you stop TCPIP and then start them again when you start TCPIP.

   b) Refresh the Policy Agent.

   If the Policy Agent is running, use the command **F PAGENT,REFRESH**

   If PAGENT is not running, then start it.

   Messages similar to the following are displayed:

```
EZZ4250I AT-TLS SERVICES ARE AVAILABLE FOR TCPIP
EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPIP : TTLS
EZD1586I PAGENT HAS INSTALLED ALL LOCAL POLICIES FOR TCPIP
```

## Enabling Integrated Cryptographic Service Facility (ICSF) to support zAware

ICSF must be enabled to support zAware user ID and password encryption.

If you are not familiar with the use of ICSF for cryptographic services, consult the *z/OS Cryptographic Services ICSF Administrator's Guide*.

The following ICSF requirements must be met before you configure an ID and password for connection to zAware:

1. ICSF must be active on any LPAR where IBM Z OMEGAMON Monitor for z/OS agents request zAware information.

   **Note:** Crypto Express cards or other cryptographic hardware is not required.
2. The ICSF data set must be concatenated in the RKANMODL DD statement for each Tivoli Enterprise Monitoring Server where zAware is enabled. The default ICSF library name is `CSF.SCSFMOD0`. The library must be APF-authorized.
   - If you have the PTF for PARMGEN APAR OA41710 installed, then you must specify the ICSF library name, `"CSF.SCSFMOD0"` in the PARMGEN global parameter, `GBL_DSN_CSF_SCSFMOD0` as part of your IBM Z OMEGAMON Monitor for z/OS configuration by using PARMGEN to generate your runtime environment. For PARMGEN configuration details, see "Specifying the ICSF load library for zAware" on page 19
   - If you do not have the PTF for APAR OA41710 installed, then you must uncomment the ICSF load library in the RKANMODL DD statement of the monitoring server.

## Configuring an ID and password for connection to zAware

A valid zAware user ID and password must be specified for each zAware appliance and each name that is used to access these appliances so that the IBM Z OMEGAMON Monitor for z/OS agent can authenticate with the zAware server.

### Before you begin

1. The Integrated Cryptographic Service Facility (ICSF) must be active on the LPARs where IBM Z OMEGAMON Monitor for z/OS agents request zAware information.
2. The ICSF data set must be added to the RKANMODL DD statement for each Tivoli Enterprise Monitoring Server where zAware is enabled.

For more information, see "Enabling Integrated Cryptographic Service Facility (ICSF) to support zAware" on page 34.

### About this task

An administrator must enter the zAware user ID and password information by using a window on the OMEGAMON enhanced 3270 user interface. If multiple zAware appliances are used by LPARs monitored from a specific hub monitoring server, then each zAware appliance must be given a user ID and password appropriate to that appliance. Though unlikely, it is possible that a single zAware appliance might be known to different LPARs by different Domain names or IP addresses. When different names are used the credentials must be set for each unique name used. For example, zAware1 might be known as `YOUR.ZAWARE.APPLIANCE.COM` on some set of LPARs while other LPARs might know zAware1 by its IP address like `9.0.0.170`. You must set user ID and password credentials for both these names.

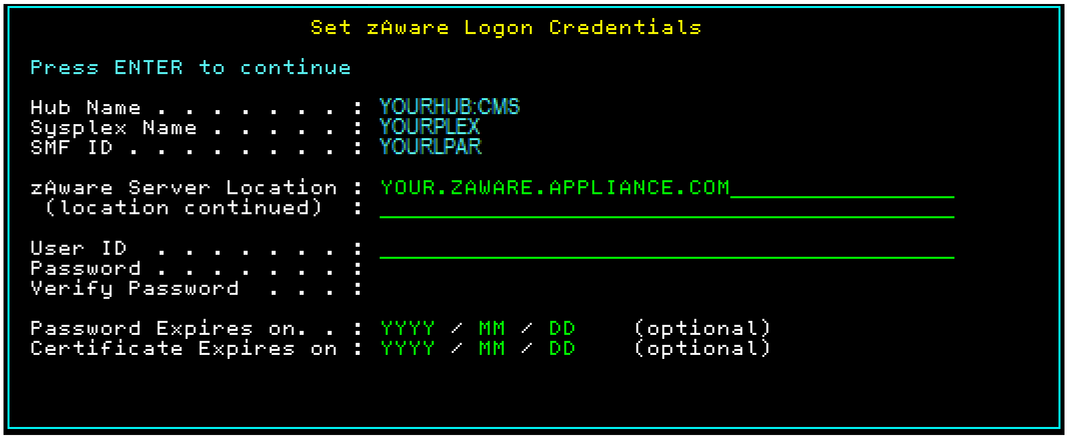
### Procedure

1. On the OMEGAMON enhanced 3270 user interface, from the **LPAR Overview for Sysplex** *plexname* workspace, select an LPAR entry and use menu option **D** to go to the **zAware Analysis** workspace.

   Note the value that is specified in the **zAware Location** column of the first sub panel. This value is the name that is used to store the user ID and password you are about to enter. Credentials must be set for every unique value that is seen in this field.

2. Place your cursor on the input field in the **zAware Client Status** field and press enter to see the **Set zAware Logon Credentials** window.

   It is populated with the **zAware Server Location** value as shown in the following example:



```
                    Set zAware Logon Credentials

 Press ENTER to continue

 Hub Name . . . . . . . . : YOURHUB:CMS
 Sysplex Name . . . . . . : YOURPLEX
 SMF ID . . . . . . . . . : YOURLPAR

 zAware Server Location : YOUR.ZAWARE.APPLIANCE.COM________________
  (location continued)  : __________________________________________

 User ID  . . . . . . . : __________________________________________
 Password . . . . . . . :
 Verify Password  . . . :

 Password Expires on. . : YYYY / MM / DD     (optional)
 Certificate Expires on : YYYY / MM / DD     (optional)
```

*Figure 6.* ***Set zAware Logon Credentials***

3. Enter the zAware **User ID**, and **Password**.

   You must enter the password a second time for verification.

4. Optional: Enter the date that the zAware certificate and password expire.

5. Navigate to the **zAware Analysis** workspace from every row in the **LPAR Overview for Sysplex** *plexname* workspace. Repeat steps “2” on page 35 to “4” on page 35 for each unique **zAware Location** value seen.

   You must repeat this procedure whenever the password expires.

## Configuring historical data collection

Tivoli Management Services provides for two kinds of history data: short-term history data, which is stored in the persistent data store (on z/OS systems) or in files (on distributed systems), and long-term history data, which is stored in the Tivoli Data Warehouse. Both short-term and long-term history are optional features that can be enabled from the Tivoli Enterprise Portal.

The Tivoli Enterprise Portal History Collection dialog box displays all of the IBM Z OMEGAMON Monitor for z/OS attribute tables that are enabled for historical collection and reporting. To enable historical data collection for these attribute groups, you must select and configure each group (attribute table) for which you want to collect data, and then start collection of those groups. If you want to warehouse the data for long-term historical reporting, you must set the Warehouse Interval to the interval at which data is warehoused.

For detailed instructions on configuring history data collection, refer to *IBM Tivoli Monitoring: Administrator's Guide*, *IBM Z OMEGAMON Monitor for z/OS: User's Guide*, and the Tivoli Enterprise Portal online Help.

## Enabling the System Programmer's Toolkit

A System Programmer's Toolkit is provided with IBM Z OMEGAMON Monitor for z/OS V5.6, fix pack 15, PTF UJXXXX. This toolkit allows you to view the Operator Log, use the z/OS console commands, and use the SDSF commands from the e3270UI.

The System Programmer's Toolkit uses System REXX functionality. In order to use it, you must make the delivered Toolkit REXX execs from RKANEXEC available to your installation REXXLIB library.

For the delivered REXX EXECs to be accessible to System REXX, the RKANEXEC library must be added to your System REXX REXXLIB concatenation:

1. Determine what System REXX libraries are available.

Use the console command `F AXR,SR,REXXLIB` to display the configured REXXLIB libraries on your system.

The following is a sample output of the command:

```
RESPONSE=RSB6

 AXR0202I SYSREXX REXXLIB DISPLAY 844

 ENTRY VOLUME  DATA SET

   1   S1LK00  RSMIS.SAXREXEC

   2   R3P102  RSRTE.SAXREXEC

   3   S1LK02  ROCKET.USER.SAXREXEC

   4   RZ205D  SYS1.SAXREXEC
```

2. ADD a new REXXLIB concatenation to point to your RKANEXEC data set. The AXR*nn* members must be updated to include your RKANEXEC dsname:

   **Tip:** There is a SYS1.SAMPLIB member (AXR00) that can be tailored and copied into SYS1.PARMLIB to override IBM® supplied defaults. Additionally, IEASYS*nn* supports a parmlib concatenation of AXR*nn* members. The AXR*nn* members need to be updated to include your RKANEXEC dsname:

   `REXXLIB ADD DSN(&`*`rhilev`*`.&`*`rte`*`.RKANEXEC)`

3. Stop and start AXR (System REXX Address Spaces).

   The Sstem REXX address space, AXR, is non-cancelable. The operator can terminate the AXR address space by issuing the following command:

   `P AXR`

   The operator can restart AXR by using the AXRPSTRT procedure, found in SYS1.PROCLIB. The syntax for restarting AXR can be one of the following:

   - `START AXRPSTRT`
   - `START AXRPSTRT,AXR=`*`aa`*
   - `START AXRPSTRT,AXR=(`*`aa`*`,`*`bb`*`)`

   where *aa* and *bb* are AXR*nn* parmlib members in SYS1.PARMLIB. If no parmlib members are specified, values from AXR00 are applied if it exists; otherwise, default values are assigned.

   Detailed information can be found in Planning to use System REXX.

**Note:** If the required REXXLIB library was not set up properly, the following messages are displayed when the System Programmer's Toolkit is first opened:

```
KM5SRASM AXRESS Failed RC=0008 RSN=0851
IRX0406E REXX exec load file REXXLIB does not contain exec member KM5RLOG
IRX0110I The REXX exec cannot be interpreted.
IRX0112I The REXX exec cannot be loaded.
```

## Enabling Warehouse agents on a z/OS hub monitoring server

If you want to store long-term history data and your hub monitoring server is on z/OS, you must transfer the catalog and attribute files for the Warehouse Proxy agent and the Summarization and Pruning agent to the hub using Manage Tivoli Monitoring Services.

The catalog and attribute data files are installed on the Tivoli Enterprise Portal Server when you install application support for IBM Z OMEGAMON Monitor for z/OS, using the *IBM Tivoli OMEGAMON Data Files for z/OS* CD. You can then FTP the files to the hub monitoring server.

If the portal server is installed on a Windows system, you can FTP the files to a z/OS hub using Manage Tivoli Monitoring Services:

1. On the host of the Tivoli Enterprise Portal Server, open the Manage Tivoli Monitoring Services application. For example:

   ```
   Start > IBM Tivoli Monitoring > Manage Tivoli Monitoring Services.
   ```

2. Right-click the name of the portal server and select **Advanced > Utilities > FTP Catalog and Attribute files**.

   The Select attribute and catalog data for transfer window dialog box is displayed.

3. Select the catalog and attribute data for the Warehouse Proxy and the Summarization and Pruning agents, then press **OK**.

   The FTP TEMS Data to z/OS dialog box is displayed.

4. Provide the following information:

   - The name of the hub Tivoli Enterprise Monitoring Server
   - A valid FTP user ID and password
   - The name of the domain name server of the monitoring server where the RKANDATV data set is located

   When you have completed these fields, click **OK**. Click **OK** again in the confirmation window.

5. After the FTP operation is complete, you receive a message that the operation completed successfully. Click **OK** to end this operation.

After you complete these steps, restart the hub monitoring server.

## Creating situations to filter DASD device collection

Because of the large DASD volume counts that have become common in recent years, monitoring DASD devices without a filter that eliminates some of the devices can lead to high CPU or storage problems and may even cause the monitoring server to fail. Due to these potential costs, IBM Z OMEGAMON Monitor for z/OS does not collect DASD device data unless a DASD filter situation is active. An auto-started warning situation (KM5_No_Sysplex_DASD_Filter_Warn) notifies you if no filtering situation is in place and no devices are being monitored.

See the *IBM Z OMEGAMON Monitor for z/OS: User's Guide* for instructions on creating a DASD device collection filtering situation.

## Setting the PROJECTCPU control in the SYS1.PARMLIB IEAOPT*xx* member

If you are not currently running System z Application Assist Processors (zAAPs) or System z Integrated Information Processors (zIIPs), but you want to use IBM Z OMEGAMON Monitor for z/OS to determine how much work can be offloaded to special processors, set the **PROJECTCPU** control in the SYS1.PARMLIB IEAOPT*xx* member to YES.

## Installing application and language support

Before data collected by IBM Z OMEGAMON Monitor for z/OS monitoring agents can be displayed in the Tivoli Enterprise Portal, support for the agents must be installed and enabled. If the self describing agent feature has been enabled, this support is installed automatically with the agent. However, if self description has been disabled, the support must be installed manually.

Application support files provide agent-specific information for workspaces, helps, situations, templates, and other data. Application support for a monitoring agent includes two types of files:

- SQL files are required for adding product-provided situations, templates, and policies to the Enterprise Information Base (EIB) tables maintained by the hub monitoring server. These SQL files are also called seed data, and installing them on a monitoring server is also called seeding the monitoring server.
- Catalog and attribute (CAT and ATR) files are required for presenting workspaces, online help, and expert advice for the agent in Tivoli Enterprise Portal.

Application support must be configured on all instances of the following infrastructure components: Tivoli Enterprise Monitoring Server (both hub and remote monitoring servers), Tivoli Enterprise Portal Server, and Tivoli Enterprise Portal desktop client, if the desktop client was installed from the installation media rather than invoked using Java Web Start. Application support for the monitoring agent is installed on the remote monitoring servers when agents are registered with the local monitoring server.

The files required for support are contained in *IBM Tivoli OMEGAMON Data Files for z/OS* DVD included in the product package. You install support on the Tivoli Enterprise Portal Server and any desktop clients on the computer on which they are installed. If your hub is on Windows or a UNIX operating system (Linux®, AIX®, Solaris), you install support on the monitoring server locally (that is, on the computer on which it is installed). If your hub is on z/OS, you install support from a Windows computer that hosts either a Tivoli Enterprise Portal Server or a Tivoli Enterprise Monitoring Server. The hub monitoring server must be running while you are installing support.

Use the procedures documented in the *IBM Tivoli Monitoring: Installation and Setup Guide* to add support to Tivoli Enterprise Portal or a hub monitoring server on Windows, AIX, or Linux. Use the instructions in *IBM Tivoli Management Services on z/OS: Configuring the Tivoli Enterprise Monitoring Server on z/OS* to add support to a z/OS hub.

If you want application data, online help, and expert advice to be displayed in a language other than English, you must also install language support.

You install language support from the *IBM Z OMEGAMON Monitor for z/OS Language Pack* CD on the same system where you install application support. Install the language packs on any system where you have installed the Tivoli Enterprise Portal or where you have installed a desktop client. (If you download and run a desktop client using Web Start, you do not need to install the language packs on the local system. They are downloaded from the portal server.) *Before you can install a language pack, you must install the component in English*.

## Enabling security for Tivoli Enterprise Portal

After you have established that IBM Z OMEGAMON Monitor for z/OS is configured correctly, you can safely enable security.

To enable security for the Tivoli Enterprise Portal through either the hub monitoring server or the Tivoli Enterprise Portal Server, review the planning information in the *Planning* section of the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Shared documentation*and refer to the appropriate guide for instructions.

To enable security for IBM Z OMEGAMON Monitor for z/OS Take Action commands, see "Authorizing users to issue Prefixed Take Action commands" on page 39.

## Authorizing users to issue Take Action commands

Certain commands, known as Take Action commands, can be issued from the Tivoli Enterprise Portal and OMEGAMON Enhanced 3270 user interface user interfaces. IBM Z OMEGAMON Monitor for z/OS supports three types of Take Action commands: z/OS system commands, UNIX commands, and agent-provided commands. Users must be authorized to issue these commands.

- "Authorizing users to issue z/OS commands" on page 38
- "Authorizing users to issue UNIX commands" on page 39
- "Authorizing users to issue Prefixed Take Action commands" on page 39

### Authorizing users to issue z/OS commands

By default, Take Action commands issued by IBM Z OMEGAMON Monitor for z/OS through the Tivoli Enterprise Portal are issued as z/OS system commands.

System commands issued using Take Action commands, whether issued by a user or triggered by situations or policies, run without any authorization or audit trail. However, a monitoring server or monitoring agent address space can be configured to redirect 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.

For more information, see "Configuring NetView authorization of z/OS commands" in *IBM Tivoli Monitoring: Configuring the Tivoli Enterprise Monitoring Server on z/OS*.

## Authorizing users to issue UNIX commands

Take Action commands issued on the Tivoli Enterprise Portal with any of the following prefixes are issued as UNIX commands:

- **`OMVS:, Omvs:, or omvs:`**
- **`UNIX:, Unix:, or unix:`**

By default, only user IDs that have been defined to z/OS UNIX System Services and have superuser, or root, authority are allowed to issue UNIX commands through the Tivoli Enterprise Portal. User IDs are defined to z/OS UNIX using RACF commands and the z/OS UNIX attributes are kept in the OMVS segment of the RACF user's profile.

To enable users with Tivoli Enterprise Portal user IDs to issue UNIX commands:

- The user's Tivoli Enterprise Portal user ID must be defined in RACF.
- The profile associated with the RACF user ID must contain an OMVS segment.
- In the OMVS segment, the z/OS UNIX user identifier (UID) must have a value of 0 (superuser).

You can override the default validation behavior by adding one of two parameters to the KDS$PENV override member of *&rhilev.&rte.*RKANPARU on the system or LPAR on which the command is being executed.

- You can allow any RACF user ID defined to z/OS UNIX System Services to issue UNIX commands, regardless of level of authorization, by adding the variable KOE_ALLOW_ANY_UID=1 to *&rhilev.&rte*.RKANPARU(KDSENV) on the LPAR where the command is to be executed.
- You can allow any RACF user ID to issue UNIX commands, whether or not it has been defined to z/OS UNIX System Services, by adding the variable KOE_ALLOW_UNDEFINED=1 to *&rhilev.&rte*.RKANPARU(KDSENV) on the LPAR where the command is to be executed.

If you want any user with a Tivoli Enterprise Portal user ID to be able to issue UNIX commands, add both KOE_ALLOW_ANY_UID=1 and KOE_ALLOW_UNDEFINED=1 parameters.

## Authorizing users to issue Prefixed Take Action commands

IBM Z OMEGAMON Monitor for z/OS provides a set of predefined Take Action commands. These commands, which are prefixed by `M5:`, are known as *agent commands*. A subset of these commands, commands that cannot also be run as console commands, can be issued using the Take Action feature on the Tivoli Enterprise Portal. In the OMEGAMON Enhanced 3270 user interface, the complete set of commands is available in action menus. Security for IBM Z OMEGAMON Monitor for z/OS Take Action commands is based on SAF security classes and resource profile names. If no resource profiles are created to control Take Action commands, all commands are denied.

The OMEGAMON Enhanced 3270 user interface validates for the following resource profile to see if users are authorized to issue the Take Action commands directed at z/OS resources:

```
KM5.msn.TAKEACTION
```

At a minimum, you must create a profile using this pattern for the global security class (RTE_SECURITY_CLASS) and give update access to the profile to all users you want to authorize to issue

IBM Z OMEGAMON Monitor for z/OS Take Action commands. You can also create other profiles for more granular access control.

For example, to control all IBM Z OMEGAMON Monitor for z/OS Take Action commands on all managed systems, use the following profile:

```
KM5.**.TAKEACTION
```

To restrict authority to issue commands to a specific managed system, specify the managed system name. For example, to control the ability to issue Take Action commands to an IBM Z OMEGAMON Monitor for z/OS agent running on Sysplex IBMTEST on Sysplex member TSTA, you would define a profile named

```
KM5.IBMTEST:TSTA:MVSSYS.TAKEACTION
```

To control access to individual commands, you must define at least one profile with the following format in either the global security class or the override security class (KM5_SECURITY_ACTION_CLASS):

```
KM5.**.TAKEACTION.commandname
```

This can be either a generic profile, or a command-specific profile. For example, to control access to all commands, create a profile like the following:

```
KM5.**.TAKEACTION.*
```

To control access to the KILL command, create a profile with the following form:

```
KM5.**.TAKEACTION.KILL
```

To control access to the KILL command on a specific managed system, create a profile with the following form:

```
KM5.msn.TAKEACTION.KILL
```

where *msn* is the managed system name of the target system. (For information on managed system names, see "Authorizing users to access IBM Z OMEGAMON Monitor for z/OS managed systems on the enhanced 3270 user interface" on page 41.)

IBM Z OMEGAMON Monitor for z/OS provides the following set of predefined Take Action commands:

```
CANCEL
CANCELDUMP
CANCELRESTART
CANCELDUMPRESTART
KILL
RESETSC
QUIESCE
RESUME
CHANGETIMELIMIT
SWAPIN
MARKSWAPPABLE
MARKNONSWAPPABLE
```

The KM5 override security class parameter (KM5_SECURITY_ACTION_CLASS, in PARMGEN) allows you to specify a separate security class to control individual IBM Z OMEGAMON Monitor for z/OS Take Action commands. However, you must still create the `KM5.**.TAKEACTION` resource profile discussed previously for the global security class.

Users must be given UPDATE access to the profiles. In addition, an SAF Pass Ticket profile must be defined to allow the OMEGAMON Enhanced 3270 user interface to authenticate between the interface and the hub monitoring server. For more information, see the *Configuring* section of the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Shared documentation*.

For information on issuing Take Action commands from the Tivoli Enterprise Portal, see the *IBM Tivoli IBM Z OMEGAMON Monitor for z/OS: User's Guide*.

## Recreating or replacing z/OS Management Console situations

If you previously ran z/OS Management Console situations, you can start corresponding situations for IBM Z OMEGAMON Monitor for z/OS or recreate comparable situations using IBM Z OMEGAMON Monitor for z/OS attributes.

For a list of z/OS Management Console situations and instructions for recreating them with IBM Z OMEGAMON Monitor for z/OS, or a list of corresponding IBM Z OMEGAMON Monitor for z/OS situations, see the *IBM Tivoli IBM Z OMEGAMON Monitor for z/OS: User's Guide*.

## Authorizing users to access IBM Z OMEGAMON Monitor for z/OS managed systems on the enhanced 3270 user interface

On all three 3270 interfaces, logon is controlled through the system authorization facility (SAF) interface. In addition, the OMEGAMON Enhanced 3270 user interface (enhanced 3270UI) performs SAF checks on users' authorization to view data for specific managed systems or managed system types, their authorization to issue Take Action commands and perform other selected commands and activities.

If no SAF security class is supplied (RTE_SECURITY_CLASS is missing or blank), users can log on to the enhanced 3270UI, can access data through queries, but cannot issue Take Action commands.

If a SAF security class is supplied, but not defined and active in SAF, no one can log on to the enhanced 3270UI.

If a SAF security class is supplied, and is defined and active in SAF, but no logon profile is defined, no one can log on to the enhanced 3270UI.

If a user is able to log on, and a different security class than the one used for logon is used for queries or for Take Action commands (but is not activated or resources are not defined in that security class), everyone can view data for any managed system and perform other commands and activities, but all Take Action commands are denied.

If a security class name is configured, resource profiles must be defined to control log on, data access, and Take Actions, and users must be given access to those profiles.

To define profiles that control access to specific IBM Z OMEGAMON Monitor for z/OS managed systems, you must specify the managed system names. Sysplex managed system names take the form:

```
plexname:MVS:SYSPLEX
```

where *plexname* is typically the true name of the Sysplex, but might be configured to be an alias for the Sysplex.

System managed system names take the form:

```
plexname:smfid:MVSSYS
```

MVS where *plexname* is typically the true name of the Sysplex, but can be configured to be an alias. The *smfid* component is the true System Management Facility (SMF) ID for the system or LPAR being monitored.

For instructions on configuring security for the enhanced 3270UI, see the *Configuring* section of the *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Shared documentation*.

For instructions on configuring security for the older 3270 interfaces, see Chapter 4, "Securing OMEGAMON," on page 53.

## Enabling z/OS Container Extensions (zCX) monitoring

zCX monitoring requires a Docker container (cAdvisor) serving port 8080 for each zCX Instance.

To enable zCX monitoring:

1. Determine the IP address used to manage and access the cAdvisor container:

   a. Open the zCX Instance joblog.

   b. Locate the “The server is listening on:” line and copy the IP address. In the following example, 192.168.12.34 is the IP address to copy:

   ```
   Please connect to IBM z/OS Container Extensions Docker CLI via your SSH client
   using port 8022
   The server is listening on: 192.168.12.34
   ```

2. Download, install, and start cAdvisor:

   a. On Windows, use PuTTY to log into a zCX Instance.

      i) In the Host Name field, specify the IP address found in step 1b.

      ii) Select Port 8022.

      iii) Select Connection type SSH.

      iv) Click Open.

   b. Enter your LDAP username and password.

   c. Right-click to paste the following command to start cAdvisor:

   ```
   docker run -v /proc:/rootfs/proc:ro -v /media:/rootfs/media:ro
   -v /var/run/docker.sock:/var/run/docker.sock:ro -v /sys:/sys:ro
   -v /var/lib/docker/:/var/lib/docker:ro -v /dev/disk/:/dev/disk:ro
   --restart always -p 8080:8080 -d --name cadvisor
   ibmcom/cadvisor-s390x:0.33.0
   ```

   **Note:** This command should not include line returns. If the line returns are copied to your clipboard, you can copy and paste into a text editor such as Notepad first, remove the line returns, and then copy and paste into PuTTY.

   d. Press Enter to download, install, and start cAdvisor.

3. Verify the installation. In your browser, navigate to the address of your zCX instance port 8080 (for example, http://192.168.12.34:8080) to see the cAdvisor main page.

**Troubleshooting:** When viewing the KM5ZCXO workspace, if you see 0 containers per instance, then cAdvisor is not installed correctly.

Docker commands are documented at https://docs.docker.com/engine/reference/commandline/cli/.

# Verifying the configuration

After you have completed any required configuration, verify the configuration to ensure that you have correctly configured the product and its components.

Before you can verify your configuration of IBM Z OMEGAMON Monitor for z/OS, the following tasks must be completed:

- The hub Tivoli Enterprise Monitoring Server must be installed and configured, and application support for IBM Z OMEGAMON Monitor for z/OS must be installed on it.
- The remote monitoring server to which an IBM Z OMEGAMON Monitor for z/OS agent reports must be installed and configured.

If use of RMF data collection is configured, the RMF Distributed Data Server (DDS) must be started and RMF Monitor III tasks must be started in all LPARs in this sysplex. IBM Z OMEGAMON Monitor for z/OS must be enabled to connect to the DDS using the RACF PassTicket service. If near-term history data collection is enabled, one or more OMEGAMON Subsystem address spaces per sysplex must be started and enabled to connect to the DDS using the RACF PassTicket service.

To verify the configuration, complete the following steps. (See "Copying started task procedures to your procedure library" on page 22 for the names of the started tasks.)

1. If the Tivoli Enterprise Monitoring Server in this runtime environment is not already running, vary the monitoring server VTAM major node active and start the monitoring server started task. The monitoring agent starts when the monitoring server starts
2. If the hub Tivoli Enterprise Monitoring Server is not already running, start it.
3. If the OMEGAMON Subsystem is not already running, start it.
4. Use a Tivoli Enterprise Portal client to log on to the hub.

   When Tivoli Enterprise Portal launches, you see the managed system name of any sysplexes you have configured listed under the z/OS Systems entry in the Navigator. Sysplex managed system names take the form *plexname*:MVS:SYSPLEX where *plexname* is either the true name of the sysplex or an alias for the sysplex, depending upon how you configured it.
5. Select (click) a sysplex.

   The Sysplex Enterprise Overview workspace should appear.
6. Verify that data for the system or systems you configured is being displayed.

## Tip

IBM Z OMEGAMON Monitor for z/OS started tasks can be started with the z/OS START command REUSASID=YES parameter. Use this parameter with the components that are likely to leave address spaces with unusable ASIDS: the OMEGAMON Subsystem, and the CSA Analyzer.

# Chapter 3. Disk space requirements for IBM Z OMEGAMON Monitor for z/OS historical data tables

The installation documentation for your OMEGAMON XE products provides the basic space requirements for the Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal, the Tivoli Enterprise Portal Server, and the monitoring agents themselves. These basic space requirements do *not* include the additional space that is required for maintaining historical data files.

The Tivoli Enterprise Portal displays two kinds of history data: short-term and long-term. Short-term history data, up to 24 hours worth, is retrieved from local storage on the host of the monitoring agent or the monitoring server to which it reports. Any data older than 24 hours is retrieved from the Tivoli Data Warehouse. Ideally, then, you want to allocate enough space for 24 hours of short-term historical data at the location of the persistent data store.

Because of the variations in client distributed systems, system size, number of managed systems, sampling intervals, and so on, it is difficult to provide actual additional disk space requirements for historical data collection. You need to experiment to determine how much space you need.

Use the default amounts to configure the data store initially, then observe how quickly space gets used. Eventually, you want to allocate enough space so that maintenance procedures only need to run once a day. The information in this appendix is provided to help you determine how much space is required.

## Understanding how the data store works

Data written to the persistent data store is organized by tables, groups, and data sets. Each attribute group, or *table*, is assigned to a group. For IBM Z OMEGAMON Monitor for z/OS, attribute tables are divided into two groups: sysplex-level attribute groups are assigned to the PLEXDATA group, and system-level attribute groups are assigned to the LPARDATA group.Table 6 on page 45 gives the mapping of attribute group names to table names.

By default, the low-level qualifier for the LPARDATA data sets is RKM5LPR* and the low-level qualifier for the PLEXDATA data sets is RKM5PLX*. Each data set is numbered consecutively up to the number (Count) you specify. By default, three data sets are assigned to each group.

Tivoli Management Services on z/OS provides automatic maintenance for the data sets in the persistent data store. When a data set becomes full, the persistent data store selects an empty data set to make it active. After that data set is active, the persistent data store checks to see if there are any more empty data sets. If there are no more empty data sets, maintenance is started on the oldest data set, and data recording is suspended.

*Table 6. Historical data table names and corresponding attribute groups*

| File name | Attribute group name |
|---|---|
| ASCPUUTIL | Address Space CPU Utilization |
| ASCSOWN | Address Space ComStor Owned |
| ASREALSTOR | Address Space Real Storage |
| ASRESRC2 | USS Address Spaces |

© Copyright IBM Corp. 2022

Table 6. Historical data table names and corresponding attribute groups (continued)

| File name | Attribute group name |
|---|---|
| ASSUMRY | Address Space Summary |
| ASVIRTSTOR | Address Space Virtual Storage |
| BPXPRM2 | USS BPXPRMxx Value |
| CHNPATHS | Channel Paths |
| COMSTOR | Common Storage |
| DASD MVS | DASD MVS |
| DASDMVSDEV | DASD MVS Devices |
| ENCTABLE | Enclave Table |
| ENQUEUE | Enqueues |
| HFSENQC2 | USS HFS ENQ Contention |
| KM5ASSTGSK | KM5 Address Space Storage SubKey |
| KM5CMSTGSK | KM5 Common Storage SubKey |
| KM5STGSTAT | KM5 Storage Shortage Status |
| LPCLUST | LPAR Clusters |
| M5ZFSDCI | KM5 zFS Directory Cache |
| M5ZFSKER | KM5 zFS Kernel |

*Table 6. Historical data table names and corresponding attribute groups (continued)*

| File name | Attribute group name |
|---|---|
| M5ZFSMCI | KM5 zFS Metadata Cache |
| M5ZFSSTI | KM5 zFS Storage |
| M5ZFSUCA | KM5 zFS User Cache |
| M5ZFSUCD | KM5 zFS User Cache DS |
| MADDSPC | Service Class Address Spaces |
| MCFCLIENT | CF Clients |
| MCFPATH | CF Path |
| MCFPOLCY | CF Policy |
| MCFSMVS | CF Structure to MVS System |
| MCFSTRCT | CF Structures |
| MCFSYS | CF Systems |
| MDASD DEV | Sysplex DASD Device |
| MDASD GRP | Sysplex DASD Group |
| MDASD SYS | Sysplex DASD |
| MGLBLENQ | Global Enqueues |
| MOUNTS2 | USS Mounted File Systems |

*Table 6. Historical data table names and corresponding attribute groups (continued)*

| File name | Attribute group name |
|---|---|
| MRESGRP | Resource Groups |
| MRPTCLS | Report Classes |
| MSRVCLS | Sysplex WLM Service Class Period |
| MSRVDEF | Service Definition |
| MSSWFA | Service Class Subsys Workflow Analysis |
| MWFAENQ | Service Class Enqueue Workflow Analysis |
| MWFAIO | Service Class I/0 Workflow Analysis |
| MWLMPR | WLM Service Class Resources |
| MXCFGRP | XCF Group |
| MXCFMBR | XCF Members |
| MXCFPATH | XCF Paths |
| MXCFSSTA | XCF System Statistics |
| MXCFSYS | XCF System |
| OEKERNL2 | USS Kernel |
| OPERALRT | Operator Alerts |
| OPS2 | USS Processes |

*Table 6. Historical data table names and corresponding attribute groups (continued)*

| File name | Attribute group name |
|---|---|
| OUSERS2 | USS Logged on Users |
| PAGEDS | Page Dataset Activity |
| PAGING | System Paging Activity |
| REALSTOR | Real Storage |
| SPINLOCK | KM5 Spin Lock |
| SUSLOCK | KM5 Suspend Lock |
| SVCDET | SVCDET |
| SYSCPUUTIL | System CPU Utilization |
| TAPEDRVS | Tape Drives |
| TOPUSER | TopUser |
| THREAD2 | USS Threads |
| URESPTM | User Response Time |
| VCMLCPU | HiperDispatch Logical Processors |
| VCMLPAR | HiperDispatch Management |

## Estimated space requirements

When you configure the persistent data store, you are asked to specify how many cylinders are allocated to each group. Ideally, you want to allocate enough space so that maintenance procedures need to run only once a day, without allocating unneeded space. Eventually, you can determine the correct amount of space by observing how often the maintenance procedures are running and adjusting space according. For your convenience, however, estimated space requirements are provided, in number of cylinders, for typical environments. You might want to make your own calculations, based on site-specific factors.

The estimates for each group (PLEXDATA and LPARDATA) were derived by calculating the size of each table in the group (in kilobytes), summing the table sizes, and dividing the total by the number of kilobytes per cylinder. The size of each table was based on the size of a row, the number of rows expected per sample, and the number of samples in one 24-hour period.

Several factors influence the size of each table. Table 7 on page 50 shows the factors considered in deriving the estimates for the tables in the LPARDATA (system-level) group for three different environments: small, medium, and large.

*Table 7. System-level data profiles for small, medium, and large environments*

| | **Type of environment** | | |
|---|---|---|---|
| **Factor** | **Small** | **Medium** | **Large** |
| ASID count per LPAR | 100 | 200 | 500 |
| Channel path count | 50 | 100 | 255 |
| Count of devices configured | 500 | 5000 | 10000 |
| Average created enclave count | 50 | 1000 | 2000 |
| Average enqueue conflict count | 3 | 10 | 50 |
| Number of CP LPARs configured | 2 | 5 | 15 |
| Number of clusters in this CPC | 1 | 2 | 3 |
| Average active Service Class Period Count | 20 | 40 | 90 |
| Average Active Report Class count | 10 | 50 | 200 |
| Average number of Local page data sets | 5 | 10 | 20 |
| Average number of Common page data sets | 1 | 2 | 4 |
| Average number of PLPA page data sets | 1 | 2 | 4 |
| Average number of Swap page data sets | 0 | 2 | 4 |
| Average active crypto service types | 0 | 75 | 75 |
| Average Configured tape Drive Count | 5 | 15 | 50 |
| Average number of tasks using crypto Service | 0 | 5 | 50 |
| Average number of active TSO users | 5 | 50 | 500 |

The factors making up the profiles for tables in the PLEXDATA group (sysplex-level data) are shown in Table 8 on page 51.

*Table 8. Sysplex-level data profiles for small, medium, and large environments*

| **Factor** | **Type of environment** | | |
|---|---|---|---|
| | **Small** | **Medium** | **Large** |
| Address Spaces per LPAR | 100 | 200 | 500 |
| LPARs in plex | 1 | 3 | 8 |
| Paths to coupling facility per LPAR | 0 | 2 | 2 |
| Coupling Facilities in plex | 0 | 2 | 4 |
| Structure connections In Plex | 0 | 60 | 180 |
| Structures in facility | 0 | 30 | 60 |
| Percent duplexed | 0 | 1 | 5 |
| Filtered devices | 50 | 100 | 200 |
| SMS groups | 5 | 20 | 50 |
| Enqueue conflicts plexwide | 0 | 3 | 5 |
| Resource Group count | 2 | 4 | 8 |
| Report Class count | 10 | 50 | 200 |
| Service Class period count | 20 | 40 | 90 |
| Subsystem per LPAR | 1 | 2 | 5 |
| Percent ASID delayed for Enqueue | 0.1 | 0.5 | 1 |
| Percent ASID doing I/O | 0.1 | 0.5 | 1 |
| XCF Paths per LPAR | 1 | 2 | 2 |

Table 9 on page 51 shows the number of cylinders estimated to be needed for the LPARDATA data sets in a small, medium, and large environment for three different sample collection intervals. A copy of the system-level files is kept on each managed system, so you can expect to allocate this much space on each system being managed.

*Table 9. Number of cylinders required for 24 hours for system-level (LPAR) data*

| **Collection interval (minutes)** | **Small environment** | | **Medium environment** | | **Large environment** | |
|---|---|---|---|---|---|---|
| | **3390 cylinders** | **3380 cylinders** | **3390 cylinders** | **3380 cylinders** | **3390 cylinders** | **3380 cylinders** |
| 5 | 78 | 93 | 567 | 681 | 1191 | 1428 |
| 15 (default) | 27 | 33 | 189 | 228 | 399 | 477 |
| 30 | 15 | 18 | 96 | 114 | 201 | 240 |

Table 10 on page 52 shows the number of cylinders estimated for the PLEXDATA group in the same three environments. Only one copy of sysplex-level files are stored in the sysplex, in shared DASD, so you allocate this space only once.

*Table 10. Number of cylinders required for 24 hours for sysplex-level (PLEX) data*

| Collection Interval (minutes) | Small Environment | | Medium Environment | | Large Environment | |
|---|---|---|---|---|---|---|
| | 3390 cylinders | 3380 cylinders | 3390 cylinders | 3380 cylinders | 3390 cylinders | 3380 cylinders |
| 5 | 21 | 27 | 87 | 105 | 414 | 498 |
| 15 (default) | 9 | 9 | 30 | 36 | 138 | 168 |
| 30 | 6 | 6 | 15 | 18 | 69 | 84 |

The numbers in these tables are the actual cylinder numbers needed to hold 24 hours of data. But because the configuration tool spreads its cylinder allocation over the number of files it is given and because the persistent data store maintenance strategy always keep one file empty, the number of cylinders that you should specify for are:

```
Cyl*(n/(n-1))
```

where

**Cyl**
is the cylinder count in the table for your profile, collection interval, and device type

***n***
is the number of files you want ICAT to allocate

So, for example, assuming the medium profile, at a 15-minute sampling interval, and 3390 devices, then Cyl = 189. If you want to use 3 files then the formula becomes 189*(3/2) = 283.5, rounding up to the next cylinder that is 284. If you use 5 files instead, this results in 189*(5/4) = 236.25 and with rounding 237. With 5 files the space per file is less, so leaving one file empty results in less “wasted” space.

For system level tables, the factors that affect total file size most are the number of DASD devices and the number of created enclaves. If you are concerned about space, consider not storing the nonplex DASD data, which is available in Resource Measurement Facility (RMF) and EPILOG.

Sysplex data demands are much smaller because the row counts per table are significantly smaller, especially with the DASD filtering situation running. IBM Z OMEGAMON Monitor for z/OS combines observations across the Sysplex, so most of the tables reflect an averaged result.

For Sysplex-level tables, the factors having the greatest effect are address space count per LPAR and the number of LPARs in the Sysplex. Several other tables can affect the storage needs by about plus or minus 10%.

## A reminder about historical data and performance impacts

Requests for historical data from tables that collect a large amount of data will have a negative impact on the performance of the product components involved.

To reduce the performance impact on your system, set a longer collection interval for tables that collect a large amount of data. For this product, the Address Space tables, the DASD MVS Devices table, and the Enclave table (for sites that are active with WebSphere®) collect a large amount of data.

# Chapter 4. Securing OMEGAMON

For OMEGAMON, security provides command validation and logon validation.

By default, OMEGAMON command validation is controlled by an internal security table, but can also be implemented using one of external SAF products. Logon validation for OMEGAMON is provided by one of the supported external SAF products (see "Securing OMEGAMON for MVS (Realtime collector)" on page 53).

## Securing OMEGAMON for MVS (Realtime collector)

Access to OMEGAMON commands is controlled by an internal security table. The security table is generated from a set of control statements.

The control statements provide the following information:

- If external security is used, the name of the module containing the external security exit routine (MODULE).
- An authorized screen space library for initialization that bypasses the security check (AUTHLIB).
- If internal security is used, the passwords for each level of security to which commands can be assigned (PASSWORD).
- The internal security levels of commands, which commands are under control external security, and whether an audit should be performed (COMMAND).
- The security options for minor commands (MINOR).

The default security module, KOMCM510, is included with LEVEL3 internal security for the following commands: APFU, CONS, CONU, CSAF, FNDU, KILL, LPAM, MCHN, MDEF, MLST, MSCN, MZAP, OCMD, RCMD, OSPC, PEEK, QLLA, SCHN, SLST, SSCN, SZAP, XMCH, XMLS, XMSC, XMZP, .DSA, ALIB, ALI, MCTL, CHAP, MNSW, MSWP, SWPI, TADR, TSNM. All other commands default to a security level of 0.

To change any of the protected commands, secure additional commands, change the passwords assigned to each level of security, or implement an external security facility, you must edit the control statements in the &*rhilev*.&*rte*.RKANPARU(KOMSUPDI) member and run the KOMSUPD job to update the security table. See "Modifying the security table" on page 53 for instructions.

Access to OMEGAMON commands can also be authorized using one of the supported external SAFs, or a combination of both internal and external security facilities. In addition, an external security facility can be used to authorize logon to OMEGAMON. If external security is implemented, users can log on to an OMEGAMON session only if they are allowed access to an "INITIAL*x*" resource name (where *x* is 0, 1, 2, 3, or blank) See "Implementing external security for OMEGAMON" on page 54 for instructions.

### Modifying the security table

You must edit the security table manually to modify it. You can edit the control statements and run the job manually. You must repeat this procedure for each runtime environment that requires OMEGAMON security.

To modify the internal security table, complete the following steps:

1. Edit the control statements in the KOMSUPDI member of &*rhilev*.&*rte*.RKANPARU.

   These control statements are described in "OMEGAMON security control statements" on page 60. Add the LIST=YES statement to create a complete listing of security information.

   **Note:** To switch from external security to internal security, complete the following steps:

   a. Add the `RESET=MODULE` command after your existing `MODULE=`*`xxxxxxxx`* command.

   b. Change commands marked EXTERNAL=YES to EXTERNAL=NO.

© Copyright IBM Corp. 2022

2. Modify and submit the &*rhilev*.&*rte*.RKANSAMU(KOMSUPD) job to update and report on the security table.

   If the update program flags statements as being in error, correct the statements and resubmit job KOMSUPD.

   See "Security update program listing" on page 67 for instructions on interpreting the list of the control statement modifications. The changes will not affect currently active sessions, but any session started after KOMSUPD is run uses the new security settings.
3. Move the KOMSUPDI member to a secured data set.
4. Modify the RKANSAMU(KOMSUPD) job to point to that new data set.

**Note:** Any time you run the job to create runtime members, the KOMSUPDI member is regenerated in RKANPARU with default values. You can modify the security table in RKANPARU as descirbed above.

## Implementing external security for OMEGAMON

External security authorization facilities (SAF) can be used for both OMEGAMON for MVS (Realtime collector) log-on authorization and command authorization.

The following external security authorization facilities are supported:

- RACF
- CA-ACF2
- CA-TOP SECRET

If external security is in force, control passes to a user-exit routine at session logon, re-logon, termination, and when a command is issued (see "Security exit processing logic" on page 69 ). If EXTERNAL=YES is specified for a command in the CONTROL command statement and no exit routine is available, OMEGAMON disables the command for the session, if the command has an associated security level of 0, or defaults to internal security if the command has a security level of 1, 2, or 3. IBM supplies sample user-exit routines.

To implement security for OMEGAMON using an external authorization facility, complete the following steps:

1. Set up rules in the external security package to interface with OMEGAMON.
2. Customize, assemble, and link the sample exit routine.
3. Update the security table to specify the use of an external security package and indicate which commands you want the package to validate.

Table 11 on page 54 shows the name of the sample exit routine for each external security package, and where to find instructions for implementing each package.

*Table 11. Choices of security facilities for implementing OMEGAMON security*

| **Security system** | **Exit name** | **Instructions** |
|---|---|---|
| RACF | KOMRACFX | "Securing OMEGAMON with RACF" on page 54 |
| CA-ACF2 | KOMACF2X | "Securing OMEGAMON with CA-ACF2" on page 56 |
| CA-TOP SECRET | KOMRACFX | "Securing OMEGAMON with CA-TOP SECRET" on page 58 |

### Securing OMEGAMON with RACF

Implementation of command and logon security using RACF requires three steps.

To implement command and logon security using RACF, complete the following steps:

1. "Set up RACF rules" on page 55
2. "Customize, assemble, and link the KOMRACFX exit routine" on page 56.

3. “Modify the security table for RACF” on page 56

### *Set up RACF rules*

In this step, you set up the RACF rules to interface with OMEGAMON.

Complete the following steps to set up the RACF rules:

1. Update the resource class description table to define a class name (for example, OMCANDLE) using the ICHERCDE macro call. If you do not use class name OMCANDLE, you must change the security exit class name to match your new class name (details are provided in the next topic). Code the ICHERCDE macro as follows:

   ```
   ICHERCDE CLASS=classname,
          ID=nnn,
          MAXLNTH=8,
          FIRST=ALPHANUM,
          OTHER=ANY,
          POSIT=nnn,
          DFTUACC=NONE
   ```

   Your configuration determines values for *classname* and *nnn*. Your installation may also require additional operands for this macro.
2. Activate the newly defined resource class.
3. Define an INITIAL*x* resource profile for logging onto OMEGAMON (where *x* is 0, 1, 2, 3, or blank). For example:

   ```
   RDEFINE classnme INITIAL UACC(READ)
   ```

   The resource name “INITIAL” permits users to change their security level with the /PWD command. Resource names “INITIAL0” through “INITIAL3” lock users to the highest matching security level (0, 1, 2, or 3) and prevent the users from changing their level with the /PWD command (this is also referred to as *locking*). These security levels are used with OMEGAMON internal security to determine if a particular command is accessible to a user.

   This example shows resource definitions to set a user to security level 2 (first define security level 0, 1, 2, and 3 as unaccessible, and then set USER02 to security level 2):

   ```
   RDEFINE classnme INITIAL0 UACC(NONE)
   RDEFINE classnme INITIAL1 UACC(NONE)
   RDEFINE classnme INITIAL2 UACC(NONE)
   RDEFINE classnme INITIAL3 UACC(NONE)
   PERMIT INITIAL2 CLASS(classnme) ID(USER02) ACC(READ)
   ```
4. Define one resource profile for each command you want to protect with RACF (each protected command will also require the EXTERNAL=YES setting in the security table).

   This step is optional. It is required only if you want to add separate external security control for specific commands. Otherwise, the regular LEVEL=*x* control is used.

   - Use the TSO RDEFINE command and specify the OMEGAMON command as the resource. Be certain to specify that only specific users may execute the command by setting UACC(NONE).
   - Use the PERMIT command to define those users who can access the resource (execute the command). Give them READ access. The following example shows how to authorize a user to execute the PEEK command:

     ```
     RDEFINE classnme PEEK UACC(NONE)
     PERMIT PEEK CLASS(classnme) ID(USER01) ACCESS(READ)
     ```
   - If the command you want to secure begins with a slash (/) or period (.), the RACF rule you define must start with a dollar sign ($) instead of the slash (/), or an at sign (@) instead of the period (.). For example, the command /LOGOUT requires a rule for $LOGOUT.

### *Customize, assemble, and link the KOMRACFX exit routine*

In this step, you set up the exit that interfaces with RACF.

Follow these steps to set up the exit:

1. Edit and modify the &*rhilev*.&*rte*.RKANSAMU(KOMRACFX) exit.

   Be sure that the resource class name in the exit matches the resource class name you defined when setting up RACF rules. The class name in the exit (default is OMCANDLE) is defined on this instruction (line 90):

   ```
   MVC U#CHCLSD,=C'OMCANDLE' ALTERNATE RESOURCE CLASS NAME
   ```

   The processing logic for this exit is provided in "Security exit processing logic" on page 69. Many sites use this exit without modification, but it is documented with comments to facilitate changes.
2. Assemble and link the exit routine. Use the &*rhilev*.&*rte*.RKANSAMU(KOMRACFA) job.

### *Modify the security table for RACF*

In this step, you set up the security table to work with RACF.

To set up the security table, complete the following steps.

1. Edit the control statements in the KOMSUPDI member of &*rhilev*.&*rte*.RKANPARU. These control statements are described in "OMEGAMON security control statements" on page 60.

   - Uncomment the MODULE command statement, and enter the name of the exit KOMRACFX on the MODULE statement as follows:

     ```
     MODULE=KOMRACFX
     ```

   - Indicate which commands are to be validated by RACF rules by setting EXTERNAL=YES on the COMMAND control statements.
   - Indicate which commands are to be validated by OMEGAMON internal security levels by setting LEVEL=*n* and EXTERNAL=NO on the COMMAND control statements.

   **Important:** To change an existing setting for a parameter, you must specify a new setting, rather than just blanking out the old setting. For example, to remove a command from external security checking, change EXTERNAL=YES to EXTERNAL=NO.
2. Modify and submit the KOMSUPD job in &*rhilev*.&*rte*.RKANSAMU to update and report on the security table. If the update program flags statements as being in error, correct the statements and resubmit the KOMSUPD job.

   See "Security update program listing" on page 67 for instructions on interpreting the list of the control statement modifications.
3. If OMEGAMON (default name IBMM2RC) is currently active, recycle OMEGAMON. Changes made to the security table are effective only when OMEGAMON has been started after the security update job completes successfully.

## Securing OMEGAMON with CA-ACF2

This section documents the steps required to implement OMEGAMON log-on and command authorization using CA-ACF2.

To set up OMEGAMON logon and command authorization using CA-ACF2, complete the following steps:

### *Set up CA-ACF2 rules*

In this step, you set up the CA-ACF2 rules to interface with OMEGAMON.

Complete these steps:

1. Define the name of the OMEGAMON started task to ACF2. The name is the started task name you specified for the realtime collector during configuration (parameter KM2_CLASSIC_STC in the configuration file).

   The started task name must have the MUSASS attribute assigned. This allows ACF2 to check the individual user's authorization rather than using the OMEGAMON address space ID.
2. Set up a resource class in CA-ACF2 to allow OMEGAMON to make the security checks. Define a generalized resource class name, for example OMS. This name will be three characters long for generalized resources. When you set up the exit, you will need to use this same class name prefixed with the letter R (for example, the OMS class name needs to be ROMS in the exit).
3. Define a CA-ACF2 rule for resource `INITIAL`*x* (where *x* is 0, 1, 2, 3, or blank) to allow users to log on to OMEGAMON. For example,

   ```
   ACFNRULE KEY(INITIAL) TYPE(OMS) ADD(UID(*********userid) ALLOW)
   ```

   where `OMS` must match the resource class name that you defined, and `UID` is a user ID or user ID mask.

   The resource name "INITIAL" permits users to change their security level with the /PWD command. Resource names "INITIAL0" through "INITIAL3" lock users to the highest matching security level (0, 1, 2, or 3) and prevent the users from changing level with the /PWD command (this is also referred to as *locking*). These security levels are used with OMEGAMON internal security to determine if a particular command is accessible to a user.

   The following example shows how to set users to specific levels:

   ```
   ACFNRULE KEY(INITIAL0) TYPE(OMS) ADD(UID(********USER02) ALLOW)
   ACFNRULE KEY(INITIAL1) TYPE(OMS) ADD(UID(********USER03) ALLOW)
   ACFNRULE KEY(INITIAL2) TYPE(OMS) ADD(UID(********USER04) ALLOW)
   ACFNRULE KEY(INITIAL3) TYPE(OMS) ADD(UID(********USER05) ALLOW)
   ```
4. Set up a CA-ACF2 rule for each command you want to protect with CA-ACF2 (each protected command will also require the EXTERNAL=YES setting in the security table: see "Modify security table for CA-ACF2" on page 57).

   The following example shows how to authorize a user to execute the PEEK command (specify the command name with the KEY operand):

   ```
   ACFNRULE KEY(PEEK) TYPE(OMS) ADD(UID(********USER01) ALLOW)
   ```

   If the command you want to secure begins with a slash (/) or period (.), the CA-ACF2 rule you define must start with a dollar sign ($) instead of the slash (/), or an "at" sign (@) instead of the period (.). For example, the command `/LOGOUT` requires a rule for `$LOGOUT`.

### Customize, assemble, and link the KOMACF2X exit routine

In this step, you set up the exit that interfaces with CA-ACF2.

Complete these steps:

1. Edit and modify the exit &*rhilev*.&*rte*.RKANSAMU(KOMACF2X).

   Be sure that the resource class you set up in the exit has the same name as the ACF2 resource class you defined, and that it is prefixed with the letter R (for example, OMS class name needs to be ROMS in the exit).

   The processing logic for this exit is provided in "Security exit processing logic" on page 69. Many sites use this exit without modification.
2. Assemble and link the exit routine. Use sample job &*rhilev*.&*rte*.RKANSAMU(KOMACF2A).

### Modify security table for CA-ACF2

In this step, you set up the security table to work with CA-ACF2.

Complete the following steps.

1. Edit the control statements in the KOMSUPDI member of &*rhilev*.&*rte*.RKANPARU. These control statements are described in "OMEGAMON security control statements" on page 60.

   a. Uncomment the MODULE command statement, and enter the name of the exit KOMACF2X on the MODULE statement as follows:

   ```
   MODULE=KOMACF2X
   ```

   b. Indicate which commands are to be validated by CA-ACF2 rules by setting EXTERNAL=YES on the COMMAND control statements.

   c. Indicate which commands are to be validated by OMEGAMON internal security levels by setting LEVEL=*n* and EXTERNAL=NO on the COMMAND control statements.

   To change an existing setting for a parameter, you must specify a new setting, rather than just blanking out the old setting. For example, to remove a command from external security checking, change EXTERNAL=YES to EXTERNAL=NO.

2. Modify and submit job KOMSUPD in &*rhilev*.&*rte*.RKANSAMU to update and report on the security table. If the update program flags statements as being in error, correct the statements and resubmit job KOMSUPD. See "Security update program listing" on page 67 for a description of the update program report.

The changes will not affect currently active sessions, but any session started after KOMSUPD is run will use the new security settings.

## Securing OMEGAMON with CA-TOP SECRET

Implementation of command and logon security using TOP SECRET requires three steps.

### *Set up CA-TOP SECRET rules*

In this step you set up the TOP SECRET rules to interface with OMEGAMON.

Complete the following steps:

1. Define a FACILITY statement for the started task for the realtime collector as a facility in the Facility Matrix Table. If the name you define in the FACILITY statement is different from the started task name, see the CA-TOP SECRET documentation for information on setting up the FACILITY statement.

   The following example shows FACILITY statements from a CA-TOP SECRET installation (some of these statements may not be relevant to your system, and others may need modification):

   ```
   FACILITY(USER3=NAME=task)
   FACILITY(task=MODE=FAIL,ACTIVE,SHRPRF)
   FACILITY(task=PGM=KOB,NOASUBM,NOABEND,NOXDEF)
   FACILITY(task=ID=3,MULTIUSER,RES,WARNPW,SIGN(M))
   FACILITY(task=NOINSTDATA,NORNDPW,AUTHINIT,NOPROMPT,NOAUDIT)
   FACILITY(task=NOTSOC,LOG(INIT,SMF,MSG,SEC9))
   ```

   The `SIGN` parameter on the FACILITY statement must be specified as `SIGN(M)`, or TOP SECRET may revoke user access. Also, verify that `MODE=FAIL` is set, and the MULTIUSER parameter has been included.

2. Add the facility to users, as follows:

   ```
   TSS ADDTO(useracid) FACILITY(cccccccc)
   ```

   where *cccccccc* is the started task name you specified for the realtime collector during configuration (parameter KM2_CLASSIC_STC in the configuration file).

3. Define a resource class to the RDT (Resource Descriptor Table), as follows:

   ```
   TSS ADDTO(RDT) RESCLASS(KOMCANDL) RESCODE(nn)
   ```

   where *nn* is any hexadecimal code between 01 and 3F.

4. Give ownership to class KOMCANDL, prefixed with `INITIAL`, as follows:

```
TSS ADDTO(deptacid) KOMCANDL(INITIAL)
```

5. Define PERMIT rules for resource INITIAL*x* (where *x* is 0, 1, 2, 3, or required blank) to allow users to log on to OMEGAMON, as in the following example:

```
TSS PERMIT(useracid) KOMCANDL(‘INITIAL ’) (trailing blank is required)
```

6. The resource name “INITIAL ” (with required blank) permits users to change their security level with the /PWD command. Resource names “INITIAL0” through “INITIAL3” lock a user to the highest matching security level (0, 1, 2, or 3) and prevent that user from changing that level with the /PWD command (this is also referred to as *locking*). These security levels can be used with OMEGAMON internal security to determine if a particular command is accessible to a user.

   The following example shows how to set users to specific levels:

```
TSS PERMIT(useracid) KOMCANDL(INITIAL0) (level 0 commands)
TSS PERMIT(useracid) KOMCANDL(INITIAL1) (level 1 commands)
TSS PERMIT(useracid) KOMCANDL(INITIAL2) (level 2 commands)
TSS PERMIT(useracid) KOMCANDL(INITIAL3) (level 3 commands)
```

7. Set up a rule for each command you want to protect with CA-TOP SECRET (each protected command will also require the EXTERNAL=YES setting in the security table).

   This step is optional. Perform this step only if you want to add separate external security control for specific commands. Otherwise, the regular LEVEL=$x$ control is used.

   This example permits a user to use the PEEK command:

```
TSS PERMIT(useracid) KOMCANDL(PEEK)
```

   If the command you want to secure begins with a slash (/) or period (.), the CA-TOP SECRET rule you define must start with a dollar sign ($) instead of the slash (/), or an at sign (@) instead of the period (.). For example, the command /LOGOUT requires a rule for $LOGOUT.

### *Customize, assemble, and link the KOMRACFX exit routine*

In this step, you set up the exit that interfaces with TOP SECRET.

To set up the exit that interfaces with TOP SECRET, complete the following steps:

1. Edit and modify the exit &*rhilev*.&*rte*.RKANSAMU(KOMRACFX) as follows:

   a. Remove both APPL=M$APPL parameters where they appear in the RACROUTE macro calls.

   b. Replace this line:

```
MVC U#CHCLSD,=C’OMCANDLE’ ALTERNATE RESOURCE CLASS NAME
```

   with the following instructions:

```
MVI U#CHCLS,X’08’ MVC U#CHCLSD,=C’KOMCANDL’
```

   The processing logic for this exit is provided in “Security exit processing logic” on page 69. Many sites use this exit without modification, but it is documented with comments to facilitate changes.

2. Assemble and link the exit routine. Use the &*rhilev*.&*rte*.RKANSAMU(KOMRACFA) sample job.

### *Modify security table for CA-TOP SECRET*

In this step, you set up the security table to work with CA-ACF2.

To set up the security table, complete the following steps.

1. Edit the control statements in the KOMSUPDI member of &*rhilev*.&*rte*.RKANPARU. These command statements are described in “Security exit processing logic” on page 69.
    a. Uncomment the MODULE command statement, and enter the name of the exit KOMRACFX on the MODULE statement as follows:

    ```
    MODULE=KOMRACFX
    ```

    b. Indicate which commands are to be validated by CA-TOP SECRET rules by setting EXTERNAL=YES on the COMMAND control statements.
    c. Indicate which commands are to be validated by OMEGAMON internal security levels by setting LEVEL=*n* and EXTERNAL=NO on the COMMAND control statements.

    To change an existing setting for a parameter, you must specify a new setting rather than just blanking out the old setting. For example, to remove a command from external security checking, change EXTERNAL=YES to EXTERNAL=NO.
2. Modify and submit job KOMSUPD in &*rhilev*.&*rte*.RKANSAMU to update and report on the security table. If the update program flags statements as being in error, correct the statements and resubmit job KOMSUPD. See “Security update program listing” on page 67 for a description of the report.

The changes will not affect currently active sessions, but any session started after KOMSUPD is run will use the new security settings.

## OMEGAMON security control statements

An internal security table controls access to OMEGAMON for MVS (realtime collector) commands. The security table is generated from a set of control statements that specify whether security is internal or external, determine which commands are protected, set the security level for those commands, and set the passwords for each level of security.

The sections that follow explain the control statements and associated keywords you use to modify the security table. The following information is provided for each control statement:

- Purpose of the control statement
- Format of the control statement
- Acceptable keywords
- Restrictions for the control statement (if any)
- Other information that is specific to the control statement (if any)

### General format rules for control statements

These general format rules apply to all control statements:

- Control statements can begin anywhere in the input record, but cannot extend beyond column 72.
- Statements can be in any order in the input stream.

  The update program processes the statements as it encounters them, with the exception of the LIST and UPDATE statements, which take effect after the update program processes all other input.
- All information for a particular control statement must fit on a single line.
- All input must be in uppercase letters.
- Statements must be in the format:

  ```
  CONTROLSTATEMENT=cccccccc,KEYWORD1=cccccccc,KEYWORD2=cccccccc, etc.
  ```

  There can be no intervening blanks. The update program treats data that follows a blank as a comment. This data prints on the control statement listing, but is ignored for processing purposes.
- To insert comment lines anywhere in the input stream, place an asterisk (*) in column 1 of the input record.

- If the update program flags statements as being in error, correct the statements and submit them again.

  To change a setting, you must specify a new setting instead of blanking out the old setting. This is especially important to remember when changing a command from EXTERNAL=YES to EXTERNAL=NO.
- The changes will not affect currently active sessions, but any session started after the KOMSUPD job is run will use the new security settings.

  The control statement listing should indicate successful completion of the update.

## AUTHLIB

The AUTHLIB control statement specifies the data set name of an authorized screen space library that contains commands to invoke at initialization, bypassing any security checks. This option lets you run protected commands as part of the initialization screen without entering a password.

Because all security checking for screens coming from the AUTHLIB data set is bypassed, WRITE access to this data set should be restricted.

Security checking resumes when OMEGAMON fetches a screen from an unauthorized library, or a screen that has been loaded into memory, or when a user enters any keystroke, including a cursor movement.

**Note:** If you create an authorized screen library and use the OMEGAMON menu system, security checking will cause initialization to fail under the following conditions:

- OMEGAMON fetches a screen containing an authorized command. Menu system users should leave the .FGO and .VAR commands unprotected.
- OMEGAMON fetches a screen space that has been loaded into memory. Alias name @ZSCRNDF is the screen that loads screen spaces into memory.

Concatenate the data set containing the authorized screens in your RKOMPROC DD statement. The data set that contains the authorized screen libraries is not an APF-authorized data set.

### Syntax

The syntax for AUTHLIB is

```
AUTHLIB=dsname,VOL={volume|NOVOLUME}
```

where *dsname* is the name of the authorized screen library you have created.

### Keywords

AUTHLIB accepts the following keyword:

**VOL**

Specifies the volume serial where the specified data set is located. This acts as an additional security measure. You can specify a volume serial number even if the data set is cataloged.

The AUTHLIB statement always requires the VOL keyword. If you do not want OMEGAMON for MVS to perform the additional volume serial number checking, specify NOVOLUME.

## COMMAND

The COMMAND control statement specifies the name of an OMEGAMON major, immediate, or INFO-line command that you want to protect. OMEGAMON protects minor commands at the level of its major command unless you specify the MINOR control statement.

When you update an INFO-line command, you must use the actual command name and not its alias. OMEGAMON automatically assigns the same protection attributes to all aliases of the command.

OMEGAMON always processes the last COMMAND statement for the command. OMEGAMON does not check for multiple COMMAND statements for the same command in the same run.

## Syntax

The syntax of COMMAND is

```
COMMAND=
        {cccc|.ccc|/cccccc}
        [,LEVEL={0|2|3|DISABLE}]
        [,EXTERNAL={YES|NO}]
           [,AUDIT={WTO|SMF|BOTH|NONE}]
```

where *cccc, .ccc*, or */cccccc* is the name of the OMEGAMON command you want to protect.

To have the control statement listing show the current security settings for a command, enter a COMMAND=*cccc*,=.ccc, or =/*cccccc* statement with no additional operands.

## Keywords

COMMAND accepts the following keywords:

**LEVEL**

Specifies the internal security level associated with this command.

- Level 0 allows the command to execute without an internal security check.
- Levels 1, 2, and 3 specify that the command executes only if you have previously entered the corresponding password for that level (or for a higher level) using the /PWD INFO-line command, or were locked to that level via external security.
- DISABLE specifies that OMEGAMON is never to execute the command.

You can audit attempts to execute the command for the session, but you cannot specify internal or external security.

**EXTERNAL**

Specifies whether an external security package checks this command.

**Note:** You can configure external security (to control logon to OMEGAMON and to lock users to a particular command level) without having to specify EXTERNAL=YES on any commands. If you do specify EXTERNAL=YES, you must define separate rules to control access to that command.

OMEGAMON ignores the EXTERNAL keyword if you specify LEVEL=DISABLE.

If you code EXTERNAL=YES for a command and no exit routine or rule is available, OMEGAMON does one of the following things:

- Disables the command for the session if it has an associated security level of 0
- Defaults to internal security if the command has a security level of 1, 2, or 3

After you specify EXTERNAL=YES, you can change EXTERNAL only by specifying EXTERNAL=NO *and* rerunning the security update program.

**AUDIT**

Specifies whether OMEGAMON is to audit the command each time a user invokes it. The possible values are:

**WTO**

Produces a one-line message on the main console.

**SMF**

Specifies that OMEGAMON write an SMF record. You must specify the SMF record number in the SMFNUM control statement.

If OMEGAMON cannot perform the SMF audit, OMEGAMON defaults to a WTO audit. See "The System Management Facilities audit" on page 70 for details about setting up the SMF audit.

**BOTH**
Specifies that OMEGAMON issue a WTO message to a console and write an SMF record.

**NONE**
Specifies no auditing. This is the default setting.

If you specify an audit for a disabled command, OMEGAMON notifies you of attempts to execute the command.

## LIST

The LIST control statement specifies whether the security update program produces a security file listing. OMEGAMON allows only one LIST statement per run. The default is `LIST=NO`.

A security file listing is a complete record of the security table that shows the following information:

- The name of the authorized screen library
- Security file volume serial number
- The name of the user exit module
- All command names, along with their corresponding security information

A security file listing does *not* list the internal security passwords.

If you also specify `UPDATE=NO`, the listing shows what the control statements and security information would look like if the update had taken place.

To generate the security file listing independent of edits to the control statements, submit `LIST=YES` as the only control statement in the input stream.

### Syntax

The format of LIST is LIST={YES|NO}

## MINOR

The MINOR control statement specifies the name of an OMEGAMON minor command you want to protect. OMEGAMON protects the minor commands independently of the majors. Therefore, any changes to minor commands apply to all minors with the same name and attributes, regardless of their major commands.

Access to a minor command requires access to the appropriate major command. If you do not specify an EXTERNAL keyword, the associated major command controls access to this minor command.

No check is made for multiple MINOR statements for the same minor command in the same run. The last MINOR statement for the minor takes effect.

### Syntax

The format of MINOR is

```
MINOR=cccc
[,LEVEL={1|2|3|DISABLE}]
[,EXTERNAL={YES|NO}
[,AUDIT={WTO|SMF|BOTH|NONE}
```

where *cccc* is the name of the minor command to be protected.

### Keywords

MINOR accepts the following keywords:

**LEVEL**

Specifies the internal security level you want to associate with this command.

**Level 0**

Allows the command to execute without an internal security check.

**Levels 1, 2, and 3**

Specifies that the command execute only if you have previously entered the corresponding password for that level (or for a higher level), using the /PWD INFO-line command.

**DISABLE**

Specifies that OMEGAMON is never to execute the command.

If you specify this value, you can audit attempts to execute the command for the session, but you cannot specify internal or external security.

**EXTERNAL**

Specifies whether an external security package checks this command.

**Note:** You can configure external security (to control logon to OMEGAMON, and to lock users to a particular command level) without having to specify EXTERNAL=YES on any commands. If you do specify EXTERNAL=YES, you must define separate rules to control access to that command.

OMEGAMON ignores the EXTERNAL keyword if you specify `LEVEL=DISABLE`.

If you code EXTERNAL=YES for a command and no exit routine or rule is available, OMEGAMON does one of the following:

- Disables the command for the session if it has an associated security level of 0
- Defaults to internal security if the command has a security level of 1, 2, or 3

Once you specify EXTERNAL=YES, you can change EXTERNAL only by specifying EXTERNAL=NO *and* rerunning the security update program.

**AUDIT**

Specifies whether OMEGAMON is to audit the command each time a user invokes it. The possible values are:

**WTO**

Produces a one-line message on the main console.

**SMF**

Specifies that OMEGAMON write an SMF record. You must specify the SMF record number in the SMFNUM control statement.

If OMEGAMON cannot perform the SMF audit, OMEGAMON defaults to a WTO audit.

See "The System Management Facilities audit" on page 70 for details about setting up the SMF audit. This option requires APF-authorization.

**BOTH**

Specifies that OMEGAMON issue a WTO message to a console and write an SMF record.

**NONE**

Specifies no auditing. This is the default setting

If you specify an audit for a disabled command, OMEGAMON notifies you of attempts to execute the command.

## MODULE

The MODULE control statement specifies the name of the module that contains the external security exit routine. You must specify the MODULE parameter for an external security check to take place. There is no default.

### Syntax

The format of MODULE is:

```
MODULE=cccccccc
```

where *cccccccc* is the name of the module that contains the external security exit routine.

Be sure that this name matches the load module name you specified in KOMACF2X or KOMRACFX.

## PASSWORD

The PASSWORD control statement specifies the 1- to 8-character password for each internal security level that you want to use with the /PWD command.

You must use a separate PASSWORD control statement for each security level.

Use unique passwords for each security level. If you assign the same password to more than one level, OMEGAMON will match it only at the lowest level and deny access to commands protected at higher levels.

When you enter a valid password for one security level, OMEGAMON allows access to commands secured at that level and to commands secured at lower levels. OMEGAMON checks the password for a match in the following order:

1. Level 1
2. Level 2
3. Level 3

### Syntax

The format of PASSWORD is

```
PASSWORD=password,LEVEL={1|2|3}
```

where *password* is the unique password for this level.

### Keywords

PASSWORD accepts the following keyword:

**LEVEL**

Specifies the security level you want to associate with this password.

OMEGAMON requires a level for a password.

Levels 1, 2, and 3 specify that the command executes only if you have previously entered the corresponding password for that level (or for a higher level), using the `/PWD` INFO-line command.

## RESET

The RESET control statement clears the current settings of the other control statements. Reset commands remain unprotected unless you specify new settings with the appropriate control statements and rerun the update program.

Only one RESET statement is allowed per run.

### Syntax

The format of RESET is

```
RESET=keyword
```

where *keyword* is one of the keywords described in the following section.

### Keywords

RESET accepts the following keywords:

**ALL**
Clears settings for all control statements and all keywords in the OMEGAMON security table.

**AUTHLIB**
Clears the name and volume serial number of the authorized library.

**INFO**
Clears settings for all INFO-line commands (on the COMMAND control statement).

For example, if you do not want to use the IBM default security levels for INFO-line commands and want to start over, enter RESET=INFO. For INFO-line commands, this resets all LEVEL settings to security level 0 and also clears any existing EXTERNAL and AUDIT settings.

**MAJOR**
Clears settings for all major and immediate commands (on the COMMAND control statement).

**MINOR**
Clears settings for all minor commands.

**MODULE**
Clears the name of the security exit routine module.

**PASSWORD**
Clears the internal passwords.

**SLASH**
Clears settings for all INFO-line commands (on the COMMAND control statement).

For example, if you do not want to use the IBM default security levels for INFO-line commands and want to start over, enter RESET=SLASH. For INFO-line commands, this resets all LEVEL settings to security level 0 and also clears any existing EXTERNAL and AUDIT settings.

**SMFNUM**
Clears the record number for SMF audits.

**YES**
Clears settings for all control statements and all keywords in the OMEGAMON security table.

## SMFNUM

The SMFNUM control statement indicates the ID number of the SMF record that OMEGAMON should use for its audit. The SMF audit is intended for use only with commands that could disrupt the system (for example, OCMD and MZAP). Use the SMF audit selectively because of its high overhead.

When creating the SMF audit, make sure that the SMF Record Exits (IEFU83 and IEFU84) and the SMF system parameters specifications (SMFPRMcc) do not suppress the ability for OMEGAMON to journal the audit activity records. The KOBSMFRP member of the &*rhilev*.&*rte*.RKANSAM data set contains a sample SMF post-processor and report generator in source code format. This is supplied as an example only.

### Syntax

The format of SMFNUM is

```
SMFNUM=nnn
```

where *nnn* is the SMF record ID number.

The ID number you assign to OMEGAMON must be between 128 and 255, inclusive, and should be different from the number that any other application is using. There is no default.

## UPDATE

The UPDATE control statement specifies whether OMEGAMON updates the control statements during this run. OMEGAMON allows only one UPDATE statement per run.

### Syntax

The format of UPDATE is `UPDATE={YES|NO}`

`UPDATE=NO` specifies that this run of the security update program should be a trial run.

## Security update program listing

The security update program produces a listing of control statement modifications. If you specify the `LIST=YES` control statement, an additional report is produced that includes all security information.

The security update program listing has four parts.

- Header
- Edited control statements
- Security files
- Update trace

### Header

The header contains the following information:

- The name of the data set where the load module is located.
- The name of the module containing the security table (KOMCM*nnn*).
- The OMEGAMON version number in the format V*nnn*COM.
- Messages indicating successful completion of the job or error conditions, such as a failure to open the SYSLIB data set or read the security table.

### Edited control statements

The update report contains a listing of the control statements that have been edited. The listing shows the previous contents (except for previous passwords), as well as the new contents. If you specified `UPDATE=YES`, OMEGAMON reports the date and time of the previous update.

The codes for the PREVIOUS CONTENTS and NEW CONTENTS of commands are positional. There are three positions:

1. The first position shows the number of the internal security level or an asterisk (*) if the command has been DISABLED.
2. The second position shows the external security option:

   **E**

   Use external security for this command.

   **b**

   A blank indicates no external security.
3. The third position shows the auditing option:

**W**
Audit this command via WTO.

**S**
Audit this command via SMF.

**B**
Audit this command via WTO and SMF.

**b**
A blank indicates no auditing.

### Security files

If you specify LIST=YES anywhere in the input stream, the security update program generates a complete listing of the security information, including the name of the authorized screen library and its volume serial number, the name of the external security user exit module, the SMF record number, and all of the commands along with their security information. The listing does not show the internal security passwords.

TYPE specifies the following kinds of OMEGAMON commands:

**C**
Major

**I**
Immediate

**S**
Slash (INFO-line)

The security level follows the command. An asterisk (*) indicates that a command has been disabled. Minor commands are listed following their corresponding majors.

### Update trace

The last part of the listing indicates whether an update has successfully completed.

## Accessing authorized commands

You can access authorized commands using the /PWD command.

To gain access to the authorized commands, use the /PWD command in the following manner:

1. Type /PWD on the INFO-line.

   When you press Enter, OMEGAMON responds with the password prompt.
2. Type your password on the INFO-line.

   The password does not display as you type it.
3. Press Enter.

   The PASSWORD ACCEPTED message displays.
4. Press Enter.

   OMEGAMON provides access to all authorized commands associated with that password, as well as lower command levels.

If you are using OMEGAMON with an external security package to authorize commands, you can prevent the use of the /PWD command. The resource name “INITIAL” permits users to change their security level with the /PWD command. Resource names “INITIAL0” through “INITIAL3” lock a user to the highest matching security level (0, 1, 2, or 3) and prevent that user from changing their level with the /PWD command (this is also referred to as *locking*). These security levels are used with OMEGAMON internal security to determine if a particular command is accessible to a user.

The /PWD command also controls the relogon function. The relogon feature is a function of the /PWD command that allows you to enter a user ID and password to the external security package from an active OMEGAMON session. This allows you to alter the security level of your session without stopping your session. (See the *IBM Z OMEGAMON Monitor for z/OS: OMEGAMON for MVS Command Reference* for details on the /PWD command).

### Changing your security level to issue authorized commands

To issue an authorized command, your session security level must be equal to (or greater than) the level defined in the security table for that command. You can change your security level if necessary.

To change your session security level, take either of the following steps:

- From an OMEGAMON session, enter the /PWD command.

## Security exit processing logic

If you are using an external security product (RACF, CA-ACF2, or CA-TOP SECRET) for OMEGAMON security, you need to use a security exit routine.

Table 12 on page 69 gives the name of the exit for each of the support external security programs. The following sectionsdescribe the processing logic for the exit routines.

*Table 12. Security exit routines for external command-level security*

| Product | Exit routine |
|---|---|
| RACF | &*rhilev*.&*rte*.RKANSAMU(KOMRACFX) |
| CA-TOP SECRET | &*rhilev*.&*rte*.RKANSAMU(KOMRACFX) |
| CA-ACF2 | &*rhilev*.&*rte*.RKANSAMU(KOMACF2X) |

### $UCHECK

Communication between OMEGAMON for MVS (Realtime collector) and the exit routine is done through the control block $UCHECK and exit return codes. The control block $UCHECK is mapped by the &*rhilev*.&*rte*.TKANMAC(KOBGMAC) macro. OMEGAMON maintains the $UCHECK control block for the entire life of the session.

At the end of $UCHECK is a 512-byte work area set up for your installation’s own use. If you require a work area larger than 512 bytes, GETMAIN additional storage and place a pointer to this storage in $UCHECK. If you modify the RACF RACROUTE macro, you must GETMAIN at least 512 bytes for use as the WORKA parameter.

### Initialization exit call sequence

A series of exit calls is done at OMEGAMON initialization:

1. At initialization, when OMEGAMON passes control to the exit routine, the initialization call is indicated by an I in the U#CHTYP field. This indicates a logon validation request. 2
2. If the user ID field length is nonzero, the user ID and password information are available.
3. If additional information or some form of retry is required, the routine can request a reshow of the screen, and reset any field lengths to indicate that no data is present (user ID, password, group, or new password).
4. To perform a reshow in VTAM mode, set a message into the U#CHMSG field (120 bytes maximum length), set the U@CHRSHO bit in U#CHRESP, and return to the caller. The message appears after the panel. Appropriate fields are filled in (original user ID and password), unless overridden (length = 0).
5. When validation is complete, a return code of 0 from the user exit indicates that the user should be allowed to log on. Any other return code will cause the session to be aborted.

6. Upon successful logon acceptance, the exit may perform resource validation and optionally assign a command security level (0, 1, 2, or 3) to the user (default is 0). Place the appropriate number into U#CHAUT4. To lock the user to this level, also set the U@CH1LOK bit in U#CHAUT1.

### Command verification exit call sequence

The following sequence of exit calls is done at command verification:

1. During command verification, OMEGAMON places a C in the U#CHTYP field.
2. The user's authorization can be checked.
3. The decision to allow or disallow a command on the first encounter cannot be changed on subsequent tries by the same user, unless security is reset with the /PWD command. However, on each try, the user exit is notified; an audit record may be written, and a customized error message may be issued.

   Return codes from the exit routine may be one of the following:

   **0**

   Indicates that the command is allowed.

   **4**

   RACF only: Indicates that the command is unknown to RACF. OMEGAMON will allow the command to execute.

   **8**

   Indicates that the command is known to the external security package, and access is denied.
4. When you authorize commands, OMEGAMON modifies the command name by replacing the slash of INFO-line commands with a dollar sign (`/cccccc` becomes `$cccccc`), and the period of immediate commands with @ (`.ccc` becomes `@ccc`).

### Re-logon exit call sequence

The following sequence of exit calls is done at re-logon:

1. At re-logon, OMEGAMON places an R in the U#CHTYP field to indicate a logon validation.
2. The processing is the same as at initialization, except that users may not enter a new password or group because OMEGAMON does not display a logon panel.

### Termination exit call sequence

At termination, OMEGAMON passes a T to the user's exit routine. You can then do any termination cleanup required, such as freeing user control blocks and FREEMAINing any GETMAINed areas.

## The System Management Facilities audit

You can generate a System Management Facilities (SMF) audit report that logs OMEGAMON logon activity and command authorization.

The SMF record contains:

- IBM header (IFASMFR maps)
- OMEGAMON Common Header ($CANHDR maps)

  You define these maps in member KOBGMAC of &*thilev*.TKANMAC.
- Security audit record ($AUDIT maps)

You define these maps in member KOBGMAC of &*thilev*.TKANMAC.

The audit record contains:

- Date/time/system stamp
- User ID/job name associated with the session
- Actual command text as you entered it on the screen

Records of minor commands also reference their associated major commands.

⚠ **CAUTION:** The SMF audit has a high overhead, so use it sparingly. Because the overhead for producing SMF records is high, you should use the audit only with sensitive commands, such as those that could disrupt the system (for example, ICMD and IZAP).

To generate the SMF report, follow these steps:

1. Copy the &*thilev*.TKANSAM(KOISMFEX) member to &*rhilev*.&*rte*.RKANSAMU(KOISMFEX).

   Modify KOISMFEX, following the instructions in the member.
2. Copy the &*thilev*.TKANSAM(KOISMFRP) member to &*rhilev*.&*rte*.RKANSAMU(KOISMFRP).

   Modify KOISMFRP to meet your site’s needs.
3. Copy the &*thilev*.TKANSAM(KOISMFA) member to &*rhilev*.&*rte*.RKANSAMU(KOISMFA). Modify KOISMFA, following the instructions in the member.
4. Use the &*rhilev.*&*rte*.RKANSAMU(KOISMFA) member to assemble and link your program.
5. Submit the job for execution.

If you generate a SMF audit report, make sure that SMF record exits (IEFU83 and IEFU84).

# Chapter 5. Customizing EPILOG historical data collector controls

The &*rhilev*.&*rte*.RKANPARU(KEPOPTN) member contains OPTIONS and COLLECT statements that control historical data collector operation for EPILOG. You customize the collector behavior by modifying these statements to specify collection options and create collection filters.

Parameters entered on the OPTIONS statement filter data which is written to the historical data store and to the SMF log. Parameters entered on the COLLECT statement filter data are written to the historical data store only.

The following topics show you how to enter collector options on the OPTIONS statement and enter filters using the COLLECT statement. You can use a text editor to enter these options.

## Controlling collection options

You control the collection options for EPILOG historical data records using the OPTIONS statement in &*rhilev*.&*rte*.RKANPARU(KEPOPTN) member and a set of keyword/value pairs.

The syntax of the OPTIONS statement is:

```
OPTIONS option1 [option2 option3...]
```

Table 13 on page 73 lists the keywords that can be substituted for *option1*, *option2*, and *option3* and possible values for each keyword.

*Table 13. Keywords used with the OPTIONS statement*

| Keyword | Function | Operand |
|---|---|---|
| ACFIELDNO ACFN | Specifies which JES accounting field contains the target data. | 0–99 (If 0, no data is collected; default = 1) |
| ACLENGTH ACFL | Specifies how many digits of accounting data to extract. | 1–12 (default = 1) |
| ACPOSITION ACFP | Specifies at what position within the batch job accounting field the target data begins. | 1–99 (default = 1) |
| ALTDATA ALTD | Collects resource data when another vendor product is used instead of RMF to monitor system resources. | |
| BATCHINT | Specifies whether or not degradation data should be collected for batch jobs at RMF-based intervals, and how many RMF intervals comprise a collection interval. | ON OFF (default) 0–9 |
| BATCHON | Specifies one or more batch jobs for which degradation data is to be collected. (If this keyword is not specified, data will not be collected for any batch jobs.) | one or more job names (accepts generic formats) |
| BATCHOFF | Turns off collection for a subgroup of the jobs specified with BATCHON. | one or more job names (accepts generic formats) |

© Copyright IBM Corp. 2022

*Table 13. Keywords used with the OPTIONS statement (continued)*

| Keyword | Function | Operand |
|---|---|---|
| EDSDATA EDSD<br>NOEDSDATA<br>NOEDSD | Specifies whether the collector should write its data to an online data store. You must specify EDSDATA if, on the Collection Control Parameters pop-up window, you requested that RMF supply the collector with its resource data. | (default = EDSDATA) |
| EDSLIST EDSL | Specifies the EPILOG data stores that are to be used for collection. (No default) | a list of EDS data set names (required) |
| EDSSWITCH<br>EDSW | Specifies the events that trigger an automatic EDS switch. | one (and only one) of the following: FULL (default), MONTH, DAY, MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, SATURDAY, SUNDAY |
| INTERVAL | Specifies the length of the collection interval in minutes when RMF is not active. | 1–60 (default = 15) |
| LOCALID | Specifies the EPILOG applid used by the Tivoli Enterprise Monitoring Server to connect to the collector. | |
| LOOPDETECT | Specifies a maximum number of CPU seconds that can be used by the collector during a single sampling interval. | 1–100 (default = 15) |
| MAINTPROC<br>MNTP | Specifies the cataloged procedure to be started by the collector at the conclusion of a successful EDS switch. | 1–8-character member name of a cataloged JCL procedure (required) (No default) |
| NOTIFY | Specifies the TSO users to be notified of major collection activity. | list of TSO user IDs (required) (No default) |
| RMFDATA RMFD<br>NORMFDATA<br>NORMFD | Specifies whether or not RMF resource data should be collected. | (Default = RMFDATA) |
| RCLON RCLOFF | Specifies one or more report classes for data collection. RCLOFF is typically used to exclude report classes implicitly specified by RCLON. | one or more report class names (accepts generic formats) |
| REMOTEID | Specifies the Tivoli Enterprise Monitoring Serverapplid used by the EPILOG collector to connect to the monitoring server. | |
| SAMPMIN<br>SAMPMIN | Allows user to set a minimum number of samples in a given RMF interval before it can be saved in a datastore. Set this value to a low number to collect data on short running steps. | Default=10<br>1 is the lowest valid value. Specifying 0 will result in the default value of 10 to be used. |
| SCLON SCLOFF | Specifies one or more service classes for data collection. SCLOFF is typically used to exclude service classes implicitly specified by SCLON. | one or more service class names (accepts generic formats) |

*Table 13. Keywords used with the OPTIONS statement (continued)*

| Keyword | Function | Operand |
|---|---|---|
| SQAMAX SQA | Specifies the amount of ESQA or SQA storage (in kilobytes) to allocate as a work area for collecting address space performance data. By default, the collector calculates the amount of space it needs when it starts up.<br>Use this keyword only if you are concerned about the ESQA/SQA storage being used by the collector. | |
| SMFDATA SMFD<br>NOSMFDATA<br>NOSMFD<br>SPILLSMFDA TA<br>SPILL | Specifies under what circumstances collected data is to be written to SMF. | (Default = SPILLSMFDATA |
| SMFNUM SMFN | Specifies the SMF record ID number to be used if SMFDATA is turned on. | 128–255 (Default=180) |
| STCINT ON OFF | Specifies whether or not degradation data should be collected for started tasks at RMF-based intervals, and how many RMF intervals comprise a collection interval. | (default) 0–9 |
| STCON | Specifies one or more started tasks for which degradation data is to be collected. (If this keyword is not specified, data is not collected for any started tasks.) | one or more started task names (accepts masks) |
| STCOFF | Turns off collection for a subgroup of the tasks specified with STCON. | one or more started task names (accepts masks) |
| SYSCHECK SYSC<br>NOSYSCHEC K<br>NOSYSC | Specifies whether a historical datastore may contain data for more than one SMF system ID. NOSYSCHECK allows the collector to write to a historical datastore that already contains data for another system. | (default = SYSCHECK) |
| TSOINT | Specifies whether or not degradation data should be collected for TSO users at RMF-based intervals, and how many RMF intervals comprise a collection interval. | ON OFF (default) 0–9 |
| TSOON | Specifies one or more TSO user IDs for which degradation data is to be collected. (If this keyword is not specified, data is not collected for any TSO sessions.) | one or more TSO user IDs (accepts generic formats) |
| TSOOFF | Turns off collection for a subgroup of the user IDs specified with TSOON. | one or more TSO user IDs (accepts generic formats) |

*Table 13. Keywords used with the OPTIONS statement (continued)*

| Keyword | Function | Operand |
|---|---|---|
| WARNING(*m*)<br>WARN(*n*) | Specifies the threshold in percent at which “EDS getting full” message should be issued and “next EDS status” messages should be issued. An operand of 100 suppresses the messages. | 1–100 (Default=80) |

# Adding a collector filter

You use the COLLECT statement to add collector filters to prevent data from being written to your historical data store. By keeping only the most useful and important data in the data store, you will keep your data store maintenance to a minimum.

Collector filters allow you to specify which records, of those already selected for collection, you want the collector to write to the historical data store. They affect only those records written to the historical data store. Collector filters do not affect records written to SMF. You can specify that all records be written to SMF regardless of filtering. See Chapter 6, “Managing EPILOG data stores,” on page 79 for more information about SMF.

## COLLECT statement

The COLLECT statement in the &*rhilev*.&*rte*.RKANPARU(KEPOPTN) member allows you to establish a set of collection filters for EPILOG historical data records already selected for collection. These filters tell the collector which records should (or should not) be written to the online historical data store.

The syntax of the COLLECT statement is:

```
COLLECT { workload| resource time-period }
```

or

```
COLLECT EXCLUDE { workload | resource: }
```

The first format filters out records for the indicated workload or resource based on a time period. Unless the record falls within the time period specified, it will be excluded. The second format excludes all records for a specified workload or resource. You cannot enter a time period with the EXCLUDE keyword.

The following example filters the collection of batch job degradation data by JES job class. Data will be written to the data store for batch jobs that run between the hours of 8:00 AM and 5:00 PM only.

```
COLLECT CLS(*) STIME(8) ETIME(17)
```

The following example filters the collection of resource data to collect this data only on weekdays. The resource data for weekdays only will be written to the data store.

```
COLLECT RALL DAY(WEEKDAY)
```

The following example filters the collection of data by program name. Data will be written to the data store for all batch jobs, started tasks, and TSO sessions except for those with names that begin with IEB.

```
COLLECT EXCLUDE PROGRAM(IEB*)
```

It is possible to have more than one COLLECT statement. If you have more than one COLLECT statement, you cause a record to be written to the historical data store whenever that record both matches at least one COLLECT statement and does not match any other COLLECT EXCLUDE statement. The following example illustrates how the conditions interact:

```
COLLECT JOB(*) STIME(8) ETIME(13)
COLLECT EXCLUDE ACCT(44224)
```

Data is collected for all jobs specified for collection, between the hours of 8 AM and 1 PM except those with account numbers of 44224.

## Conditions when you have more than one COLLECT statement

If you have more than one COLLECT statement, you cause a record to be written to the historical data store whenever that record both matches at least one COLLECT statement and does not match any other COLLECT EXCLUDE statement.

The following example illustrates how the conditions interact:

```
COLLECT JOB(*) STIME(8) ETIME(13)
COLLECT EXCLUDE ACCT(44224)
```

Data is collected for all jobs specified for collection, between the hours of 8 AM and 1 PM except those with account numbers of 44224.

## Workload keywords for COLLECT

Workload keywords specify how workload degradation data is selected: by installation account code, by JES job class, by program name, or by performance group symbolic name.

Table 14 on page 77 contains the workload keywords available for use with the COLLECT statement. For more information on workload keywords, see the *IBM Z OMEGAMON Monitor for z/OS: EPILOG Command Reference*.

*Table 14. Workload keywords for COLLECT statement*

| Keyword | Function |
|---|---|
| ACCOUNT ACCT | Selects batch job or TSO session degradation data by installation account code. |
| CLASS CLS | Selects batch job degradation data by JES job class. |
| PROGRAM PGM | Selects batch job, started task, or TSO session degradation data by program name. |
| SYMBOLIC SYM | Selects degradation data for a performance group by user-defined symbolic name. |

## Resource keywords for COLLECT

Resource keywords specify the types of system resources for which information is to be collected

Table 15 on page 77 lists the resource keywords available for use with the COLLECT statement. See the *IBM Z OMEGAMON Monitor for z/OS: EPILOG Command Reference* for more information.

*Table 15. Resource keywords for COLLECT statement*

| Keyword | Description |
|---|---|
| RALL | All resource types |
| RCCH | Cache subsystem statistics |
| RCHN | Channel activity |
| RCPU | Hardware and address space CPU activity |
| RDAS | DASD device information |

Table 15. Resource keywords for COLLECT statement (continued)

| Keyword | Description |
|---|---|
| RINF | General system information (CPU model, MVS level, current WLM service policy, and so on) |
| RLCU | I/O queuing data |
| RPAG | Real and virtual storage usage with paging and swapping activity |
| RPDS | Page data set statistics |
| RSCL | WLM service class and report class statistics |
| RSDS | Swap data set statistics |
| RSRM | SRM MPL settings |
| RSWA | Swap activity statistics |
| RSWR | Swap reason statistics |
| RVLF | VLF class statistics. VLF data is collected by default. Use EXCLUDE to stop collection of VLF data. |

## Date and time keywords for COLLECT

Date and time keywords available for use with the COLLECT statement for workloads. If you selected PDSDATA, you must also specify a time range for each of the time ranges you selected.

The types of data available include:

- WLMPDATA *time-range*
- RXCFDATA *time-range*
- RXESDATA *time-range*

Table 16 on page 78 lists the available date and time keywords. For more information on date and time keywords, see the *IBM Z OMEGAMON Monitor for z/OS: EPILOG Command Reference*.

Table 16. Date and time keywords for COLLECT statement

| Keyword | Function |
|---|---|
| BAND | Collects data between the start and end times on the specified days. (Default value) |
| DAYOFWK DAY | Collects data only for the specified days (MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, SATURDAY, SUNDAY, WEEKDAY, WEEKEND). The days used with this keyword can be abbreviated to an unambiguous short form. For example, WEDNESDAY can be shortened to W, but SATURDAY can only be shortened to SA. |
| ENDTIME | Collects data until this time of day on specified days. |
| RANGE | Collects data from the start time and date to end time and date. |
| STARTTIME | Collects data starting with this time of day on specified days. |

# Chapter 6. Managing EPILOG data stores

OMEGAMON uses two types of data stores: historical EPILOG data stores (EDS) and profile data stores (PRDS). The historical data stores capture resource and degradation data written to them by the historical collector. From these data stores, you can display the data online or generate batch reports. The profile data store is used to store averaged samples of historical data that are derived from the historical data stores. This data can then be used with the Workload Profile Facility (WPF) to compare current performance to past performance.

The historical collector writes the resource and degradation data it collects to a circular queue of historical data stores, where data is available for online historical displays and batch reports. Writing to a data store continues until it becomes full or a site-specified time period has elapsed. At that time, the collector starts writing to the next available data store in the queue. Maintenance (the archiving of data and clearing of a data store) is normally scheduled for the data store with the oldest data and can be done at the same time the historical collector is running. Reporting of historical data is not available while EDS maintenance is running.

The collector selects historical data stores in the order you specify. After selecting a data store, the collector writes to it exclusively until it becomes full, or until a site-specified trigger for a data store switch has been reached. Writing is then switched to the next available data store in the list. After using the last data store in the list, the collector wraps around to the first data store in the list. The collector keeps a historical data store available for recording by automatically scheduling a maintenance procedure to archive and reset the data store with the oldest data. If there are no data stores available, the collector optionally writes to SMF so that data is not lost.

There is no correct number of data stores. You determine the appropriate number based on the requirements at your site. The minimum number for automated maintenance is three. Three data stores provide:

- An active data store where the collector is currently writing, which will be somewhere between 0% and 100% full.
- The previously used data store, which will be 100% full.
- The next scheduled data store, which will be empty and initialized, ready to be used when the current data store becomes full.

This provides a minimum of one full data store of historical data and assumes that after each switch, the data store with the oldest data is archived and re-initialized. You can then add data stores as you gain experience with the collector's operation.

## Examples of chronological switching

Your data center may be asked to supply data to support some of your company's business functions such as capacity planning, service level reporting, and system performance problem resolution. Chronological switching (monthly, weekly, or daily) is used in these cases in addition to switching based on a full status, which always occurs if the active data store becomes full.

The following examples use chronological switching to support the business functions mentioned previously:

- For capacity planning, a minimum of 3 months' data is usually required to establish trends. The following two examples illustrate how you might store the required data:
  - Five data stores, switching monthly. Three will hold one month's data each; the fourth will be the active data store (the one currently being written to); the fifth will be available for next month.
  - Sixteen data stores, switching weekly. Fourteen will hold 1 week's data each; the fifteenth will be the active data store; the last will be available for next week.
- For service level reporting, a minimum of one month's data is usually required for management reporting. For example, you might store the required data in seven data stores, switching weekly. Five

will hold one week's data each; the sixth will be the active data store; the last will be available for next week.

- For performance problem resolution, a minimum of one week's data is usually required to analyze and detect problems occurring in the recent past. For example, you may use nine data stores, switching daily. Seven will hold one day's data each; the eighth will be the active data store; the last will be available for tomorrow.

If all 3 functions (capacity planning, service level reporting, and performance problem resolution) are performed at your data center, 16 data stores of 1 week each should be effective and efficient.

**Note:** Chronological switching causes the collector to initiate automatic data store switching when it detects data for a new time period (month, week, or day). However, because the historical data collector gathers data from multiple (possibly asynchronous) sources, a data store for a specific time period might contain some data from the last RMF interval of the previous time period.

# Providing automatic data store maintenance

Automatic data store maintenance supports uninterrupted historical data collection by ensuring that there is always a data store available to the historical data collector through an automated process. Automatic maintenance requires that multiple data stores be allocated and then defined to the collector as an ordered list.

The example in Table 17 on page 80 describes automatic maintenance on a system where the collector's data store list contains four data stores and automatic switching is initiated only when the current data store becomes full.

*Table 17. Automatic maintenance processing*

| **Triggering event** | **Result** |
|---|---|
| The collector starts for the first time. | The collector writes its data to the first data store in the datastore list. |
| The *first* data store becomes full. | The collector stops writing to the first data store and starts writing to the second data store. This process is called *switching*. |
| The *second* data store becomes full. | The collector switches to the third data store. |
| The *third* data store becomes full. | The collector switches to the fourth (last) data store in the ordered list. |
| The collector finishes switching to the *fourth* data store and detects that the next (first) data store is full. | The collector starts the automatic maintenance procedure, which archives, empties, and re-initializes the first data store so that it can be switched to when the fourth data store becomes full. |

As the example illustrates, automatic maintenance is triggered for the first time when the collector switches to the fourth data store in the list and detects that the next data store is full. Thereafter, each switch to the next data store causes automatic maintenance to be performed on the data store that contains the oldest data.

## Conditions that suppress automatic maintenance

Automatic maintenance is not triggered when it is likely to result in the premature maintenance of a data store.

The automatic maintenance procedure will not start if any of the following conditions exist:

- The switch was manual (operator-requested).
- The switch was to SMF.

- The switch was made out of sequence, that is, the collector skipped one or more data stores in order to find an available data store to write to.
- After the switch completed, the collector could not access the next data store to see if it required maintenance.

### Required authorizations

Before you begin the process of specifying an automatic maintenance procedure for your site, be sure that you have the required authorizations.

Be sure that you have the following authorizations:

- The maintenance procedure has access to the datastore and any other data sets that it uses.
- The KEPSTCTO program has been authorized by adding an AUTHPGM(KEPSTCTO) statement to SYS1.PARMLIB(IKJTSO*xx*).

  Before you can install this authorization, you must first modify IKJTSO*xx* by supplying the appropriate suffix. Once IKJTSO*xx* has been modified, you can dynamically authorize KEPSTCTO by issuing the following TSO command under ISPF:

  ```
  PARMLIB UPDATE(xx)
  ```

  where *xx* is the suffix of the IKJTSOxx member in SYS1.PARMLIB. (Authorization of KEPSTCTO can be accomplished through an IPL instead of dynamically as described here, if you choose to do so.) Secure the KEPSTCTO program.

## Monitoring the status of the data stores

Under ordinary circumstances, you do not need to monitor the status of a historical data store, since the data stores in the queue are being maintained by the automatic maintenance procedure you defined. However, there are special circumstances when you might want to monitor the status of a historical data store.

For example, consider the following situations:

- After historical data collection begins for the first time, you may want to monitor the space utilization of your data stores to verify that you chose the correct size.
- If there is a sudden increase in activity on your system, and your data store switching criterion is time-oriented, you may want to check that the active data store is not becoming full prematurely.

To display the status of all the data stores in the data store queue on the operator's console, enter the following MVS operator command:

```
MODIFY cccccccc,STATUS
```

where *cccccccc* is the started task name you specified for the historical data collector configuration (parameter KM2_EPILOG_COLLECTOR_STC in the configuration file). This command generates the Collector Status Display, which includes a numbered list of the historical data stores. The number reflects the order in which they will be used by the historical data collector.

Table 18 on page 81 describes the column headers in the Collector Status Display.

*Table 18. Column headers in Collector Status Display*

| Column heading | Description |
|---|---|
| (first column) | The position of the data store in the queue. |
| EDS STATUS | The status of each data store from the point of view of the collector. It is explained in more detail in Table 19 on page 82. |

*Table 18. Column headers in Collector Status Display (continued)*

| Column heading | Description |
|---|---|
| REASON | The reason that the collector switched from this data store. It is explained in more detail under SWITCHED and UNAVAILABLE in the table bellow. |
| UTIL | The percentage utilization of the data store. This value is based on the number of extents currently allocated to the data store. This percentage value will fluctuate as new extents are allocated. |
| SYSID | The SMFID of the system where the historical data was collected. |
| DATE RANGE | The historical data in this data store was collected in the time period shown. |

Table 19 on page 82 explains the values that can appear in the EDS STATUS column.

*Table 19. EDS STATUS column values*

| EDS status | Description |
|---|---|
| ACTIVE | This is the data store to which the historical data collector is currently writing. |
| AVAILABLE | This data store is available for writing by the collector, but is not currently being used. The collector changes the status of a data store from AVAILABLE to ACTIVE when it is selected for recording. |
| SWITCHED | The historical data collector has stopped writing to this data store. The cause is in the REASON column of the status display. The collector will not use this data store again until it has been made AVAILABLE (archived and initialized).<br>**FULL**<br>The automatic switch occurred because the active data store has run out of free space.<br>**MONTH**<br>The automatic switch occurred because you specified switching by month, and you have started a new calendar month.<br>**DAY**<br>The automatic switch occurred because you specified switching by day, and you have started a new day.<br>***day-of-week***<br>The automatic switch occurred because you specified switching by day-of-week, and you have started a new day-of-week.<br>**MANUAL**<br>The switch was done by the operator. |

Table 19. EDS STATUS column values (continued)

| EDS status | Description |
|---|---|
| UNAVAILABLE | This data store is not eligible for collection. The cause is in the REASON column of the status display:<br>**ALLOC**<br>The data store could not be allocated.<br>**OPEN**<br>The data store could not be opened.<br>**INVALID**<br>The data set organization, record format, key length, or record length is invalid; or the initialization record is missing.<br>**LRECL**<br>The VSAM maximum record size is incompatible with that of the other data stores in the queue.<br>**SYSCHECK**<br>The data store already contains data for another SYSID. |

## Adding a data store

The number of data stores in the list can remain static for long periods of time. However, you may occasionally need to increase the number of data stores.

For example, consider the following situations:

- Your site's historical reporting needs may change to require that you keep historical data online for a longer period of time than is possible with the current number of data stores in the data store list.

Keep the following requirements in mind when adding data stores:

- All data stores in the data store list must have the same record size. The record size is 32,700 bytes.
- Historical data stores cannot be shared among collectors. Each collector's data store list must be unique. However, the historical displays can read from any data store list.
- If two collectors are running on different systems, it is not advisable to place the two sets of data stores on the same volume.

Complete the following steps to add a data store:

1. Allocate the new datastore as follows:
   a. Edit CLIST KEPDEFEC in &*rhilev*.&*rte*.RKANCLI or batch job KEPDEFEJ in &*rhilev*.&*rte*.RKANCLI.

      These members contain definition and initialization steps to allocate a new datastore.
   b. Enter the new data store name in the definition and initialization steps as directed in the comments section of the member.
   c. Execute CLIST KEPDEFEC or submit job KEPDEFEJ to allocate the new data store.
2. Manually edit RKANPARU members KEPOPTN and KEPEDS to add the newly created data store.

   In KEPOPTN, add the eds name to the EDSLIST keyword. In KEPEDS add the eds name on a new line.

   If system variables are being used, you must follow the instructions in the KEP$PEDS and KEP$POPT override members in PARMGEN to add a new data store, instead of this manual procedure.
3. Make the new data store available as follows:
   - Stop and restart the started task for the historical data collector to make the new data store available to the collector.
   - Stop and restart the started task for the historical data interface to make the new data store available to the historical displays.

## Dropping a data store

Although the number of data stores in the data store list can remain constant for long periods of time, you may occasionally need to reduce the number of data stores in the list.

For example, consider the following situations:

- The initial number of data stores chosen when historical data collection was configured may be too high, and you may need to delete a data store as part of the customization of the product.
- Your system's VSAM storage constraints may increase, and you may be asked to reduce the amount of historical data that you keep online.

To drop a data store, complete the following steps:

1. Manually edit the &*rhilev*.&*rte*.RKANPARU KEPOPTN and KEPEDS members to remove the obsolete data stores.
2. Make the new data store lists available as follows:
    - Stop and restart the started task for the historical data collector to make the new data store available to the collector.
    - Stop and restart the started task for the historical data interface to make the new data store available to the historical displays.
3. Delete the data store using the IDCAMS DELETE command.

## Switching to another data store without stopping the collector

There are times when you want to stop the collector from writing to the active data store, but do not want to interfere with the data collection process. For example, if you determine that the active data store is too small, you may want to stop writing to it immediately so you can reallocate it and make it larger. You would like to accomplish this task without stopping the collector from writing data. You can achieve your goal by switching the writing of data to another datastore according to the instructions that follow.

When you perform a manual switch, you must also manually run the maintenance procedure against the switched data store.

To switch the active historical collector data store, enter the following MVS operator command:

```
MODIFY cccccccc,action
```

where:

**cccccccc**
Is the name of the name of the started task for the historical data collector.

**action**
Specifies what action is to be taken by the collector. The valid values are as follows:

**SWITCH**
Initiates a switch to the next available datastore in the datastore queue. If no other datastore is available, the collector will decide what to do next based on the option selected in the Datastore Switch and List pop-up window:

**SPILLSMF DATA**
Start writing to SMF

**SMFDATA**
Continue writing to SMF

**NOSMFD ATA**
Terminate

**SWITCH(*n*)**
Initiates a switch to the data store currently in the data store queue at position *n*, where *n* is a positive decimal integer representing the sequence number of a data store in the queue. The

sequence numbers of the data stores in the queue may be obtained from the collector status display.

**SWITCH(SMF)**
Requests the collector to stop data store recording and start or continue writing to SMF.

## Manually starting the maintenance procedure

Under ordinary circumstances, the historical data collector will start the maintenance procedure to archive and reset the next data store in the historical collector's data store queue. However, there are several conditions that will cause the collector to switch from the current data store without starting the maintenance procedure.

If any of the following conditions is in effect, you will have to start the maintenance procedure manually:

- The switch was manual (operator-requested).
- The data store activated by the switch was selected out of sequence; that is, the collector skipped one or more data stores in order to find a data store with the status of AVAILABLE.
- The data store that follows the active data store in the queue has a status other than SWITCHED.
- After the switch, the collector could not access the next data store to see if it required maintenance.

To manually start the maintenance procedure, enter the following MVS operator command:

```
START ccccccchp,EDSDSN= ‘datastore’,EDSVOL=volser
```

where:

**ccccchp**
Is the member name of your maintenance procedure. (cccccc is the 4–character applid prefix and 2–character product code you specified during configuration.)

**datastore**
Is the data set name of the data store to be maintained.

**volser**
Is the volume serial number of the DASD volume of the data store to be maintained.

## Recovering data from SMF

The historical detail and trend displays cannot access data from a sequential SMF file. If you need to use historical displays to analyze data that resides in an SMF file, you must first load the data to a historical datastore.

In the following procedure, do not identify the active data store as your target data store. You cannot restore data to a data store while the collector is writing to it.

To restore SMF data to a data store, perform the following steps:

1. Create a job similar to the one illustrated on the following page to extract SMF data and load selected records to a historical data store. There is also an example job in the KEPMAINT member in the &*rhilev*.&*rte*.RKANSAM data set.
2. Modify the IFASMFDP step of your job as follows:
   - Identify the SMF input data by modifying the parameters on the SMFDATA DD statement.
   - Identify the sequential output file that will hold the SMF data by modifying the parameters on the RKM2SMF DD statement.
   - Modify the SMF record type on the SYSIN DD statement if you specified an SMF record type other than 180 for the collector's records.
   - Modify the date selections on the SYSIN DD statement.
3. Modify the SORT step of your job as follows:

   - Modify column 7 to reflect the desired time in binary format.
   - Modify column 11 to reflect the desired date in *yyddd* format.
   - Modify column 15 to reflect the SYS ID.

4. Modify the KEBMAINT step of your job as follows:

   - Modify the high-level qualifiers on the STEPLIB, RKANPAR, and RKM2EDSX DD statements.
   - Identify the sequential input file that holds the SMF data on the RKM2SMF DD statement using the name you supplied in step 2.
   - Modify the LOAD statement or statements to select the SMF data to load to the historical datastore, according to the LOAD parameter table that follows in this section.

5. Submit your job to extract the SMF data and load it to a historical datastore.

## Sample job to load SMF data

This sample job reads data from an SMF archive tape and then loads the data to a historical datastore.

```
//LOAD JOB ...
//*
//******** Extract records from SMF.
//*
//SMF EXEC PGM=IFASMFDP
//SMFDATA DD DSN=smfdata,UNIT=TAPE,VOL=SER=vvvvvv,
// DISP=(OLD,KEEP)
//RKM2SMF DD DSN=smfwork,VOL=SER=wwwwww,
// DISP=(,CATLG),UNIT=SYSDA,SPACE=(CYL,(10,5))
//SYSPRINT DD SYSOUT=*
//SYSIN DD *
INDD(SMFDATA,OPTIONS(DUMP))
OUTDD(RKM2SMF,TYPE(41(3),70:78,180))
DATE(99218,99218) <---- Extract only data from Aug 6
START(0000)
END(2400)
/*
//******** Sort records from SMF before loading historical datastore.
//*
//SORTSTEP EXEC PGM=SORT,REGION=3M
//SORTIN DD DSN=sortin,DISP=SHR
//SORTOUT DD DSN=sortout,DISP=(NEW,PASS,DELETE)
// UNIT=work,SPACE=(CYL,(18,9),RLSE)
//SORTWK01 DD UNIT=work,SPACE=(CYL,(1,1))
//SORTWK02 DD UNIT=work,SPACE=(CYL,(1,1))
//SORTWK03 DD UNIT=work,SPACE=(CYL,(1,1))
//SORTWK04 DD UNIT=work,SPACE=(CYL,(1,1))
//SORTWK05 DD UNIT=work,SPACE=(CYL,(1,1))
//SYSPRINT DD SYSOUT=*
//SYSOUT DD SYSOUT=*
//SYSIN DD *
column 7 is the time in binary format.
column 11 is the date in yyddd format.
column 15 is the system id.
SORT FIELDS(15,4,CH,A,11.0,4,PD,A,7,4,BI,A)
/*
//******** Load records to historical datastore.
//*
//MAINT EXEC PGM=KEBMAINT,REGION=4096K,TIME=1440,
// PARM=’EPPROD=EP’
//STEPLIB DD DSN=rhilev.midlev.RKANMOD,DISP=SHR
//RKANPAR DD DSN=rhilev.midlev.RKANPAR,DISP=SHR
//RKM2EDSX DD DSN=zzzzzz.MVS,DISP=OLD
//RKM2SMF DD DSN=smfwork,VOL=SER=wwwwww,
// DISP=SHR,UNIT=SYSDA
//RKM2OUTM DD SYSOUT=*
//RKM2OUTR DD SYSOUT=*
//RKM2IN DD *
*
LOAD PGN(2) <--- Load only performance group 2 and
LOAD RALL <--- all resource data from Aug 6
/*
```

## LOAD statement syntax

The syntax of the LOAD statement is:

```
LOAD {workload|resource} -
    [time-period -
     SMF(nnn) -
     SYSID(cccc) -
     DUPRECORD(INSERT|SKIP) -
     EXCLUDE]
```

where:

***workload***

Is the workload type to load. Valid workload types are:

```
ACCOUNT CLASS JOBNAME
PERFGROUP PGPERIOD PROGRAM
REPTCLAS SERVCLAS
STARTTSK SYMBOLIC SYSTEM TSOUSER
```

Workload keywords are described in detail in the *IBM Z OMEGAMON Monitor for z/OS: EPILOG Command Reference*.

***resource***

Is the resource type to load. Valid resource types are:

```
RALL RCCH RCHN RCPU RDAS RDOM
RINF RLCU RPAG RPDS RPGN RSCL
RSDS RSRM RSWA RSWR RVLF
```

None of these resource keywords accepts operands on the LOAD statement. Resource keywords are described in detail in the *IBM Z OMEGAMON Monitor for z/OS: EPILOG Command Reference*.

***time-period***

Is the date-time range for the records to load. Values, in abbreviated form, are some combination of the following:

**BAND|RANGE**

BAND spans time between start time and end time of each day within the date range. RANGE spans time continuously from start time of start date to end time of end date. Use BAND or RANGE.

**DAY(*day day ...*)**

Days of week specified within parentheses.

**SDATE(*date*) EDATE(*date*)**

Start date and end date. Type dates in parentheses as *mm/dd/yy* or *yyddd*.

**STIME(*time*) ETIME(*time*)**

Start time and end time. Type times in parentheses as *hh:mm:ss*.

**LMONTH LWEEK LYEAR**

Last month, last week, or last year.

**TMONTH TWEEK TYEAR**

This month, this week, or this year.

**TDAY YDAY**

Today or yesterday.

**SMF(*nnn*)**

Specifies the SMF record type of the collector’s records. The default is 180 for workload degradation records.

**SYSID(*cccc*)**

Specifies the SMF system ID of the records to load. This keyword is required if input records:

- Have SMF system IDs different from the system on which you are running the job.
- Contain more than one SMF system ID.

The SYSID of the system on which your are running the job is the default.

**DUPRECORD (INSERT|SKIP)**

Prevents the job from terminating if a duplicate record is read. INSERT causes both records to be loaded. SKIP causes the first record to be loaded and the second to be skipped. Default: the job terminates.

**EXCLUDE**

Reverses the meaning of all keywords on the LOAD statement. All data is loaded to the data store except the data specified on the LOAD statement.

# Documentation library

This appendix contains information about the publications in the OMEGAMON XE library and about other publications related to IBM Z OMEGAMON Monitor for z/OS.

## OMEGAMON XE library

The following documents are available for OMEGAMON XE:

- *Program Directory GI13-5209-00*

  Contains information about the material and procedures associated with the installation of IBM Z Monitoring Suite. The Program Directory is intended for the system programmer responsible for program installation and maintenance.
- *Planning and Configuration Guide*

  Provides information that helps plan the deployment and configuration of IBM Z OMEGAMON Monitor for z/OS and the required common services component. It also provides detailed instructions for configuring product components. This document is intended for system administrators and others who are responsible for configuring IBM Z OMEGAMON Monitor for z/OS.
- *User's Guide*

  Introduces the features, workspaces, attributes, and predefined situations for the IBM Z OMEGAMON Monitor for z/OSS product and supplements the user assistance provided with this product. This document is written for data center operators and analysts responsible for monitoring and troubleshooting system performance and availability or performing trend analysis for resource planning.
- *Parameter Reference*

  Provides names and descriptions for all IBM Z OMEGAMON Monitor for z/OS configuration parameters.
- *Troubleshooting Guide*

  Provides explanations for the messages issued by the IBM Z OMEGAMON Monitor for z/OS product. This book also provides troubleshooting advice for installation and configuration, security, and usage problems, and instructions for setting up tracing on z/OS.
- *OMEGAMON for MVS User's Guide*

  Describes the features and commands used in OMEGAMON for MVS. Reference information for OMEGAMON major and minor commands is included by functional area, along with a description of the following features: User Profile Facility, Exception Analysis, CSA Analyzer, Bottleneck Analysis, DEXAN, Impact Analysis, Workload Profile Facility.
- *OMEGAMON for MVS Command Reference*

  Contains complete descriptions of OMEGAMON for MVS commands, organized alphabetically by command name. Includes a chapter on “Command Groupings” that is an introduction organized by topic (exception analysis, hiperspace, paging, and so on) where you can refresh your memory as to the proper spelling of a command or keyword.
- *EPILOG User's Guide*

  Describes the basic reporting features of EPILOG for MVS. The introduction provides a product overview and a discussion of the EPILOG approach to performance management. The rest of the manual explains how to use the reporter, including the various types of reports and the use of the DISPLAY command. Topics such as advanced reporting options, the Workload Profile Facility, exception filtering, and exporting historical data are also documented.
- *EPILOG Command Reference*

  Contains complete descriptions of EPILOG for MVS commands, organized alphabetically by command name.

© Copyright IBM Corp. 2022

## IBM Z Monitoring Suite and Tivoli Management Services on z/OS common library

The shared documentation covers installing, planning, and configuration topics common to all the OMEGAMON products. The documentation is available on the IBM Knowledge Center at http://www.ibm.com/support/knowledgecenter/SSAUBV/welcome.

## IBM Tivoli Monitoring library

The publications in this library provide information about the components of Tivoli Management Services (IBM Tivoli Monitoring) that are installed on distributed platforms.

- *Quick Start Guide*

  Introduces the components of IBM Tivoli Monitoring.
- *Installation and Setup Guide*, SC22-5445

  Provides instructions for installing and configuring IBM Tivoli Monitoring components on Windows, Linux, and UNIX systems.
- *High Availability Guide for Distributed Systems*, SC22-5455

  Gives instructions for several methods of ensuring the availability of the IBM Tivoli Monitoring components.
- *Administrator's Guide*, SC22-5446

  Describes the support tasks and functions required for the Tivoli Enterprise Portal Server and clients, including Tivoli Enterprise Portal user administration.
- *Command Reference*, SC22-5448

  Provides detailed syntax and parameter information, as well as examples, for the commands you can use in IBM Tivoli Monitoring.
- *Messages*, SC22-5450

  Lists and explains messages generated by all IBM Tivoli Monitoring components and by z/OS-based Tivoli Management Services components (such as Tivoli Enterprise Monitoring Server on z/OS, the OMEGAMON enhanced 3270 user interface, and TMS:Engine).
- *Troubleshooting Guide*, GC22-5449

  Provides information to help you troubleshoot problems with the software, including Tivoli Management Services on z/OS components.
- Tivoli Enterprise Portal online help

  Provides context-sensitive reference information about all features and customization options of the Tivoli Enterprise Portal. Also gives instructions for using and administering the Tivoli Enterprise Portal.
- *Tivoli Enterprise Portal User's Guide*, SC22-5447

  Complements the Tivoli Enterprise Portal online help. The guide provides hands-on lessons and detailed instructions for all Tivoli Enterprise Portal features.
- *Agent Builder User's Guide*, SC32-1921

  Explains how to use the Agent Builder for creating monitoring agents and their installation packages, and for adding functions to existing agents.
- *Tivoli Universal Agent User’s Guide*, SC32-9459

  Introduces you to the IBM Tivoli Universal Agent, an agent of IBM Tivoli Monitoring. The IBM Tivoli Universal Agent enables you to use the monitoring and automation capabilities of IBM Tivoli Monitoring to monitor any type of data you collect.
- *Performance Analyzer User’s Guide*, SC27-4004

Explains how to use the Performance Analyzer to understand resource consumption trends, identify problems, resolve problems more quickly, and predict and avoid future problems.

- *IBM Tivoli Universal Agent API and Command Programming Reference Guide*, SC32-9461

  Explains the procedures for implementing the IBM Tivoli Universal Agent APIs and provides descriptions, syntax, and return status codes for the API calls and command-line interface commands.

## Other sources of documentation

You can also obtain technical documentation about Tivoli Monitoring and OMEGAMON products from the following sources:

- IBM Tivoli Integrated Service Management Library

  http://www.ibm.com/software/brandcatalog/ismlibrary/

  The Integrated Service Management Library is an online catalog that contains integration documentation as well as other downloadable product extensions. This library is updated daily.
- Redbooks®

  http://www.redbooks.ibm.com/

  IBM Redbooks, Redpapers, and Redbooks Technotes provide information about products from platform and solution perspectives.
- Technotes

  You can find Technotes through the IBM Software Support Web site at http://www.ibm.com/software/support/probsub.html, or more directly through your product Web site, which contains a link to Technotes (under **Solve a problem**).

  Technotes provide the latest information about known product limitations and workarounds.

# Accessibility

Accessibility features help users with physical disabilities, such as restricted mobility or limited vision, to use software products successfully. OMEGAMON monitoring products support several user interfaces. Product functionality and accessibility features vary according to the interface.

The major accessibility features in this product enable users in the following ways:

- Use assistive technologies, such as screen-reader software and digital speech synthesizer, to hear what is displayed on the screen. Consult the product documentation of the assistive technology for details on using those technologies with this product.
- Operate specific or equivalent features using only the keyboard.
- Magnify what is displayed on the screen.

In addition, the product documentation was modified to include the following features to aid accessibility:

- All documentation is available in both HTML and convertible PDF formats to give the maximum opportunity for users to apply screen-reader software.
- All images in the documentation are provided with alternative text so that users with vision impairments can understand the contents of the images.

## Interface information

The Tivoli Enterprise Portal interface offers the greatest range of functionality, but is not entirely accessible. The OMEGAMON enhanced 3270 user interface offers more limited functionality, but is entirely accessible. (The enhanced 3270 user interface supports all the accessibility features supported by your emulator. If you are using IBM Personal Communications, you can find information on its accessibility features at http://www-01.ibm.com/support/knowledgecenter/SSEQ5Y_6.0.0/com.ibm.pcomm.doc/books/html/quick_beginnings10.htm. If you are using a third-party emulator, see the documentation for that product for accessibility information.)

The OMEGAMON ("classic") interface uses an ISPF style interface. Standard and custom PF Key settings, menu options, and command-line interface options allow for short cuts to commonly viewed screens. While basic customization options allow for highlights and other eye-catcher techniques to be added to the interface, the customization options are limited.

## IBM and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility.

© Copyright IBM Corp. 2022

# Support information

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

**Online**
Go to the IBM Software Support site at http://www.ibm.com/software/support/probsub.html and follow the instructions.

**Troubleshooting Guide**
For more information about resolving problems, see the product's Troubleshooting Guide.

© Copyright IBM Corp. 2022

# Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law**:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX  78758    U.S.A.

© Copyright IBM Corp. 2022

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.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

# Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

# Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user’s user name for purposes of session management, authentication, and single sign-on configuration. These cookies cannot be disabled.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

# Glossary

**agent**
See *monitoring agent*.

**CA-Multi-Image Manager (MIM)**
MIM is a third-party product that uses the control file that is on a shared DASD to coordinate all the tape drive allocation requests.

**Common user access (CUA)**
A Systems Application Architecture® (SAA) specification that gives a series of guidelines describing the way information should be displayed on a screen, and the interaction techniques between users and computers. The OMEGAMON II for MVS interface conforms to CUA guidelines.

**component**
A separate product or feature of a product provided by IBM

**configuring**
Making a product operational by completing the configuration of the product using the PARMGEN method and completing the additional manual steps required.

**consolidated software inventory (CSI)**
A key-sequenced VSAM data set, used by SMP/E and logically divided into zones.

**CSI**
See *consolidated software inventory*.

**CUA**
See common user access.

**cumulative maintenance**
Maintenance through a given date that is customer approved.

**customizing**
Modifying the defaults for options and settings and other changes that reflect the needs of your site.

**ENQplex**
a group of z/OS images in two or more sysplexes under common enqueue management. A resource in one ENQplex is distinct from a resource having the same name in another ENQplex. Two or more sysplexes having the same ENQplex name share qname/rname resources.

**hub**
The Tivoli Enterprise Monitoring Server that has been designated to act as the focal point to which all Tivoli Enterprise Portal servers connect. A non-hub, or remote, Tivoli Enterprise Monitoring Server passes its collected data to the hub to be made available to clients, thereby creating an Enterprise-wide view.

**installing**
Loading the contents of the IBM product and maintenance.

**TMS:Engine**
A component of the Tivoli Management Services used for all z/OS-based Tivoli OMEGAMON XE products. It allows common portable “C” and “C++” based code to make platform independent system calls, allowing the Tivoli Enterprise Monitoring Server code to be compiled for and executed on z/OS as well as Windows and UNIX platforms.

**managed system name**
From the standpoint of IBM Z OMEGAMON Monitor for z/OS, sysplexes and systems are *managed systems*. In the Tivoli Enterprise Portal Navigator, managed systems are identified by *managed system names*.

Sysplex managed system names take the form *plexname*:MVS:SYSPLEX, where *plexname* is normally the true name of the sysplex, but could be configured to be an alias for the sysplex.

System managed system names take the form *plexname*:*smfid*:MVSSYS, where *plexname* is normally the true name of the sysplex, but could be configured to be an alias for the sysplex.

© Copyright IBM Corp. 2022

**migrating**
Preserving the customized data so that you can use it in a newer version of the product.

**monitoring agent**
Component that monitors systems, subsystems, or applications on the system where they are installed.

**OMEGAMON II**
Component that collects and displays data in the OMEGAMON II user interface(s). These include:

- The menu driven CUA interface that is IBM SAA/CUA compliant
- The facility that allows multiple OMEGAMON IIs to execute in the same address space and that communicates with all of them;
- The Common Interface (CI) for some OMEGAMON IIs, the command driven Classic interface z/OS

**OMEGAMON subsystem**
Component that is a z/OS subsystem running in its own address space, that enables OMEGAMON IIs running in other address spaces to monitor dynamic device activity.

**PDS**
See persistent data store.

**persistent data store (PDS)**
Component that records and stores historical data.

**presentation files**
Installed with the Server, presentation.dat and presentation.idx store the workspace definitions, link definitions, and terminal emulator scripts.

**preventive maintenance**
Fixes that can be applied to avoid known problems

**Resource Measurement Facility (RMF)**
An IBM licensed program or optional element of z/OS that measures selected areas of system activity and presents the data collected in the format of printed reports, System Management Facility (SMF) records, or display reports. RMF is used to evaluate system performance and identify reasons for performance problems.

**runtime environment**
A group of runtime libraries that provide an operational environment on a z/OS system.

**runtime libraries**
Libraries in the runtime environment that are used by the product when the product is started.

**remote**
A Tivoli Enterprise Monitoring Server that reports to a central, or hub, monitoring server.

**seeding**
The process of seeding initializes the Tivoli Enterprise Monitoring Server and the Tivoli Enterprise Portal Server with application-specific data. Also known as installing agent support.

**sysplex proxy**
A Tivoli Enterprise Monitoring Server that acts as a data consolidation point for sysplex monitoring. Historical data for the sysplex is collected at the proxy, and sysplex situations are evaluated there.

**System Modification Program/Extended (SMP/E)**
An IBM licensed program used to install software and software changes on z/OS systems. In addition to providing the services of SMP, SMP/E consolidates installation data, allows more flexibility in selecting changes to be installed, provides a dialog interface, and supports dynamic allocation of data sets.

**target libraries**
SMP/E controlled libraries that contain the data from the distribution media.

**Tivoli Enterprise Portal**
The Java-based graphical user interface used to display and work with data provided by the monitoring products.

**Tivoli Enterprise Portal Server**

A collection of software services for the Tivoli Enterprise Portal that enables retrieval, manipulation and, analysis of data from the monitoring agents running on systems in your enterprise. The Tivoli Enterprise Portal Server connects to the hub Tivoli Enterprise Monitoring Server.

**Tivoli Enterprise Monitoring Server**

The component of the Tivoli Management Services that:

- Consolidates the data collected by the monitoring agents and distributes the data to the Tivoli Enterprise Portal.
- In some cases, receives commands from the Tivoli Enterprise Portal and distributes them to the appropriate agent or OMEGAMON XE product
- Stores historical data and prototypes for configuration in the form of seed data

**Tivoli Data Warehouse**

A long-term data store for the performance and analysis data collected by monitoring agents. The warehoused data is written to a Microsoft SQL Server relational database. You can view the data stored in the warehouse in CandleNet Portal workspaces, or use third-party analysis and reporting tools on it.

**Tivoli Management Services**

The infrastructure shared by OMEGAMON XE, IBM Tivoli Monitoring and other products, whose components include Tivoli Enterprise Portal desktop client, Tivoli Enterprise Portal Server, Tivoli Enterprise Monitoring Server, and Tivoli Data Warehouse.

**warehouse proxy agent**

A process that periodically moves data from the binary history files maintained at the Tivoli Enterprise Monitoring Server or monitoring agent to the warehouse.

**Workload Profiling Facility (WPF)**

A feature of OMEGAMON II for MVS that creates profiles of averaged historical performance data using the workloads and selection criteria that you specify. WPF then saves the information so you can later use it to create reports and make comparisons of past and present performance.

# Index

IBM®