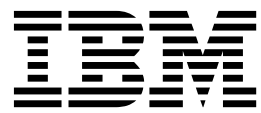


*OMEGAMON for Storage on z/OS
Planning and Configuration Guide*



*OMEGAMON for Storage on z/OS
Planning and Configuration Guide*



Contents

About this guide	v	Chapter 8. Upgrading to version 5.1.0	33
Chapter 1. Planning for deployment.	1	Chapter 9. Upgrading to version 5.2.0	35
Product overview	1	Chapter 10. Upgrading to version 5.3.0	37
Configuring Realtime Data Set Metrics Web Viewer	1	Chapter 11. Upgrading to version 5.4.0	39
Stages of planning, installation, and configuration	3	Chapter 12. Upgrading to version 5.5.0	41
Overview of prerequisites	4	Chapter 13. Appendix A. Creating a presentation address space for OMEGAMON II for SMS	43
Planning security	5	Chapter 14. Appendix B. Forwarding events to other Tivoli products	45
AT/TLS Configuration	5	Obtaining and activating the ks3.baroc file	45
Storage Toolkit.	8	Relation of *.baroc files and *.map files	46
Storage Agent	9	Chapter 15. Appendix C. Configuring the collection and display of historical data	49
OMEGAMON II for SMS.	10	Mechanisms for collecting historical data	49
Other considerations	18	Short-term history and long-term history	49
Chapter 2. Configuring common z/OS components	19	Table of metrics regarding the persistent data store	50
Step 1: Configuration using PARMGEN	19	Chapter 16. Appendix D. Documentation library	63
Step 2: Setting up a runtime environment	19	OMEGAMON for Storage library	63
Step 3: Configuring the Tivoli Enterprise Monitoring Server	19	OMEGAMON and Tivoli Management Services on z/OS common library	63
Chapter 3. Configuring Tivoli OMEGAMON for storage on z/OS	21	IBM Tivoli Monitoring Library	64
Chapter 4. Additional steps	23	Related publications	64
Chapter 5. Configuring Realtime Data Set Metrics Web Viewer	25	Other sources of documentation	65
Chapter 6. Upgrading from version 4.1.0 to version 4.2.0.	27	Chapter 17. Support information.	67
Chapter 7. Upgrading to version 4.2.0 Interim Features 1 and 2	29	Using IBM Support Assistant	67
Setting the historical configuration collection interval.	29	Obtaining fixes	68
Upgrading to version 4.2.0 Interim Feature 1	29	Obtaining PTFs (Program Temporary Fixes)	69
Data collection restrictions	30	Receiving weekly support updates	69
Upgrading to version 4.2.0 Interim Feature 2	30	Contacting IBM Software Support	70
Data collection restrictions	31	Determining the business impact	71
Migrating user DASD group definitions	31	Describing problems and gathering information	71
		Submitting problems	71
		Chapter 18. Notices	73
		Trademarks	74
		Index	75

About this guide

This guide provides specific configuration information regarding IBM IBM OMEGAMON for Storage on z/OS.

Find the common documents that provide planning and configuration information that applies to all monitoring agents, including IBM OMEGAMON for Storage on z/OS on http://www.ibm.com/support/knowledgecenter/SSAUBV/com.ibm.omegamon_share.doc_6.3.0.2/welcome.

Users of this book need to be familiar with the following topics:

- The IBM z/OS operating system
- Performance monitoring concepts
- TCP/IP and VTAM

The document assumes no previous experience with OMEGAMON products or with IBM Tivoli Monitoring. To learn about this family of products access the documentation at <http://www-306.ibm.com/software/tivoli/solutions/availability/products.html>.

If you are configuring multiple OMEGAMON agents at one time, you can do the configurations at the same time. Follow the instructions that are provided in the common documents at http://www.ibm.com/support/knowledgecenter/SSAUBV/com.ibm.omegamon_share.doc_6.3.0.2/welcome.

Chapter 1. Planning for deployment

Find topics describing how to plan deployment at http://www.ibm.com/support/knowledgecenter/SSAUBV/com.ibm.omegamon_share.doc_6.3.0.2/welcome.

The following topics describe issues that are unique or that deserve special attention for OMEGAMON for Storage:

- Product overview
- Stages of planning, installation, and configuration
- Overview of prerequisites
- Planning security

Product overview

IBM OMEGAMON for Storage on z/OS is a monitoring agent that runs in a z/OS environment. The product helps you anticipate storage-related performance, availability, and space problems and warns you when critical events take place on your systems. The product assists you in monitoring, analyzing, and managing I/O subsystems and storage devices, including the interaction of those resources with other software applications. With OMEGAMON for Storage, you can set threshold levels as needed to alert you when the conditions reach critical points.

The OMEGAMON for Storage monitoring agent uses the IBM Tivoli Management Services infrastructure, which consists of a set of components that are common to all the products in the OMEGAMON product suite. Some components of the infrastructure, such as the Tivoli Enterprise Portal, must run on systems other than z/OS. In other words, the components must run on Windows, Linux, or UNIX-based systems, also called distributed systems. The Tivoli Enterprise Monitoring Server can run on either a distributed or a z/OS system.

Configuring Realtime Data Set Metrics Web Viewer

This topic discusses prerequisites and other information related to installing the Realtime Data Set Metrics Web Viewer in OMEGAMON for Storage version 5.5.0.

Requirements

Prerequisites

z/OS Requirements

- All OMEGAMON for Storage beta content must be installed, including TEP/TEPS application support.
- Node.js runtime v6.14.x or higher. The trial version can be obtained from <https://developer.ibm.com/node/sdk/ztp/>.
- zFS directory (allocation = 100MB)
- SAF credentials are required to login to the web UI

PC Requirements

- Your default browser must be Chrome v54 or later or Firefox v44 or later.

Target System Selection

The RDM schedule and other options will be defined for a single Storage agent within a PLEX. This is done by the application admin or storage admin using the TEP or e3270 UI.

The system holding that information is referred to as the controlling system. A single instance of the RDM Web UI must be installed and configured on the controlling system.

zFS RDM Install Directory We recommend using the following PARMGEN parameters to build your zFS directory path. This will allow future maintenance to be deployed via PARMGEN.

These parameters can be found in your WCONFIG PARMGEN member:

```
$RTE_USS_RTEDIR  
$RTE_NAME
```

Using those parms, create a directory named: \$RTE_USS_RTEDIR/\$RTE_NAME/KS3/rdm/

If RTE_USS_RTEDIR is /proj/itm and RTE_NAME is S3TMS99, then your full directory path would be: /proj/itm/S3TMS99/KS3/rdm/

Allocate this zFS directory with 100MB of space.

File permissions should be as follows:

```
Owner: rwx  
Group: rwx  
World: r-x
```

Group must have the same authorities as TEMS STC.

Expansion Instructions Log into USS and CD to <RDM install directory> Assuming your RTE HLQ is TDSMS.OMSTOR, use the following command to unpx the archive into the current directory:

```
px -r -px -pp -z -f "'/'TDSMS.OMSTOR.TKANDATV(KS3RDMZ)'"
```

Setup Instructions

Copy KS3APPNN and KS3APSNN members from RTE dataset TKANSAM to system PROCLIB.

- Change the prefix as needed so that it matches the other OM Storage STCs.
- Use 'NN' or other parts to define a unique identifier, as needed.
- Both started tasks should have the same authorizations as the TEMS STC. If you are using a different STC Owner from TEMS STC, then ensure there is an OMVS segment. Ensure that the default program for your OMVS segment is /bin/sh. This requirement will be removed in an upcoming PTF. Contact IBM support for a workaround if you are not able to change the default program.

Edit both members as follows:

- Set SYS, RHILEV as done for SUB and TMS procs by PARMGEN.
- Set PATH_TO_YOUR_APP_SERVER to be /proj/omstor.

Configuration Instructions

Copy TKANPAR(KS3AINIT) to RKANPARU and then edit as follows:

- Set NODE_HOME to the installation directory of Node.js
- Set AS_LISTENER_ADDR to an IP address that is accessible from your TEP users.

This will typically be the non-loopback address of the LPAR.

Performance Statement

The Realtime Data Set Metrics Web Viewer can support up to 10 users performing intensive investigation, based on the number of database traversals being executed per minute.

A database traversal occurs when the user pushes the “Run Query” button or the user clicks a column header to change sort. Highly selective filter/sort combinations, such as a complex dataset mask sorted by allocated tracks may result in slow response time. Navigating the results (via Page Next/Prev) does not result in a database traversal.

Realtime Data Set Metrics Web Viewer response times may increase as the number of simultaneous users increases, based on the size of the result set, and based on the filter/sort combinations in use. If the database traversal activity exceeds certain resource limits, the RDM REST server may reject some requests, and the user may need to come back when fewer users are on the system.

Stages of planning, installation, and configuration

Before you begin

About this task

Planning, installation, and configuration takes place in the following stages:

Procedure

1. Install product package, following instructions in the Program Directory. The OMEGAMON Products: Preinstallation Requirements and Instructions Technote contains a checklist of requirements and instructions for preinstallation tasks common to OMEGAMON products and Tivoli Management Services components being installed on z/OS. See Appendix D: Documentation library, for information on accessing Technotes. You can search the Tivoli Support Web site for "preinstallation requirements," or find the Technote at <http://www-01.ibm.com/support/docview.wss?uid=swg21318692>.
2. Read the Planning, Installing, and Configuring topics at http://www.ibm.com/support/knowledgecenter/SSAUBV/com.ibm.omegamon_share.doc_6.3.0.2/welcome, then configure the Tivoli Enterprise Monitoring Server using the Parameter Generator (PARMGEN) Workflow tool.
3. For additional specific installation instructions regarding components of IBM Tivoli Monitoring, follow the instructions in the Installation and Setup Guide at http://www.ibm.com/support/knowledgecenter/SSTFXA_6.3.0.2/com.ibm.itm.doc_6.3fp2/install/itm_install.htm.
4. Configure OMEGAMON for Storage using the Parameter Reference and PARMGEN.

What to do next

Support for the monitoring agent, in the form of application-specific data, is installed on the distributed infrastructure components from the CD. (The CD is also used to install application data onto a hub Tivoli Enterprise Monitoring Server on z/OS systems.)

The monitoring agent is installed on each z/OS system you want to monitor. You must install the monitoring agent in the same address space with a monitoring server.

Overview of prerequisites

Versions of all the required products are provided in the OMEGAMON for Storage product package.

The following documents provide details regarding the required software and hardware:

- A complete list of hardware and software prerequisites is located in the Program Directory.
- Prerequisites for the distributed IBM Tivoli Management Services components are located in the Program Directory.
- Prerequisites for the historical reporting components are located in the Planning and Configuration Guide.
- OMEGAMON platform version 350/360-based monitoring agents.
- OMEGAMON Version 4.1.0 monitoring agents.

Supported SAF products for a Tivoli Enterprise Monitoring Server on z/OS

Security on Tivoli Enterprise Monitoring Server on z/OS is based on password validation using the local operating system. You can use Resource Access Control facility (RACF), which is part of the z/OS operating system, or another SAF (security authorization facility) product to provide user authentication.

Supported versions of z/OS for the IBM OMEGAMON for Storage on z/OS

z/OS systems on which zSeries monitoring agents such as IBM OMEGAMON for Storage on z/OS are installed must be running z/OS version 1 Release 8 or higher.

Supported hardware

Most of the hardware required to run IBM OMEGAMON for Storage on z/OS is determined by operating system considerations. For example, the requirements for the UNIX systems where parts of the IBM Tivoli Management Services are running is determined by the operating system. For most hardware prerequisites, consult the *IBM Tivoli OMEGAMON platform* documentation. The following prerequisite applies to IBM OMEGAMON for Storage on z/OS.

Requirements for z/OS systems where monitoring agents are deployed

IBM OMEGAMON for Storage on z/OS monitoring agents can be deployed on any z/OS environment that is capable of running z/OS version 1 Release 8 or higher.

You must also ensure that you have adequate disk space to accommodate the products you are installing. Before installing your OMEGAMON products, you must review the space requirements and considerations for an SMP/E installed environment to make sure that sufficient hard disk drive storage is available.

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 on the hard disk drive. Monitor your SMP/E CSI library regularly to determine how many splits have occurred and the amount of free space remaining using the Data Set Group facility of IBM OMEGAMON for Storage on z/OS. The User's Guide describes how to use the Data Set Group facility to monitor splits by defining a data set group and writing a situation for splits. To reorganize the CSI, use your site's approved utility and method for managing VSAM files. For more information about CSIs, see http://www.ibm.com/support/knowledgecenter/SSAUBV/com.ibm.omegamon_share.doc_6.3.0.2/welcome.

The newest releases of OMEGAMON products are expected to be installed into shared libraries. If you are installing from a product tape, the DOCFILE on the product tape includes member (DASDINFO) that contains detailed information on the product libraries. Be aware that those estimates presuppose that these products were installed as standalone applications. When multiple OMEGAMON products are installed into a shared CSI environment, hard disk drive requirements are less.

Planning security

AT/TLS Configuration

This document discusses how to configure your AT/TLS Policy Agent to provide secure communication between the different components that support the Data Set Metrics Web UI.

AT/TLS Configuration

Realtime Dataset Metrics has been enhanced with a Web UI. Follow the steps in this topic to enable TLS (HTTPS) communication between all components. This document discusses how to configure your AT/TLS Policy Agent to provide secure communication between the different components that support the Data Set Metrics web user interface:

Syntax Note

The syntax used in this document for referring to specific properties of specific rules uses a “dot” notation: <rule name>.<property> as in the following example TTLS rule.

```
TTLSRule KS3_RDM
{
  LocalAddr                127.0.0.1
  LocalPortRange           12345 (or any available port number)
  Direction                 Inbound
}
```

Jobname	S3TMSXXX (example)
Priority	4
TTLSTGroupActionRef	gAct1~KS3
TTLSEnvironmentActionRef	eAct1~KS3_SRV
TTLSTConnectionActionRef	cAct1~KS3_SRV

This topic will refer to the LocalPortRange property of this specific rule as

KS3_RDM.LocalPortRange

The rule names in the sample AT/TLS rules file were chosen to be unique, and therefore should not conflict with any rule names that you already have. If you are able to keep the same rule names in your AT/TLS parameters, then it should be easier to relate instructions in this topic with your AT/TLS rules.

Certificates/Keyrings

Create a keyring named KS3TRNG and generate or obtain a “cryptographic identity” (private key and corresponding certificate) and place it in that keyring. The App Server and OM Storage TEMS address spaces should run under the same userid (for example, KS3STC), and that user id needs access to the new keyring. If you use a different keyring name, then you must adjust the following parameter accordingly:

keyring~KS3.Keyring

Parameters to customize

***.priority**

This value should be changed to fit in with the priority numbering that is appropriate for your site. These rules are pretty specific, so it should be safe to set the Priority as “high” (for example, 128).

The example TLS Rules to follow are based on the default configuration values shipped with the product in the KS3AINIT parm member (RKANPARU). If you have not changed default values, then you should be able to use the example TLS Rules as-is. If you have made configuration changes, then adjust the following TLS values accordingly. In the list below, the parameter is in bold, with the value following each parameter.

- **KS3_RDM.LocalPortRange** RDM_PORT in KS3AINIT
- **KS3_RDM.Jobname** OM Storage TEMS job name defined by PARMGEN
- **KS3_APPSRV_TO_RDM.RemotePortRange** RDM_PORT in KS3AINIT
- **KS3_APPSRV.LocalPortRange** AS_PORT in KS3AINIT
- **KS3_APPSRV_TO_APPSRV.RemotePortRange** AS_PORT in KS3AINIT

Optional parameters to customize

The following values are given defaults and only recommended to be changed in KS3AINIT and in the corresponding TLS configuration if instructed to by support:

- **KS3_APPSRV_TO_RDM.RemoteAddr** RDM_LISTENER_ADDR in KS3AINIT
- **KS3_RDM.LocalAddr** RDM_LISTENER_ADDR in KS3AINIT
- **KS3_APPSRV_TO_APPSRV.RemoteAddr** Unlikely to need to be changed except to account for special network configurations on the host system

Example TLS Rules

```

TTLRule KS3_RDM
{
    LocalAddr 127.0.0.1
    LocalPortRange 12345
    Direction Inbound
    Jobname S3TMS95D
    Priority 4
    TLSGroupActionRef gAct1~KS3
    TLSEnvironmentActionRef eAct1~KS3_SRV
    TLSConnectionActionRef cAct1~KS3_SRV
}
TTLRule KS3_APPSRV_TO_RDM
{
    RemoteAddr 127.0.0.1
    RemotePortRange 12345
    Direction Outbound
    Priority 4
    TLSGroupActionRef gAct1~KS3
    TLSEnvironmentActionRef eAct1~KS3_CLIENT
    TLSConnectionActionRef cAct1~KS3_CLIENT
}
TTLRule KS3_APPSRV
{
    LocalPortRange 48700
    Direction Inbound
    Priority 4
    TLSGroupActionRef gAct1~KS3
    TLSEnvironmentActionRef eAct1~KS3_SRV
    TLSConnectionActionRef cAct1~KS3_SRV
}
TTLRule KS3_APPSRV_TO_APPSRV
{
    RemoteAddr 127.0.0.1
    RemotePortRange 48700
    Direction Outbound
    Priority 4
    TLSGroupActionRef gAct1~KS3
    TLSEnvironmentActionRef eAct1~KS3_CLIENT
    TLSConnectionActionRef cAct1~KS3_CLIENT
}
TLSGroupAction gAct1~KS3
{
    TLSEnabled On
    Trace 4
}
TLSEnvironmentAction eAct1~KS3_CLIENT
{
    HandshakeRole Client
    EnvironmentUserInstance 0
    TLSEnvironmentAdvancedParmsRef eAdv1~KS3
    TLSKeyringParmsRef keyring~KS3
    Trace 4
}
TLSEnvironmentAction eAct1~KS3_SRV
{
    HandshakeRole Server
    EnvironmentUserInstance 0
    TLSEnvironmentAdvancedParmsRef eAdv1~KS3
    TLSKeyringParmsRef keyring~KS3
    Trace 4
}
TLSConnectionAction cAct1~KS3_SRV
{
    HandshakeRole Server
    TLSCipherParmsRef cipher-KS3
    TLSConnectionAdvancedParmsRef cAdv1~KS3
}

```

```

        CtraceClearText      On
        Trace                4
    }
    TLSConnectionAction      cAct1~KS3_CLIENT
    {
        HandshakeRole        Client
        TTLS cipherParmsRef   cipher-KS3
        TLSConnectionAdvancedParmsRef cAdv1~KS3
        CtraceClearText      On
        Trace                4
    }
    TLSConnectionAdvancedParms cAdv1~KS3
    {
        ResetCipherTimer      0
        SecondaryMap          Off
    }
    TLSKeyringParms          keyring~KS3
    {
        Keyring               S3STC/KS3TRNG
    }
    TTLSEnvironmentAdvancedParms eAdv1~KS3
    {
        ClientAuthType        PassThru
        ApplicationControlled  Off
        SSLv2                 Off
        SSLv3                 Off
        TLSv1                 Off
        TLSv1.1               Off
        TLSv1.2               On
    }
    TTLS cipherParms          cipher-KS3
    {
        V3CipherSuites        TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
        V3CipherSuites        TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
        V3CipherSuites        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
        V3CipherSuites        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
        V3CipherSuites        TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
        V3CipherSuites        TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
        V3CipherSuites        TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        V3CipherSuites        TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    }
}

```

Storage Toolkit

The Storage Toolkit allows users to initiate z/OS commands from the Tivoli Enterprise Portal. There are some specific security settings that you must use:

About this task

In the following example scenario, a user is monitoring data sets in OMEGAMON for Storage workspaces and determines that certain data sets are wasting space:

Procedure

1. The user decides to release the unused space.
2. Using the Storage Toolkit dialog box, the user constructs a request to issue the **DFSMSdss RELEASE** command against the data sets. When the user clicks **OK**, the request is sent to the OMEGAMON for Storage monitoring agent.
3. The agent generates and submits a batch job to process the command.

What to do next

A user can submit requests to issue the following types of commands on the z/OS system where the monitoring agent runs:

- DFSMSdss (Device Support Services)
- DFSMShsm (Hierarchical Storage Manager)
- ICKDSF (Device Support Facilities)
- IDCAMS (Access Method Services)
- DFSMSrmm (DFSMS Removable Media Manager)
- Mainframe (z/OS console command)
- TSO (Time Sharing Option)

Additionally, a user can submit requests to execute user-defined JCL streams. All requests run as batch jobs on the z/OS system.

Tasks that the monitoring agent performs to satisfy a request are executed under a security environment established on the z/OS system where the monitoring agent runs. A security environment is created when a user submits a request and is destroyed when the request ends. The types of activities that are processed within the security context include these:

- Creating and accessing temporary data sets required by the batch job
- Submitting the batch job
- Accessing the JCL data set and other data sets that contain substitution variables (when processing user-defined JCL)

The security environment is unique to the user who submits the request, because the monitoring agent uses the portal user ID to establish the security environment. This approach requires that the user accounts (IDs) that are defined to the portal server match the mainframe IDs on the z/OS system where the monitoring agent runs. If a user attempts to submit a request when the portal ID is not also a valid mainframe user ID, the request fails.

You can create user accounts after you complete and validate the configuration. First, determine the mainframe IDs of your users. Then define user accounts with matching IDs to the portal server.

Also, to ensure the security of Storage Toolkit commands, some type of security authentication must govern the users who log on to the Tivoli Enterprise Portal. If you use a UNIX-based hub monitoring server, the user IDs on the monitoring server must exactly match, including case sensitivity, the user IDs on the z/OS system that hosts the monitoring agent.

Storage Agent

You must establish security authorization for the Tivoli Enterprise Monitoring Server, as defined in the DFSMSrmm product documentation. The TEMS started task must be authorized to issue the following RMM commands:

- **LISTCONTROL**
- **LISTOWNER**
- **SEARCHVOLUME**
- **SEARCHDATASET**
- **SEARCHVRS**

The TEMS started task must also have RACF CONTROL access to profile STGADMIN.EDG.LISTCONTROL in FACILITY class.

OMEGAMON II for SMS

OMEGAMON for Storage includes, as a component, OMEGAMON II for SMS. OMEGAMON for Storage relies on OMEGAMON II for SMS for some of the data that it presents in the Tivoli Enterprise Portal. You can also access OMEGAMON II for SMS using the OMEGAMON for Storage interface, which is based on the IBM Common User Access (CUA) standard. You must configure the OMEGAMON II for SMS component as part of the process of configuring OMEGAMON for Storage.

OMEGAMON II for SMS uses the persistent data store component for historical data collection and reporting. The data is presented through the CUA interface, which increases usability. You do not need to configure a historical data store for OMEGAMON II for SMS if you do not intend to use it to collect and report historical data.

The information in this section is provided to help you understand and perform the required configuration steps. If you want to customize and use the OMEGAMON II for SMS interface, see the OMEGAMON II for SMS User's Guide that is included on the OMEGAMON for Storage documentation CD.

Note: Be aware that the OMEGAMON II for SMS documentation has not been updated for this release. However, the information contained in these books is still valid.

OMEGAMON Subsystem component

The OMEGAMON Subsystem is a z/OS subsystem that enables OMEGAMON for Storage to monitor performance at the data set level. For example, OMEGAMON for Storage provides information about the number of I/Os to a volume and the response time for that volume (and all the components of that response time). The OMEGAMON Subsystem address space allows you to turn on data set-level monitoring in order to track each of those I/Os beyond the device level and to determine which data set on the device was targeted, while assigning the response time and I/O activity to the specific data set.

See the section "Data set monitoring: Reducing demand on system resources" in the IBM Tivoli OMEGAMON for Storage on z/OS: Tuning Guide for important information to help you avoid unnecessary CPU overhead in the subsystem address space.

Sharing the OMEGAMON Subsystem

The OMEGAMON Subsystem has the following system requirements:

- The OMEGAMON Subsystem requires 4K of ECSA (extended common service area, which is a major element of z/OS virtual storage above the 16MB line).
- The OMEGAMON Subsystem must be defined to z/OS as a subsystem.
- The initialization module, KCNDLINT, must be located in a link list authorized library. The DF initialization module is KDFSMAIN.
- An IPL is required to initialize the OMEGAMON Subsystem unless the keyword parameter form of the **IEFSSNxx PARMLIB** member is used. In this case, MVS dynamic SSI services can be started.

Note: The example for **IEFSSNxx**, a positional parameter, works as shown on z/OS systems. If you want to update SYS1.PARMLIB(IEFSSNxx) in accordance with IBM z/OS documentation, then use the following syntax:

```
SUBSYS                                SUBNAME(CNDL)

INITRTN(KCNDLINT)

INITPARM('SSPROC=CANSCN')
```

Starting the OMEGAMON Subsystem automatically

A sample OMEGAMON Subsystem procedure is created in the rhilev.RKANSAMU library during product configuration, where rhilev is the high-level qualifier for the runtime library. You can modify this procedure to fit your configuration standards, and then copy the procedure to a system procedure library.

If you want the OMEGAMON Subsystem address space to be started automatically at system IPL, then the name given to the JCL job stream must match the value of the SSPROC keyword in the **IEFSSNxx** member of SYS1.PARMLIB.

Determining whether or not to install the OMEGAMON Subsystem

You must upgrade from your current OMEGAMON Subsystem to the current version that is included with OMEGAMON for Storage. This upgrade ensures that new PTF maintenance is correctly installed. The latest version of the OMEGAMON Subsystem can be used with earlier versions of the OMEGAMON products.

If you have installed another OMEGAMON product at your site, at the same level as included with the OMEGAMON for Storage V4.2 product, you might have already installed the OMEGAMON Subsystem.

Determining the dispatching authority to use

The OMEGAMON Subsystem is a provider of services to other OMEGAMON products and must not be made to wait for CPU service.

- If you are running in compatibility mode, you might raise the JCL dispatching priority from (14,15). Do not lower it.
- If you are running in goal mode, JCL dispatching priority is ignored. Therefore, you must make sure that the OMEGAMON Subsystem is running at a service level that keeps it from waiting for CPU service.

Restarting Tivoli Subsystem, Tivoli Enterprise Monitoring Server, and OMEGAMON for Storage tasks

System programmers and Console Operators must ensure that the Tivoli Subsystem and Tivoli Enterprise Monitoring Server are started and restarted in the correct order.

Before you begin

If they start the Tivoli Enterprise Monitoring Server before they start the Tivoli Subsystem, the following error message is recorded in the Tivoli Enterprise Monitoring Server RKLVL0G file:

```
KDFD021E KDFDSCIN: DATASET COLLECTOR INITIALIZATION FAILED; SSRQ RC=8
S$$ERR=0 INIT RC=0
```

Furthermore, performance-related information at the data set level is not made available to Tivoli Enterprise Portal or OMEGAMON for Storage interfaces. Such information includes:

- Data set response time
- I/O system queue time
- Pend time
- Connect and disconnect times
- I/O per second

In the Tivoli Enterprise Portal, performance-related information at the data set level is displayed in the following locations:

- The Application Data Set Performance report
- The Data Set Performance Summary
- The Data Set Details workspace

If you decide to restart OMEGAMON for Storage, you must wait until the Tivoli Enterprise Monitoring Server starts before you log in. If the Tivoli Enterprise Monitoring Server has not started, an error message is displayed:

```
KDFAPT33 OMEGAMON II For SMS is unable to connect to CT/DSR
```

After the Tivoli Enterprise Monitoring Server starts, you can log in to the OMEGAMON for Storage interface.

About this task

Before you begin, you must access a z/OS console.

After you stop and restart the Tivoli Subsystem, you must restart the Tivoli Enterprise Monitoring Server.

Procedure

1. To start the Tivoli subsystem, type `s CANSCN`.
2. To start the Tivoli Enterprise Monitoring Server, type `s CANSDSST`.
3. Optional: To start OMEGAMON II, type `s CANSDF`. The order in which you restart OMEGAMON for Storage is unimportant. However, the Tivoli Enterprise Monitoring Server must start before you can log in to the OMEGAMON for Storage interface.

Setting security for OMEGAMON II for SMS

This section discussed the types of security for OMEGAMON II for SMS and ways to implement it.

Types of security

The following types of security are available for OMEGAMON for Storage

Security level	Description
Product-level	Provides user ID and password validation to detect and prevent unauthorized access to the OMEGAMON for Storage product.

Security level	Description
Command-level	Prevents the unauthorized use of sensitive OMEGAMON commands from OMEGAMON for Storage panels and by OMEGAMON users.

You must implement both product-level and command-level security. If you intend to use external product-level security for the Tivoli Enterprise Monitoring Server, you must select external product-level security also for OMEGAMON II for SMS.

Ways to implement security types

You can implement product-level security and command-level security in the following ways.

Security type	Description
Internal	This implementation uses the security included with OMEGAMON for Storage to control access at the product level (Network Access Method (NAM)) and the command level.
External	This implementation uses another security package, Resource Access Control facility (RACF), which is part of the z/OS operating system, or another system authorization facility (SAF) product. This alternate security package controls access at the product level and the command level.

External security: product level: Background about product level security

This section discusses the product level method of implementing external security. This method controls user access to OMEGAMON II for SMS using the resource rules of an external security package.

Product access

With product level external security, access to OMEGAMON II for SMS is assigned to users through the external security package using resource rules defined by the product administrator. If a user ID is not defined to the resource, the user is not allowed to log onto OMEGAMON II for SMS. If an unauthorized user attempts to log on, an error message appears and the user is denied access to the product.

Resource rules for users

You must write resource rules in your external security package to define authorized user IDs. The resource name is: OMIISMS@PRODUCT@ACCESS.

External security: access level: Background about access level security

This section discusses the access level method of implementing external security. This method controls user access to critical functions within OMEGAMON II for SMS by using resource rules to assign each user an authority level.

Authority levels

Access level external security uses the same authority levels that are used in internal security. The authority levels are: product administrator, storage administrator, and general user.

Assigning authorities to users

With access level external security, authority levels are assigned to users through the external security package using resource rules defined by the product administrator. Two resource classes are defined as:

- product administrator
- storage administrator

If a user ID is not defined in one of the previous resources, then the user defaults to a general user authority level. Access level external security disables the Assign Authority Level for User function on the User Authorities panel.

Assigning authorities to functions

With access level external security, you continue to use internal security for assigning authority levels to functions.

Resource rules for users

You must write resource rules in your external security package to define authorized user IDs. The resource name is: OMIISMS@PRODUCT@ACCESS.

External security: function level: Background about function level security

This section discusses the function level method of applying external security. This method controls access to critical functions within OMEGAMON II for SMS by assigning each function to a resource, and then defining the users with access to that resource.

Authority levels

Function level external security does not use the authority levels of the internal security structure to control access to critical functions. Instead, each controlled function is associated with a resource defined to the external security system as described in the following sections.

Assigning access to functions

With function level external security, you write the resource rules within the security package that define each OMEGAMON II for SMS critical function and the users with access to that function. You also write an access level rule to define the product administrator. Function level external security does not use authority levels for the controlled functions shown on the **Set Authority Levels for Functions** panel. However, some product administrator functions, such as site profile maintenance, are not defined in the function security resource list. These functions are controlled by the product administrator defined in the external security resource rules. Function level external security disables the User Authorities function on the **Options** pull-down.

Resource rules for functions

Each resource rule controls a function or a set of functions. Users are allowed to perform a controlled function only when they have access to the resource associated with the function. If you select function level external security, it is recommended that you define all resources in this set. A function cannot be controlled if it is not associated with a resource rule. The product administrator does not have access to the functions in the resource rules unless specifically designated. Any change to this set of resources takes effect immediately once it is visible to OMEGAMON II for SMS. For RACF, you can use this **MVS MODIFY** to refresh the resource list: F jobname,NAM RACLIST.

External security: resource tables:

Product level resource

If you are using product level external security, you must define a resource for the product access.

Table 1. Product level resources

Resource name	Authorization
OMIISMS@PRODUCT@ACCESS	Product access

Access level resources

If you are using access level external security, you must define a resource for the product administrator and storage administrator.

Table 2. Access level resources

Resource name	Authorization
OMIISMS@PRODUCT@ADMIN	Product administrator authority level
OMIISMS@STORAGE@ADMIN	Storage administrator authority level

A user defined as both a product administrator and a storage administrator is considered a product administrator.

Function level resources

If you are using function level external security, you must define the product level resource described in the product level table plus a resource for each function controlled by the external security package. Also, you must define a product administrator resource to allow a user to perform the product administrator functions not included in this resource table.

Table 3. Function level resources

Resource name	Authorization
OMIISMS@PRODUCT@ADMIN	Product administrator authority
OMIISMS@HSM@HR	Hold/Release HSM functions
OMIISMS@HSM@CANCEL	Cancel queued HSM requests
OMIISMS@HSM@COMMAND	Issue HSM commands
OMIISMS@HSM@ACTION	Initiate HSM volume actions
OMIISMS@HSM@DATASET	Initiate HSM data set actions

Table 3. Function level resources (continued)

Resource name	Authorization
OMIISMS@DFDSS@ACTION	Initiate DFSMSdss volume actions
OMIISMS@DFDSS@DATASET	Initiate DFSMSdss data set actions
OMIISMS@SYS@OPERATOR	Issue system operator commands
OMIISMS@COM@SETCACHE	Issue SETCACHE commands
OMIISMS@COM@LISTUSER	List users of a volume
OMIISMS@DEFINE@CHP	Define online channel path list
OMIISMS@DEFINE@CACHE	Define list of cached/DFW devices
OMIISMS@DEFINE@GROUP	Define user DASD groups to monitor
OMIISMS@DEFINE@APPL	Define applications to monitor

A user defined as both a product administrator and a storage administrator is considered a product administrator.

External security: defining for RACF:

About this task

To set up RACF rules to interface with OMEGAMON II for SMS, follow these steps.

Procedure

1. Update the resource class description table to define a class name using the ICHERCDE macro call. We recommend coding the ICHERCDE macro as follows:

```
ICHERCDE CLASS=classnme,
ID=nnn,
MAXLNTH=28,
FIRST=ALPHANUM,
OTHER=ANY,
POSIT=nnn,
DFTUACC=NONE
```

Values for *classnme* and *nnn* are determined by your installation. Additional operations for this macro may also be required at your installation.

2. Activate the newly defined resource class.

Defining product level resource rules:

Define resource rules to represent authorized user access.

Procedure

1. Define a resource that represents authorized users access using the **TSO RDEFINE** command and specifying the access level resource name previously in this section. RDEFINE classnme OMIISMS@PRODUCT@ACCESS UACC(NONE)
2. Grant product access to selected users. For example: PERMIT OMIISMS@PRODUCT@ACCESS CLASS (classnme) ID (userid) ACC (READ)

Defining access level resource rules:

Define resource rules to represent product and storage administrator access levels. These access levels can be used with OMEGAMON II for SMS internal security to determine if a particular function is accessible to a user.

Procedure

1. Define resources that represent product and storage administrator access levels using the **TSO RDEFINE** command and specifying the access level resource name listed previously in this section. RDEFINE classnme OMIISMS@PRODUCT@ADMIN
UACC(NONE)
RDEFINE classnme OMIISMS@STORAGE@ADMIN UACC(NONE)
2. Grant product and storage administrator authority to selected users. For example: PERMIT OMIISMS@PRODUCT@ADMIN CLASS (classnme) ID (userid) ACC (READ)

Defining function level resource rules:

Procedure

1. Specify the function level resource name listed previously in this section using the **TSO RDEFINE** command. Be sure to specify that only specific users may execute the function by setting UACC(NONE). RDEFINE classnme OMIISMS@PRODUCT@ADMIN UACC(NONE)
RDEFINE classnme OMIISMS@STORAGE@ADMIN UACC(NONE)
2. Define those users who can access the resource (execute the command) using the **PERMIT** command to give them READ access. For example: RDEFINE classnam OMIISMS@HSM@ACTION UACC(NONE) PERMIT OMIISMS@HSM@ACTION CLASS (classnme) ID (userid) ACCESS (READ)
3. Define the resource that represents product administrator access level using the **TSO RDEFINE** command and specifying the access level resource name listed previously in this section. RDEFINE classnme OMIISMS@PRODUCT@ADMIN UACC(NONE)
4. Grant product administrator authority to selected users. For example: PERMIT OMIISMS@PRODUCT@ADMIN CLASS(classnme) ID (userid) ACC (READ)

Recognizing a new RACF user:

When a new user is granted access, you must refresh the OMEGAMON II for SMS copy of the RACF resource list. To do this, use **MVS MODIFY** to issue a **NAM RACLIST** command.

Before you begin

For example:

```
F jobname,NAM RACLIST where jobname is the name of the OMEGAMON II
for SMS address space.
```

About this task

Alternatively, you can perform an OMEGAMON II for SMS recycle which is to:

Procedure

1. Stop all OMEGAMON II for SMS started tasks.
2. Restart all OMEGAMON II for SMS started tasks.

Results

This results in security updates being initialized, and external security now in effect.

Other considerations

OMEGAMON for Storage uses the IBM LSPACE service to collect information about DASD space and fragmentation.

This service places an exclusive enqueue on the volume VTOC when it runs. To avoid the possibility of leaving this enqueue on the VTOC if a severe error occurs during VTOC processing, the agent will force a U0001 abend of the subtask if it takes more than 15 seconds to complete. Typically, this operation completes in less than a second, however during periods of high volume activity (such as backups or disk copy operations) this limit can be exceeded even though there is no real problem. This abend is generated for the sole purpose of forcing LSPACE to release the enqueue. It does not indicate an actual problem and therefore the dump it generates is not needed.

To avoid capturing the dumps and incurring the CPU overhead required to take them, place the following SLIP trap in the IEASLPxx member of SYS1.PARMLIB.

```
SLIP SET, C=U0001,JOBNAME=tems_taskname,A=NOSVCD, ID=xxxx,END
```

The dump will be bypassed and the only indication of the abend will be in the EREP reports.

Chapter 2. Configuring common z/OS components

Before you configure the OMEGAMON for Storage on z/OS product, there are common components that must be configured.

- Step 1: Configuration using PARMGEN
- Step 2: Setting up a runtime environment
- Step 3: Configuring the Tivoli Enterprise Monitoring Server

Step 1: Configuration using PARMGEN

For configuration of the framework and common components, see the shared publications at http://www.ibm.com/support/knowledgecenter/SSAUBV/com.ibm.omegamon_share.doc_6.3.0.2/welcome.

Step 2: Setting up a runtime environment

For a description on how to perform this step, view the documents at http://www.ibm.com/support/knowledgecenter/SSAUBV/com.ibm.omegamon_share.doc_6.3.0.2/welcome. Furthermore, the “Planning your deployment” section in those topics helps you decide what types of runtime environments to set up.

Step 3: Configuring the Tivoli Enterprise Monitoring Server

Because the IBM OMEGAMON for Storage on z/OS monitoring agent is installed in the same address space as a monitoring server, you must configure a Tivoli Enterprise Monitoring Server on z/OS. In addition, the monitoring server must be configured from a monitoring agent.

Before you configure that monitoring server, you might want to review “Configuring your products,” which describes best practices that apply to the configuration of all products. This can be found at http://www.ibm.com/support/knowledgecenter/SSAUBV/com.ibm.omegamon_share.doc_6.3.0.2/welcome.

To configure the monitoring server on z/OS, see the Configuring TEMS manual, which describes how to perform this step. The sample product environment uses a hub monitoring server on z/OS.

Note: The SNA communication protocol must be enabled for the monitoring servers in an environment where IBM OMEGAMON for Storage on z/OS is installed. The Configuring TEMS manual includes descriptions of how to configure communication protocols. If a monitoring server is already installed when you set up OMEGAMON for Storage, you can add the SNA option to the server configuration at this time.

Chapter 3. Configuring Tivoli OMEGAMON for storage on z/OS

Configure IBM OMEGAMON for Storage on z/OS using the IBM OMEGAMON for Storage on z/OS Parameter Reference and the PARMGEN information located at http://www.ibm.com/support/knowledgecenter/SSAUBV/com.ibm.omegamon_share.doc_6.3.0.2/welcome.

Chapter 4. Additional steps

Other configuration activities include the following tasks:

- Adding application support. This step is not discussed further in the current document, but is described in the topics at http://www.ibm.com/support/knowledgecenter/SSAUBV/com.ibm.omegamon_share.doc_6.3.0.2/welcome.
- Reviewing the KDSENV member in your runtime environment's RKANPARU data set. The *KGL_GMMSTORE* and *KDS_HEAP_SIZE* environment variables must be included and assigned a value of 256, as follows:

```
KGL_GMMSTORE=256
```

```
KDS_HEAP_SIZE=256
```

Add or change them, as necessary.

- The OMEGAMON Subsystem must be started prior to the start of the TEMS on the same z/OS image. Once started, the OMEGAMON subsystem must not be stopped or cancelled prior to the termination of the TEMS address space on the same z/OS image. The subsystem JCL must be modified to meet your installation requirements so that it is not subject to time out. This may require that you modify the **TIM** parameter on the generated OMEGAMON subsystem JCL procedure.

Chapter 5. Configuring Realtime Data Set Metrics Web Viewer

This topic discusses prerequisites and other information related to installing the Realtime Data Set Metrics Web Viewer in OMEGAMON for Storage version 5.5.0.

Requirements

Prerequisites

z/OS Requirements

- All OMEGAMON for Storage beta content must be installed, including TEP/TEPS application support.
- Node.js runtime v6.14.x or higher. The trial version can be obtained from <https://developer.ibm.com/node/sdk/ztp/>.
- zFS directory (allocation = 100MB)
- SAF credentials are required to login to the web UI

PC Requirements

- Your default browser must be Chrome v54 or later or Firefox v44 or later.

Target System Selection

The RDM schedule and other options will be defined for a single Storage agent within a PLEX. This is done by the application admin or storage admin using the TEP or e3270 UI.

The system holding that information is referred to as the controlling system. A single instance of the RDM Web UI must be installed and configured on the controlling system.

zFS RDM Install Directory We recommend using the following PARMGEN parameters to build your zFS directory path. This will allow future maintenance to be deployed via PARMGEN.

These parameters can be found in your WCONFIG PARMGEN member:

```
$RTE_USS_RTEDIR  
$RTE_NAME
```

Using those parms, create a directory named: `$RTE_USS_RTEDIR/$RTE_NAME/KS3/rdm/`

If `RTE_USS_RTEDIR` is `/proj/itm` and `RTE_NAME` is `S3TMS99`, then your full directory path would be: `/proj/itm/S3TMS99/KS3/rdm/`

Allocate this zFS directory with 100MB of space.

File permissions should be as follows:

```
Owner: rwx  
Group: rwx  
World: r-x
```

Group must have the same authorities as TEMS STC.

Expansion Instructions Log into USS and CD to <RDM install directory>
Assuming your RTE HLQ is TDSMS.OMSTOR, use the following command to unpax the archive into the current directory:

```
pax -r -px -pp -z -f "'/'TDSMS.OMSTOR.TKANDATV(KS3RDMPZ)'"
```

Setup Instructions

Copy KS3APPNN and KS3APSNN members from RTE dataset TKANSAM to system PROCLIB.

- Change the prefix as needed so that it matches the other OM Storage STCs.
- Use 'NN' or other parts to define a unique identifier, as needed.
- Both started tasks should have the same authorizations as the TEMS STC. If you are using a different STC Owner from TEMS STC, then ensure there is an OMVS segment. Ensure that the default program for your OMVS segment is /bin/sh. This requirement will be removed in an upcoming PTF. Contact IBM support for a workaround if you are not able to change the default program.

Edit both members as follows:

- Set SYS, RHILEV as done for SUB and TMS procs by PARMGEN.
- Set PATH_TO_YOUR_APP_SERVER to be /proj/omstor.

Configuration Instructions

Copy TKANPAR(KS3AINIT) to RKANPARU and then edit as follows:

- Set NODE_HOME to the installation directory of Node.js
- Set AS_LISTENER_ADDR to an IP address that is accessible from your TEP users.

This will typically be the non-loopback address of the LPAR.

Performance Statement

The Realtime Data Set Metrics Web Viewer can support up to 10 users performing intensive investigation, based on the number of database traversals being executed per minute.

A database traversal occurs when the user pushes the “Run Query” button or the user clicks a column header to change sort. Highly selective filter/sort combinations, such as a complex dataset mask sorted by allocated tracks may result in slow response time. Navigating the results (via Page Next/Prev) does not result in a database traversal.

Realtime Data Set Metrics Web Viewer response times may increase as the number of simultaneous users increases, based on the size of the result set, and based on the filter/sort combinations in use. If the database traversal activity exceeds certain resource limits, the RDM REST server may reject some requests, and the user may need to come back when fewer users are on the system.

Chapter 6. Upgrading from version 4.1.0 to version 4.2.0

This section describes the actions to take if you want to upgrade a previous version of the product to Version 4.2.0 of IBM OMEGAMON for Storage on z/OS.

See the following topics for further information regarding upgrades:

http://www.ibm.com/support/knowledgecenter/SSAUBV/com.ibm.omegamon_share.doc_6.3.0.2/welcome.

The following table lists the actions that you should follow to ensure a successful upgrade of IBM OMEGAMON for Storage on z/OS. It is important to remember that you must load existing RTEs after an SMP/e installation.

Table 4. Upgrade activities for version 4.2.0 of the IBM OMEGAMON for Storage on z/OS

Step	Required?	Activity	Description
Upgrade Step 1 of 3 (Optional), Enable TS7700 Monitoring resources	No	Configure TS7700 Monitoring	If you want to monitor TS7700 resources, you must configure this feature.
Upgrade Step 2 of 3 (Required), Enable Storage Toolkit support	Yes	Configure Storage Toolkit	The Storage Toolkit must be configured to enable support in the 4.2.0 product.
Upgrade Step 3 of 3 (Required), Reregister and load components	Yes	Reregister and Load	This step must be followed to completion to ensure that the necessary configuration files are created.

Perform the actions listed in the previous table after you complete the product installation using the SMP/e program. You perform these actions using the IBM OMEGAMON for Storage on z/OS Parameter Reference and the PARMGEN information located at http://www.ibm.com/support/knowledgecenter/SSAUBV/com.ibm.omegamon_share.doc_6.3.0.2/welcome

Restart the Tivoli Enterprise Monitoring Server and the OMEGAMON for Storage interface so that your changes take effect.

Chapter 7. Upgrading to version 4.2.0 Interim Features 1 and 2

This section provides guidelines for setting the historical configuration collection interval, lists the new set of functions and enhancements that affect specific attributes groups and workspaces, and explains data collection restrictions when you upgrade to IBM OMEGAMON for Storage on z/OS Version 4.2.0 Interim Feature 1 or Interim Feature 2.

- If you upgrade to Interim Feature 1, see:
 - Setting the historical configuration collection interval
 - Upgrading to version 4.2.0 Interim Feature 1
- If you upgrade to Interim Feature 2, see:
 - Setting the historical configuration collection interval
 - Upgrading to version 4.2.0 Interim Feature 1
 - Upgrading to version 4.2.0 Interim Feature 2

IF2 is a cumulative upgrade that would include all sections for IF1 and IF2.

Setting the historical configuration collection interval

When collecting data for the affected attribute groups that are listed in the following sections for each interim feature, use the History Collection Configuration dialog box to set the collection interval to your Resource Monitoring Facility (RMF) collection interval. If the collection interval is set to a value smaller than the RMF interval, data is collected only on the RMF interval. If a collection interval is greater than the RMF interval, intervals of RMF data are missed.

Upgrading to version 4.2.0 Interim Feature 1

By using Interim Feature 1, you can take advantage of the powerful set of functions available in warehousing, summarization, and pruning of historical data.

This interim feature affects the following attribute groups:

- S3 Cache Control Unit
- S3 Channel Path
- S3 Logical Control Unit
- S3 Volume Group Summary

This capability extends the history from near-term to long-term history trending and management. To support this new functionality, you must reallocate the persistent datastore. The format of the attribute groups has changed. (For more information, see Defining function level resource rules.) You must delete or rename existing short-term persistent datastore data for OMEGAMON for Storage on z/OS and reallocate the persistent datastore by using the OMEGAMON for Storage Parameter Reference and the PARMGEN information located at http://www.ibm.com/support/knowledgecenter/SSAUBV/com.ibm.omegamon_share.doc_6.3.0.2/welcome. See the SYSMOD++HOLD data for more information.

While upgrading your OMEGAMON for Storage agents to Interim Feature 1, you might have pre-IF1 agents and IF1 agents in the same environment. During this migration period, the following workspaces on pre-IF1 agents are not supported:

- Channel Path Trend
- Cache CU Status Trend
- Cache CU Performance Trend
- Cache CU Destaging Trend
- Cache CU Staging Trend
- Cache CU DFW Retry Trend
- Cache CU Read Hit Percent Trend
- Cache CU Write Hit Percent Trend
- Logical Control Unit Trend
- SMS Storage Groups Performance Trend
- SMS Storage Groups Space Trend
- User DASD Groups Performance Trend
- User DASD Groups Space Trend

During this migration period, if you use the Time Span tool, the following workspaces on pre-IF1 agents are not supported:

- Channel Path
- Cache CU Status
- Cache CU Performance
- Logical Control Unit
- SMS Storage Groups Performance
- SMS Storage Groups Space
- User DASD Groups Performance
- User DASD Groups Space

These workspaces function correctly when each agent is upgraded to IF1.

Data collection restrictions

Do not use the History Collection Configuration dialog box to request history collection for the S3 Cache Control Unit, S3 Channel Path, S3 Logical Control Unit, or S3 Volume Group Summary attribute groups on pre-Interim Feature 1 agents (v420, v410, and v310). Doing so causes excessive error messages to be written to the RKLVLLOG member and can adversely affect spool space.

Upgrading to version 4.2.0 Interim Feature 2

By using Interim Feature 2, you can take advantage of the powerful set of functions available in warehousing, summarization, and pruning of historical data.

In addition to the changes indicated in Upgrading to version 4.2.0 Interim Feature 1, this interim feature affects the following attribute groups:

- S3 DASD Volume Performance
- S3 DASD Volume Space
- S3 Cache Devices
- S3 DASD Group Vol Perform
- S3 DASD Group Vol Space
- S3 DASD UDG Cache Devices

This capability extends the history from near-term to long-term history trending and management. To support this new functionality, you must reallocate the persistent datastore. (For more information, see Defining function level resource rules.) You must delete or rename existing short-term persistent datastore data for OMEGAMON for Storage on z/OS and reallocate the persistent datastore by using the OMEGAMON for Storage Parameter Reference and the PARMGEN information located at http://www.ibm.com/support/knowledgecenter/SSAUBV/com.ibm.omegamon_share.doc_6.3.0.2/welcome. See the SYSMOD++HOLD data for more information.

During this migration period, if you use the Time Span tool, the following workspaces on pre-IF2 agents are not supported:

- Cache CU Volume DFW Retry History
- Cache CU Volume Read Hit Percent History
- Cache CU Volume Write Hit Percent History
- User DASD Group Volume Historical Cache
- User DASD SMS Storage Group Historical Volume Performance
- User DASD Group Volume Historical Space
- Volume Cache History
- Volume Destaging History
- Volume Group Space History
- Volume Staging History

Data collection restrictions

Do not use the History Collection Configuration dialog box to request history collection for the S3 DASD Volume Performance, S3 DASD Volume Space, S3 Cache Devices, S3 DASD Group Vol Perform, S3 DASD Group Vol Space, or S3 DASD UDG Cache Devices attribute groups on pre-Interim Feature 2 agents (v420, v420 IF1, v410, and v310). Doing so causes excessive error messages to be written to the RKLVLLOG member and can adversely affect spool space.

Note: When using volume level history you can consume considerable disk space in the persistent data store and Tivoli Data Warehouse. See Defining function level resource rules for more information.

Migrating user DASD group definitions

Existing user DASD groups are not visible until you migrate the DASD groups. See Chapter 13 in the User's Guide for more information on migrating user DASD group definitions.

Chapter 8. Upgrading to version 5.1.0

This section provides the steps necessary to upgrade to OMEGAMON for Storage Version 5.1.0.

- If you have installed version 4.2.0 Interim features 1 and 2, then you have no additional configuration steps to perform.
 1. Perform the install of version 5.1.0.
 2. Load the Run Time Environments (RTEs) to upgrade the parameters and executables.
 3. Restart the STCs
- If you have not installed version 4.2.0 Interim features 1 and 2, then you must perform a reconfiguration of OMEGAMON for Storage by following the steps beginning in Chapter 2, Configuring common z/OS components.
- If you want to use the E3270 interface, then you must configure that component through the PARMGEN configuration.

Chapter 9. Upgrading to version 5.2.0

This section provides the steps necessary to upgrade to OMEGAMON for Storage Version 5.2.0.

- If you have installed version 5.1.0, then you have no additional configuration steps to perform.
 1. Perform the install of version 5.2.0.
 2. Load the Run Time Environments (RTEs) to upgrade the parameters and executables.
 3. Restart the STCs.
- If you have installed version 4.2.0 Interim Features 1 and 2, then you have no additional configuration steps to perform.
 1. Perform the install of version 5.2.0.
 2. Load the Run Time Environments (RTEs) to upgrade the parameters and executables.
 3. Restart the STCs.
- If you have not installed at least version 4.2.0 Interim Features 1 and 2, then you must perform a reconfiguration of OMEGAMON for Storage by following the steps beginning in Chapter 2, Configuring common z/OS components.
- If you want to use the E3270 interface, then you must configure that component through the PARMGEN configuration.

Chapter 10. Upgrading to version 5.3.0

This section provides the steps necessary to upgrade to OMEGAMON for Storage Version 5.3.0.

If you already have an existing version of OMEGAMON for Storage:

Modify your TEMS started task JCLs in your production proclib to include the following DD statement: DD RKS3IDC0 DUMMY before continuing.

- If you have installed version 5.2.0, then you have no additional configuration steps to perform.
 1. Perform the install of version 5.3.0.
 2. Load the Run Time Environments (RTEs) to upgrade the parameters and executables.
 3. Restart the STCs
- If you have installed version 5.1.0, then you have no additional configuration steps to perform.
 1. Perform the install of version 5.3.0.
 2. Load the Run Time Environments (RTEs) to upgrade the parameters and executables.
 3. Restart the STCs
- If you have installed version 4.2.0 Interim features 1 and 2, then you have no additional configuration steps to perform.
 1. Perform the install of version 5.3.0.
 2. Load the Run Time Environments (RTEs) to upgrade the parameters and executables.
 3. Restart the STCs
- If you have not installed at least version 4.2.0 Interim features 1 and 2, then you must perform a reconfiguration of OMEGAMON for Storage by following the steps beginning in Chapter 2, Configuring common z/OS components.
- If you want to use the E3270 interface, then you must configure that component through the PARMGEN configuration.

Chapter 11. Upgrading to version 5.4.0

This section provides the steps necessary to upgrade to OMEGAMON for Storage Version 5.4.0.

If you already have an existing version of OMEGAMON for Storage:

If the TEMS running OMEGAMON for Storage on z/OS is on a z/OS image of 2.1 or higher, then persistent data store (PDS) V2 is automatically used instead of the original PDS. See Short-term history and Persistent Data Store V2 for more information. It is strongly recommended that the PDS V2 data sets be placed into an SMS data class that contains the Extent Constraint Relief attribute. You must do this using the SMS ACS routines. This allows the PDS to grow based on the amount of storage required to contain the attribute groups that have been designated for historical collection. These data sets have a name with the low-level qualifier beginning with an "H," for example, `hlq.xxxxx.H *`.

- If you have installed version 5.3.0, then you have no additional configuration steps to perform.
 1. Perform the install of version 5.4.0.
 2. Load the Run Time Environments (RTEs) to upgrade the parameters and executables.
 3. Restart the STCs
- If you have installed version 5.2.0, then you have no additional configuration steps to perform.
 1. Perform the install of version 5.4.0.
 2. Load the Run Time Environments (RTEs) to upgrade the parameters and executables.
 3. Restart the STCs
- If you have installed version 5.1.0, then you have no additional configuration steps to perform.
 1. Perform the install of version 5.3.0.
 2. Load the Run Time Environments (RTEs) to upgrade the parameters and executables.
 3. Restart the STCs
- If you have installed version 4.2.0 Interim features 1 and 2, then you have no additional configuration steps to perform.
 1. Perform the install of version 5.3.0.
 2. Load the Run Time Environments (RTEs) to upgrade the parameters and executables.
 3. Restart the STCs
- If you have not installed at least version 4.2.0 Interim features 1 and 2, then you must perform a reconfiguration of OMEGAMON for Storage by following the steps beginning in Chapter 2, Configuring common z/OS components.
- If you want to use the E3270 interface, then you must configure that component through the PARMGEN configuration.

Chapter 12. Upgrading to version 5.5.0

This section provides the steps necessary to upgrade to OMEGAMON for Storage Version 5.5.0.

If you already have an existing version of OMEGAMON for Storage:

Modify your TEMS started task JCLs in your production proclib to include the following DD statement: DD RKS3IDC0 DUMMY before continuing.

- If you have installed version 5.2.0 or later, then you have no additional configuration steps to perform.
 1. Perform the install of version 5.5.0.
 2. Load the Run Time Environments (RTEs) to upgrade the parameters and executables.
 3. Restart the STCs
- If you have installed version 5.1.0, then you have no additional configuration steps to perform.
 1. Perform the install of version 5.5.0.
 2. Load the Run Time Environments (RTEs) to upgrade the parameters and executables.
 3. Restart the STCs
- If you have installed version 4.2.0 Interim features 1 and 2, then you have no additional configuration steps to perform.
 1. Perform the install of version 5.5.0.
 2. Load the Run Time Environments (RTEs) to upgrade the parameters and executables.
 3. Restart the STCs
- If you have not installed at least version 4.2.0 Interim features 1 and 2, then you must perform a reconfiguration of OMEGAMON for Storage by following the steps beginning in Chapter 2, Configuring common z/OS components.
- If you want to use the E3270 interface, then you must configure that component through the PARMGEN configuration.

Realtime Dataset Metrics

OMEGAMON for Storage version 5.5.0 has a new feature, Realtime Dataset Metrics. This is a browser user interface, which you can launch from the Dataset Attributes System Summary, in the TEP user interface to OMEGAMON for Storage.

Realtime Dataset Metrics is a complete overhaul of the Dataset Attributes Database collector that improves both performance and timeliness of data. This function was delivered in version 5.4.0. Refer to this technote for more information on the Realtime Dataset Metrics collection: <http://www-01.ibm.com/support/docview.wss?uid=swg22009862>

The key features of Realtime Data Set Metrics are as follows:

- Summarize by key attributes

- Flexible filtering to quickly build ad-hoc queries
- Quickly choose the columns needed
- Sorting across the entire result set
- Access to all data through on-demand pagination

Chapter 13. Appendix A. Creating a presentation address space for OMEGAMON II for SMS

The presentation address space enables sign-on to the OMEGAMON II for SMS environment through a 3270 mainframe terminal. Accessing the OMEGAMON II for SMS environment is optional because OMEGAMON for Storage automatically acquires the monitoring data that it needs from OMEGAMON II for SMS.

Create a presentation address space only if it is required in this runtime environment using the OMEGAMON for Storage Parameter Reference and the PARMGEN information located at http://www.ibm.com/support/knowledgecenter/SSAUBV/com.ibm.omegamon_share.doc_6.3.0.2/welcome.

Chapter 14. Appendix B. Forwarding events to other Tivoli products

OMEGAMON for Storage supports event forwarding, as described in this topic.

If your company environment uses the IBM Tivoli Enterprise Console or IBM Tivoli Netcool/OMNIBus to manage events in your enterprise, you can now forward events reported by IBM Tivoli Monitoring monitoring agents to these event management products. The IBM Tivoli Monitoring: Installation and Setup Guide provides extensive planning and installation information regarding event forwarding.

Before events can be forwarded, event forwarding must be enabled on the hub monitoring server, and a default destination server must be defined. In addition, the IBM Tivoli Enterprise Console server or the Tivoli Netcool/OMNIBus server (the event server) must be configured to receive the events, a situation update forwarding process must be installed on the event server, and, for events forwarded to IBM Tivoli Enterprise Console the BAROC file for the agent must be installed and imported on the event server.

The Installation and Setup section provides detailed instructions for enabling event forwarding from a distributed Tivoli Enterprise Monitoring Server and for configuring IBM Tivoli Enterprise Console and Tivoli Netcool/OMNIBus to receive the events, including the installation of the event synchronization component.

After situation forwarding is enabled, by default all situation events are forwarded to the specified event server. However, you can customize which situation events are forwarded and to which event server, using the Situation Editor in the Tivoli Enterprise Portal. You might also need to assign an event status compatible with the target event server. For information on specifying which situation events to forward, see the Tivoli Enterprise Portal online help.

Obtaining and activating the ks3.baroc file

Support for forwarding the OMEGAMON for Storage events to IBM Tivoli Enterprise Console is provided by the ks3.baroc file, which is included with the application support for the monitoring agent.

About this task

You obtain and activate the file according to the following general process:

Procedure

1. You install application support on a distributed monitoring server, as described in the Configuring TEMS manual. As a result of this step, the ks3.baroc file is stored in the following path:
 - On Windows systems: itm_home\cms\TECLIB, where itm_home is the directory where you installed IBM Tivoli Monitoring.
 - On UNIX-based systems: itm_home/tables/ms_name/TECLIB directory, where itm_home is the directory where you installed IBM Tivoli Monitoring and ms_name is the name of the monitoring server.

Note: The ks3.baroc file that is located on this monitoring server is merely stored. This copy of the file is not run or referenced by any software application on this monitoring server.

2. You copy the ks3.baroc file to the event server for Tivoli Enterprise Console. OMEGAMON for Storage has only one *.baroc file, ks3.baroc. However, the related ks3.map file allows you to customize the event data that is produced by IBM Tivoli Monitoring. This data is forwarded to a listening event integration facility (EIF). A Tivoli Enterprise Console server is an example of an EIF. You can customize the configuration of the ks3.map file. For related information, see Relation of *.baroc files and *.map files.
3. On the Tivoli Enterprise Console event server, you run a series of Tivoli Enterprise Console commands that import, compile, and load the ks3.baroc file in Tivoli Enterprise Console.

What to do next

Note: You obtain the omegamon.baroc file, which is required for event synchronization, during the installation of event synchronization on the event server. You do not obtain this file from the application support software for the monitoring agent.

Relation of *.baroc files and *.map files

This section provides facts about *.baroc files and *.map files and how they are related.

Before you begin

Characteristics of a *.baroc file:

- Required to enable event forwarding from IBM Tivoli Monitoring to Tivoli Enterprise Console.
- Does not have a role in event forwarding for the Tivoli Netcool/OMNIBus product.
- Must be installed into the IBM Tivoli Enterprise Console rulebase before monitored events can be received by the IBM Tivoli Enterprise Console server.

Characteristics of a *.map file:

- Controls the event data from IBM Tivoli Monitoring that is forwarded to a listening event integration facility (EIF).
- Can control the forwarding of event data to both Tivoli Netcool/OMNIBus servers and Tivoli Enterprise Console servers, because both products are EIFs.
- Must be synchronized with a corresponding *.baroc file, whenever event handling for Tivoli Enterprise Console is modified.

About this task

You can modify the *.map file to decrease the amount of event data that is forwarded to listening EIF servers. This capability could be useful in the following scenario for Tivoli Enterprise Console:

Procedure

1. An event attribute table of a situation in IBM Tivoli Monitoring contains large numbers of attributes.

2. Because you might be monitoring an event which could produce multiple sub-objects, you want to reduce the number of attributes that are forwarded for the event.
3. You adjust the *.map file to prevent hidden event attributes from being passed when the event is triggered. As a result, less data is forwarded to a IBM Tivoli Enterprise Console server.
4. Apply corresponding changes to the *.baroc file, so that event data handling by both files remain synchronized.

Chapter 15. Appendix C. Configuring the collection and display of historical data

This topic describes the mechanisms and display options for historical data.

Mechanisms for collecting historical data

Two completely separate mechanisms control the collection of historical data for OMEGAMON for Storage, as described in the following table.

Table 5. Comparison of mechanisms for collecting historical data

Name of configuration method	Storage place for the data	Typical type of data*	Procedure	Purpose
PARMGEN	Persistent data store (PDS)	Short-term history *	You use PARMGEN to configure the runtime environment (RTE). The configuration process includes the option to turn on collection of historical data for certain tables.	Collect data at a fixed interval, when the RMF (Resource Measurement Facility) interval ends.
Tivoli Enterprise Portal	Tivoli Data Warehouse	Long-term history *	You use the Historical Configuration dialog box in the Tivoli Enterprise Portal to turn on collection of historical data for all other tables.	Collect data at varied intervals. Note: You have the option to turn collection on or off only.
* This column identifies the type of data that is typically configured. However, there are cases where each of the two configuration mechanisms affect the other type of data, long-term or short-term data, respectively.				

To decide how to size the data sets for these tables, you consider the amount of data that you are collecting and the amount of "short-term history" that you want to maintain. Table of metrics regarding the persistent data store provides reference information regarding sizing.

Short-term history and long-term history

This section compares short-term history (from the persistent data store) and long-term history (from Tivoli Data Warehouse).

Short-term data from PDS data sets can be written to the Tivoli Data Warehouse for long-term retention. You can use History Configuration dialog boxes from within the Tivoli Enterprise Portal to specify the time interval (such as hourly or daily) at which short-term data is written to the warehouse. You can then retrieve the long-term historical data for display with the portal.

When a portal display is generated, data comes from the sources that are listed in the following table:

Table 6. Comparison of short-term and long-term history

Source of data	Type of data	Time span of the data
Persistent data store	Short-term history	24 hours or less
Tivoli Data Warehouse	Long-term history	Over 24 hours

For some tables, collection of data in Tivoli Data Warehouse is not available. In these cases, the portal can display data from the persistent data store only.

When you allocate space for persistent data stores, allow sufficient space for 24 hours of data. When collection of data in Tivoli Data Warehouse is not available, you can allocate extra space to enable the persistent data store to collect data for a longer period of time, for example, 48 hours. If you set the Time-Span tool in a portal workspace to display data for the last 48 hours from one of these tables, you see 48 hours of data, if you have allocated sufficient storage space in the persistent data store.

Table of metrics regarding the persistent data store

Use the information in the following tables to learn about these issues:

- Which tables are contained in which data sets
- Where collection is controlled for each table
- Which tables are warehouse-enabled

In addition, the following table provides information to help you allocate the correct size for the data sets of your persistent data store.

Table 7. Groups and data sets of the persistent data store

Group	Data Sets
RKDFDSA	RKDFDSA1 RKDFDSA2 RKDFDSA3
RKDFDSB	RKDFDSB1 RKDFDSB2 RKDFDSB3
PDSGROUP	RPDSGRP1
GENHIST	RGENHIS1 RGENHIS2 RGENHIS3
RKS3DSA1	RKS3DSA1 RKS3DSA2 RKS3DSA3

The following table provides the following information:

- Which attribute tables are contained in which data sets in the persistent data store
- The collection control mechanism (PARMGEN or Tivoli Enterprise Portal)
- Attribute tables that are enabled for Tivoli Data Warehouse

Items in the table that are marked **Yes** in the Warehouse Enabled? column are eligible to be warehoused in Tivoli Data Warehouse ("TDW" in the table).

- Estimated space requirements for data sets in the persistent data store:
 - Space estimates apply to one managed system for a 24-hour period.
 - Space estimates assume a 15-minute Resource Monitoring Facility (RMF) interval or 15-minute collection interval, as appropriate.
 - The following formula is used to estimate space requirements: $((60 / 15) \times 24 \times \text{Record size} \times \text{frequency})$.

* The Attribute History Name/Description column in the following table provides the name of the attribute group for each table. For data sets that are not configured in the Tivoli Enterprise Portal, this column contains a description of the table.

Table 8. Configuration data for the persistent data store

* Attribute history name/ description	Table name	Group	Collection control	TDW enabled?
CUA Interface	DASDPDS	RKDFDSB	RKDFDSB ICAT\ (DASDHIST)	No
Data Set Performance	HDSN_IO_ST	RKDFDSB	ICAT\ (DSNHIST)	No
S3 Application Data Set Details	APPL_DSDET	RKS3DSA1	TEPS	Yes
S3 Application Monitoring	APPL	RKS3DSA1	TEPS	Yes
S3 Cache Control Unit	CACHE_CU	RKS3DSA1	TEPS	Yes
S3 Cache Devices	CACHE_DEV	RKDS3DSA1	TEPS	Yes
S3 Cache Raid Rank	RRANK	RKS3DSA1	TEPS	No
S3 Channel Path	CHAN_PATH	RKS3DSA1	TEPS	Yes
S3 DASD Group Vol Perform	DASDUGPE	RKS3DSA1	TEPS	Yes
S3 DASD Group Vol Space	DASDUGSP	RKS3DSA1	TEPS	Yes
S3 DASD Volume Performance	DASDPERF	RKS3DSA1	TEPS	Yes
S3 DASD Volume Space	DASDSPAC	RKS3DSA1	TEPS	Yes
S3 Data Set Attributes Blocksize Summary	DA_BLKSUM	RKS3DSA1	TEPS	Yes
S3 Data Set Attributes CA Split Summary	DA_CASSUM	RKS3DSA1	TEPS	Yes
S3 Data Set Attributes Catalog Summary	DA_CATSUM	RKS3DSA1	TEPS	Yes
S3 Data Set Attributes CI Split Summary	DA_CISSUM	RKS3DSA1	TEPS	Yes
S3 Data Set Attributes Creation Date Summary	DA_CRTSUM	RKS3DSA1	TEPS	Yes
S3 Data Set Attributes DSORG Detail	DA_ORGDTL	RKS3DSA1	TEPS	Yes
S3 Data Set Attributes DSORG Summary	DA_ORGSUM	RKS3DSA1	TEPS	Yes
S3 Data Set Attributes Extent Summary	DA_EXTSUM	RKS3DSA1	TEPS	Yes

Table 8. Configuration data for the persistent data store (continued)

* Attribute history name/ description	Table name	Group	Collection control	TDW enabled?
S3 Data Set Attributes Inefficient Blocksize Summary	DA_IBKSUM	RKS3DSA1	TEPS	Yes
S3 Data Set Attributes Mature Data Set Summary	DA_MATSUM	RKS3DSA1	TEPS	Yes
S3 Data Set Attributes Never Referenced Data Set Summary	DA_NRFSUM	RKS3DSA1	TEPS	Yes
S3 Data Set Attributes Newborn Data Set Summary	DA_NEWSUM	RKS3DSA1	TEPS	Yes
S3 Data Set Attributes Reference Date Summary	DA_REFSUM	RKS3DSA1	TEPS	Yes
S3 Data Set Attributes SMS Class Detail	DA_SMSDTL	RKS3DSA1	TEPS	Yes
S3 Data Set Attributes SMS Class Summary	DA_SMSSUM	RKS3DSA1	TEPS	Yes
S3 Data Set Attributes Space Allocated Summary	DA_ALCSUM	RKS3DSA1	TEPS	Yes
S3 Data Set Attributes Space Unused Summary	DA_UNUSUM	RKS3DSA1	TEPS	Yes
S3 Data Set Attributes System Summary	DA_SYSSUM	RKS3DSA1	TEPS	Yes
S3 Data Set Attributes Uncataloged Data Set Detail	DA_UNCDTL	RKS3DSA1	TEPS	Yes
S3 Data Set Attributes Uncataloged Data Set Summary	DA_UNCSUM	RKS3DSA1	TEPS	Yes
S3 Data Set Group Detail Attrs	DSNG_ATTR	RKS3DSA1	TEPS	Yes
S3 Data Set Group Details	DSNG_DETL	RKS3DSA1	TEPS	Yes
S3 Data Set Group Details Volume	DSNG_DVOL	RKS3DSA1	TEPS	Yes
S3 Data Set Group Summary	DSNG_SUMM	RKS3DSA1	TEPS	Yes
S3 DSN Attr Group Detail	DAGDSNDTL	RKS3DSA1	TEPS	Yes
S3 DSN Attr Group Summary	DAG_SUMM	RKS3DSA1	TEPS	Yes
S3 HSM CDS	HSM_CDS	RKS3DSA1	TEPS	Yes
S3 HSM Common Storage	KS3HSCSTOR	RKS3DSA1	TEPS	Yes

Table 8. Configuration data for the persistent data store (continued)

* Attribute history name/ description	Table name	Group	Collection control	TDW enabled?
S3 HSM Cross System CRQ Hosts	KS3HCRQXHS	RKS3DSA1	TEPS	Yes
S3 HSM Cross System CRQplex	KS3HCRQXPX	RKS3DSA1	TEPS	Yes
S3 HSM Function Details	KS3HSXFUDA	RKS3DSA1	TEPS	Yes
S3 HSM Function Statistics	HSM_FUN_DA	RKS3DSA1	TEPS	Yes
S3 HSM Function Summary	HSM_ACTVTY	RKS3DSA1	TEPS	Yes
S3 HSM Host Function Status	KS3HSFUNST	RKS3DSA1	TEPS	Yes
S3 HSM Host Request Summary	KS3HSWATRQ	RKS3DSA1	TEPS	Yes
S3 HSM Host Status	KS3HSHSTAT	RKS3DSA1	TEPS	Yes
S3 HSM Private Storage	KS3HSPSTOR	RKS3DSA1	TEPS	Yes
S3 HSM Requests	HSM_REQS	RKS3DSA1	TEPS	Yes
S3 HSM Status	HSM_STATUS	RKS3DSA1	TEPS	Yes
S3 Logical Control Unit	LCU	RKS3DSA1	TEPS	Yes
S3 Logical Control Unit Hyperpav	LCUC	RKS3DSA1	TEPS	No
S3 RMM Config	RMMCFCG	RKS3DSA1	TEPS	Yes
S3 RMM Control Data Set	RMMCDS	RKS3DSA1	TEPS	Yes
S3 RMM Summary	RMMSUM	RKS3DSA1	TEPS	Yes
S3 SMS Cache Sets	CACHE_SET	RKS3DSA1	TEPS	Yes
S3 SMS Configuration	SMS_CONFIG	RKS3DSA1	TEPS	Yes
S3 SMS Data Class	SMS_DAT_CL	RKS3DSA1	TEPS	Yes
S3 SMS Management Class	SMS_MAN_CL	RKS3DSA1	TEPS	Yes
S3 SMS Storage Class	SMS_ST_CL	RKS3DSA1	TEPS	Yes
S3 SMS Storage Group	SMS_ST_GRP	RKS3DSA1	TEPS	Yes
S3 SMS Storage Group Status	ST_GRP_STA	RKS3DSA1	TEPS	Yes
S3 SMS Systems	SMS_SYSTEM	RKS3DSA1	TEPS	Yes
S3 Symmetrix Configuration	SYM_CONFIG	RKS3DSA1	ICAT\ (DASDHIST)	No
S3 Symmetrix Devices	SYM_DSK_DV	RKS3DSA1	ICAT\ (DASDHIST)	No
S3 Symmetrix Directors	SYM_DSK_DR	RKS3DSA1	ICAT\ (DASDHIST)	No
S3 Tape Device	TAPE_DEV	RKS3DSA1	TEPS	Yes

Table 8. Configuration data for the persistent data store (continued)

* Attribute history name/ description	Table name	Group	Collection control	TDW enabled?
S3 Tape Group	TAPE_GRP	RKS3DSA1	TEPS	Yes
S3 TotalStorageDS Array	TDS_ARRAY	RKS3DSA1	ICAT\ (DASDHIST)	No
S3 TotalStorageDS Configuration	TDS_CONFIG	RKS3DSA1	ICAT\ (DASDHIST)	No
S3 TotalStorageDS Extent Pool	TDS_EXPOOL	RKS3DSA1	ICAT\ (DASDHIST)	No
S3 TotalStorageDS Rank	TDS_RANK	RKS3DSA1	ICAT\ (DASDHIST)	No
S3 UDG Cache Devices	CACUGDEV	RKS3DSA1	TEPS	Yes
S3 Volume Group Summary	DASD_SUMM	RKS3DSA1	TEPS	Yes
S3 VTS Cache Partition Container Summary	S3VTCACHPC	RKS3DSA1	TEPS	Yes
S3 VTS Cache Preference Group Summary	S3VTCHPGRP	RKS3DSA1	TEPS	Yes
S3 VTS Cluster Summary	S3VTCLUSTR	RKS3DSA1	TEPS	Yes
S3 VTS Tape Volume Cache Summary	S3VTTPVOLC	RKS3DSA1	TEPS	Yes
VTS Cache VTS Capacity VTS Composite Library VTS Overview VTS Physical Devices VTS Virtual Devices	HVIRTULTAP	RKDFDSA	ICAT(VTSHIST)	No
VTS Virtual Devices Summary	HVTSDEVICE	RKDFDSA	ICAT(VTSHIST)	No

The following table, Table 8. Configuration data for the persistent data store (continued), shows additional fields for the attributes.

* Attribute history name/ description	Record size	Frequency	Estimated space req
CUA Interface	1088	1 record per logical volume per RMF interval	606000 kilobytes (assumes 8000 devices)
Data Set Performance	1152	1 record per monitored Data Set per application accessing the data set per RMF interval	56250 kilobytes (assumes 2000 data set records)

* Attribute history name/ description	Record size	Frequency	Estimated space req
S3 Application Data Set Details	142	1 record per data set per monitored application per interval	5325 kilobytes (assumes 20 monitored applications with 20 active data sets each)
S3 Application Monitoring	202	1 record per monitored application	371 kilobytes (assumes 20 monitored applications)
S3 Cache Control Unit	203	1 record per cache control unit per RMF interval	609 kilobytes (assumes 32 control units)
S3 Cache Devices	421	1 record per logical volume per RMF interval	315750 kilobytes (assumes 8000 devices)
S3 Cache Raid Rank	2112	1 record per cache control unit with raid rank per RMF interval	6336 kilobytes (assumes 32 control units with raid rank)
S3 Channel Path	194	1 record per channel path per RMF interval	1164 kilobytes (assumes 64 channel paths online)
S3 DASD Group Vol Perform	316	1 record per user DASD group per logical volume in group per RMF interval	2963 kilobytes (assumes total of 100 logical volumes in user DASD groups)
S3 DASD Group Vol Space	311	1 record per user DASD group per logical volume in group per RMF interval	2916 kilobytes (assumes total of 100 logical volumes in user DASD groups)
S3 DASD Volume Performance	243	1 record per logical volume per RMF interval	182250 kilobytes (assumes 8000 devices)
S3 DASD Volume Space	217	1 record per logical volume per RMF interval	162750 kilobytes (assumes 8000 devices)
S3 Data Set Attributes Blocksize Summary	132	9 records (in other words, number of distinct ranges) per Data Set Attribute collection cycle	1 kilobytes (assumes 1 Data Set Attribute collection cycle per 24 hours)
S3 Data Set Attributes CA Split Summary	230	(1 record * Top N value) per Data Set Attribute collection cycle	5 kilobytes (assumes 1 Data Set Attribute collection cycle per 24 hours and default Top N value of 20)

* Attribute history name/ description	Record size	Frequency	Estimated space req
S3 Data Set Attributes Catalog Summary	160	(1 record * Top N value) per Data Set Attribute collection cycle	3 kilobytes (assumes 1 Data Set Attribute collection cycle per 24 hours and default Top N value of 20)
S3 Data Set Attributes CI Split Summary	230	(1 record * Top N value) per Data Set Attribute collection cycle	5 kilobytes (assumes 1 Data Set Attribute collection cycle per 24 hours and default Top N value of 20)
S3 Data Set Attributes Creation Date Summary	132	(1 record * Top N value) per Data Set Attribute collection cycle	1 kilobytes (assumes 1 Data Set Attribute collection cycle per 24 hours)
S3 Data Set Attributes DSORG Detail	182	8 records (in other words, number of distinct ranges) per Data Set Attribute collection cycle	60 kilobytes (assumes 1 Data Set Attribute collection cycle per 24 hours and default Top N value of 20)
S3 Data Set Attributes DSORG Summary	160	(17 records * Top N value) per Data Set Attribute collection cycle	3 kilobytes (assumes 1 Data Set Attribute collection cycle per 24 hours)
S3 Data Set Attributes Extent Summary	182	17 records (in other words, number of DSORGs) per Data Set Attribute collection cycle	3 kilobytes (assumes 1 Data Set Attribute collection cycle per 24 hours and default Top N value of 20)
S3 Data Set Attributes Inefficient Blocksize Summary	182	(1 record * Top N value) per Data Set Attribute collection cycle	4 kilobytes (assumes 1 Data Set Attribute collection cycle per 24 hours and default Top N value of 20)
S3 Data Set Attributes Mature Data Set Summary	214	(1 record * Top N value) per Data Set Attribute collection cycle	4 kilobytes (assumes 1 Data Set Attribute collection cycle per 24 hours and default Top N value of 20)
S3 Data Set Attributes Never Referenced Data Set Summary	194	(1 record * number of volumes with Uncataloged data sets) per Data Set Attribute collection cycle	4 kilobytes (assumes 1 Data Set Attribute collection cycle per 24 hours and default Top N value of 20)

* Attribute history name/ description	Record size	Frequency	Estimated space req
S3 Data Set Attributes Newborn Data Set Summary	174	(1 record * Top N value) per Data Set Attribute collection cycle	3 kilobytes (assumes 1 Data Set Attribute collection cycle per 24 hours and default Top N value of 20)
S3 Data Set Attributes Reference Date Summary	132	(1 record * Top N value) per Data Set Attribute collection cycle	1 kilobytes (assumes 1 Data Set Attribute collection cycle per 24 hours)
S3 Data Set Attributes SMS Class Detail	208	8 records (in other words, number of distinct ranges) per Data Set Attribute collection cycle	408 kilobytes (assumes 1 Data Set Attribute collection cycle per 24 hours, 100 total SMS constructs and default Top N value of 20)
S3 Data Set Attributes SMS Class Summary	158	(1 record * Top N value) * (number of SMS Data + Storage + Management Classes + Storage Groups) per Data Set Attribute collection cycle	16 kilobytes (assumes 1 Data Set Attribute collection cycle per 24 hours and 100 total SMS constructs)
S3 Data Set Attributes Space Allocated Summary	182	(1 record * Top N value) per Data Set Attribute collection cycle	3 kilobytes (assumes 1 Data Set Attribute collection cycle per 24 hours and default Top N value of 20)
S3 Data Set Attributes Space Unused Summary	182	(1 record * Top N value) per Data Set Attribute collection cycle	3 kilobytes (assumes 1 Data Set Attribute collection cycle per 24 hours and default Top N value of 20)
S3 Data Set Attributes System Summary	406	1 record * (number of SMS Data + Storage + Management Classes + Storage Groups) per Data Set Attribute collection cycle	0.4 kilobytes (assumes 1 Data Set Attribute collection cycle per 24 hours)
S3 Data Set Attributes Uncataloged Data Set Detail	174	1 record per Data Set Attribute collection cycle	870 kilobytes (assumes 1 Data Set Attribute collection cycle per 24 hours, 250 volumes with Uncataloged data sets and default Top N value of 20)

* Attribute history name/ description	Record size	Frequency	Estimated space req
S3 Data Set Attributes Uncatalogued Data Set Summary	122	(1 record * Top N value * number of volumes with Uncataloged data sets) per Data Set Attribute collection cycle	30 kilobytes (assumes 1 Data Set Attribute collection cycle per 24 hours and 250 volumes with Uncataloged data sets)
S3 Data Set Group Detail Attrs	220	1 record per Data Set Group per Data Set per interval	7163 kilobytes (assumes 20 Data Set Groups with 20 data sets each)
S3 Data Set Group Details	826	1 record per Data Set Group per Data Set per interval	29438 kilobytes (assumes 20 Data Set Groups with 20 data sets each)
S3 Data Set Group Details Volume	305	1 record per Data Set Group per Data Set per Volume per interval	10950 kilobytes (assumes 20 Data Set Groups with 20 data sets each with 1 volume each)
S3 Data Set Group Summary	392	1 record per Data Set Group per interval	717 kilobytes (assumes 20 Data Set Groups)
S3 DSN Attr Group Detail	607	1 record per Data Set Attribute Group per Data Set, up to a maximum of 5000 records per group (plus 1 record per Data Set Attribute Group update per Data Set, per interval, up to a maximum of 5000 records per group) per Data Set Attribute Collection cycle	237 kilobytes (assumes 20 Data Set Attribute Groups containing 20 Data Sets each and 1 Data Set Attribute Collection cycle per 24 hours with no group updates)
S3 DSN Attr Group Summary	474	1 record per Data Set Attribute Group (plus 1 record per Data Set Attribute Group update per interval) per Data Set Attribute Collection cycle	9 kilobytes (assumes 20 Data Set Attribute Groups and 1 Data Set Attribute Collection cycle per 24 hours with no group updates)
S3 HSM CDS	98	1 record per control data set (CDS) per interval	37 kilobytes (assumes single data set CDS)
S3 HSM Common Storage	74	1 record per interval	7 kilobytes
S3 HSM Cross System CRQ Hosts	104	1 record per HSM host per interval	20 kilobytes (assumes 2 HSM hosts)
S3 HSM Cross System CRQplex	121	1 record per CRQplex in the HSMplex	12 kilobytes (assumes 1 CRQplex)

* Attribute history name/ description	Record size	Frequency	Estimated space req
S3 HSM Function Details	128	1 record per HSM function per HSM host per interval	254 kilobytes (assumes 2 HSM hosts)
S3 HSM Function Statistics	148	1 record per HSM function per interval	65 kilobytes
S3 HSM Function Summary	87	1 record per function per interval	41 kilobytes
S3 HSM Host Function Status	143	1 record per HSM host per interval	19 kilobytes (assumes 2 HSM hosts)
S3 HSM Host Request Summary	98	1 record per HSM host per interval	18 kilobytes (assumes 2 HSM hosts)
S3 HSM Host Status	217	1 record per HSM host per interval	41 kilobytes (assumes 2 HSM hosts)
S3 HSM Private Storage	86	1 record per HSM host per interval	16 kilobytes (assumes 2 HSM hosts)
S3 HSM Requests	216	1 record per request at time of interval per interval	186 kilobytes (assumes 10 queued requests)
S3 HSM Status	250	1 record per interval	14 kilobytes
S3 Logical Control Unit	378	1 record per logical control unit per RMF interval	1134 kilobytes (assumes 32 logical control units)
S3 Logical Control Unit Hyperpav	1080	1 record per logical control unit with Hyperpav	3240 kilobytes (assumes 32 logical control units with Hyperpav)
S3 RMM Config	364	1 record per interval	34 kilobytes
S3 RMM Control Data Set	224	1 record per control data set (CDS) entry type per interval	84 kilobytes (assumes journal CDS and single cluster CDS)
S3 RMM Summary	397	(201 + number locations + number accounts + number owners + number jobs + number programs + number VRS) records per RMM collection cycle	47067 kilobytes (assumes 1 RMM collection cycle per 24 hours and 4 locations, 100 accounts, 100 owners, 100 jobs, 100 programs, 200 VRS)
S3 SMS Cache Sets	203	1 record per cache set per interval	609 kilobytes (assumes 10 cache sets)
S3 SMS Configuration	479	1 record per interval	18 kilobytes
S3 SMS Data Class	317	1 record per data class per interval	594 kilobytes (assumes 20 data classes)

* Attribute history name/ description	Record size	Frequency	Estimated space req
S3 SMS Management Class	301	1 record per management class per interval	562 kilobytes (assumes 20 management classes)
S3 SMS Storage Class	273	1 record per storage class per interval	512 kilobytes (assumes 20 storage classes)
S3 SMS Storage Group	473	1 record per storage group per interval	861 kilobytes (assumes 20 storage groups)
S3 SMS Storage Group Status	99	1 record per storage group per interval	186 kilobytes (assumes 20 storage groups)
S3 SMS Systems	69	1 record per system in the SMSplex per interval	52 kilobytes (assumes 8 systems)
S3 Symmetrix Configuration	1088	1 record per Symmetrix storage facility per RMF interval	129 kilobytes (assumes 4 Symmetrix storage facilities)
S3 Symmetrix Devices	104 - 32744 bytes. 44 + (20 per device)	1 record per Symmetrix storage facility per RMF interval	15219 kilobytes (assumes 4 Symmetrix storage facilities with 2024 devices each)
S3 Symmetrix Directors	196 - 8512 bytes. 64 + (132 per director)	1 record per Symmetrix storage facility per RMF interval	1560 kilobytes (assumes 4 Symmetrix storage facilities with 64 directors each)
S3 Tape Device	115 bytes	1 record per tape device per interval	345 kilobytes (assumes 32 tape drives)
S3 Tape Group	288	1 record per tape group per interval	193 kilobytes (assumes 8 tape groups)
S3 TotalStorageDS Array	1108	1 record per TotalStorageDS array per RMF interval	372 kilobytes (assumes 128 arrays)
S3 TotalStorageDS Configuration	1102	1 record per TotalStorageDS storage facility per RMF interval	53 kilobytes (assumes 4 TotalStorage DS storage facilities)
S3 TotalStorageDS Extent Pool	1104	1 record per TotalStorageDS extent pool per RMF interval	591 kilobytes (assumes 32 extent pools)
S3 TotalStorageDS Rank	1106	1 record per TotalStorageDS rank per RMF interval	2520 kilobytes (assumes 128 ranks)

* Attribute history name/ description	Record size	Frequency	Estimated space req
S3 UDG Cache Devices	394	1 record per user DASD group per logical volume in group per RMF interval	3738 kilobytes (assumes total of 100 logical volumes in user DASD groups)
S3 Volume Group Summary	653	(1 record per storage group + 1 record per user dasd group) 4 intervals per day	6306 kilobytes (assumes a total of 50 SMS groups and 50 user DASD groups)
S3 VTS Cache Partition Container Summary	136	8 records per cluster per interval	2176 kilobytes
S3 VTS Cache Preference Group Summary	144	8 records per cluster per interval	2304 kilobytes
S3 VTS Cluster Summary	132	1 record per cluster per interval	264 kilobytes
S3 VTS Tape Volume Cache Summary	128	1 record per cluster per interval	256 kilobytes
VTS Cache VTS Capacity VTS Composite Library VTS Overview VTS Physical Devices VTS Virtual Devices	1072	1 record per VTS per hour	193 kilobytes (assumes 4 vts units)
VTS Virtual Devices Summary	112 - 4144 bytes. 48 + (64 per virtual device)	1 record per VTS per hour	389 kilobytes (assumes 4 vts units with 64 virtual drives each)

Chapter 16. Appendix D. Documentation library

This appendix contains information about the publications in the Tivoli OMEGAMON for Storage on z/OS library and about other publications related to Tivoli OMEGAMON for Storage on z/OS.

For all the documentation related to OMEGAMON for Storage, see <http://www-01.ibm.com/support/knowledgecenter/SSAUBV/welcome>.

To find publications for the previous version of a product, click **Previous versions** on the left pane for the product.

OMEGAMON for Storage library

The following documents are available for OMEGAMON for Storage at http://www-01.ibm.com/support/knowledgecenter/SS2JFP/com.ibm.oxes530.doc/welcome_storage530.htm:

- **Planning and Configuration Guide**
Documents the installation and configuration tasks necessary for the implementation of IBM OMEGAMON for Storage on z/OS. This document is written for z/OS systems programmers and others who are responsible for installing and configuring OMEGAMON for Storage.
- **Parameter Reference**
Documents the parameters used for setting and storing configuration values necessary for the implementation of IBM OMEGAMON for Storage on z/OS. This document is written for z/OS systems programmers and others who are responsible for installing and configuring IBM OMEGAMON for Storage on z/OS.
- **User's Guide**
Introduces the features, workspaces, attributes, and predefined situations for the IBM OMEGAMON for Storage on z/OS product and supplements the user assistance provided with this product.
- **Tuning Guide**
Provides information on enhancing the performance of OMEGAMON for Storage so that you can get the maximum benefit with the least amount of resources.
- **Troubleshooting Guide**
Contains messages for the IBM OMEGAMON for Storage on z/OS product and OMEGAMON II for SMS component and information to help solve problems with the IBM OMEGAMON for Storage on z/OS product.

OMEGAMON and Tivoli Management Services on z/OS common library

The documents in this library are common to some or all of the OMEGAMON products or Tivoli Management Services on z/OS and can be found at http://www.ibm.com/support/knowledgecenter/SSAUBV/com.ibm.omegamon_share.doc_6.3.0.2/welcome

IBM Tivoli Monitoring Library

The following publications provide information about IBM Tivoli Monitoring V6.3 and about the commonly shared components of Tivoli Management Services which can be found at <http://www-01.ibm.com/support/knowledgecenter/SSAUBV/welcome>:

- *Quick Start Guide*
Introduces the components of IBM Tivoli Monitoring.
- *Installation and Setup Guide*
Provides instructions for installing and configuring IBM Tivoli Monitoring components on Windows, Linux, and UNIX systems.
- *Program Directory for IBM Tivoli Management Services on z/OS*
Gives instructions for the SMP/E installation of the Tivoli Management Services components on z/OS.
- *Configuring the Tivoli Enterprise Monitoring Server on z/OS*
Gives detailed instructions for using PARMGEN to configure Tivoli Enterprise Monitoring Server on z/OS systems. Includes scenarios for using batch mode to replicate monitoring environments across the z/OS enterprise. Also provides instructions for setting up security and for adding application support to a Tivoli Enterprise Monitoring Server on z/OS.
- *Administrator's Guide*
Describes the support tasks and functions required for the Tivoli Enterprise Portal Server and clients, including Tivoli Enterprise Portal user administration.
- *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.
- *User's Guide*
Complements the Tivoli Enterprise Portal online help. The guide provides hands-on lessons and detailed instructions for all Tivoli Enterprise Portal features.
- *Command Reference*
Provides detailed syntax and parameter information, as well as examples, for the commands you can use in IBM Tivoli Monitoring.
- *Troubleshooting Guide*
Provides information to help you troubleshoot problems with the software.
- *Messages*
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 and TMS: Engine).

Related publications

You can find useful information about the OMEGAMON XE Monitoring Agent at <http://www-01.ibm.com/support/knowledgecenter/SSAUBV/welcome>.

This set of documents includes the following items, which are related to configuration of the OMEGAMON II for SMS component, which is a required component for OMEGAMON for Storage.

- *OMEGAMON II for SMS Configuration and Customization Guide*

- *OMEGAMON II for SMS User's Guide*
- *OMEGAMON II for SMS Administrator's Guide*
- *OMEGAMON II for SMS Tuning Guide*

Other sources of documentation

You can also obtain technical documentation about IBM Tivoli Monitoring and OMEGAMON products from the following sources:

- IBM Tivoli Open Process Automation Library (OPAL)
<http://www.ibm.com/software/tivoli/opal>
OPAL is an online catalog that contains integration documentation and other downloadable product extensions. This library is updated daily.
- IBM Tivoli Distributed Monitoring and Application Management wiki
<http://www.ibm.com/developerworks/wikis/display/tivolimonitoring/Home>
The IBM Tivoli Distributed Monitoring and Application Management wiki is a source of best practices, white papers, discussion forums, and more. The wiki includes integration documentation as well as downloadable product extensions.
- IBM Redbooks
<http://www.redbooks.ibm.com/>
IBM Redbooks, Redpapers, and Redbooks Technotes provide information about products from platform and solution perspectives.
- Technotes
Technotes provide the latest information about known product limitations and workarounds. You can find Technotes through the IBM Software Support Web site at <http://www.ibm.com/software/support>.

Chapter 17. Support information

If you have a problem with your IBM software, you want to resolve it quickly. This section describes the following options for obtaining support for IBM software products:

- Using IBM Support Assistant
- Obtaining fixes
- Obtaining PTFs (Program Temporary Fixes)
- Receiving weekly support updates
- Contacting IBM Software Support

Using IBM Support Assistant

The IBM Support Assistant is a free, standalone application that you can install on any workstation. You can then enhance the application by installing product-specific plug-in modules for the IBM products you use.

Before you begin

The IBM Support Assistant saves you time searching product, support, and educational resources. It also helps you gather support information when you need to open a problem management record (PMR), which you can then use to track the problem.

The product-specific plug-in modules provide the following resources:

- Support links
- Education links
- Ability to submit problem management reports

For more information, see the IBM Support Assistant Web site at <http://www.ibm.com/software/support/isa>.

About this task

Install and set up the IBM Support Assistant as follows:

Procedure

1. Download the IBM Support Assistant installation software from <http://www.ibm.com/software/support/isa>.
2. Unzip or untar the downloaded file.
3. Run the installation file and respond to the prompts from the installer.
4. Launch the IBM Support Assistant. For example, on Windows XP click **IBM Support Assistant** in the following menu path: **Start > All Programs > IBM Support Assistant**. The Welcome page is displayed.
5. Select the **Updater** hyperlink to access the Updater page.
6. Access the **Upgrades** tab and the **IBM Support Assistant** tab to select the product-specific plug-in modules that you want to install.

What to do next

If you cannot find the solution to your problem in the IBM Support Assistant, you can also check the following Internet resources for information that might help you resolve your problem:

- Forums and news groups
- Google.com

Obtaining fixes

About this task

A product fix might be available to resolve your problem. To determine what fixes are available for your IBM software product, follow these steps:

Procedure

1. Go to the IBM Software Support Web site at <http://www.ibm.com/software/support>.
2. Select **Tivoli** in the **Select a brand and/or product** drop-down list to access the **Select a product** drop-down list.
3. Select **OMEGAMON for Storage** in the **Select a product** drop-down list.
4. Click the **Go** arrow that is located to the right of the drop-down list. The product support Web page is displayed, including the blue **OMEGAMON for Storage support** list box on the right.

Note: The links in this list box go to dedicated Web pages for the product regarding topics such as downloads and troubleshooting. In many cases, using these links leads you to product-specific information more quickly than entering search terms.

5. To obtain information on APARs, perform the following steps:
 - a. Click **Troubleshoot** in the **OMEGAMON for Storage support** list box to access the **Troubleshoot** support page.
 - b. Click **APARs** in the **Browse by document type** area to access a list of APARs, with the most recent APARs first.
 - c. Enter search terms to find specific types of APARs, as needed.
6. To obtain information on fixes, fix packs, and other service updates for OMEGAMON for Storage, perform the following steps:
 - a. Click **Download** in the **OMEGAMON for Storage support** list box to access the **Download** support page.
 - b. Click the **Recommended fixes** link to access the **Recommended Maintenance Service Levels** page. Information for IBM OMEGAMON for Storage on z/OS is provided in several places on this page.

What to do next

For more information about the types of fixes that are available, see the IBM Software Support Handbook at <http://techsupport.services.ibm.com/guides/handbook.html>.

Obtaining PTFs (Program Temporary Fixes)

About this task

The following steps describe how to identify and obtain required maintenance, known as PTFs (Program Temporary Fixes):

Procedure

1. Access the “Technical help database page for mainframe Preventive Service Planning (PSP) buckets” Web page at <http://www14.software.ibm.com/webapp/set2/psp/srchBroker>.
2. Find relevant PSP Buckets. Search for PSP Buckets that have the OMEGAMON for Storage, V4.2.0 prefix: **OMXES4200**.
3. Consult each PSP Bucket to learn what PTFs are required.
4. Access the Shop z-Series Web site to obtain the PTFs at <https://www14.software.ibm.com/webapp/ShopzSeries/ShopzSeries.jsp>.

Receiving weekly support updates

About this task

To receive weekly e-mail notifications about fixes and other software support news, follow these steps:

Procedure

1. Go to the IBM Software Support Web site at <http://www.ibm.com/software/support>.
2. Click **My support** in the far upper-right corner of the page under **Personalized support**.
3. If you have already registered for **My support**, sign in and skip to the next step. If you have not registered, click **register now**. Complete the registration form using your e-mail address as your IBM ID and click **Submit**.
4. Click **Edit profile**.
5. In the **Products** list, select **Software**. A second list is displayed.
6. In the second list, select a product segment, for example, **Systems management**. A third list is displayed.
7. In the third list, select a product sub-segment, for example, **Application Performance & Availability**. A list of applicable products is displayed.
8. Select the products for which you want to receive updates.
9. Click **Add products**.
10. After selecting all products that are of interest to you, click **Subscribe to email** on the **Edit profile** tab.
11. Select **Please send these documents by weekly email**.
12. Update your e-mail address as needed.
13. In the **Documents** list, select **Software**.
14. Select the types of documents that you want to receive information about.
15. Click **Update**.

What to do next

If you experience problems with the **My support** feature, you can obtain help in one of the following ways:

- Online
Send an e-mail message to erchelp@ca.ibm.com, describing your problem.
- By phone
Call 1-800-IBM-4YOU (1-800-426-4968).

Contacting IBM Software Support

IBM Software Support provides assistance with product defects.

Before you begin

Before contacting IBM Software Support, your company must have an active IBM software maintenance contract, and you must be authorized to submit problems to IBM. The type of software maintenance contract that you need depends on the type of product you have:

- For IBM distributed software products (including, but not limited to, Tivoli, Lotus®, and Rational® products, as well as DB2 and Websphere products that run on Windows, or UNIX operating systems), enroll in Passport Advantage in one of the following ways:
 - Online
Go to the Passport Advantage Web site at http://www-306.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm.
 - By phone
For the phone number to call in your country, go to the IBM Software Support Web site at <http://techsupport.services.ibm.com/guides/contacts.html> and click the name of your geographic region.
- For customers with Subscription and Support (S & S) contracts, go to the Software Service Request Web site at <https://techsupport.services.ibm.com/ssr/login>.
- For customers with IBMLink, CATIA, Linux, OS/390, iSeries®, pSeries, zSeries, and other support agreements, go to the IBM Support Line Web site at <http://www.ibm.com/services/us/index.wss/so/its/a1000030/dt006>.
- For IBM eServer software products (including, but not limited to, DB2 and Websphere products that run in zSeries, pSeries, and iSeries environments), you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for eServer software products, go to the IBM Technical Support Advantage Web site at <http://www.ibm.com/servers/eserver/techsupport.html>.

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States. From other countries, go to the contacts page of the IBM Software Support Handbook on the Web at <http://techsupport.services.ibm.com/guides/contacts.html> and click the name of your geographic region for phone numbers of people who provide support for your location.

About this task

To contact IBM Software Support, follow these steps:

Procedure

1. Determining the business impact
2. Describing problems and gathering information
3. Submitting problems

Determining the business impact

When you report a problem to IBM, you are asked to supply a severity level. Therefore, you need to understand and assess the business impact of the problem that you are reporting.

Use the following criteria:

- Severity 1
The problem has a critical business impact. You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.
- Severity 2
The problem has a significant business impact. The program is usable, but it is severely limited.
- Severity 3
The problem has some business impact. The program is usable, but less significant features (not critical to operations) are unavailable.
- Severity 4
The problem has minimal business impact. The problem causes little impact on operations, or a reasonable circumvention to the problem was implemented.

Describing problems and gathering information

When describing a problem to IBM, be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently.

To save time, know the answers to these questions:

- What software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can you re-create the problem? If so, what steps were performed to re-create the problem?
- Did you make any changes to the system? For example, did you make changes to the hardware, operating system, networking software, and so on.
- Are you currently using a workaround for the problem? If so, be prepared to explain the workaround when you report the problem.

Submitting problems

You can submit your problem to IBM Software Support in one of two ways:

- Online
Click **Submit and track problems** on the IBM Software Support site at <http://www.ibm.com/software/support/probsub.html>. Type your information into the appropriate problem submission form.
- By phone

For the phone number to call in your country, go to the contacts page of the IBM Software Support Handbook at <http://techsupport.services.ibm.com/guides/contacts.html> and click the name of your geographic region.

If the problem you submit is for a software defect or for missing or inaccurate documentation, IBM Software Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Software Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the Software Support Web site daily, so that other users who experience the same problem can benefit from the same resolution.

Chapter 18. Notices

This information was developed for products and services offered in the U.S.A.

This material may be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

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 be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right 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 have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM® Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

1623-14, Shimotsuruma, Yamato-shi

Kanagawa 242-8502 Japan

The following paragraph does not apply in 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 not apply to you.

This publication might 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 make improvements and/or changes in the products and/or the programs described in this publication at any time without notice.

Licensees of this program who want to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

2Z4A/101

11400 Burnet Road

Austin, TX 78758 U.S.A.

Such information 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 Programming License Agreement, or any equivalent agreement between us.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, 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.

Index

A

About This Guide v
Additional steps 23

C

Configuring common z/OS components 19
Configuring the collection and display of historical data 49
Configuring the TEMS server 19
Configuring Tivoli OMEGAMON for storage on z/OS 21
Configuring using PARMGEN 19
Contacting IBM Software Support 70
Creating a presentation address space 43

D

Data collection restrictions 30, 31
Defining access level resource rules 17
Defining function level resource rules 17
Defining product level resource rules 16
Describing problems and gathering information 71
Determining the business impact 71

E

External security: access level 13
External security: defining for RACF 16
External security: function level 14
External security: product level 13
External security: resource tables 15

F

Forwarding events to other Tivoli products 45

I

IBM Tivoli Monitoring Library 64

M

Mechanisms for collecting historical data 49
Migrating user DASD group definitions 33

N

Notices 73

O

Obtaining and activating the ks3.baroc file 45
Obtaining fixes 68
Obtaining PTFs 69
OMEGAMON and Tivoli Management Services on z/OS Common library 64
OMEGAMON II for SMS 10
Other considerations 18
Other sources of documentation 65
Overview of prerequisites 4

P

Planning for deployment 1
planning_security 5
Product overview 1

R

Receiving weekly support updates 69
Recognizing a new RACF user 17
Related publications 64
Relation of *.baroc files and *.map files 46
Restarting Tivoli subsystem 11

S

Setting security 12
Setting the historical configuration collection interval 29
Setting up a runtime environment 19
Short-term history and long-term history 50
Stages of planning, installation, and configuration 3
Storage agent 9
Storage toolkit 8
Submitting problems 71
Subsystem component 10
Support information 67

T

Table of metrics regarding the persistent data store 50
Trademarks 74

U

Upgrading from version 4.1.0 to version 4.2.0 27
Upgrading to version 4.2.0 Interim Feature 1 29
Upgrading to version 4.2.0 Interim Feature 2 30

Upgrading to version 4.2.0 Interim Features 1 and 2 29
Upgrading to version 5.1.0 33
Upgrading to version 5.2.0 35
Upgrading to version 5.3.0 37
Upgrading to version 5.4.0 39
Upgrading to version 5.5.0 41
Using IBM Support Assistant 67



Printed in USA

SC27-4378-04

