5.5

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

SC27-4378-06

Note

Before using this information and the product it supports, read the information in “Notices” on page 31.

Edition notice

2023-09-21

This edition applies to Version 5.5 of OMEGAMON for Storage on z/OS and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

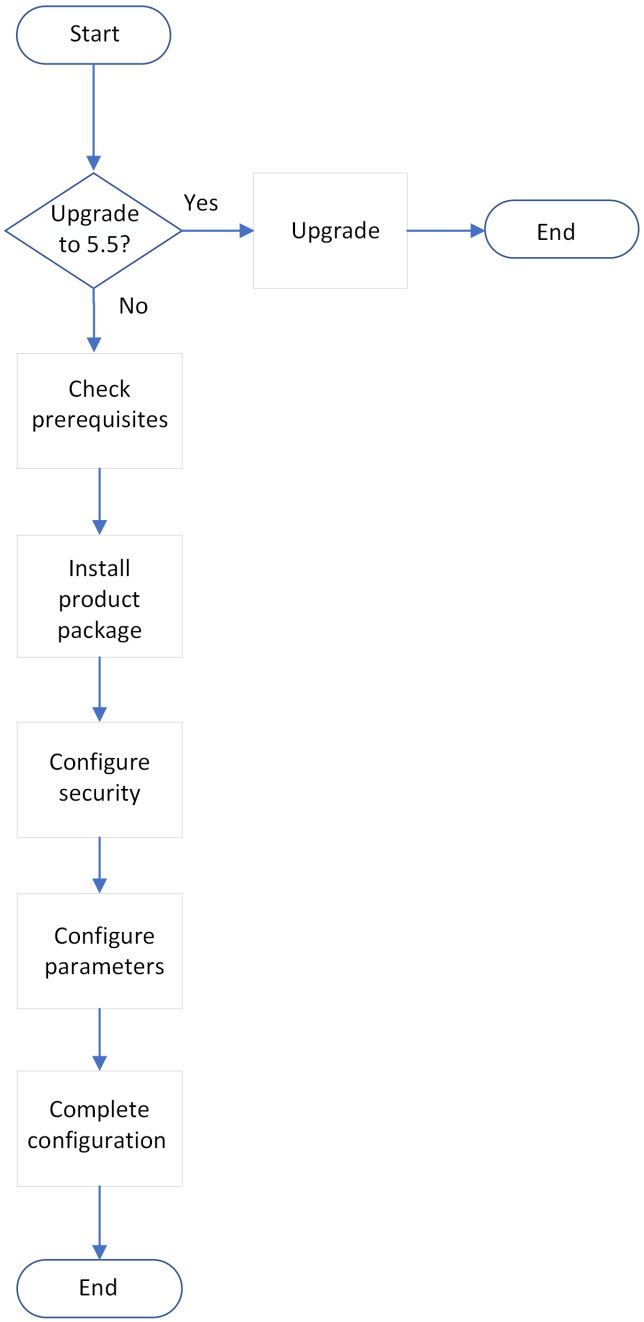
Chapter 1. Planning your deployment

This document is intended for anyone deploying OMEGAMON for Storage for monitoring in the z/OS environment.

Use the information to plan, upgrade, install, or configure OMEGAMON for Storage on z/OS. While planning for the OMEGAMON for Storage on z/OS configuration, you must ensure that you have the required products and the security measure guidelines available.

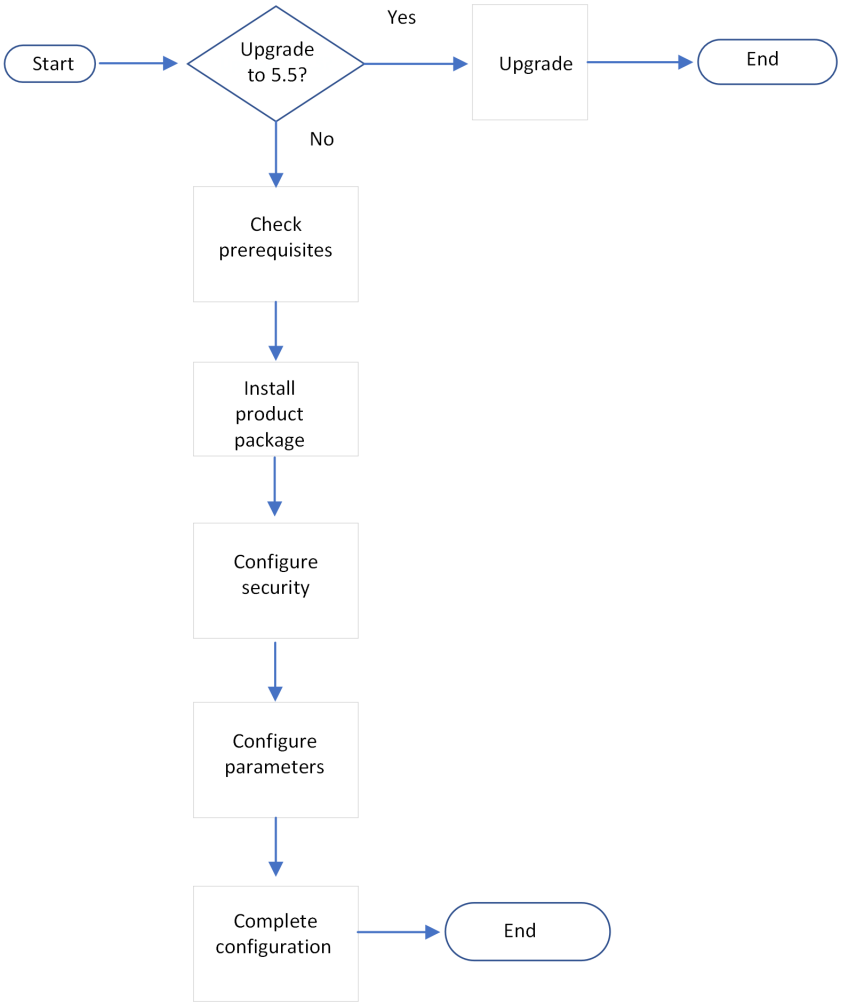
Deployment workflow

Refer to the workflow diagram to understand the stages of the OMEGAMON for Storage on z/OS deployment process.



Deployment workflow

Refer to the workflow diagram to understand the stages of the OMEGAMON for Storage on z/OS deployment process.



Upgrading to version 5.5

OMEGAMON for Storage on z/OS supports upgrading from releases 4.2, interim features 1 and 2, 5.1 or later to version 5.5. Note that after you upgrade to version 5.5, you cannot roll back to the previous versions.

If you already have an existing version of OMEGAMON for Storage on z/OS, perform the following steps.

1. Ensure that the OMEGAMON platform monitoring agents and the OMEGAMON version 5.5.0 monitoring agents are updated. You must have z/OS® -- 630 FP2 and distributed -- 630 FP7.

   To upgrade these components, refer to *OMEGAMON and Tivoli Management Services on z/OS: Upgrade Guide* on OMEGAMON shared documentation.
2. Modify your IBM Tivoli Management Services (TEMS) started task JCLs in your production proclib to include the following DD statement: `DD RKS3IDCO DUMMY`.
3. Load the Run Time Environments (RTEs) to upgrade the parameters and the executables.
4. Restart the started task controls (STCs).
5. Optional: To use the E3270 interface, you must configure the component parameters.

   The configuration steps are available at OMEGAMON shared documentation.

Deployment prerequisites

Each component in the OMEGAMON for Storage on z/OS deployment process requires a distinct set of prerequisites.

Component	Required or Optional	Resource location
OMEGAMON for Storage on z/OS	Required	• For installing prerequistes, see *IBM OMEGAMON for Storage on z/OS: Program Directory*. • For configuring the OMEGAMON for Storage on z/OS parameter values, see "KS3 and KDF parameters configuration" on page 9.
Distributed IBM Tivoli Management Services	Required	• For installing prerequistes, see *IBM OMEGAMON for Storage on z/OS: Program Directory*. • For configuring IBM Tivoli Management Services, see "Configuring Tivoli Management Services" on page 9. • For forwarding events from IBM Tivoli Enterprise Monitoring Agent, see "Forwarding events from IBM Tivoli Enterprise Monitoring Agent" on page 23.
Historical reporting	Required	• For historical component prerequisites, see the *IBM Tivoli Monitoring: Installation and Setup Guide* at OMEGAMON shared documentation. • For historical data collection mechanism specific to OMEGAMON for Storage on z/OS, see "Mechanisms for collecting historical data" on page 12.
OMEGAMON subsystem	Required	To start the OMEGAMON subsystem, see "Starting the OMEGAMON subsystem" on page 10.
Zowe	Optional	Required only if you want to use the Realtime Dataset Metrics web user interface. For supported Zowe versions, see the "Selecting target system" on page 11.
OMEGAMON enhanced 3270 user interface	Optional	To configure this component, see OMEGAMON shared documentation.

Chapter 2. Configuring IBM OMEGAMON for Storage on z/OS

Configuring IBM OMEGAMON for Storage on z/OS requires customizing the values for a set of configuration parameters with your preferred configuration tool.

To configure IBM OMEGAMON for Storage on z/OS, you must do the following:

1. Implement security based on your enterprise setup.
2. Configure the KS3 and the KDF parameters.
3. Complete the configuration steps.
4. Review the mechanism for collecting historical data.

   This is an optional step.
5. Forward events from IBM Tivoli Enterprise Monitoring Agent.

   This is an optional step.

Security considerations

Before you begin the deployment process, you must secure the TLS (HTTPS) communication for the IBM OMEGAMON for Storage on z/OS components and follow the required authentication and authorization steps.

Implementing security for IBM OMEGAMON for Storage on z/OS is unique to your enterprise setup. You can use the information in the following sections to understand the security guidelines.

For IBM Tivoli Management Services, you can use one of the following for user authentication:

- Resource Access Control facility (RACF®) , a part of z/OS
- Security Authorization Facility (SAF)

Configuring Storage Agent

With IBM® Tivoli® Storage Manager for Storage Area Networks, client systems can write and read data directly to or from the storage devices that are attached to a storage area network (SAN).

You must establish security authorization for Tivoli Enterprise Monitoring Server (TEMS), as defined in the DFSMSrmm product documentation.

1. Authorize the TEMS started task to issue the following RMM commands:
   - **LISTCONTROL**
   - **LISTOWNER**
   - **SEARCHVOLUME**
   - **SEARCHDATASET**
   - **SEARCHVRS**
2. Ensure that the TEMS started task has `RACF CONTROL` access to profile `STGADMIN.EDG.LISTCONTROL` in `FACILITY` class.

Configuring AT-TLS

You must configure your Application Transparent Transport Layer Security (AT-TLS) Policy Agent to provide secure TLS (HTTPS) communication for the components that support the Realtime Dataset

Metrics Web (RDM) user interface. Configuring AT-TLS involves creating certificates or keyrings and customizing the parameters.

The syntax for referring to specific properties of specific rules in this procedure uses a ‘dot’ notation: <rule name>.<property> as in the following example TTLS rule. The port number can be any available port between 1 and 65535 inclusive. In this example, the LocalPortRange value is 12345 and the `LocalPortRange` property of this specific rule is referred as `KS3_RDM.LocalPortRange`. The rule names in the sample AT-TLS rules file is unique to prevent conflict with any exisiting rule names. If you can keep the same rule names in your AT-TLS parameters, then you can relate the steps with your AT-TLS rules.

1. 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 must run under the same user id (for example, KS3STC), and the user id needs access to the new keyring.
2. Optional: To use a different keyring name, you must adjust the following parameter : `keyring~KS3.Keyring`
3. Change the `*.priority` value to fit in with the priority numbering for your site.

   These rules are specific, so you can 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 do not change the default values, then you can use the existing example TLS Rules.
4. Optional: To make configuration changes, adjust the following required and optional TLS parameters values:

   Required parameters

   - **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

   Note:

   Change these optional default values in KS3AINIT and in the corresponding TLS configuration only when you receive instruction from support:

   - **KS3_APPSRV_TO_RDM.RemoteAddr** RDM_LISTENER_ADDR in KS3AINIT
   - **KS3_RDM.LocalAddr** RDM_LISTENER_ADDR in KS3AINIT
   - **KS3_APPSRV_TO_APPSRV.RemoteAddr** Change only to account for special network configurations on the host system

The port range values in this example are samples. The port numbers can be any available port between 1 and 65535 inclusive.

```
TTLSRule                          KS3_RDM
{
  LocalAddr                       127.0.0.1
  LocalPortRange                  12345
  Direction                       Inbound
  Jobname                         S3TMS95D
  Priority                        4
  TTLSGroupActionRef              gAct1~KS3
  TTLSEnvironmentActionRef        eAct1~KS3_SRV
  TTLSConnectionActionRef         cAct1~KS3_SRV
}
TTLSRule                          KS3_APPSRV_TO_RDM
{
  RemoteAddr                      127.0.0.1
  RemotePortRange                 12345
  Direction                       Outbound
```

```
  Priority                          4
  TTLSGroupActionRef                gAct1~KS3
  TTLSEnvironmentActionRef          eAct1~KS3_CLIENT
  TTLSConnectionActionRef           cAct1~KS3_CLIENT
}
TTLSRule                            KS3_APPSRV
{
  LocalPortRange                    48700
  Direction                         Inbound
  Priority                          4
  TTLSGroupActionRef                gAct1~KS3
  TTLSEnvironmentActionRef          eAct1~KS3_SRV
  TTLSConnectionActionRef           cAct1~KS3_SRV
}
TTLSRule                            KS3_APPSRV_TO_APPSRV
{
  RemoteAddr                        127.0.0.1
  RemotePortRange                   48700
  Direction                         Outbound
  Priority                          4
  TTLSGroupActionRef                gAct1~KS3
  TTLSEnvironmentActionRef          eAct1~KS3_CLIENT
  TTLSConnectionActionRef           cAct1~KS3_CLIENT
}
TTLSGroupAction                     gAct1~KS3
{
  TTLSEnabled                       On
  Trace                             4
}
TTLSEnvironmentAction               eAct1~KS3_CLIENT
{
  HandshakeRole                     Client
  EnvironmentUserInstance           0
  TTLSEnvironmentAdvancedParmsRef eAdv1~KS3
  TTLSKeyringParmsRef               keyring~KS3
  Trace                             4
}
TTLSEnvironmentAction               eAct1~KS3_SRV
{
  HandshakeRole                     Server
  EnvironmentUserInstance           0
  TTLSEnvironmentAdvancedParmsRef eAdv1~KS3
  TTLSKeyringParmsRef               keyring~KS3
  Trace                             4
}
TTLSConnectionAction                cAct1~KS3_SRV
{
  HandshakeRole                     Server
  TTLSCipherParmsRef                cipher-KS3
  TTLSConnectionAdvancedParmsRef  cAdv1~KS3
  CtraceClearText                   On
  Trace                             4
}
TTLSConnectionAction                cAct1~KS3_CLIENT
{
  HandshakeRole                     Client
  TTLSCipherParmsRef                cipher-KS3
  TTLSConnectionAdvancedParmsRef  cAdv1~KS3
  CtraceClearText                   On
  Trace                             4
}
TTLSConnectionAdvancedParms         cAdv1~KS3
{
  ResetCipherTimer                  0
  SecondaryMap                      Off
}
TTLSKeyringParms                    keyring~KS3
{
  Keyring                           S3STC/KS3TRNG
}
TTLSEnvironmentAdvancedParms        eAdv1~KS3
{
  ClientAuthType                    PassThru
  ApplicationControlled             Off
  SSLv2                             Off
  SSLv3                             Off
  TLSv1                             Off
  TLSv1.1                           Off
  TLSv1.2                           On
}
TTLSCipherParms                     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
}
```

Prevent AT-TLS connection failure with RDM and Application server encryption.

RDM and Application server encryption

Application Transparent Transport Layer Security (AT-TLS) provides a secure session for Realtime Dataset Metrics (RDM) and OMEGAMON for Storage. You can prevent connection AT-TLS connection failures by enabling encryption for both RDM and the Application server.

A connection failure occurs when the RDM server and Application server do not both have encryption enabled, or when you use the Application server both as the self client and receiver, and encryption is not enabled for both. When this happens, both the Standard Output (STDOUT) and in the AT-TLS log file displays error messages.

Storage Toolkit

With Storage Toolkit, you can initiate z/OS commands from Tivoli Enterprise Portal (TEP). Note that the monitoring agent uses the portal user ID to establish the security environment and the security environment is unique to the user who submits the request. Hence, you must ensure to take security measures before initiating any commands.

You can use Storage Toolkit to issue the following commands on the z/OS system where the monitoring agent is running.

- **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, you can also 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 complete a request are executed under a security environment on thez/OS system where the monitoring agent runs. A security environment is created when you submit a request and is destroyed when the request ends. The types of activities that are processed within the security context include:

- Creating and accessing temporary data sets required for 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)

These 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. In this approach, the user accounts (IDs) defined to the portal server must 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 also not a valid mainframe user ID, the request fails.

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

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 match the user IDs on the z/OS system that hosts the monitoring agent.

KS3 and KDF parameters configuration

You must accept or customize the KS3 and the KDF parameter values to configure OMEGAMON for Storage on z/OS.

OMEGAMON for Storage on z/OS and the related components use parameters that are common to all the OMEGAMON monitoring agents, such as the runtime environments and the IBM Tivoli Management Services parameters. Some parameters are specific to a particular agent.

The *Parameter Reference* document provides details of the parameters specific to OMEGAMON for Storage on z/OS. It is recommended to use Configuration Manager though PARMGEN is also supported. To configure the parameters, see OMEGAMON shared documentation. The prerequisite for performing the instructions is that a Tivoli Enterprise Monitoring Server is already configured in the runtime environment. Install the OMEGAMON for Storage on z/OS monitoring agent in the same address space as the monitoring server.

Complete the configuration

After you configure IBM OMEGAMON for Storage on z/OS using your preferred configuration tool, you must complete the following post-configuration steps.

Table 1. Post-configuration steps

Step	**Required or Optional**
Configuring Tivoli Management Services	Required
Starting the OMEGAMON subsystem	Required
Configuring the Realtime Dataset Metrics (RDM) user interface	Optional

Configuring Tivoli Management Services

You must configure an instance of Tivoli Enterprise Monitoring Server (TEMS) on z/OS to ensure that IBM OMEGAMON for Storage on z/OS monitoring agent is installed in the same address space as a monitoring server. In addition, you must configure the monitoring server from a monitoring agent.

Refer to the resources at OMEGAMON shared documentation for the following information:

- To apply the best practices for the configuration, see the 'Configuring your products' document.
- To configure the monitoring server on z/OS, see the Configuring the TEMS manual.
- To configure the Tivoli Enterprise Monitoring Server, read the planning, installing, and configuring topics.

1. Enable the SNA communication protocol 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 the communication protocols.
2. If a monitoring server is already installed when you set up OMEGAMON for Storage, add the SNA option to the server configuration.
3. Optional: For forwarding events to other Tivoli products, see “Forwarding events from IBM Tivoli Enterprise Monitoring Agent” on page 23.

Starting the OMEGAMON subsystem

You must start the OMEGAMON Subsystem before starting Tivoli Enterprise Monitoring Server (TEMS) on the same z/OS image. You cannot stop or cancel the OMEGAMON subsystem before the termination of the TEMS address space on the same z/OS image.

1. Modify the subsystem JCL to meet your installation requirements to prevent time out.
2. Modify the **TIM** parameter on the generated OMEGAMON subsystem JCL procedure.

Realtime Dataset Metrics Web user interface

The Realtime Dataset Metrics (RDM) is a browser user interface, which you can launch from the Dataset Attributes System Summary in the Tivoli Enterprise Monitoring Server (TEMS) user interface.

Realtime Dataset Metrics replaces the Dataset Attributes Database collector to improve performance and timely data delivery. The Dataset Attributes Database collector function was delivered in version 5.4.0. For more information on the RDM collection, see New Feature – Real-time Dataset Metrics.

The key features of RDM are:

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

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

A database traversal occurs when the user clicks the **Run Query** button, or the user clicks a column header to change sort. Highly selective filter or sort combinations, such as a complex dataset mask the allocated tracks sort, might result in slow response time. Navigating the results through the Page Next or Prev option does not result in a database traversal.

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

Prerequisites for configuring Realtime Dataset Metrics Web user interface

You must gather the following components before starting the Realtime Dataset Metrics Web user interface configurations steps.

z/OS requirements

- OMEGAMON for Storage agent with completed Dataset Attribute Collection.
- The 5698-ZWE IBM Z Distribution for Zowe 1.0 with installed PTFs UO01942 and UO01943, or the 5698-ZWG IBM Z Distribution for Zowe 2.0 with installed PTFs UO02049 and UO02050.
- zFS directory (allocation = 100MB)
- SAF credentials to login to the web UI

Browser requirements

- Chromium based v79 (Chrome and Edge) or later
- Firefox v68 or later

Selecting target system

The target system is the system software libraries and other data sets that you are installing. You must select the target system to configure Realtime Dataset Metrics (RDM) for data retrieval.

1. Log on to Zowe.
2. Open Data Set Metrics to see the server list of currently added RDM systems.
3. If your system is present in the list, select it and specify the credentials from the target system.
4. If the system is not present in the list, click the **Gear** button to open the **Configuration** dialog.
5. Click **Add server +** and specify the DNS or IP address and port for the system that has RDM configured.

   The port is also printed in the RKLVLOG: KS3S0166I KS3SDADW: HTTP SERVER ON PORT = xxxxx STARTED.

Configuring the Realtime Dataset Metrics server

You must configure the parameters values to generate the RKANPARU member KS3AINIT that the OMEGAMON for Storage agent reads to run the Realtime dataset Metrics (RDM) daemon. It is recommended to use Configuration Manager though PARMGEN is also supported.

Configure the following KS3 parameters:

- **KS3_NODEJS_HOME**
  The NODE_HOME directory where NODE.js is installed. If this value is not specified, it is presumed that the Realtime Dataset Metrics Web UI is not required at your site.
- **KS3_AS_LISTENER_ADDR**
  The IP address that is accessible from TEP. Typically, it is the non-loop back address of the LPAR.
- **KS3_AS_SERVICE_ADDR**
  The address (URL) that TEP clients uses to connect to the RDM Application Server.
- **KS3_APP_ZFS_DIR**
  This is the ZFS directory where the RDM Application Server is to be installed. If this is not specified, the value {{/#rtehome/#rtename/KS3/rdm }}is used.
- **KS3_APP_PORT**
  The port on which Zowe with RDM is used.

  Required (value between 48901 and 65535), for example: KS3_APP_PORT=48902
- **KS3_RDM_PORT**
  As with KS3_APP_PORT, this is a value in KS3AINIT, except that the value must be between 1 and 65535, for example: KS3_RDM_PORT=48903

  On this port, the OMEGAMON for Storage agent starts the RDM daemon, which is used for communication between RDM UI and Agent's data.
- **KS3_AS_PROTO**
  The Application Server protocol: http or https.

  If you use AT-TLS configuration for TEMS, use the https value.

Installing Realtime Dataset Metrics plugins

After the configuration tool processes the Realtime Dataset Metrics (RDM), you must install the RDM plugins to get the enhanced capabilities of the feature.

The 'rdm_plugins' directory contains the plugins required for RDM. You must install these plugins on Zowe.

1. Locate the plugins in the directory specified in KS3_APP_ZFS_DIR.

   The default location is `/#rtehome/#rtename/KS3/rdm`.
2. Find the RDM plugins installation instructions in ++HOLD for each PTF that has the RDM changes.

Mechanisms for collecting historical data

For configuring the historical reporting component in OMEGAMON for Storage, you must be aware of the mechanisms for collecting historical data.

Table 2. Comparison of mechanisms for collecting historical data

Name of configuration method	Storage place for the data	Typical type of data*	Procedure	Purpose
PARMGEN or Configuration Manager **Note:** It is recommended to use Configuration Manager though PARMGEN is also supported.	Persistent data store (PDS)	Short-term history *	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 *	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, consider the amount of data that you are collecting and the amount of 'short-term history' that you want to maintain. For more information regarding sizing, see Table of metrics for persistent data store.

Short-term history and long-term history

While the short-term history is generated from the persistent data store (PDS), the long-term history is generated from Tivoli Data Warehouse.

You can write the short-term data from PDS data sets to Tivoli Data Warehouse for long-term retention. Use the 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 3. 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, keep sufficient space for 24 hours of data. When the option for 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 for Persistent Data Store

The Persistent Data Store (PDS) metrics have separate tables that contain the data sets, collection control, and warehouse enablement information. You must also know how to allocate the correct size for the data sets of your PDS.

Table 4. 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) x 24 x Record size x 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 5. 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

Table 5. Configuration data for the persistent data store (continued)

* Attribute history name/ description	Table name	Group	Collection control	TDW enabled?
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
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

Table 5. Configuration data for the persistent data store (continued)

* Attribute history name/ description	Table name	Group	Collection control	TDW enabled?
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
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

Table 5. Configuration data for the persistent data store (continued)

* Attribute history name/ description	Table name	Group	Collection control	TDW enabled?
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	RMMCFG	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
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

Table 5. Configuration data for the persistent data store (continued)				
*** Attribute history name/ description**	**Table name**	**Group**	**Collection control**	**TDW enabled?**
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)
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)

* Attribute history name/ description	Record size	Frequency	Estimated space req
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)
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)

* Attribute history name/ description	Record size	Frequency	Estimated space req
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)
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)

* Attribute history name/ description	Record size	Frequency	Estimated space req
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)
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)

* Attribute history name/ description	Record size	Frequency	Estimated space req
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)
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)

* Attribute history name/ description	Record size	Frequency	Estimated space req
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)
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)

* Attribute history name/ description	Record size	Frequency	Estimated space req
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)
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)

Forwarding events from IBM Tivoli Enterprise Monitoring Agent

If you use IBM Tivoli Enterprise Console or IBM Tivoli Netcool/OMNIbus to manage events in your enterprise, you can forward events from IBM Tivoli Enterprise Monitoring Agent to these event management products.

You must enable event forwarding and install the event synchronization component to forward events from IBM Tivoli Enterprise Monitoring Agent.

1. Enable event forwarding on the hub monitoring server and define a default destination server.
2. Configure the IBM Tivoli Enterprise Console server, or the Tivoli Netcool/OMNIbus event server to receive the events.
3. Install a situation update forwarding process on the event server.
4. Install and import the BAR0C file for the agent on the event server for events forwarded toIBM Tivoli Enterprise Console.

   For detailed instructions on enabling event forwarding and installation of the event synchronization component, see the IBM Tivoli Monitoring: Installation and Setup guide.
5. Optional: With Situation Editor in the Tivoli Enterprise Portal, select the situation events to forward to your chosen event server.
6. Optional: Assign an event status compatible with the target event server.

   For information on specifying the situation events to forward, see the Tivoli Enterprise Portal online help.

Activating the ks3.baroc file

In OMEGAMON for Storage, the ks3.baroc file provides the event forwarding feature to IBM Tivoli Enterprise Console.

The ks3.baroc file, which is included with the application support you install for the monitoring agent. You obtain the omegamon.baroc file required for event synchronization during the installation of event synchronization on the event server. You cannot obtain this file from the application support software for the monitoring agent.

1. Install application support on a distributed monitoring server.

   For detailed steps, see Configuring Tivoli Enterprise Monitoring Server at OMEGAMON shared documentation.

   The ks3.baroc file gets stored in one of the following locations:

   - On Windows systems: itm_home\cms\TECLIB, where itm_home is the directory you installed IBM Tivoli Monitoring.
   - On UNIX-based systems: itm_home/tables/ms_name/TECLIB directory, where itm_home is the directory you installed IBM Tivoli Monitoring and ms_name is the name of the monitoring server.

   Note: The ks3.baroc file located on this monitoring server is only for storing. Hence, no software application runs or references this file on this monitoring server.
2. Copy the ks3.baroc file to the event server for IBM Tivoli Enterprise Console.
3. On the IBM Tivoli Enterprise Console event server, run a series of IBM Tivoli Enterprise Console commands that import, compile, and load the ks3.baroc file in IBM Tivoli Enterprise Console.

Relation of *.baroc files and *.map files

All the OMEGAMON products use the *.baroc files. The ks3.baroc file is the only *.baroc file in OMEGAMON for Storage. With the related ks3.map file, however, you can customize the event data IBM Tivoli Monitoring forwards to a listening event integration facility (EIF), such as the Tivoli Enterprise Console server.

*.baroc file

The *.baroc file is required for event forwarding from IBM Tivoli Enterprise Monitoring Agent to IBM Tivoli Enterprise Console. It is not required for event forwarding to Tivoli Netcool/OMNIbus. You must install the file into the IBM Tivoli Enterprise Console rulebase before the server receives the monitored events.

*.map file

The *.map file controls the event data from IBM Tivoli Enterprise Monitoring Agent forwarded to a listening event integration facility (EIF). You can use it to control event forwarding to both Tivoli Netcool/OMNIbus servers and Tivoli Enterprise Console servers, because both are EIFs. You must synchronize it with a corresponding *.baroc file whenever event handling for IBM Tivoli Enterprise Console is modified.

You can also modify the *.map file to decrease the event data volume forwarded to the listening EIF servers. This capability to decrease the volume is useful for IBM Tivoli Enterprise Console in the following scenarios:

- When an event attribute table of a situation in IBM Tivoli Enterprise Monitoring Agent contains large numbers of attributes.
- When you are monitoring an event, which can produce multiple sub-objects, and you want to reduce the number of attributes that are forwarded for the event.

You can adjust the *.map file to prevent hidden event attributes from passing when the event is triggered. As a result, less data is forwarded to an IBM Tivoli Enterprise Console server.

You must apply the corresponding changes to the *. baroc file, so that event data handling by both the files remains synchronized.

Index

Accessibility

Accessibility features help users with physical disabilities, such as restricted mobility or limited vision, to use software products successfully. OMEGAMON® XE monitoring products support several user interfaces. Product functionality and accessibility features vary according to the interface.

The major accessibility features in this product enable users in the following ways:

- Use assistive technologies, such as screen-reader software and digital speech synthesizer, to hear what is displayed on the screen. Consult the product documentation of the assistive technology for details on using those technologies with this product.
- Operate specific or equivalent features using only the keyboard.
- Magnify what is displayed on the screen.

In addition, the product documentation was modified to include the following features to aid accessibility:

- All documentation is available in both HTML and convertible PDF formats to give the maximum opportunity for users to apply screen-reader software.
- All images in the documentation are provided with alternative text so that users with vision impairments can understand the contents of the images.

Interface information

The Tivoli® Enterprise Portal interface offers the greatest range of functionality, but is not entirely accessible. The OMEGAMON Enhanced 3270 user interface offers more limited functionality, but is entirely accessible. (The enhanced 3270 user interface supports all the accessibility features supported by your emulator. If you are using IBM® Personal Communications, you can find information on its accessibility features at http://publib.boulder.ibm.com/infocenter/pcomhelp/v6r0/index.jsp?topic=/com.ibm.pcomm.doc/books/html/quick_beginnings10.htm. If you are using a third-party emulator, see the documentation for that product for accessibility information.)

The OMEGAMON ("classic") and OMEGAMON II (CUA) 3270 interfaces use an ISPF style interface. Standard and custom PF Key settings, menu options, and command line interface options allow for short cuts to commonly viewed screens. While basic customization options allow for highlights and other eye-catcher techniques to be added to the interface, the customization options are limited.

Related accessibility information

You can view the publications using the Adobe Acrobat Reader.

IBM and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility.

Notices

This information was developed for products and services offered in the US. This material might 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 may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

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 jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

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

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

SC27-4378-06