MAINVIEW
Best Practices:
Event Management

Supporting
MAINVIEW products

May 21, 2008
**Contacting BMC Software**

You can access the BMC Software website at [http://www.bmc.com](http://www.bmc.com). From this website, you can obtain information about the company, its products, corporate offices, special events, and career opportunities.

**United States and Canada**

<table>
<thead>
<tr>
<th>Address</th>
<th>Telephone</th>
<th>Fax</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMC SOFTWARE INC</td>
<td>713 918 8800 or 800 841 2031</td>
<td>713 918 8000</td>
</tr>
<tr>
<td>2101 CITYWEST BLVD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HOUSTON TX 77042-2827 USA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Outside United States and Canada**

<table>
<thead>
<tr>
<th>Telephone</th>
<th>Fax</th>
</tr>
</thead>
<tbody>
<tr>
<td>(01) 713 918 8800</td>
<td>(01) 713 918 8000</td>
</tr>
</tbody>
</table>

© Copyright 2008 BMC Software, Inc.

BMC, BMC Software, and the BMC Software logo are the exclusive properties of BMC Software, Inc., are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other BMC trademarks, service marks, and logos may be registered or pending registration in the U.S. or in other countries. All other trademarks or registered trademarks are the property of their respective owners.

IBM, CICS, DB2, IMS, Tivoli Enterprise Console, VTAM, and WebSphere are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Linux is the registered trademark of Linus Torvalds.

BMC Software considers information included in this documentation to be proprietary and confidential. Your use of this information is subject to the terms and conditions of the applicable End User License Agreement for the product and the proprietary and restricted rights notices included in this documentation.

**Restricted rights legend**

U.S. Government Restricted Rights to Computer Software. UNPUBLISHED -- RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES. Use, duplication, or disclosure of any data and computer software by the U.S. Government is subject to restrictions, as applicable, set forth in FAR Section 52.227-14, DFARS 252.227-7013, DFARS 252.227-7014, DFARS 252.227-7015, and DFARS 252.227-7025, as amended from time to time. Contractor/Manufacturer is BMC SOFTWARE INC, 2101 CITYWEST BLVD, HOUSTON TX 77042-2827, USA. Any contract notices should be sent to this address.
Customer support

You can obtain technical support by using the BMC Software Customer Support website or by contacting Customer Support by telephone or e-mail. To expedite your inquiry, see “Before contacting BMC.”

Support website

You can obtain technical support from BMC 24 hours a day, 7 days a week at http://www.bmc.com/support_home. From this website, you can

- read overviews about support services and programs that BMC offers
- find the most current information about BMC products
- search a database for issues similar to yours and possible solutions
- order or download product documentation
- download products and maintenance
- report an issue or ask a question
- subscribe to receive proactive e-mail alerts when new product notices are released
- find worldwide BMC support center locations and contact information, including e-mail addresses, fax numbers, and telephone numbers

Support by telephone or e-mail

In the United States and Canada, if you need technical support and do not have access to the web, call 800 537 1813 or send an e-mail message to customer_support@bmc.com. (In the subject line, enter SupID:<yourSupportContractID>, such as SupID:12345). Outside the United States and Canada, contact your local support center for assistance.

Before contacting BMC

Have the following information available so that Customer Support can begin working on your issue immediately:

- product information
  - product name
  - product version (release number)
  - license number and password (trial or permanent)
- operating system and environment information
  - machine type
  - operating system type, version, and service pack or other maintenance level such as PUT or PTF
  - system hardware configuration
  - serial numbers
  - related software (database, application, and communication) including type, version, and service pack or maintenance level
- sequence of events leading to the issue
- commands and options that you used
- messages received (and the time and date that you received them)
  - product error messages
  - messages from the operating system, such as file system full
  - messages from related software
# Contents

## About this book
- Related publications ........................................ 10
- Conventions .................................................. 11

## Chapter 1  Introduction
- What are Best Practices? ................................. 14
- What is covered and what is not ....................... 15
- Terms and concepts ......................................... 16

## Chapter 2  Important MAINVIEW metrics
- Types of metrics ............................................. 20
- How MAINVIEW collects metrics ....................... 21
  - Data collectors and views ............................... 21
  - Alarms ......................................................... 21
  - Background monitors .................................. 22
  - Alerts .......................................................... 22
- Responding to metrics .................................... 23
- How to use the metric tables ........................... 24
- Operating system metrics ................................. 25
  - z/OS metrics ............................................... 25
  - Linux metrics .............................................. 28
  - UNIX System Services metrics ....................... 29
  - Storage Resource Manager (SRM) metrics .......... 30
- Subsystems and application server metrics .......... 32
  - CICS metrics ............................................. 32
  - DB2 metrics ................................................ 38
  - IMS metrics ............................................... 42
  - WebSphere Application Server metrics............... 46
- Networks and communications metrics ............... 48
  - TCP/IP metrics .......................................... 48
  - WebSphere MQ metrics ................................ 49

## Chapter 3  Managing applications
- Why manage the application ............................ 56
- Collect information about the application .......... 57
- Define a workload to monitor the application .... 58
  - Best Practices for workload definitions ............ 59
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage application availability</td>
<td>60</td>
</tr>
<tr>
<td>Manage application exceptions</td>
<td>61</td>
</tr>
<tr>
<td>Best Practices for alarms</td>
<td>62</td>
</tr>
<tr>
<td>Manage application transactions</td>
<td>64</td>
</tr>
<tr>
<td>Summary of Best Practices: Managing the application</td>
<td>65</td>
</tr>
<tr>
<td>Chapter 4  Automating event management</td>
<td>67</td>
</tr>
<tr>
<td>Why automate</td>
<td>68</td>
</tr>
<tr>
<td>What to automate</td>
<td>68</td>
</tr>
<tr>
<td>Collect information about events</td>
<td>69</td>
</tr>
<tr>
<td>Create Rules to automate a solution</td>
<td>70</td>
</tr>
<tr>
<td>Best Practices for Rules</td>
<td>71</td>
</tr>
<tr>
<td>Configuration recommendations for MAINVIEW AutoOPERATOR</td>
<td>74</td>
</tr>
<tr>
<td>Beyond basic event management</td>
<td>75</td>
</tr>
<tr>
<td>Summary of Best Practices: Automating event management</td>
<td>76</td>
</tr>
<tr>
<td>Appendix A  Event management worksheets</td>
<td>77</td>
</tr>
<tr>
<td>Application information worksheet</td>
<td>78</td>
</tr>
<tr>
<td>Message automation request form</td>
<td>80</td>
</tr>
<tr>
<td>Event automation worksheet</td>
<td>82</td>
</tr>
<tr>
<td>Index</td>
<td>85</td>
</tr>
</tbody>
</table>
Tables

z/OS metrics ................................................................. 25
Linux metrics ............................................................... 28
UNIX System Services metrics ........................................ 29
Storage Resource Manager (SRM) metrics ....................... 30
CICS metrics ............................................................... 32
CICS monitor metrics ..................................................... 37
DB2 metrics ................................................................. 38
DB2 monitor metrics ....................................................... 41
IMS metrics ................................................................. 42
IMS monitor metrics ....................................................... 45
WebSphere Application Server metrics ............................ 46
TCP/IP metrics ............................................................. 48
WebSphere MQ metrics ................................................... 49
Best Practices: Managing the application ......................... 65
Best Practices: Automating event management .................. 76
About this book

This book contains recommendations for establishing an event management strategy for your mainframe environment. This book is intended for

- CIOs and director-level management
- systems programmers, application programmers, Help Desk personnel, analysts, and other troubleshooters
- capacity planners, software installers, and anyone who requires supporting metrics

Like most BMC documentation, this book is available in printed and online formats. To request printed books or to view online books and notices (such as release notes and technical bulletins), see the Customer Support website at http://www.bmc.com/support_home. Most product shipments also include the books on a documentation CD.

**NOTE**

Online books are formatted as PDF or HTML files. To view, print, or copy PDF books, use the free Adobe Reader from Adobe Systems. If your product installation does not install the reader, you can obtain the reader at http://www.adobe.com.
## Related publications

The following related publications supplement this book:

<table>
<thead>
<tr>
<th>Category</th>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>installation documents</td>
<td>MAINVIEW Customization Guide</td>
<td>provides instructions for manually customizing the MAINVIEW environment for your products</td>
</tr>
<tr>
<td>product customization guides</td>
<td>MAINVIEW User Guide</td>
<td>provides information about working with MAINVIEW products in windows mode, in full-screen mode, and from MAINVIEW Explorer, and explains how to customize views</td>
</tr>
<tr>
<td>product user guides</td>
<td>MAINVIEW Alarm Management Guide</td>
<td>explains how to create and install alarm definitions that indicate when exceptions occur in a sysplex</td>
</tr>
<tr>
<td></td>
<td>MAINVIEW AutoOPERATOR Basic Automation Guide, Volume 2</td>
<td>provides procedures for performing additional basic automation tasks</td>
</tr>
</tbody>
</table>
This book uses the following special conventions:

- All syntax, operating system terms, and literal examples are presented in this typeface.

- Variable text in path names, system messages, or syntax is displayed in *italic* text:
  
  testsys/instance/fileName

- Brackets [ ] enclose optional parameters or keywords.

- Braces { } enclose a list of required parameters; one parameter must be chosen.

- A vertical bar | separates alternative options; one option can be chosen.

- An [underlined](#) parameter is the default.

- The symbol => connects items in a menu sequence. For example, **Actions => Create Test** instructs you to choose the Create Test command from the Actions menu.
This chapter presents the following topics:

What are Best Practices? ...................................................... 14
What is covered and what is not ........................................... 15
Terms and concepts ............................................................ 16
What are Best Practices?

The goal of any Best Practices book is to provide the reader with

- answers to common questions and issues
- proven tips and techniques
- lessons learned from the experience of others
- recommendations and guidance for the completion of tasks
- available options, with the benefit of each option clearly identified

The goal of this Best Practices book is to help you establish a basic event management strategy that leverages the power of your MAINVIEW products. This book will help you

- understand mainframe metrics

  Chapter 2 explains the various types of metrics; how MAINVIEW collects them, ways to respond to them; and which metrics are important to monitor in a particular environment.

- determine the state of critical business services

  Chapter 3 helps you target an application; collect information about it; define workloads to monitor it; set alarms on exceptions; and track its transactions across systems and subsystems.

- automate a response to events that impact critical business services

  Chapter 4 helps you choose an area of your IT infrastructure to automate; determine which events to manage, who to notify and what action to take; and create Rules to manage those events.

Throughout this book you will find Best Practices for defining workloads, alarms, and automation Rules.

In addition to the MAINVIEW products discussed in this book, several other BMC and non-BMC products can help you further evolve your event management strategy to fully align your IT infrastructure with your business processes. Detailed information about those products is beyond the scope of this book, but some of those products are summarized briefly in “Beyond basic event management” on page 75.
What is covered and what is not

While this Best Practices book offers some "do's and don'ts" that might be covered in other MAINVIEW documents, it generally does not duplicate information that is provided elsewhere. This book frequently refers to other BMC documents for detailed information.

This book does not answer every possible technical question or provide for every contingency, but following its recommendations will help you to manage your MAINVIEW environment in the best way possible.

The information presented in this book applies to the following MAINVIEW products:

- CMF MONITOR, version 5.6 or later
- MAINVIEW AutoOPERATOR, version 6.5 or later
- MAINVIEW Infrastructure, version 5.0 or later
- MAINVIEW Storage Resource Manager (SRM), version 7.4 or later
- MAINVIEW SYSPROG Services, version 3.4 or later
- MAINVIEW Transaction Analyzer, version 2.1 or later
- MAINVIEW VistaPoint, version 1.1 or later
- MAINVIEW for CICS®, version 5.9 or later
- MAINVIEW for DB2®, version 8.2 or later
- MAINVIEW for DBCTL, version 4.2 or later
- MAINVIEW for IMS™, version 4.2 or later
- MAINVIEW for IP, version 2.4 or later
- MAINVIEW for Linux® – Servers, version 1.3 or later
- MAINVIEW for UNIX® System Services, version 1.5 or later
- MAINVIEW for VTAM®, version 1.3 or later
- MAINVIEW for WebSphere® Application Server, version 2.4 or later
- MAINVIEW for WebSphere MQ, version 4.3 or later
- MAINVIEW for z/OS®, version 2.8 or later
## Terms and concepts

This section introduces some terms that are central to understanding the MAINVIEW event management environment.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>alarm report</td>
<td>in MAINVIEW Alarm Management, an exception message that is generated when an alarm definition is evaluated as true</td>
</tr>
<tr>
<td>alarm definition</td>
<td>in MAINVIEW Alarm Management, a specification that determines what MAINVIEW data elements are evaluated, when they are evaluated, and how any exceptions are reported</td>
</tr>
<tr>
<td>alert</td>
<td>in MAINVIEW AutoOPERATOR, a message that MAINVIEW AutoOPERATOR creates to notify operators of exception situations that might require manual intervention and attention</td>
</tr>
<tr>
<td>An alert differs from an alarm report; an alert can cause automation to occur while an alarm report, by itself, cannot initiate automated actions.</td>
<td></td>
</tr>
<tr>
<td>background monitor</td>
<td>in several MAINVIEW products, an online service that measures resources or workloads at user-defined intervals and issues warnings when user-defined thresholds are exceeded</td>
</tr>
<tr>
<td>Best Practice</td>
<td>a proven activity or process that has been used successfully by multiple organizations</td>
</tr>
<tr>
<td>business process</td>
<td>a process that is owned and carried out by the business</td>
</tr>
<tr>
<td>A business process contributes to the delivery of a product or service to a business customer. For example, a retailer might have a purchasing process that helps to deliver services to their business customers. Many business processes rely on IT Services.</td>
<td></td>
</tr>
<tr>
<td>event</td>
<td>a notification created by any IT service or monitoring tool (for example, a notification that a batch job has completed)</td>
</tr>
<tr>
<td>Events typically require IT operations personnel to take actions, and they often lead to incidents being logged.</td>
<td></td>
</tr>
<tr>
<td>event management</td>
<td>the process that manages events throughout their lifecycles</td>
</tr>
<tr>
<td>exception</td>
<td>a condition or event that cannot be managed by normal processing</td>
</tr>
<tr>
<td>Terms and concepts</td>
<td></td>
</tr>
<tr>
<td>------------------------------------</td>
<td></td>
</tr>
<tr>
<td>impact</td>
<td></td>
</tr>
<tr>
<td>a measure of the effect of an incident, problem or change on business processes</td>
<td></td>
</tr>
<tr>
<td>Impact is often based on how Service Levels will be affected.</td>
<td></td>
</tr>
<tr>
<td>IT infrastructure</td>
<td></td>
</tr>
<tr>
<td>all of the hardware, software, networks, and facilities that are required to develop, test, deliver, or support IT services</td>
<td></td>
</tr>
<tr>
<td>The term refers to the information technology but not the associated people, processes, and documentation.</td>
<td></td>
</tr>
<tr>
<td>MAINVIEW Alarm Management</td>
<td></td>
</tr>
<tr>
<td>a component that provides management by exception in conjunction with other MAINVIEW products</td>
<td></td>
</tr>
<tr>
<td>MAINVIEW Alarm Management generates alarm reports based on performance goals.</td>
<td></td>
</tr>
<tr>
<td>Rule</td>
<td></td>
</tr>
<tr>
<td>in MAINVIEW AutoOPERATOR, a conditional statement that includes selection criteria and actions</td>
<td></td>
</tr>
<tr>
<td>When the conditions of the selection criteria are true, the actions are performed. Rules can be organized and grouped into Rule Sets.</td>
<td></td>
</tr>
<tr>
<td>service level agreement (SLA)</td>
<td></td>
</tr>
<tr>
<td>an agreement between an IT service provider and a customer</td>
<td></td>
</tr>
<tr>
<td>The SLA describes the IT service, documents service level targets, and specifies the responsibilities of the IT service provider and the customer. A single SLA may cover multiple IT services or multiple customers.</td>
<td></td>
</tr>
<tr>
<td>workload definition</td>
<td></td>
</tr>
<tr>
<td>a group of units of work that is created by using various MAINVIEW product views</td>
<td></td>
</tr>
<tr>
<td>A workload definition contains a unique name, a description, an initial status, a current status, and selection criteria by which address spaces are selected for inclusion in the workload.</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 2

Important MAINVIEW metrics

This chapter presents the following topics:

Types of metrics ................................................................. 20
How MAINVIEW collects metrics ........................................ 21
  Data collectors and views .................................................. 21
  Alarms ........................................................................... 21
  Background monitors ....................................................... 22
  Alerts ............................................................................. 22
Responding to metrics ....................................................... 23
How to use the metric tables .............................................. 24
Operating system metrics .................................................. 25
  z/OS metrics ................................................................. 25
  Linux metrics ................................................................. 28
  UNIX System Services metrics ......................................... 29
  Storage Resource Manager (SRM) metrics ....................... 30
Subsystem and application server metrics ......................... 32
  CICS metrics ................................................................. 32
  DB2 metrics ................................................................. 38
  IMS metrics ................................................................. 42
  WebSphere Application Server metrics .......................... 46
Networks and communications metrics ............................. 48
  TCP/IP metrics .............................................................. 48
  WebSphere MQ metrics .................................................. 49
Types of metrics

The MAINVIEW monitoring products collect data about the IT infrastructure and present that data as metrics in views — thousands of metrics in hundreds of views. How do you know which metrics are most important to the overall health of your IT infrastructure and your critical business services? It is helpful to consider the following hierarchy of metrics:

<table>
<thead>
<tr>
<th>Class of metric</th>
<th>Most useful to</th>
<th>Most useful for</th>
</tr>
</thead>
</table>
| Class A - Availability              | CIOs and director-level management               | determining whether critical systems, subsystems, business applications, and their components are available and ready to do business.
                                                                                                           | Examples include information about started tasks, system services, files, databases, programs, transactions, terminals, connections, and communication devices. |
| Class B - Performance                | systems programmers, application programmers, Help Desk personnel, analysts, and other troubleshooters | determining infrastructure performance and resource contention, and whether service levels are being met.
                                                                                                           | Examples include system throughput and response times.                                                             |
| Class C - Decision support, configuration, and capacity planning | capacity planners, software installers, and anyone who requires supporting metrics | determining the root cause of issues that impact availability and performance; planning for installation and configuration changes; understanding long-term resource requirements and predicting changes to those requirements.
                                                                                                           | Examples include information about the utilization of hardware and software resources such as CPU, memory, and DASD. |

When critical business applications are

- not available, Class A (Availability) metrics are critically important and other metrics do not matter
- available but performing poorly, Class B (Performance) metrics are important
- available and performing satisfactorily, Class C (Decision support) metrics are relevant

**BEST PRACTICE**

Focus on Class A (Availability) metrics first; they indicate the status of your critical business services.

This chapter provides tables of metrics for several areas of the IT infrastructure. Those tables indicate the class for each metric.
How MAINVIEW collects metrics

The MAINVIEW monitoring products collect IT infrastructure metrics by using data collectors, alarms, background monitors, and alerts. These facilities offer varying levels of monitoring and event management, from passive monitoring of view data, to automated responses to system events.

Data collectors and views

The MAINVIEW products use data collectors to collect metrics, which are presented as data in views. Many views are predefined with thresholds that cause data in the views to change color when the threshold is met or exceeded. Additional thresholds can be added by using view customization. However, someone must continually look at the views to determine if a threshold has been exceeded and whether something should be done about. No exception message is issued, no notification is sent, and no automated response can be defined.

Alarms

MAINVIEW Alarm Management lets you set alarms on view fields. When the user-defined threshold for a field is not within acceptable limits, an alarm is generated and can be

- written to an operator console (WTO)
- written to CONTROL-O
- turned into a MAINVIEW AutoOPERATOR alert and processed to automate notification and response

With MAINVIEW Alarm Management, you can display and manage exceptions more efficiently than simple monitoring with views, but an alarm by itself cannot perform any automation. You are still required to respond manually to problems.
Background monitors

Background monitors are provided with several MAINVIEW products and are typically activated at product startup. The monitors measure resources or workloads at user-defined intervals and issue warning messages when the user-defined thresholds are exceeded. The warning messages can be:

- viewed in a MAINVIEW product
- written to an operator console (WTO)
- written to the MAINVIEW journal log (BBJRNRL)
- turned into alerts and processed by MAINVIEW AutoOPERATOR to automate notification and response

Background monitors offer some notification and a path to automation.

Alerts

Alerts are messages that notify operators of exceptional events that might require intervention. Alerts can be generated by:

- Alarm Management alarm definitions
- monitors that are provided with the MAINVIEW products for IBM® CICS®, DB2®, and IMS™ subsystems
- MAINVIEW for CICS macros
- MAINVIEW SRM
- MAINVIEW SYSPROG Services Exception Monitor messages
- the MAINVIEW AutoOPERATOR Rule Processor
- REXX EXECs that use the AOEXEC ALERT ADD function

Alerts can be sent to the Alert Management component (MVALERT) of MAINVIEW and are accessible from the EZALERT Easy Menu.

Alerts that are generated by the MAINVIEW AutoOPERATOR Rule Processor can perform automation based on ALRT event type Rules. These Rules can perform many automation actions, including scheduling EXECs to perform more complex automation tasks.

Alerts can also be published through BMC Impact Integration for z/OS® to BMC Impact Manager, to further manage the IT infrastructure from a business services perspective.
Responding to metrics

You can respond in several ways to metrics that indicate an exceptional condition:

- Ignore or suppress the exception.
- Track exceptions by logging them or setting automation variables.
- Notify someone about the exception by
  - sending a message to a TSO user ID
  - sending a page
  - sending an e-mail message
  - opening a problem ticket
- Raise a better exception by rewording a cryptic message.
- Take action to resolve the exception by
  - issuing a command
  - performing more complex actions by scheduling an EXEC

---

**BEST PRACTICE**

Consider the severity of the exception and its impact when deciding how to respond.
How to use the metric tables

The remainder of this chapter contains tables of metrics for areas of the IT infrastructure. You can use the information in these tables to help you

- focus on the metrics that best indicate the health of your critical business services
- review and customize the exception thresholds according to your site’s needs
- create MAINVIEW Alarm Management alarm definitions to notify you when problems occur and to trigger automation to solve those problems

Each table contains

- metrics and the problems that they might indicate
- the names of the view and field that display the metric
- the internal element name of the field
- an optional view filter to limit the data in the view
- a recommended element threshold to specify in the alarm definition (you might need to adjust the threshold for site-specific processing)

For an example of using the information in the tables to set an alarm, see “Manage application exceptions” on page 61.

To help you focus on the most important metrics, each table is sorted by the following classes and then alphabetically by metrics within each class:

Class A - Availability metrics
Class B - Performance metrics
Class C - Decision support metrics

Not all of the tables contain all of these classes. For more information about these classes, see “Types of metrics” on page 20.
Operating system metrics

This section describes important metrics for the following operating systems:

- “z/OS metrics” on page 25
- “Linux metrics” on page 28
- “UNIX System Services metrics” on page 29
- “Storage Resource Manager (SRM) metrics” on page 30

z/OS metrics

The following metrics are available in the MAINVIEW for z/OS views. For information about using this table, see “How to use the metric tables” on page 24.

Before you create alarms based on these metrics, review “Best Practices for alarms” on page 62.

Table 1  z/OS metrics  (part 1 of 3)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>batch jobs</td>
<td>jobs that should be active are not active</td>
<td>JESTATR</td>
<td>Status</td>
<td>DESCR</td>
<td>NAME = ‘xxx’</td>
<td>DESCR &lt;&gt; 'ACTIVE'</td>
</tr>
</tbody>
</table>
### Table 1  z/OS metrics (part 2 of 3)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>coupling facility (CF)</td>
<td>how much CF CPU is consumed by CF activity</td>
<td>CFOVERZ</td>
<td>% CPU Util</td>
<td>CFIPRCPC</td>
<td>none</td>
<td>CFIPRCPC &gt; 90</td>
</tr>
<tr>
<td></td>
<td>When close to 100% CF, tasks have to wait and application delays might occur. CF delays are not displayed in the JDELAY view.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CFOVERZ</td>
<td>% Stor Util</td>
<td>CFISTGPC</td>
<td>none</td>
<td>CFISTGPC &gt; 80</td>
</tr>
<tr>
<td></td>
<td>CF-dedicated storage is overcommitted, which can cause application delays</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>These delays are not displayed in the JDELAY view.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>how much CF storage is in use by any individual structure</td>
<td>CFSTRUZ</td>
<td>Struct Stor%</td>
<td>CFGSSZPC</td>
<td>none</td>
<td>CFGSSZPC &gt; 40</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSA over-committed</td>
<td>CSA is nearing maximum</td>
<td>CSASUM</td>
<td>%</td>
<td>CSRECSUP</td>
<td>none</td>
<td>CSRECSUP &gt; 80</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DASD RESERVES</td>
<td>cross-system RESERVES are preventing access to a DASD volume</td>
<td>SENQR</td>
<td>Rsv</td>
<td>RCRSV</td>
<td>none</td>
<td>RCRSV = 'ON’</td>
</tr>
<tr>
<td></td>
<td>Use the alarm persistence feature on at least two intervals.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I/O rate and response</td>
<td>DASD slow down</td>
<td>DEVSTAT</td>
<td>Resp time</td>
<td>DXISRVAT</td>
<td>VOLSER IN (volser1, volser2...)</td>
<td>DXISRVAT &gt; 10</td>
</tr>
<tr>
<td>Performance Index (PI)</td>
<td>jobs that are not meeting PIs</td>
<td>WMSCLLS</td>
<td>Max PI</td>
<td>MXIPI</td>
<td>none</td>
<td>MXIPI &gt; 1</td>
</tr>
</tbody>
</table>
### Table 1  z/OS metrics (part 3 of 3)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>z/OS slow downs</td>
<td>which jobs are delayed due to resource contention</td>
<td>JDELAYR</td>
<td>Total Delay %</td>
<td>ASLDLYP</td>
<td>(ASGNAME IN (aspc1, aspc2...) AND ASGFLSC &lt;&gt; 'OTHER')</td>
<td>ASLDLYP &gt; nnnn where nnnn exceeds acceptable values for the address spaces selected</td>
</tr>
<tr>
<td></td>
<td>Contention for z/OS managed resources can slow critical applications.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Class C - Decision support metrics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSA utilization</td>
<td>who is using CSA, both active and ended</td>
<td>CSAREM</td>
<td>UnRel</td>
<td>CDRETUP</td>
<td>CDREJNAM='%remain'</td>
<td>CDRETUP &gt; 5</td>
</tr>
<tr>
<td>logical volume response time</td>
<td>poor I/O response time at the volume level and possible application response time problems</td>
<td>DEVSTAT</td>
<td>Resp Time</td>
<td>DXISRVAT</td>
<td>DXGSER IN (vol1, vol2...)</td>
<td>DXISRVAT &gt; 25</td>
</tr>
<tr>
<td></td>
<td>Use this metric only for supporting information; monitor the actual work, such as the transaction or job. Logical volume response time is the I/O response to a DASD device as reported by the I/O Supervisor (IOS).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The following metrics are available in the MAINVIEW for Linux views. For information about using this table, see “How to use the metric tables” on page 24.

Before you create alarms based on these metrics, review “Best Practices for alarms” on page 62.

### Table 2 Linux metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>file status</td>
<td>all mounted file systems display</td>
<td>FSLMNTR</td>
<td>FileSysName</td>
<td>(Mount Point)</td>
<td>none</td>
<td>FSSENNAME &lt;&gt; filname1 AND FSSENNAME &lt;&gt; filname2 AND…</td>
</tr>
<tr>
<td>process status</td>
<td>required Linux® processes</td>
<td>PELSTATR</td>
<td>Status</td>
<td>RPGSTAT</td>
<td>RPGSTAT = 'MISSING'</td>
<td>RPGSTAT = 'MISSING'</td>
</tr>
<tr>
<td>system availability</td>
<td>whether required Linux instances are available</td>
<td>PLEX</td>
<td>Status</td>
<td>STATUS</td>
<td>CONTEXT IN (LNX1, LNX2…)’</td>
<td>STATUS = 'INACTIVE'</td>
</tr>
<tr>
<td>process activity</td>
<td>process activity by user</td>
<td>USLOVRZR</td>
<td>State</td>
<td>PSRESTAT</td>
<td>PSRESTAT IN (WAIT, STOP, ZOMB)</td>
<td>PSRESTAT IN (WAIT, STOP, ZOMB)</td>
</tr>
<tr>
<td>process status</td>
<td>required Linux processes</td>
<td>PELSTATR</td>
<td>Status</td>
<td>RPGSTAT</td>
<td>RPGSTAT = 'MISSING'</td>
<td>RPGSTAT = 'NOTSCHED'</td>
</tr>
</tbody>
</table>
UNIX System Services metrics

The following metrics are available in the MAINVIEW for UNIX System Services views. For information about using this table, see “How to use the metric tables” on page 24.

Before you create alarms based on these metrics, review “Best Practices for alarms” on page 62.

Table 3 UNIX System Services metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>file status</td>
<td>required UNIX® System Services file systems are available</td>
<td>FSSTAT</td>
<td>Status</td>
<td>RHGSTAT</td>
<td>RHGSTAT = 'MISSING'</td>
<td>RHGSTAT = 'MISSING'</td>
</tr>
<tr>
<td>process status</td>
<td>status of critical UNIX System Services processes</td>
<td>PESTAT</td>
<td>Status</td>
<td>RPGSTAT</td>
<td>RPGSTAT = 'MISSING'</td>
<td>RPGSTAT = 'MISSING'</td>
</tr>
<tr>
<td>processes nearing maximum</td>
<td>the number of processes active on the system is nearing the maximum allowable number</td>
<td>BPXPRM</td>
<td>Processes/Current %</td>
<td>PMDPRSP</td>
<td>none</td>
<td>PMDPRSP &gt;= 95</td>
</tr>
</tbody>
</table>

Class A - Availability metrics

Class B - Performance metrics
Storage Resource Manager (SRM) metrics

The following metrics are available in the MAINVIEW for Storage Resource Manager views. For information about using this table, see “How to use the metric tables” on page 24.

Before you create alarms based on these metrics, review “Best Practices for alarms” on page 62.

Table 4  Storage Resource Manager (SRM) metrics  (part 1 of 2)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>indexed VTOC status</td>
<td>the status of the VTOC index as Enabled, Disabled, Error, OS-VTOC, or Excluded</td>
<td>SPVOLPU</td>
<td>Indx VTOC</td>
<td>S13IVTOC</td>
<td>none</td>
<td>S13IVTOC &lt;&gt; 'T' OR 'N'</td>
</tr>
<tr>
<td></td>
<td>A VTOC index that is disabled, or otherwise broken, can delay access to data sets on the volume.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data sets extents</td>
<td>data sets that have a high number of extents</td>
<td>DEXTNT</td>
<td>Exts</td>
<td>W21EXTS</td>
<td>none</td>
<td>For VSAM: W21EXTS &gt; 11</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>For non-VSAM: W21EXTS &gt; 11</td>
</tr>
<tr>
<td>fragmentation index</td>
<td>volumes that have a high fragmentation index and are due for a scheduled defragmentation</td>
<td>SPVOLFR</td>
<td>Frag Index</td>
<td>S13FRAGX</td>
<td>none</td>
<td>S13FRAGX &gt; 450</td>
</tr>
<tr>
<td>logical volume response time</td>
<td>poor I/O response time at the volume level and possible application response time problems</td>
<td>VOLPRRT</td>
<td>Resp Time</td>
<td>M06RSPCA</td>
<td>M06VOL IN (vol1, vol2…)</td>
<td>M06RSPCA &gt; 25</td>
</tr>
<tr>
<td></td>
<td>Use this metric only for supporting information; monitor the actual work, such as the transaction or job.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Logical volume response time is the I/O response to a DASD device as reported by the I/O Supervisor (IOS).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metric</td>
<td>Indicates</td>
<td>View name</td>
<td>Field name</td>
<td>Element name</td>
<td>Recommended view filter</td>
<td>Recommended field threshold (adjust for site-specific processing)</td>
</tr>
<tr>
<td>--------</td>
<td>-----------</td>
<td>-----------</td>
<td>------------</td>
<td>--------------</td>
<td>-------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>physical platter response time</td>
<td>poor I/O response time at the physical volume level and widespread problems with many logical volumes and the applications sharing those volumes. Set response thresholds low to provide an early warning of developing problems. Physical response time is the average response of all I/O activity to a real DASD volume by all logical volumes mapped to that volume. MAINVIEW calculates physical response time as an average of all logical volumes.</td>
<td>PHYPRRTZ</td>
<td>Resp Time</td>
<td>M06RSPCA</td>
<td>none</td>
<td>M06RSPCA &gt; 15</td>
</tr>
<tr>
<td>storage group and user defined pools percent used or free space</td>
<td>relative usage of available DASD space</td>
<td>SPPOOL</td>
<td>%Full</td>
<td>S03PERFC</td>
<td>none</td>
<td>S03PERFC &gt; 80</td>
</tr>
<tr>
<td>VSAM data set with high used RBA or percent full</td>
<td>fragmented VSAM files, possibly affecting performance and availability</td>
<td>DVSAM</td>
<td>Percent Used</td>
<td>W21PUSEC</td>
<td>none</td>
<td>W21PUSEC &gt; 80</td>
</tr>
</tbody>
</table>
Subsystems and application server metrics

This section describes important metrics for the following subsystems and application servers:

- “CICS metrics”
- “DB2 metrics” on page 38
- “IMS metrics” on page 42
- “WebSphere Application Server metrics” on page 46

CICS metrics

MAINVIEW for CICS views and background monitors provide important metrics for CICS, as described in “CICS metrics provided by views” and “CICS metrics provided by monitors” on page 37.

CICS metrics provided by views

The following metrics are available in the MAINVIEW for CICS views. For information about using this table, see “How to use the metric tables” on page 24.

Before you create alarms based on these metrics, review “Best Practices for alarms” on page 62.

Table 5  CICS metrics  (part 1 of 5)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>available subsystem</td>
<td>the status of critical regions</td>
<td>PLEXOVER</td>
<td>Status</td>
<td>STATUS</td>
<td>ASGNAME IN (region_name)</td>
<td>STATUS &lt;&gt; 'ACTIVE'</td>
</tr>
<tr>
<td>CICS availability</td>
<td>CICS is available on the system</td>
<td>CREGAGT</td>
<td>Region Status</td>
<td>CRGNREGNSC</td>
<td>CRGNREGNSC &lt;&gt; 'ACTIVE'</td>
<td>CRGNREGNSC '&lt;' 'ACTIVE'</td>
</tr>
</tbody>
</table>
Table 5  CICS metrics  (part 2 of 5)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>connection status</td>
<td>the status of required connections</td>
<td>CCONN</td>
<td>Connect Status</td>
<td>ACCONNSTATC</td>
<td>ACCONNECTIO IN (rgn1, rgn2...)</td>
<td>ACCONNSTATC &lt;&gt; 'ACQUI*'</td>
</tr>
<tr>
<td></td>
<td>For communications between a CICS region and other subsystems, connections must be defined and enabled.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>An alert can be built if the connection status is not ENABLED.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DB2 connection availability</td>
<td>whether the interface between CICS and DB2 is available</td>
<td>CREGDB2</td>
<td>Attachment Status</td>
<td>RE7ASTATC</td>
<td>RE7ASTATC IN (INACTIVE, TERMINATE)</td>
<td>RE7ASTATC = 'INACTIVE'</td>
</tr>
<tr>
<td></td>
<td>Communications between a CICS region and DB2 requires the connection and the status must be READY.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This metric is also available from a monitor. See Table 6 on page 37.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>file status</td>
<td>the status of required files</td>
<td>CFILE</td>
<td>Enable Status</td>
<td>AAENABLESTC</td>
<td>Sample values shown: (AAENABLESTC NOT IN ('E*','N*') AND AANAME NOT IN ('DFH*','DBU*','FDB*') AND J@TARGET IN ('A01*CICS', IPA1CICS, PRA2CICS))</td>
<td>AAENABLESTC &lt;&gt; 'ENABLED'</td>
</tr>
<tr>
<td></td>
<td>Certain files must be allocated and ENABLED for the application to be available.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>An alert can be built if the file status is not ENABLED.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 5  CICS metrics (part 3 of 5)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMS connection availability and status</td>
<td>the availability and status of the interface between CICS and IMS</td>
<td>CREGDBC</td>
<td>Attachment Status</td>
<td>RE8STATUS</td>
<td>RE8JOBNAME &lt;&gt; ‘ ’</td>
<td>RE8STATUS = ‘READY’</td>
</tr>
<tr>
<td></td>
<td>Communications between a CICS region and IMS requires a connection with the DBCTL region and the status must be READY. This metric is also available from a monitor. See Table 6 on page 37.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAINVIEW for CICS active in CICS region</td>
<td>whether MAINVIEW is active</td>
<td>CREGAGT</td>
<td>Extract Status</td>
<td>CRGNEXTRSC</td>
<td>CRGNEXTRSC = ‘INACTIVE’</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If not, no internal monitoring of CICS can be seen.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MQ connection availability</td>
<td>that a required MQ subsystem is not attached to the region and no messaging can take place</td>
<td>CREGMQS</td>
<td>Connection Status</td>
<td>RE9STATUSC</td>
<td>J@TARGET IN (rgn1, rgn2, rgn3…) and RE9SUBSYS = mqid</td>
<td>RE9STATUSC &lt;&gt; ‘CONNECTED’</td>
</tr>
<tr>
<td></td>
<td>Communications between a CICS region and an IBM WebSphere® MQ subsystem requires a connection to a queue manager and the connection status must be READY.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>program status</td>
<td>the status of required programs</td>
<td>CPROG</td>
<td>Ena</td>
<td>ABENAC</td>
<td>ABNAME NOT IN (DFH*, CSQCAPX)</td>
<td>ABENAC &lt;&gt; ‘ENABLED’</td>
</tr>
<tr>
<td></td>
<td>Certain application programs must be ENABLED or the application transaction will fail. An alert can be built if the program status is not ENABLED.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 5  CICS metrics (part 4 of 5)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>transaction availability</td>
<td>the status of defined transactions within the region</td>
<td>CTRAN</td>
<td>T1TRANID</td>
<td>&lt;&gt; (C*) and A9STATUSC &lt;&gt; 'ENABLED'</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Identify any required transactions that have not been enabled for use.</td>
<td></td>
<td></td>
<td>(trid1, trid2…)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Class B - Performance metrics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ASRA abend</td>
<td>data exception abends</td>
<td>CDUMPCD</td>
<td>TEADUMPCDE</td>
<td>IN (ASRA)</td>
<td>TEADUMPCD &gt;= 5</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Curr Dumps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>TEACDUMPS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>interval current value monitor</td>
<td>any MAINVIEW monitors in warning status</td>
<td>CSERV</td>
<td>MONSERV IN</td>
<td>(svc1, svc2, svc3…)</td>
<td>MONIPWRN &gt; 100</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>% Warning</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MONIPWRN</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>region at maximum tasks</td>
<td>the CICS region has reached the maximum number of tasks and no additional tasks can start</td>
<td>CREGION</td>
<td>CRGNTARG IN</td>
<td>(rgn1, rgn2, rgn3…)</td>
<td>CRGRPMXT &gt; 80</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>%Max Task</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CRGRPMXT</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>transaction abends</td>
<td>general transaction abends</td>
<td>CDUMPCD</td>
<td>(TEADUMPCDE NOT IN (ASRA) AND TEATYPEC IN ('TRANS*'))</td>
<td>TEADUMPCD &gt;= 20</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Curr Dumps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>TEACDUMPS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The CHISTORY view <strong>ABENDed Task</strong> field must be set to YES to display transactions in the CHIST view.</td>
<td>CHIST</td>
<td>TRANID IN</td>
<td>(user1,user2)</td>
<td>Return code &gt; 0</td>
<td></td>
</tr>
</tbody>
</table>
### Table 5  CICS metrics (part 5 of 5)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>transaction throughput</td>
<td>the current CICS transaction throughput rate</td>
<td>CREGION</td>
<td>Tran Rate</td>
<td>CRGITRTE</td>
<td>CRGNTARG IN (rgn1, rgn2, rgn3…)</td>
<td>CRGITRTE &lt; nn</td>
</tr>
<tr>
<td></td>
<td>A less-than-normal transaction throughput rate for a region can indicate a problem elsewhere.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>transactions with high CPU time</td>
<td>transactions exceeding CPU time objectives</td>
<td>TASK</td>
<td>CPU Time</td>
<td>T1FCPUTIM</td>
<td>T1TRANID NOT IN ('C*', 'J*', 'BCRT') and T1TTYPE = 'U'</td>
<td>T1FCPUTIM &gt; '1'</td>
</tr>
<tr>
<td></td>
<td>Identify critical tasks in regions and groups of regions; do not use a context of ALL unless filters are used on Tran ID column in the TASK view.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>transactions with high elapsed time</td>
<td>transactions exceeding elapsed time objectives</td>
<td>TASK</td>
<td>Elapsed Time</td>
<td>T1ELAPSTM</td>
<td>T1TRANID = filter and T1TTYPE = 'U'</td>
<td>T1ELAPSTIM &gt; '00:05:00'</td>
</tr>
<tr>
<td></td>
<td>Identify critical tasks in regions and groups of regions; do not use a context of ALL unless filters are used on Tran ID column in the TASK view.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>workload objectives</td>
<td>how well workloads are meeting response objectives</td>
<td>COBJ</td>
<td>% &lt;= Resp Goal</td>
<td>MONIPJOB</td>
<td>MONIPARM IN (wkld1, wkld2, wkld3…)</td>
<td>MONIPJOB &lt; 100</td>
</tr>
</tbody>
</table>
CICS metrics provided by monitors

The metrics in Table 6 are available from the MAINVIEW for CICS background monitors.

You can specify monitor options, such as WIF, to ensure that a condition persists for a certain number of intervals before issuing a warning. For more information about monitor options, see the MAINVIEW for CICS Monitors Guide.

Table 6  CICS monitor metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>Monitor</th>
<th>Monitor message</th>
<th>Recommended monitor value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Class A - Availability metrics</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DB2 connection availability</td>
<td>whether the interface between CICS and DB2 is available</td>
<td>@DB2N</td>
<td>FT517W</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>Communications between a CICS region and DB2 requires the connection and the status must be READY.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This metric is also available in a view. See page 33.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMS connection availability and status</td>
<td>the availability and status of the interface between CICS and IMS</td>
<td>@IMSN</td>
<td>FT518W</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>Communications between a CICS region and IMS requires a connection with the DBCTL region and the status must be READY.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This metric is also available in a view. See page 34.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Class B - Performance metrics</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>region at maximum tasks</td>
<td>the CICS region has reached the maximum number of tasks and no additional tasks can start</td>
<td>MXTC</td>
<td>FT1070W</td>
<td>WVAL=75</td>
</tr>
<tr>
<td></td>
<td>This metric is also available in a view. See page 35.</td>
<td>@PRB1</td>
<td>FT054W</td>
<td>WLIM=5</td>
</tr>
</tbody>
</table>
**DB2 metrics**

MAINVIEW for DB2 views and background monitors provide important metrics for DB2, as described in “DB2 metrics provided by views” and “DB2 metrics provided by monitors” on page 41.

### DB2 metrics provided by views

The following metrics are available in the MAINVIEW for DB2 views. For information about using this table, see “How to use the metric tables” on page 24.

Before you create alarms based on these metrics, review “Best Practices for alarms” on page 62.

#### Table 7  DB2 metrics (part 1 of 3)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>PLEX</td>
<td>Status</td>
<td>STATUS</td>
<td>AREA == 'DB2'</td>
<td>STATUS &lt;&gt; 'ACTIVE'</td>
</tr>
<tr>
<td>region availability</td>
<td>whether critical DB2 regions are available</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>STWARN DB2 Connect Failure</td>
<td>STFLAG19</td>
<td>none</td>
<td></td>
<td>STFLAG19 &lt;&gt; 'NO'</td>
</tr>
<tr>
<td>resource availability</td>
<td>the status of critical databases or objects</td>
<td>OBJLIST</td>
<td>Access</td>
<td>O100ACC</td>
<td>O100DBNM IN (dbn1, dbn2) OR O100PSNM IN (obj1, obj2)</td>
<td>O100ACC NOT RW OR STATUS NOT ''</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>O100ACC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Class B - Performance metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DBM1 storage utilization</td>
<td>available storage is too low</td>
<td>DB2STOR</td>
<td>Available</td>
<td>AVLSTORG</td>
<td>none</td>
<td>AVLSTORG &lt; 200 (MB)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&lt; 2GB</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This metric is provided by a monitor. See Table 8 on page 41.
Table 7  DB2 metrics (part 2 of 3)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDF threads and connections</td>
<td>This metric is provided by a monitor. See Table 8 on page 41.</td>
<td>STDB2</td>
<td>Act Thrd</td>
<td>STATOT</td>
<td>STDB2TARG IN (rgn1, rgn2)</td>
<td>STATOT &gt; thresh OR STATOT &lt; thresh OR (SISCOMIT &gt; thresh) OR (SISGET &gt; thresh) OR (STTEXTOT &lt;&gt; '')</td>
</tr>
<tr>
<td>general performance status</td>
<td>overview of DB2 activity</td>
<td>STDB2</td>
<td>Act Thrd</td>
<td>STATOT</td>
<td>STDB2TARG IN (rgn1, rgn2)</td>
<td>STATOT &gt; thresh OR STATOT &lt; thresh OR (SISCOMIT &gt; thresh) OR (SISGET &gt; thresh) OR (STTEXTOT &lt;&gt; '')</td>
</tr>
<tr>
<td>general performance status</td>
<td>failure or degradation</td>
<td>STWARN</td>
<td>(30 conditions are monitored on this view)</td>
<td>Warning</td>
<td>STWRNFLG</td>
<td>STWRNFLG &lt;&gt; ''</td>
</tr>
<tr>
<td>locking</td>
<td>This metric is provided by a monitor. See Table 8 on page 41.</td>
<td>LKEVENT</td>
<td>any field</td>
<td>any element</td>
<td>none</td>
<td>any data in these views represents an event that might indicate a problem</td>
</tr>
<tr>
<td>lockouts</td>
<td>timeout or deadlock events</td>
<td>LKEVENT</td>
<td>any field</td>
<td>any element</td>
<td>none</td>
<td>any data in these views represents an event that might indicate a problem</td>
</tr>
<tr>
<td>locks - user</td>
<td>contention problems and work not completing due to deadlocks and timeouts</td>
<td>STLOCK</td>
<td>provides 15 minute average of various deadlocks</td>
<td>any field</td>
<td>any element</td>
<td>MONPARM IN (wkld1, wkld2, wkld3)</td>
</tr>
<tr>
<td>response - thread average elapsed time in DB2</td>
<td>response or elapsed time issues</td>
<td>THDACTV</td>
<td>Elapsed Time</td>
<td>UTCBTIME</td>
<td>filter out long running threads</td>
<td>UTRNELAP &gt; site-specific threshold</td>
</tr>
</tbody>
</table>

This metric is also available from a monitor. See Table 8 on page 41.
### Table 7  DB2 metrics (part 3 of 3)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>users suspended for lock</td>
<td>current thread lock wait times</td>
<td>LSTSUSPZ</td>
<td>Lock Wait Time</td>
<td>L100LELP</td>
<td>none</td>
<td>L100LELP &gt; 2</td>
</tr>
<tr>
<td>workload objectives</td>
<td>how well workloads are meeting response objectives</td>
<td>DOBJ</td>
<td>% &lt;= Resp Goal</td>
<td>MONIPOBJ</td>
<td>MONPARMIN (wkld1, wkld2, wkld3)</td>
<td>MONIPOBJ &lt; 100</td>
</tr>
</tbody>
</table>
### DB2 metrics provided by monitors

The metrics in Table 8 are available from the MAINVIEW for DB2 background monitors.

You can specify monitor options, such as WIF, to ensure that a condition persists for a certain number of intervals before issuing a warning. For more information about monitor options, see the *MAINVIEW for DB2 User Guide, Volume 2: Analyzers, Monitors, and Traces*.

**Table 8  DB2 monitor metrics**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>Monitor</th>
<th>Monitor message</th>
<th>Recommended monitor values</th>
</tr>
</thead>
<tbody>
<tr>
<td>archive impacts</td>
<td>potential service disruption because the job that archives the active log is waiting to execute</td>
<td>various monitors</td>
<td>DZ0030I</td>
<td>none</td>
</tr>
<tr>
<td>DDF threads and connections</td>
<td>various monitors show queuing or low allocations</td>
<td>CNVLM, DBTQD, DBTUT, RMTUT</td>
<td>DS1160W, DS0650W, DS1680W, DS1210W</td>
<td>WVAL&gt;0, WVAL&gt;0, WVAL&gt;80%, WVAL&gt;80%</td>
</tr>
<tr>
<td>locking</td>
<td>deadlocks, timeouts, escalations, and suspensions</td>
<td>LTME, GSUSP, LDEAD, LESCL</td>
<td>DS0280W, DS1430W, DS0260W, DS0290W</td>
<td>WVAL=3, WVAL=3, WVAL=3, WVAL=3</td>
</tr>
<tr>
<td>response - thread average elapsed time in DB2</td>
<td>response or elapsed time issues</td>
<td>@ELPD</td>
<td>DW0150W</td>
<td>WVAL=5</td>
</tr>
<tr>
<td>runaway threads</td>
<td>a thread with an attach type of xxx for user xxxxxxx is using resources that exceed the defined thresholds</td>
<td>DMRBEX</td>
<td>DZ06nnW</td>
<td>MSG=DZ06nnW, ACTIVE=YES, CYC LES=4, ELAPSED=7200, CPU=0, Threshold=120 seconds of elapsed time</td>
</tr>
</tbody>
</table>
IMS metrics

MAINVIEW for IMS views and background monitors provide important metrics for IMS, as described in “IMS metrics provided by views” and “IMS metrics provided by monitors” on page 45.

IMS metrics provided by views

The following metrics are available in the MAINVIEW for IMS views. For information about using this table, see “How to use the metric tables” on page 24.

Before you create alarms based on these metrics, review “Best Practices for alarms” on page 62.

Table 9 does not provide recommended view filters. However, you can specify filters to focus a view on a particular application, especially if the application resources, for example, transactions, databases, and programs, use a similar naming convention. If you specify filters, be sure to update the filters to reflect changes in the application, and reapply the filters after the installation of product maintenance or new product versions.

Table 9  IMS metrics (part 1 of 3)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>database status</td>
<td>the status of critical databases</td>
<td>IDBEXCP</td>
<td>DBD/PART</td>
<td>PA7DBDNM</td>
<td>none</td>
<td>PA7DBDNM = *</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DEDB area</td>
<td>the status of critical DEDB areas</td>
<td>IFPSUMR</td>
<td>Status 1</td>
<td>PA8STAT1</td>
<td>none</td>
<td>PA8STAT1 &lt;&gt; ‘OPENED’</td>
</tr>
<tr>
<td>IMS regions</td>
<td>that no message regions are available</td>
<td>IMSRGNR</td>
<td>MPP Regions</td>
<td></td>
<td>none</td>
<td>IMSRGMPP &lt; 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>that no Fast Path regions are available</td>
<td>IMSRGNR</td>
<td>IFP Regions</td>
<td></td>
<td>none</td>
<td>IMSRGFPS &lt; 1</td>
</tr>
</tbody>
</table>
Table 9  IMS metrics (part 2 of 3)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Recommended field name</th>
<th>Recommended field element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAINVIEW for IMS PAS</td>
<td>the PAS to CAS communications is not active, or the PAS is not active</td>
<td>PLEX Status</td>
<td>none</td>
<td>none</td>
<td>STATUS &lt; 'ACTIVE'</td>
<td></td>
</tr>
<tr>
<td>MSC logical link</td>
<td>status of link</td>
<td>IMCLLNKR Logical Link Status</td>
<td>none</td>
<td>none</td>
<td>MSLKSTAT NOT IN(&quot;PSTP&quot;, &quot;IWAT&quot;, &quot;NOPN&quot;, &quot;COLD&quot;)</td>
<td></td>
</tr>
<tr>
<td>MSC physical link</td>
<td>status of link</td>
<td>IMCPLNKR PLink Status</td>
<td>none</td>
<td>none</td>
<td>MSPLKSTA NOT IN('PSTOPPED')</td>
<td></td>
</tr>
<tr>
<td>OTMA connection status</td>
<td>the status of the OTMA connection</td>
<td>IOTMASUM Connection Status</td>
<td>none</td>
<td>none</td>
<td>CONSTAT NOT IN ('ENABLED', ACCEPT)</td>
<td></td>
</tr>
<tr>
<td>program status</td>
<td>programs that have an exception status</td>
<td>IPGEXCP Program Name</td>
<td>none</td>
<td>none</td>
<td>PRGMNAME = *</td>
<td></td>
</tr>
<tr>
<td>transaction status</td>
<td>transactions that have an exception status</td>
<td>ITREXCP Tran Code</td>
<td>none</td>
<td>none</td>
<td>TRANCODE = *</td>
<td></td>
</tr>
<tr>
<td>IMS Connect work unit</td>
<td>work unit delay</td>
<td>IRGNICSM Session / Time</td>
<td>none</td>
<td>none</td>
<td>ICONTIME &gt; 2</td>
<td></td>
</tr>
<tr>
<td>lock waits</td>
<td>This metric is provided by a monitor. See Table 10 on page 45.</td>
<td>ICONTIME</td>
<td>none</td>
<td>none</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### IMS metrics (part 3 of 3)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>message processing</td>
<td>whether the message processing rate is within the site-defined threshold</td>
<td>IMSPLXGR</td>
<td>Process Rate</td>
<td>IMSORRTE</td>
<td>none</td>
<td>IMSORRTE &gt; site-defined threshold IMSORRTE &lt; site-defined threshold</td>
</tr>
<tr>
<td>messages queued</td>
<td>messages are queued and waiting to be processed</td>
<td>IMSDDSHOR</td>
<td>FF Queue</td>
<td>IMSFFMSQ</td>
<td>none</td>
<td>IMSFFMSQ &gt; 60</td>
</tr>
<tr>
<td></td>
<td>These view fields are hidden and can be displayed by customizing the view.</td>
<td>IMSDDSHOR</td>
<td>FastPath Queue</td>
<td>IMSFPMSQ</td>
<td>none</td>
<td>IMSFPMSQ &gt; 60</td>
</tr>
<tr>
<td>region occupancy</td>
<td>percentage of time the region is busy processing or scheduling transactions</td>
<td>IRGOCCR</td>
<td>Rgn Occ</td>
<td>RGNOROCC</td>
<td>none</td>
<td>RGNOROCC &gt; 80</td>
</tr>
</tbody>
</table>
IMS metrics provided by monitors

The metrics in Table 10 are available from the MAINVIEW for IMS background monitors.

You can specify monitor options, such as WIF, to ensure that a condition persists for a certain number of intervals before issuing a warning. For more information about monitor options, see the MAINVIEW for IMS Online Analyzers, Monitors, and Traces Reference Manual.

Table 10  IMS monitor metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>Monitor</th>
<th>Monitor message</th>
<th>Recommended monitor values</th>
</tr>
</thead>
<tbody>
<tr>
<td>lock waits</td>
<td>that a region is in IRLM suspend state</td>
<td>LWAIT</td>
<td>RM0880W</td>
<td>INTERVAL=00:00:02, WVAL=2, WLIM=999</td>
</tr>
<tr>
<td></td>
<td>that a region is in a long program isolation (PI) wait</td>
<td>WAIT</td>
<td>RM0600W</td>
<td>INTERVAL=00:00:02, WVAL=2, WLIM=999</td>
</tr>
<tr>
<td>transaction average elapsed time</td>
<td>elapsed time issues</td>
<td>@ELAP</td>
<td>WM0020W</td>
<td>INTERVAL=00:00:15, WVAL=3, WLIM=999</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Specify additional selection criteria if you want to focus on specific applications and transactions.</td>
</tr>
<tr>
<td>transaction average response time</td>
<td>response time issues</td>
<td>@RESP</td>
<td>WM0030W</td>
<td>INTERVAL=00:00:15, WVAL=3, WLIM=999, PGMTYPE=MPP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Specify additional selection criteria if you want to focus on specific applications and transactions.</td>
</tr>
</tbody>
</table>
WebSphere Application Server metrics

The following metrics are available in the MAINVIEW for WebSphere Application Server views. For information about using this table, see “How to use the metric tables” on page 24.

Before you create alarms based on these metrics, review “Best Practices for alarms” on page 62.

Table 11  WebSphere Application Server metrics (part 1 of 2)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class A - Availability metrics</td>
<td></td>
<td></td>
<td>PMIJDBCZ</td>
<td>Connection Type</td>
<td>none</td>
<td>R830CTYPE NOT IN('conn1', 'conn2', 'conn3'...)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>R830CTYPE</td>
<td></td>
<td></td>
<td>Use the INclude operator to ensure that all expected databases are available.</td>
</tr>
<tr>
<td>DB2 connections</td>
<td>whether expected JDBC servers are available</td>
<td></td>
<td>J2EEAPPS</td>
<td>J2ee/Keyword</td>
<td>none</td>
<td>KEYWORD &lt;&gt; 'appl1' AND 'appl2' AND...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>J2EEAPPS</td>
<td>KEYWORD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>deployed applications</td>
<td>whether required applications are installed</td>
<td></td>
<td>JEJBS</td>
<td>EJB / Name</td>
<td>none</td>
<td>KEYWORD &lt;&gt; 'appl1' AND 'appl2' AND...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>JEJBS</td>
<td>EJB / Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>deployed beans</td>
<td>whether required beans (applications) are installed</td>
<td></td>
<td>PMIJ2CPZ</td>
<td>Connection Type</td>
<td>none</td>
<td>R820CTYPE NOT IN('conn1', 'conn2', 'conn3'...)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>PMIJ2CPZ</td>
<td>R820CTYPE</td>
<td></td>
<td>Use the INclude operator to ensure that all expected databases are available.</td>
</tr>
<tr>
<td>other back end connectors,</td>
<td>whether expected J2C connectors are available</td>
<td></td>
<td>SVRSTA</td>
<td>Open Bus</td>
<td>none</td>
<td>W30J20P &lt;&gt; 'y*'</td>
</tr>
<tr>
<td>from the J2C Connection pool</td>
<td></td>
<td></td>
<td>SVRSTA</td>
<td>W30J20P</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 11  WebSphere Application Server metrics (part 2 of 2)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>appl and servlet usage and response</td>
<td>performance of deployed applications</td>
<td>PMISRVLZ</td>
<td>Web Application R810WEBAPP</td>
<td></td>
<td>R810WEBAPP IN (appl1, appl2…)</td>
<td>R81ISRVART (&gt; threshold) OR (R81IERRORS &gt; threshold)</td>
</tr>
<tr>
<td>JVM garbage collection</td>
<td>whether garbage collection is slowing response time</td>
<td>PMIJVMR</td>
<td>GC Calls R93IGCCAL</td>
<td>none</td>
<td>(R93IGCCAL &gt; 5) OR (R93IGCAVG &gt; 10) OR (R93IFREEM &lt; threshold) OR (R93ITBAVG &lt; 180)</td>
<td></td>
</tr>
<tr>
<td>server performance by WLM</td>
<td>poor service by WLM, which can cause application performance problems</td>
<td>WLMSVCLD</td>
<td>%-EXCEED GO W32PTOM</td>
<td>none</td>
<td>W32PTOM &lt; 100</td>
<td></td>
</tr>
</tbody>
</table>
Networks and communications metrics

This section describes important metrics for the following networks and communication technologies:

- “TCP/IP metrics”
- “WebSphere MQ metrics” on page 49

TCP/IP metrics

The following metrics are available in the MAINVIEW for IP views. For information about using this table, see “How to use the metric tables” on page 24.

Before you create alarms based on these metrics, review “Best Practices for alarms” on page 62.

Table 12   TCP/IP metrics (part 1 of 2)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>critical network devices</td>
<td>the availability of critical network devices</td>
<td>APING</td>
<td>State</td>
<td>APNGSTAT</td>
<td>none</td>
<td>APNGSTAT NOT IN (ACTIVE, IDLE, WAIT) OR APNGSxxx &gt; threshold</td>
</tr>
<tr>
<td>defined network device status</td>
<td>status of required devices</td>
<td>TACLNKS</td>
<td>Link</td>
<td>FLAG1DEV</td>
<td>none</td>
<td>FLAG1DEV NE ’READY’</td>
</tr>
<tr>
<td>critical connection with a bad status</td>
<td>dropped connections and communication failures</td>
<td>AMON</td>
<td>State</td>
<td>AMONSTAC</td>
<td>none</td>
<td>AMONSTAC NE ’ESTABLISHED’</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(AMON is available with MAINVIEW for IP version 2.5.00)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The following metrics are available in the MAINVIEW for WebSphere MQ views. For information about using this table, see “How to use the metric tables” on page 24.

Before you create alarms based on these metrics, review “Best Practices for alarms” on page 62.

Table 12  TCP/IP metrics (part 2 of 2)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>connection response time</td>
<td>network response time for jobs that use TCP/IP services</td>
<td>JOBRESP</td>
<td>Avg Net Resp</td>
<td>AVGNET</td>
<td>JOBNAME IN (name1, name2…) (AVGNET &gt; threshold) OR (AVGHOST &gt; threshold)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Avg Host Resp</td>
<td>AVGHOST</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTP activity</td>
<td>FTP activity for critical applications</td>
<td>TACFTPA</td>
<td>FTP Code</td>
<td>FTPCODE</td>
<td>none</td>
<td>FTPCODE NE 250</td>
</tr>
</tbody>
</table>

WebSphere MQ metrics

The following metrics are available in the MAINVIEW for WebSphere MQ views. For information about using this table, see “How to use the metric tables” on page 24.

Before you create alarms based on these metrics, review “Best Practices for alarms” on page 62.

Table 13  WebSphere MQ metrics (part 1 of 5)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>application statistics</td>
<td>important statistics by application This metric can be used as alternative to the LQ, DLQ, XQ, and QP views.</td>
<td>APST</td>
<td>various fields</td>
<td>various elements</td>
<td>none</td>
<td>Set thresholds according to site experience. Any threshold out of the normal range can indicate a potential problem.</td>
</tr>
<tr>
<td>channel initiator</td>
<td>channel initiator availability</td>
<td>DQMD</td>
<td>Status</td>
<td>CHICISC</td>
<td>none</td>
<td>CHICISC &lt;&gt; 'ACTIVE'</td>
</tr>
</tbody>
</table>
### Table 13  WebSphere MQ metrics (part 2 of 5)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>channel status</td>
<td>that channels are not running</td>
<td>CHANNELS</td>
<td>CHLNAME</td>
<td>CHLSTAT</td>
<td>CHLSTAT NOT IN (RUNNING, INACTIVE, STOPPED)</td>
<td></td>
</tr>
<tr>
<td>coupling facility structure</td>
<td>XCF structure availability</td>
<td>CPSS</td>
<td>Status</td>
<td>CFSTRST</td>
<td>none</td>
<td>CFSTRST &lt;&gt; 'ACTIVE'</td>
</tr>
<tr>
<td>DB2 connections</td>
<td>DB2 connection availability</td>
<td>QSG</td>
<td>DB2 Conn Status</td>
<td>QSGDB2C</td>
<td>none</td>
<td>QSGDB2C &lt;&gt; 'ACTIVE'</td>
</tr>
<tr>
<td>IMS connections</td>
<td>the status of IMS connections</td>
<td>LQ</td>
<td>Open Inp</td>
<td>QUOPIC</td>
<td>(QUQMGR IN (MQP1,MQI1) AND QUQ IN (<em>.BRIDGE) and QUUSAGE = 'N</em>')</td>
<td>QUOPIC = '0'</td>
</tr>
<tr>
<td>IMS connections</td>
<td>TPIPE availability</td>
<td>OTMAD</td>
<td>Tpipe Status</td>
<td>OTMABLKF</td>
<td>none</td>
<td>OTMABLKF = 'SUSPENDED'</td>
</tr>
<tr>
<td>INITQ status</td>
<td>application-related Initiator Queue availability</td>
<td>LQ</td>
<td>Open Inp</td>
<td>QUOPIC</td>
<td>QUQ IN ('appq1','appq2'..) AND QUUSAGE = 'N*'</td>
<td>Summary = S (QUOPIC:SUM = '0')</td>
</tr>
<tr>
<td>listeners</td>
<td>the status of various listeners (TCP/IP, LU 6.2)</td>
<td>DQMD</td>
<td>Group TCP/IP Listener -Status</td>
<td>CHIGTLSC</td>
<td>none</td>
<td>CHI***** &lt;&gt; 'STARTED'</td>
</tr>
<tr>
<td>MQ manager</td>
<td>MQ manager availability</td>
<td>QM</td>
<td>Status</td>
<td>QMSTAT</td>
<td>none</td>
<td>QMSTAT &lt;&gt; 'ACTIVE'</td>
</tr>
</tbody>
</table>
Table 13  WebSphere MQ metrics (part 3 of 5)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name Field name Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>page set status</td>
<td>presence of persistent messages in a nonpersistent page set \nIf you are segregating persistent messages, consider issuing an alarm when a message appears in the wrong queue to avoid losing persistent messages in the event of a failure.</td>
<td>PS</td>
<td>SPSSID = page set ID</td>
<td>SPSNPPGS &gt; 0</td>
</tr>
<tr>
<td>queue manager status</td>
<td>availability of required queue managers, some additional overall problems, and other metrics</td>
<td>W2OVER</td>
<td>WZOQMGR IN(qmgr1, qmgr1...)</td>
<td>WZOQMST &lt;&gt; 'ACTIVE' OR WZOEVTA &lt;&gt; 'ACTIVE' OR WZOCMDSV &lt;&gt; 'RUNNING'</td>
</tr>
<tr>
<td>Queue Depth High event</td>
<td>that a Queue Depth High event has been triggered and created a potential shortage of space in the queue for upcoming work</td>
<td>LQ</td>
<td>QUUSAGE = 'N*'</td>
<td>QUDEPHI = 'Y*'</td>
</tr>
<tr>
<td>queue depth threshold</td>
<td>whether incoming messages are waiting to be processed by an application</td>
<td>LQ</td>
<td>QUUSAGE = 'N*'</td>
<td>QUDEPP (%full) or QUDEPC (msg-count) \nThe threshold values for %full and msg-count are site-specific and depend on how the queue is processed.</td>
</tr>
<tr>
<td>transmit queue status and depth</td>
<td>whether outgoing messages are waiting to be transmitted to other locations</td>
<td>XQ</td>
<td>QUQ IN (appl_xmitq1, appl_xmitq2...)</td>
<td>QUDEPC &gt; 0</td>
</tr>
</tbody>
</table>

**Class B - Performance metrics**

| Channel initiator            | the number of active channel connections is approaching the maximum                                                                                                                                           | DQMD                              | none                  | CHICCA > 90% CHICCCA                                              |
### Table 13  WebSphere MQ metrics (part 4 of 5)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>intra-group queuing</td>
<td>the status of intra-group queuing, which should be enabled in most cases when the queue manager is part of a queue-sharing group</td>
<td>QMMVSD</td>
<td>Intra-Group Queuing - Status</td>
<td>QMIQIQI</td>
<td>none</td>
<td>QMIQIQI = 'ENABLED'</td>
</tr>
</tbody>
</table>
| MQ CPU usage                  | CPU usage of MQ                                                           | QMMVSS     | CPU Time/Percent-Interval | QMICPUP                | none                    | QMICPUP < low-threshold or QMICPUP > high-threshold
<p>|                               |                                                                           |            |             |                        |                         | The threshold values are site-specific and depend on how the queue is processed. |
| MQ definition problems        | whether objects have been defined incorrectly                            | TOPOLOGY   | Exception Count | TRECEXC                | none                    | TRECEXC &gt; 0                                                    |
| MQ events                     | all outstanding MQ events                                                | EVENTS     | Event Type  | SMZRSEVT               | none                    | SMZRSEVT = *                                                   |
|                               | If you are using MAINVIEW AutoOPERATOR or another event processor to remove past events from the queue, any message on the queue might indicate a potential problem. |
| MQ message flow               | whether MQ messages are being processing                                  | QMMVS      | various elements |                        | none                    | Set thresholds according to site experience. Any threshold out of the normal range can indicate a potential problem. |
| page set free space          | the percentage of page space available for use                           | PS         | Free Percent | SPFREE                 | (SSPID NOT IN ('5') AND J[@TARGET NOT IN ('MQI1')] ) | SPFREE &lt; 50                                                   |</p>
<table>
<thead>
<tr>
<th>Metric</th>
<th>Indicates</th>
<th>View name</th>
<th>Field name</th>
<th>Element name</th>
<th>Recommended view filter</th>
<th>Recommended field threshold (adjust for site-specific processing)</th>
</tr>
</thead>
<tbody>
<tr>
<td>page set usage</td>
<td>that a page set that should contain only transient data contains nontransient data</td>
<td>PSU</td>
<td>Current Depth</td>
<td>PSUONAME IN (qname1, qname2, qname3)</td>
<td>PSUCTYPE = QLOCAL AND PSUMSGCT &gt; 0 (check persistence of condition by using the MAINVIEW Alarm Management alarm persistence feature)</td>
<td>PSUMSGCT &gt; 0</td>
</tr>
<tr>
<td>queue performance and throughput</td>
<td>the throughput of messages to queues that are used by the application</td>
<td>QP</td>
<td>Current Depth</td>
<td>QSQDEPTH</td>
<td>none</td>
<td>QSQDEPTH &gt; thresh OR ((QSISGETR &lt; low-get-thresh) OR (QSISGETR &gt; hi-get-thresh)) OR ((QSISPUTR &lt; low-put-thresh) OR (QSISPUTR &gt; hi-put-thresh))</td>
</tr>
<tr>
<td>how well the queue is being serviced</td>
<td></td>
<td>QPDC</td>
<td>Successful Get</td>
<td>QSQQUEUE = target-queue-name</td>
<td>(QSRTLG &gt; nnnn) OR (QSRTLP &gt; nnnn) OR (QSOLDMSA &gt; nnnn)</td>
<td></td>
</tr>
</tbody>
</table>
Managing applications

This chapter presents the following topics:

- Why manage the application .......................................................... 56
- Collect information about the application ........................................... 57
- Define a workload to monitor the application .................................... 58
  Best Practices for workload definitions ............................................. 59
- Manage application availability ....................................................... 60
- Manage application exceptions ....................................................... 61
  Best Practices for alarms ............................................................... 62
- Manage application transactions ..................................................... 64
- Summary of Best Practices: Managing the application ....................... 65
Why manage the application

Applications consist of various parts of the IT infrastructure, including batch jobs, online transactions, data constructs, web-based interfaces, and network connections. Within applications, transactions perform critical business services such as sales, brokerage trades, reservations, and online quotes. By monitoring the entire application, instead of individual processes, you can

- determine which users are impacted by systems issues
- relate applications to business processes
- relate IT infrastructure failures to specific applications
- monitor fewer, more meaningful metrics
- monitor exceptions that directly impact users and require human intervention
- notify users proactively about problems
- define application specific thresholds based on service level agreements

Managing an application involves the following tasks:

1. Choose a critical business application and collect information about the application.

2. Define workloads to monitor the application by using any of several MAINVIEW products.

3. Manage application availability and performance by using MAINVIEW VistaPoint (or other MAINVIEW products) to look at workloads.

4. Manage application exceptions by setting MAINVIEW Alarm Management alarms on the metrics that indicate availability and performance.

5. Manage application transactions across systems and subsystems by using MAINVIEW Transaction Analyzer.

These tasks are discussed in the following sections.
Collect information about the application

Before you begin managing an application, you will need to collect some information about it. Answer the following questions to gain an understanding of the application and its users. You can print the “Application information worksheet” on page 78 to help with this task.

What are the components of the application?

Identify the components of the application, for example

- batch jobs
- CICS transactions
- DASD volumes
- DB2 databases and plans
- IMS transactions, programs, and databases
- JES resources such as lines and printers
- LPARs dedicated to application
- started tasks
- TSO users
- USS processes
- VTAM and TCP/IP resources
- WebSphere MQ queue manager queues

Talk to the application programmers to get a clear picture of what their code does. Explain that you are collecting information to help ensure the availability and performance of the application; they are likely to be supportive.

Talk to the systems programmers who support the application’s components and environments to get additional details about the application.

Where do the application components execute or reside?

Identify interfaces to other platforms through WebSphere MQ, where the transactions and databases execute, and the use of UNIX System Services resources. If possible, relate the databases to DASD volumes or SMS entities.

Who uses the application?

Determine the core users of the application and any critical time periods for them to use the application.
Define a workload to monitor the application

Which metrics should you monitor?

Focus on the metrics that are most likely to impact the core users. You can add additional metrics as your monitoring needs evolve. See Chapter 2, “Important MAINVIEW metrics” for more information.

What is the business process flow?

Consider creating a diagram of the application’s business process flow. A visual representation of the process flow can help you identify components, connections, and considerations that you might otherwise overlook. A sample diagram is shown here.

Define a workload to monitor the application

After you have collected information about the application, define a workload to monitor the application.

- Establish some basic service level objectives for the application, for example
  - 90% of all transactions should be finished within one second
  - transactions MTGF and MDB2 represent the majority of the Finance workload and 95% of these transactions should be finished within 0.5 seconds
Best Practices for workload definitions

Use the following Best Practices when creating workload definitions:

- Create workload definitions in one BBPARM data set and share that data set with all of the PASs to reduce the number of workload definitions.

- Use a consistent naming convention for workload definitions to allow easy identification and to facilitate sorting and filtering in views. Use names that reflect the work performed by the target of the workload.

  **EXAMPLE**
  
  You might use the workload name DB2PAY1A for DB2 payroll transactions running on the DB21A subsystem.

- Specify a composite name for workload definitions. All workloads definitions that share the same composite name are grouped together for a given target and are reported to MAINVIEW VistaPoint as a single entity.

- Identify critical workload monitoring periods and create workload definitions for those time periods.
Manage application availability

After you have installed the workload definition to collect data about the application, you can use the MAINVIEW products to display information about the application.

If MAINVIEW VistaPoint is installed

Start with the MAINVIEW VistaPoint APOVER view to display application performance data. You can drill down on the *Interval %Obj* field in this view and subsequent views to see increasingly detailed information. You can see which workloads within an application have met their service level objectives and perform more detailed analysis of any problems.

If MAINVIEW VistaPoint is not installed

Use the workload objective views provided by your MAINVIEW products, for example

- COBJ (MAINVIEW for CICS)
- DOBJ (MAINVIEW for DB2)
- IOBJ (MAINVIEW for IMS)
- WOBJ (MAINVIEW for z/OS)

These views show the response time or elapsed time performance of transactions that occur within workloads.

**BEST PRACTICE**

For quick access to application performance data that is collected by several MAINVIEW products, create a customized screen definition that combines the workload objective views from those products. You can save the screen definition in your personal screen data set or in a site data set that is shared by users. For more information about creating a screen definition, see the *MAINVIEW User Guide*. 
Manage application exceptions

MAINVIEW Alarm Management can help you manage application exceptions by setting alarms on important MAINVIEW metrics. Alarms eliminate the need to monitor views constantly to find exception conditions. Instead, exceptions can be displayed automatically on a single screen. By responding to the alarms, you can proactively address small problems before they become big problems—often before users are even aware of the problem. Alarms also provide a path to automation because exception events can be sent to MAINVIEW AutoOPERATOR.

To set an alarm on a view field

- Choose a metric from a table in Chapter 2, “Important MAINVIEW metrics.”
- Display the view listed in the table.
- Use the MAKEALARM wizard to create the alarm definition.
- Activate the alarm definition.
- Optionally, use the deployment wizard to deploy the alarm definition to multiple systems.

**EXAMPLE**

To monitor DB2 users that are suspended for locks, you would

- find “users suspended for locks” in the table of DB2 metrics (page 38)
- display the LSTSUSPZ view in MAINVIEW for DB2
- use view customization to review the threshold for the **Lock Wait Time** field (element L100LELP) and do one of the following actions:
  - Accept the default threshold (if one exists) and exit view customization.
  - Update the threshold to the recommended threshold shown in the table of DB2 metrics, which is L100LELP > 2, and save the customized view.
  - Update the threshold as appropriate for your situation and save the customized view.

- position the cursor on the **Lock Wait Time** field
- use the MAKEALARM wizard to create an alarm definition
- activate the alarm

Customizing the threshold for the field **before** invoking MAKEALARM ensures that the view and alarm definition use the same threshold.

For more information about alarms and the wizards, see the

- online Help
- MAINVIEW Alarm Management User Guide
Best Practices for alarms

Use the following Best Practices to effectively use alarms in your event management strategy:

Set alarms judiciously

- Set alarms only for conditions that require intervention; do not set alarms for informational purposes. Raising a lot of insignificant alarms might result in all alarms being ignored, and clutters the exception displays with irrelevant information.

- Reduce false alarms by using reasonable thresholds and alarm persistence to ignore short-term exceptions due to data anomalies.

Avoid unnecessary alarm overhead

- Specify the predefined SSI context CURRSYS in the Context field of the alarm definition. This context reduces the number of records processed by MAINVIEW Alarm Management, and lets you install the alarm definition on multiple LPARs without having to change the alarm definition.

- Avoid setting alarms on views that supply hundreds or thousands of records, such as the following views:
  - device views in MAINVIEW for z/OS
  - transaction views in MAINVIEW for CICS
  - thread views in MAINVIEW for DB2
  - queue views in MAINVIEW for WebSphere MQ

  If you have to set alarms on these views (and there are instances when you should), set the frequency of the alarm to at least 60 seconds, and preferably to 120 seconds or more.

- Use an alarm frequency of 60 seconds to avoid excessive alarms.

Make alarms more effective

- Avoid setting alarms on interval views. If possible, set alarms from real-time views. Real-time views use a smaller, rolling sample set to provide more consistent, relevant data. In those instances where interval views must be used, validate the persistence of the condition prior to raising the alarm externally.

- Use a consistent naming convention for alarm definition directories.

- Assign queue names to summarize alarms.
- Do not accept the default values for the Message ID and Message Text when creating an alarm definition. Instead, specify a Message ID that identifies the business application affected by the alarm, and a Message Text that explains the impact on that application.

**EXAMPLE**

The default values might result in the following message in the alarm displays:

```
JDELAYAAS00 IDSYSBDEMO Jobname: QMRP ( >= 50)
```

However, specifying your own message ID and text will result in a more descriptive and useful message, such as the following example:

```
PAY0001 Payroll application jobs unacceptably delayed for lack of resources
```

**Improve the usefulness of alarm views**

- Establish a single point of control by displaying all alarms on one dashboard. For example, the ALERTxx or ALARMxx views are available in the MAINVIEW mainframe products and MAINVIEW Explorer. Customized views that focus on specific business applications are highly recommended.

- Use view customization to customize hyperlinks to shorten the navigation path to problem details.

- Avoid using alarm library names and alarm group names greater than eight characters. Alarm group and library names can contain up to 16 characters, however, due to space constraints, the distributed alarm views display only the first eight characters of these names. If you need to use library and group names longer than eight characters, you can create customized views that display up to 16 characters. This recommendation applies only to group and library names; MAINVIEW Alarm Management fully supports alarm names up to 16 characters.

For more information about alarms, see the **MAINVIEW Alarm Management Guide**.
Manage application transactions

Managing an application’s transactions lets you track business services across the systems and subsystems that support those services.

If MAINVIEW Transaction Analyzer is installed

MAINVIEW Transaction Analyzer correlates data collected by

- MAINVIEW for CICS
- MAINVIEW for DB2
- MAINVIEW for IMS
- MAINVIEW for MQSeries

and lets you manage transaction workloads throughout z/OS, across system and subsystem boundaries. You need only one piece of identifying information about the transaction, such as the transaction ID or user ID, to identify all of the components that belong to a transaction.

Start with the EZTA Easy Menu, and use the component and summary search dialogs to display the data that is most useful for analyzing your transactions. By drilling down to the lowest level of detail, you can see the topology of the transaction and find the root cause of problems.

For more information about managing transactions, see the MAINVIEW Transaction Analyzer User Guide.

If Q Nami! is installed

While MAINVIEW Transaction Analyzer correlates all of the mainframe components of a business transaction, the Q Nami! product from MQSoftware provides transaction monitoring for the non-mainframe components. Q Nami! provides a robust transaction monitoring solution for many distributed technologies. BMC sells and supports the Q Nami! to compliment MAINVIEW Transaction Analyzer.

For more information about Q Nami!, see the

Summary of Best Practices: Managing the application

Table 14  Best Practices: Managing the application

<table>
<thead>
<tr>
<th>✓ Decision or task</th>
<th>Best Practice</th>
</tr>
</thead>
</table>
| Collect information about the business application that you want to manage. | ■ Determine the application’s components, core users, critical time periods, and process flow.  
■ Find pertinent metrics for the application in Chapter 2, “Important MAINVIEW metrics.”  
■ Use the “Application information worksheet” on page 78 to record the information. |
| Define workloads to monitor the application.           | ■ Establish some basic service level objectives for the application.  
■ Employ the “Best Practices for workload definitions” on page 59.  
■ Create workload definitions for the application by using the MAINVIEW products for IBM CICS, DB2, IMS, or z/OS. |
| Manage application availability and performance.       | ■ Use MAINVIEW VistaPoint to monitor workloads.  
■ If MAINVIEW VistaPoint is not installed, use the MAINVIEW products for IBM CICS, DB2, IMS, or z/OS to monitor workloads. Create a customized screen definition that combines the workload objective views from those products. |
■ Set MAINVIEW Alarm Management alarms on the metrics that indicate availability and performance. |
| Manage application transactions across systems and subsystems. | ■ Use MAINVIEW Transaction Analyzer to track transactions on the mainframe.  
■ Use Q Nami! product from MQSoftware to track non-mainframe transactions. |
Automating event management

This chapter presents the following topics:

Why automate ................................................................. 68
What to automate .............................................................. 68
Collect information about events ........................................... 69
Create Rules to automate a solution ...................................... 70
    Best Practices for Rules .................................................... 71
    Configuration recommendations for MAINVIEW AutoOPERATOR . 74
Beyond basic event management ........................................... 75
Summary of Best Practices: Automating event management ........... 76
Why automate

MAINVIEW AutoOPERATOR takes application management to the next level by automating the ability to react to and correct events as they occur. Adding automation to your enterprise can help you

- proactively address small problems before they become big problems
- reduce or avoid outages and improve service
- notify support personnel as soon as a problem occurs instead of waiting for a user to report it
- control costs and reduce resource consumption
- leverage existing technical staff expertise

What to automate

Consider the following tasks and areas of your IT infrastructure when deciding what to automate:

- repetitive, well-defined tasks such as system startup and shutdown
- notification of support personnel
- restart of failed processes such as jobs, started tasks, transactions, programs, databases, and queues
- system data and messages
- complex areas of IT or areas that lack skilled staff and expertise

MAINVIEW AutoOPERATOR automation can be triggered by alarms on fields in a view (MAINVIEW metrics), or by various system messages.

You can create a MAINVIEW AutoOPERATOR Rule to trap WTOs, WTORs, MLWTOs, IMS messages, CICS transient data queue (TDQ) messages, ALERTs, journal messages, WebSphere MQ messages on a queue, and more.
Collect information about events

After determining a particular area of your IT infrastructure that could benefit from automation, select a couple of events that can have a negative impact on users. Answer the following questions to help determine how to automate those events. You can print the “Event automation worksheet” on page 82 to help with this task.

Which events?

Talk to application programmers, system programmers, and operators to isolate some critical events, such as

- DB2 threads that use too much CPU
- runaway CICS transactions
- abending transactions

Determine the best indicator of those events. Can you use any of the MAINVIEW metrics described in Chapter 2, “Important MAINVIEW metrics”? Or is a particular message, for example, a WTO or journal message, a better indicator of the event? If so, gather any available information about the message.

Who should be notified and how?

Determine who should be notified of the events and how they should notified. The automated solution can

- send a TSO message
- send an e-mail message
- page personnel by using a notification system such as AlarmPoint
- open a problem ticket by interacting with an incident tracking system, such as Remedy Service Desk
- forward the event to an event management system, such as BMC Impact Manager

What action should be taken?

Determine what actions should be taken when the event occurs. The automated solution can involve a simple action or a series of more complex actions. A simple action might

- issue a z/OS, IMS, CICS, DB2, MQ, or other type of command
Create Rules to automate a solution

When you have determined what events to manage, who should be notified, and what action should be taken, you are ready to create a MAINVIEW AutoOPERATOR Rule to manage the event.

Start with the MAINVIEW AutoOPERATOR Event Activity Statistics panel. From this panel, you can select an event and then progress through a series of panels to specify

- automation criteria
- actions to be performed if the criteria is met
- whether alerts should be sent to operators
- whether events should be sent to BMC Impact Manager

For more information about creating Rules, see

- “Best Practices for Rules” on page 71
- “Configuration recommendations for MAINVIEW AutoOPERATOR” on page 74
- MAINVIEW AutoOPERATOR online Help
- MAINVIEW AutoOPERATOR Basic Automation Guide, Volume 1: Using Rules
Best Practices for Rules

Consider the following Best Practices for creating and maintaining Rules. For more detailed information about Rules, see the MAINVIEW AutoOPERATOR Basic Automation Guide, Volume 1: Using Rules.

Get consensus

- Centralize the function of creating Rules to a single operator or systems person to reduce the possibility of several people creating conflicting Rules, and to make it easier to review and manage Rules.

- Decide on naming conventions for Rules, EXECs, and Alert Queues, preferably before you begin creating Rules or EXECs. Standardized names make it easier to manage automation routines, especially as the number of Rules and EXECs increase.

- Provide console operators with a form to request automation for messages that are not yet managed by a Rule. For a sample form, see “Message automation request form” on page 80.

- Discuss requests for new Rules with the operations staff (all shifts) to ensure that the Rules do not adversely affect them.

Create effective Rules for messages

- Specify a Rule ID that matches the message identifier that the Rule traps. If you create more than one Rule for the same message, use a suffix to differentiate the Rules, which makes it easier to find the Rules for a particular message in displays. If you or someone else attempts to reuse the same message ID as a Rule ID, the Rule ID will be reset to RULnnnnn, indicating that the Rule ID is already in use.

- When creating a Rule to trap a message, consult the documentation for that message to ensure that all variations of the message are trapped by the Rule.

- If you create a Rule for the PM0010I message, which indicates that MAINVIEW AutoOPERATOR has started trapping z/OS messages, specify an Event Type of JRNL (journal) to ensure that the Rule fires for the BBI-SS PAS in which MAINVIEW AutoOPERATOR is active.

- Do not suppress messages from SYSLOG unless absolutely necessary. Suppressing these messages removes evidence that might be useful for troubleshooting.

- Do not reword a WTO unless absolutely necessary. Rewording a WTO causes the message in the SYSLOG to be reworded, which removes evidence that might be useful for troubleshooting. Instead of rewording a WTO, consider suppressing it and issuing an alert.
Simplify console automation by using a standard format for WTO messages that are issued by Rules and EXECs and make sure they contain the correct information.

--- EXAMPLE ---
Use a Text ID that is prefixed by the EXEC name or Rule ID that created it and, if necessary, suffixed by a numeric to distinguish it from other messages issued by the same EXEC or Rule.

Use variables

Use variable names instead of TSO user IDs in notification fields. Use variable names instead of specific values for alert targets and alert queue names. By using variables, you can update many Rules by changing a single variable value. Variables also help with standardization of Rules.

Organize Rule Sets

Separate Rules into Rule Sets by event type. Set the filter option for each Rule Set to the event type and use a consistent naming convention for the Rule Sets, such as

- RULALRM for MAINVIEW Alarms (from MAINVIEW Alarm Management)
- RULCICS for CICS Transient Data Queue messages
- RULCMD for z/OS commands
- RULDB2 for MAINVIEW for DB2 (this Rule Set is unnecessary if you use MAINVIEW AutoOPERATOR for z/OS to trap DB2 messages)
- RULIMS for IMS Master Terminal messages (from the IMS AOI exit)
- RULJRNL for MAINVIEW Journal messages from MAINVIEW for CICS, MAINVIEW for DB2, and MAINVIEW for IMS
- RULMQ for WebSphere MQ events
- RULTIME for time-initiated rules
- RULZOS for z/OS console messages

In a shared DASD environment, store Rule Sets in a single, shared data set to simplify Rules management.

Keep obsolete Rules in a disabled Rule Set in case you need to use them again. Give the Rule Set a descriptive name, for example, RULOLD. When you want to retire a Rule, select the disabled Rule Set (which puts it into a LOADED state), disable the obsolete Rule, add comments to the Rule as appropriate, move (do not copy) the obsolete Rule into the Rule Set, and disable the Rule Set. Be sure to keep both the Rule Set and Rules within it disabled to avoid accidentally firing the Rules.
- Avoid firing more than one Rule for the same event unless a single Rule cannot perform all of the necessary actions. Firing a single Rule per event will simplify the administration, troubleshooting, and maintenance of Rules.

**Optimize performance**

- Create Rules instead of EXECs whenever possible. A Rule uses fewer resources than an EXEC.

- Except when specifying a message ID, specify the minimum selection criteria required to fire the Rule. Extraneous selection criteria increases processing time.

- Avoid using an asterisk as the first character in the **Text String** field unless a **Text ID** is specified. Excessive pattern matching will result in inefficient Rule processing and might impact system performance. Avoid using leading asterisks for pattern matching in selection criteria because they are very inefficient. If possible, replace leading asterisks with more specific selection criteria.

- Move the Rules that fire most often to the top of each Rule Set that uses an automation strategy of FIRST to eliminate unnecessary overhead. To determine which Rules fire most often, run MAINVIEW AutoOPERATOR for a day or more, and then sort the Rule Set Overview panel by the **Fired** column, and note the five or ten Rules at the top of the list. Then unsort the list, and move the most-fired Rules to the top of the list by using the M (move), A (after), and B (before) line commands.

For more detailed information about Rules, see the **MAINVIEW AutoOPERATOR Basic Automation Guide, Volume 1: Using Rules**.
Configuration recommendations for MAINVIEW AutoOPERATOR

To facilitate the Best Practices discussed in this book, use the following MAINVIEW AutoOPERATOR parameter settings:

<table>
<thead>
<tr>
<th>Library</th>
<th>Member</th>
<th>Parameter and recommended value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UBBPARM</td>
<td>BBISSP00</td>
<td>ALRTRCVE=YES</td>
<td>specifies that the BBI-SS PAS can receive product alerts from other BMC products</td>
</tr>
<tr>
<td>BBPARM</td>
<td>BBISSP00</td>
<td>MCTSIZE=4080 (or greater)</td>
<td>specifies the total number of unique messages to be displayed on the message activity statistics panel</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specify MCTSIZE=4080 or greater. For efficient use of storage, the value should be a multiple of 510. The default is 510.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Tip:</strong> To determine an appropriate MCTSIZE value, run MAINVIEW AutoOPERATOR for about a week, display the Event Activity Statistics panel, note the number in the <strong>Unique</strong> field in the upper right corner of the panel, and increase the number to a multiple of 510. Specifying this number will ensure that the MCTSIZE value is sufficient for the number of unique message IDs processed by MAINVIEW AutoOPERATOR in a week.</td>
</tr>
<tr>
<td>BBPARM</td>
<td>AAOPRM00</td>
<td>RULESCAN=INDIVIDUAL</td>
<td>specifies that each Rule Set can have its own (individual) automation strategy</td>
</tr>
<tr>
<td>UBBPARM</td>
<td>$$INSYS0</td>
<td>AEWALERT=YES</td>
<td>specifies that exception monitors send messages to MAINVIEW AutoOPERATOR for use as Alerts</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$$INSYS0 is a MAINVIEW SYSPROG Services member.</td>
</tr>
</tbody>
</table>

For more information about these parameters, see the MAINVIEW AutoOPERATOR Customization Guide.
Beyond basic event management

The Best Practices discussed in this book provide a good foundation on which to build your event management strategy. However, there are many ways to expand that strategy. For example, you can perform additional notification by sending e-mail messages and communicating with wireless devices, including pagers, as described in the MAINVIEW AutoOPERATOR Solutions Guide.

You can also take advantage of the integration between BMC products and other products to show the impact of mainframe outages and slowdowns on critical business services. For example, you can

- send events from MAINVIEW AutoOPERATOR to BMC Impact Manager from a Rule or EXEC, as described in the BMC Impact Integration for z/OS with MAINVIEW AutoOPERATOR User Guide

- send notification requests from MAINVIEW AutoOPERATOR to AlarmPoint, which manages various notification methods and problem escalation

- use MAINVIEW AutoOPERATOR to send Simple Network Management Protocol (SNMP) traps to other event management systems, such as IBM Tivoli Enterprise Console® or Computer Associates Unicenter, as described in the MAINVIEW AutoOPERATOR Solutions Guide

- publish MAINVIEW AutoOPERATOR alerts to PATROL Enterprise Manager or BMC Event Manager workstations, as described in the MAINVIEW AutoOPERATOR Basic Automation Guide, Volume 1: Using Rules

- open trouble tickets with an incident tracking product such as Remedy Service Desk, either by publishing MAINVIEW AutoOPERATOR alerts to PATROL Enterprise Manager workstations, or by sending e-mail messages generated by MAINVIEW AutoOPERATOR to Remedy


These methodologies and products can help you evolve your event management strategy even further — to fully align your IT infrastructure with your business services goals.
# Summary of Best Practices: Automating event management

## Table 15  Best Practices: Automating event management

<table>
<thead>
<tr>
<th>✓</th>
<th>Decision or task</th>
<th>Best Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Collect event information.</td>
<td>■  Determine which events to automate, who to notify, and what actions to perform.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■  Use the “Event automation worksheet” on page 82 to record the information.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■  Adopt the “Configuration recommendations for MAINVIEW AutoOPERATOR” on page 74.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■  Use MAINVIEW AutoOPERATOR to create Rules to trap events and trigger automation.</td>
</tr>
<tr>
<td></td>
<td>Extend your event management strategy.</td>
<td>■  Use the “Application information worksheet” on page 78.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■  Perform advanced automation and event management by using the integration between BMC products and other products.</td>
</tr>
</tbody>
</table>
Event management worksheets

This appendix provides worksheets that can help you in implementing and maintaining an event management strategy. You can print and use these worksheets, or use them as a model for creating your own printed or electronic worksheets.

Use the “Application information worksheet” on page 78 to collect information about an application that you want to manage.

Console operators can use the “Message automation request form” on page 80 to request message automation for those messages that are not yet managed by a MAINVIEW AutoOPERATOR Rule.

Use the “Event automation worksheet” on page 82 to collect information about events for which you want to automate a solution.
# Application information worksheet

Use this worksheet to collect information about an application that you want to manage.

<table>
<thead>
<tr>
<th>Name of application:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Business services provided by application:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Application users and critical time periods of use:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Application component</th>
<th>Component name</th>
<th>Where component executes or resides, if applicable</th>
</tr>
</thead>
<tbody>
<tr>
<td>batch jobs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CICS transactions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DASD volumes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DB2 databases</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DB2 plans</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMS databases</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMS programs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMS transactions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>JES resources such as lines and printers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LPARs dedicated to application</td>
<td></td>
<td></td>
</tr>
<tr>
<td>started tasks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP/IP resources</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TSO users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>USS processes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VTAM resources</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WebSphere MQ queue manager queues</td>
<td></td>
<td></td>
</tr>
<tr>
<td>other components</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Metrics that should be monitored


<table>
<thead>
<tr>
<th>Metric</th>
<th>View name</th>
<th>View field</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Business process flow diagram

 Optionally, use this page to create a diagram of the application’s business process flow.
Console operators can use this form to request message automation for messages that are not yet managed by a MAINVIEW AutoOPERATOR Rule. See the form instructions on the next page.

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Message automation request form

Form Instructions

Message ID Specify the message ID or the first word of the message (all characters prior to the first blank). Optionally, provide the entire message in the Notes column, print the message from the console, or record the time the message was issued, so it can be located it in the SYSLOG.

Action Specify the action that you want performed when the message is issued. Choose one of the following actions or provide your own action:

- **Suppress** The message is not needed. Indicate whether the message currently appears on the z/OS console or the Alerts display in the Notes column.
- **Alert** The message is important and should appear on the Alerts display. Indicate the priority or color of the alert and the alert queue in the Notes column:
  
  | CLEAR  | GREEN |
  |INFO    | LTBLUE |
  |WARN    | DKBLUE |
  |MINOR   | YELLOW |
  |MAJOR   | PINK |
  |CRITICAL| RED |
- **Change** Alert The message is currently on the Alerts display, but the priority, color, or queue is wrong. Indicate the changes you want in the Notes column.
- **Reply** The message is a WTOR which should always be replied to the same way. Indicate the desired reply in the Notes column.
- **Action** When the message occurs, someone should take a specific action. This can be either a single command (for example, cancel or start a job) or a series of simple actions. Indicate the desired action(s) in the Notes column.
- **Other** Events such as timer-driven actions can be included here (they do not require a Message ID, just an interval). Include any suggestions for automation in the Notes column.

Notes Provide any additional helpful information.

Example

This example shows a possible Automation Request Form for this sample automation request:

- **Suppress** the message $HASP000 OK
- **Reply** WAIT to the message IEF238D REPLY DEVICE NAME, 'WAIT', OR 'CANCEL'
- **Issue an alert** for the message DFH507 CICS IS UNDER STRESS

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>$HASP000</td>
<td>Suppress</td>
<td>$HASP000 OK currently appears on the console</td>
</tr>
<tr>
<td>IEF238D</td>
<td>Reply</td>
<td>WAIT</td>
</tr>
<tr>
<td>DFH507</td>
<td>Alert</td>
<td>CRITICAL priority (red), CICS Queue</td>
</tr>
</tbody>
</table>
# Event automation worksheet

## Event

Indicate which event you want to automate, for example, CICS transaction abends or DB2 threads with high CPU utilization:

## Event notification

When the event occurs, perform the following notification. Check any notification types that apply and provide user names, TSO user IDs, or product names as appropriate.

- Send a TSO message to:
- Send an e-mail message to:
- Send a page to:
- Open a Help Desk ticket with:
- Forward the event to an event management system, such as BMC Impact Manager:
- Perform another type of notification:

## Event automation

When the event occurs, perform the following actions. Check any actions that apply and provide the required information. See “Collect information about events” on page 69 of the *MAINVIEW Best Practices: Event Management* book for more information about the following actions.

- Issue a command (provide command):
- Log diagnostic information to the MAINVIEW AutoOPERATOR journals or system logs:
- Raise a more informative exception by rewording a cryptic message:
- Correlate the event with previous events to provide a more meaningful exception:
- Schedule a REXX EXEC:
- Perform another action:
Index

Symbols

$$\text{INSYS0 member}$$ 74

A

AAOPRM00 member 74
abends
ASRA 35
CICS transaction 35
active log archival impact 38, 41
AEWALERT parameter 74
AlarmPoint 75
alarms
avoiding false 62
Best Practices 62
deployment wizard 61
description 16
naming conventions 62
overview 21
alerts
description 16
overview 22
ALRTRCVE parameter 74
application information worksheet 78
applications
benefits of managing 56
collecting information about 57
defining workload for 58
exceptions 61
monitoring availability 60
archive impacts 38, 41
ASRA abends 35
automation
benefits of 68
form to request 77

B

background monitors. See monitors
batch jobs 25
BBISSP00 member 74
BBPARM
AAOPRM00 member 74
BBISSP00 member 74
beans, deployed EJB 46

Best Practices
alarms 62
description 14–15
Rules 71
workload definitions 59
BMC Impact Integration 75
BMC Software, contacting 2

C

CF (coupling facility) 26
channel initiator, WebSphere MQ 49, 51
CICS metrics 32
classes of metrics 20
Computer Associates Unicenter 75
configuration recommendations for MAINVIEW
AutoOPERATOR 74
collections
CICS 33
DB2 33, 37, 50
DDF 39, 41
IMS 34, 37, 50
J2C 46
JDBC servers 46
MQ 34
OTMA 43
remote 48
CONTROL-O 21
conventions, documentation 11
coupling facility (CF) 26
cross coupling facility (XCF) structures 50
CSA
overcommitted 26
utilization 27
CURRSYS in alarm definition 62
customer support 3

D

DASD RESERVES 26
data collectors 21
data sets extents 30
database availability  
   DB2 38  
   IMS 42  
DB2 metrics 38  
DBM1 storage utilization 38  
DDF threads and connections 41  
deadlock events, DB2 39  
DEDB areas 42  
deployment wizard for alarms 61  
device status, TCP/IP 48  
documentation overview 10  

E  
elapsed time, DB2 thread 39  
Enterprise JavaBeans (EJB) 46  
event automation worksheet 82  
events, automating a solution 68  
exceptions, managing by 61  
extents, data sets 30  

F  
false alarms, avoiding 62  
file status  
   CICS 33  
   Linux 28  
   UNIX 29  
form to request automation 77  
fragmentation index 30  
FTP activity 49  

G  
garbage collection 47  

H  
help desk ticket, Remedy 75  

I  
I/O rate and response 26  
IBM Tivoli Enterprise Console 75  
IMS Connect work unit 43  
IMS metrics 42  
incident tracking, Remedy 75  
indexed VTOC status 30  
Initiator Queue status 50  
INITQ status 50  
intra-group queuing, WebSphere MQ 52  

J  
J2C connections 46  
J2EE deployed applications 46  
Java servlet usage 47  
JVM garbage collection 47  

L  
Linux metrics 28  
listeners (TCP/IP and LU 6.2) 50  
locks  
   DB2 41  
   DB2 users suspended for 40  
   IMS 45  
logical volume response time 27  
logical volumes 30  

M  
MAINVIEW Alarm Management 17, 61  
MAINVIEW AutoOPERATOR  
   See also Rules  
   benefits 68  
   configuration recommendations 74  
MAINVIEW Transaction Analyzer 64  
MAKEALARM wizard 61  
MCTSIZE parameter 74  
message automation request form 80  
metrics  
   CICS 32  
   classes of MAINVIEW 20  
   DB2 38  
   how MAINVIEW collects 21  
   IMS 42  
   Linux 28  
   responding to 23  
   Storage Resource Manager (SRM) 30  
   TCP/IP 48  
   UNIX 29  
   WebSphere Application Server 46  
   WebSphere MQ 49  
   z/OS 25  
monitors  
   CICS 37  
   DB2 41, 45  
   IMS 45  
   overview 22  
monitors in warning status 35  
MQ CPU usage 52  
MQ manager 50  
MQSoftware Q Nami! 64  
MSC link status 43  
MVS metrics. See z/OS metrics
naming conventions
alarms 62
Rules 71
workloads 59
notification
as part of automated solution 69
wireless devices 75

object availability, DB2 38
OTMA connection 43

page set status 51, 52
pagers, sending notification to 75
PATROL Enterprise Manager 75
performance
alarms 62
Class B metrics 20
Rules 73
Performance Index (PI) problems 26
physical platter response time 31
PI (Performance Index) problems 26
pools, user defined 31
process status
Linux 28
UNIX 29
product support 3
program status
CICS 34
IMS 43
publications, related 10

Q
Q Nami! 64
queues, WebSphere MQ
manager status 51
performance 53

recommendations
for alarms 62
for Rules 71
for workloads 59
MAINVIEW AutoOPERATOR configuration 74
regions
CICS 32, 35, 37
DB2 38
IMS 42, 44
related publications 10
Remedy Service Desk 75
remote connections 48
Rule Sets, organizing 72
Rules
Best Practices 71
configuration recommendations 74
creating 70
naming conventions 71
variables in 72
RULESCAN parameter 74
runaway DB2 threads 41

server, WebSphere Application Server 46
servlet usage 47
Simple Network Management Protocol (SNMP) traps 75
SNMP (Simple Network Management Protocol) traps 75
SRM metrics 30
storage groups 31
Storage Resource Manager (SRM) metrics 30
support, customer 3
supported products 15

tasks 35, 37
TCP/IP metrics 48
technical support 3
terminology, MAINVIEW 16
threads, DB2
DDF 41
elapsed time 39, 41
runaway 41
throughput, CICS transactions 36
Tivoli Enterprise Console 75
tracking transactions 64
transaction availability, CICS 35
transaction management 64
transactions
abends 35
IMS 43
throughput 36
with high CPU time 36
with high elapsed time 36
traps, Simple Network Management Protocol (SNMP) 75
trouble tickets 75

UBBPARM
$$INSYS0 member 74
BBISSP00 74
Unicenter 75
UNIX metrics 29
user defined pools 31
users suspended for locks 40

V
variables in Rules 72
volumes
  DASD RESERVES 26
  fragmentation index 30
  logical 27, 30
  physical 31
  VTOC index 30
VSAM data sets 31

W
web application usage 47
WebSphere Application Server metrics 46
WebSphere MQ metrics 49
wireless devices, sending notification to 75
WLM performance 47
workload manager performance 47
workload objectives
  CICS 36
  DB2 40
workloads
  Best Practices 59
  naming conventions 59
  sample objectives 58
worksheet
  application information 78
  event automation 82
  message automation request 80

X
XCF (cross coupling facility) structures 50

Z
z/OS metrics 25