

M



Solution Management Guide

SAPTM Master Data Management

Release 2.00

Document Version 1.00 - October 21, 2003

For SAP Internal Use Only



SAP AG

Neurottstraße 16
69190 Walldorf
Germany
T +49/18 05/34 34 24
F +49/18 05/34 34 20
www.sap.com

© Copyright 2003 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft®, WINDOWS®, NT®, EXCEL®, Word®, PowerPoint® and SQL Server® are registered trademarks of Microsoft Corporation.

IBM®, DB2®, DB2 Universal Database, OS/2®, Parallel Sysplex®, MVS/ESA, AIX®, S/390®, AS/400®, OS/390®, OS/400®, iSeries, pSeries, xSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere®, Netfinity®, Tivoli®, Informix and Informix® Dynamic Server™ are trademarks of IBM Corporation in USA and/or other countries.

ORACLE® is a registered trademark of ORACLE Corporation.

UNIX®, X/Open®, OSF/1®, and Motif® are registered trademarks of the Open Group.

Citrix®, the Citrix logo, ICA®, Program Neighborhood®, MetaFrame®, WinFrame®, VideoFrame®, MultiWin® and other Citrix product names referenced herein are trademarks of Citrix Systems, Inc.

HTML, DHTML, XML, XHTML are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

JAVA® is a registered trademark of Sun Microsystems, Inc.

JAVASCRIPT® is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

MarketSet and Enterprise Buyer are jointly owned trademarks of SAP AG and Commerce One.

SAP, SAP Logo, R/2, R/3, mySAP, mySAP.com, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies.

Disclaimer






Some components of this product are based on Java™. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressly prohibited, as is any decompilation of these components.

Any Java™ Source Code delivered with this product is only to be used by SAP's Support Services and may not be modified or altered in any way.

Typographic Conventions

Type Style	Represents
<i>Example Text</i>	Words or characters that appear on the screen. These include field names, screen titles, and pushbuttons, as well as menu names, paths, and options.
Example text	Emphasized words or phrases in body text, titles of graphics, and tables
EXAMPLE TEXT	Cross-references to other documentation
Example text	Names of elements in the system. These include report names, program names, transaction codes, table names, and individual key words of a programming language, when surrounded by body text, for example, SELECT and INCLUDE.
Example text	Screen output. This includes file and directory names and their paths, messages, names of variables and parameters, source code, as well as names of installation, upgrade, and database tools.
Example text	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
<Example text>	Variable user entry. Pointed brackets indicate that you replace these words and characters with appropriate entries.
EXAMPLE TEXT	Keys on the keyboard, for example, function keys (such as F2) or the Strg key.

Icons

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

Contents

1	GETTING STARTED	6
1.1	GLOBAL DEFINITIONS	6
1.2	IMPORTANT SAP NOTES	7
1.3	HISTORY OF CHANGES	8
2	TECHNICAL SYSTEM LANDSCAPE	9
2.1	SCENARIO/COMPONENT MATRIX	9
2.2	RELATED DOCUMENTATION	9
3	MONITORING OF SAP MASTER DATA MANAGEMENT 2.00	10
3.1	ALERT MONITORING WITH CCMS	10
3.1.1	<i>Component alert monitoring</i>	10
3.1.2	<i>Scenario alert monitoring</i>	11
3.2	MONITORING DETAILS, TRACE AND LOG FILES	11
3.2.1	<i>Master Data Server 2.0</i>	11
3.2.2	<i>User Management Engine 3.0</i>	12
3.2.3	<i>Content Integrator 2.0</i>	12
3.2.4	<i>SAP J2EE Server 6.20</i>	13
3.2.5	<i>Exchange Infrastructure</i>	14
3.2.6	<i>Enterprise Portal</i>	17
3.2.7	<i>Solution Manager 3.1</i>	17
3.2.8	<i>Internet Transaction Server</i>	17
3.3	APPENDIX	19
3.3.1	<i>Setting up Monitoring for Web Application Server 6.20 based components</i>	19
3.3.2	<i>Setting up Monitoring for SAP J2EE Server</i>	21
3.3.3	<i>Setting up Monitoring for ITS 6.20</i>	29
3.3.4	<i>Setting up GRMG Availability Monitoring</i>	32
4	MANAGEMENT OF MYSAP TECHNOLOGY	33
4.1	ADMINISTRATION TOOLS OF SOFTWARE COMPONENTS	34
4.2	STARTING AND STOPPING	34
4.2.1	<i>Controlled starting and stopping of single components</i>	34
4.2.2	<i>Unplanned starting and stopping</i>	35
4.3	BACKUP/RESTORE AND RECOVERY	35
4.3.1	<i>General remarks</i>	35
4.3.2	<i>Backup of individual components in an MDM landscape</i>	37
4.3.3	<i>B&R for individual system components</i>	39
4.3.4	<i>Point in Time Recovery of single components</i>	41
4.4	SYSTEM COPY	44
4.5	PERIODICAL TASKS	44
4.5.1	<i>Required periodical tasks (Components)</i>	44
4.5.2	<i>General</i>	46
4.6	LOGON AND LOAD BALANCING	46
4.7	USER MANAGEMENT	47
4.8	PRINTING	47
5	HIGH AVAILABILITY	48
5.1	SYSTEM LANDSCAPE OF THE SOLUTION	48
5.2	HIGH AVAILABILITY MATRIX FOR THE INDIVIDUAL COMPONENTS	48
5.3	RELEVANT DOCUMENTATION	49
6	SOFTWARE CHANGE MANAGEMENT	51
6.1	SAP MASTER DATA MANAGEMENT	51
6.1.1	<i>Transport and Change Management</i>	51

6.1.2	<i>Support Packages and SAP Notes Implementation</i>	52
7	TROUBLESHOOTING	53
8	SERVICES FOR SAP MASTER DATA MANAGEMENT	53
9	APPENDIX	54
9.1	CATEGORIES OF SYSTEM COMPONENTS FOR BACKUP & RECOVERY	54
9.2	RELATED GUIDES.....	55
9.3	RELATED INFORMATION	55

1 Getting Started



This guide does not replace the daily operations handbook that we recommend customers to create for their specific productive operations.

About this Guide

Designing, implementing, and running your mySAP solution at peak performance 24 hours a day has never been more vital for your business success than today.

This guide provides a starting point for managing your mySAP solutions and keeping them up and running optimally. It contains specific information for various tasks, and lists the tools that you can use to carry them out. It also refers to documentation required for these tasks. You can use this guide only in connection with other guides such as the Master Guide, Technical Infrastructure Guide, and the SAP Library.

The chapters *Monitoring of mySAP Technology* and *Managing of mySAP Technology* describe the related topics on the mySAP solution level. The chapter *Business Process Management* describes related topics on the mySAP solution and/or business scenario level.

Target Groups

- Technical consultants
- System administrators
- Solution Consultants
- Business Process Owner
- Support Specialist

1.1 Global Definitions

mySAP Solution:

A mySAP solution represents a market view on groups of related business scenarios. The delivery of a solution contains mySAP components, which are essential to implement all solution related business scenarios, processes and functions. Together with a solution the implementation knowledge is allocated.

Business scenario:

From a microeconomic perspective the business scenario is a cycle, which consists of several different timely and logical processes affiliated with each other. Typically a business scenario passes several company departments and could get involved with other business partners. From a technical point of view a business scenario needs for the cycle at least one or more mySAP application components (SAP R/3, SAP APO, ...) and maybe other third party systems. A business scenario is a unit, which could be implemented and has releases.

A business scenario is a customer's perspective course of business.

Component:

Components are the smallest units, which will be considered separately within the Solution Development Lifecycle because they are separately producible, deliverable, installable and maintainable units.

1.2 Important SAP Notes



Check regularly, which SAP Notes are available for the Solution Management Guide.

Important SAP Notes

SAP Note Number	Title	Comment
371023	Monitoring of Operating System Data	
19227	Get the Latest Saposcol	
212876	The New Archiving Tool SAPCAR	
418285	Installation of the ITS Plug-In for the CCMS Agent	
588568	SAP Exchange Infrastructure 2.0: Patch Procedure	
651321	MDM 2.00: Delivery of MDM Web Application for XI	
535199	CCMS Agents: Monitoring Log Files	

1.3 History of Changes



Make sure you use the **current** version of the Solution Management Guide.

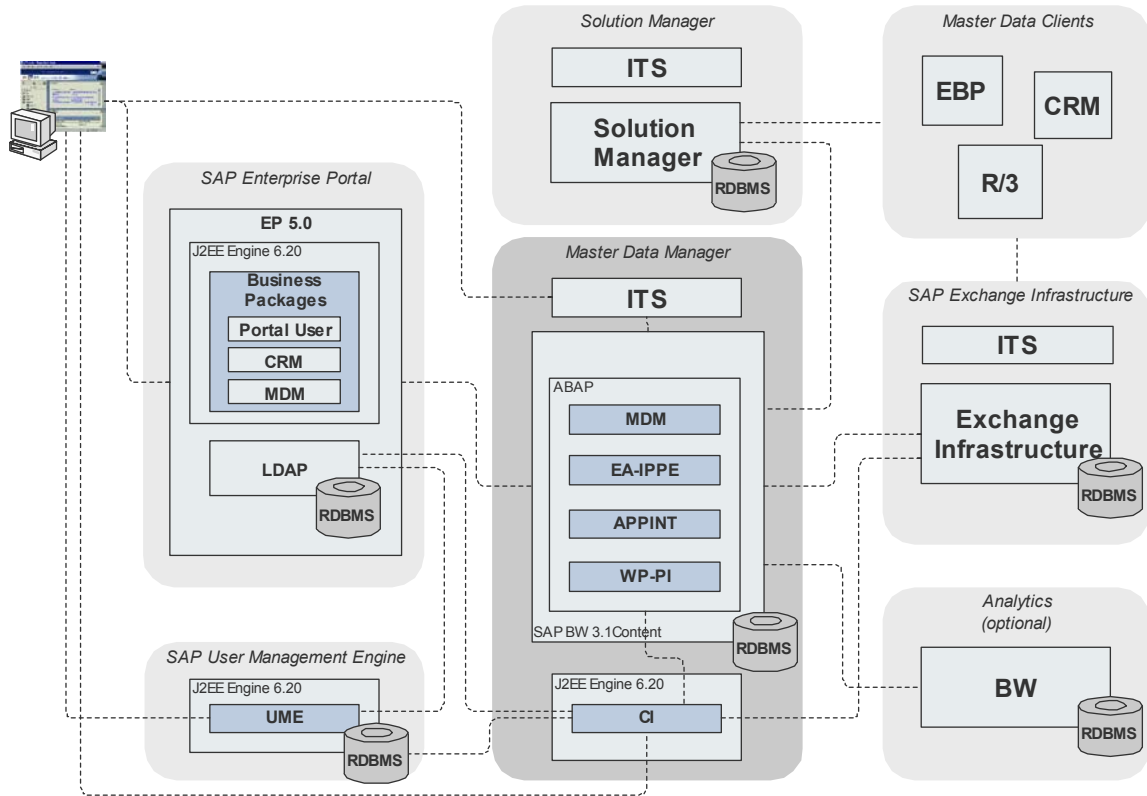
You can find the current version of the Solution Management Guide on the *SAP Service Marketplace* under the Internet address service.sap.com/instguides.

The following table provides an overview of the most important changes in prior versions.

Version	Important Changes
1.0	First version of the SAP MDM Solution Management Guide

2 Technical System Landscape

2.1 Scenario/component matrix



2.2 Related documentation

The following table lists where you can find more information about the technical system landscape.

Topic	Guide/Tool	Quick Link to the SAP Service Marketplace (service.sap.com)
Application and industry-specific components such as SAP Financials and SAP Retail	Master Guide	instguides
Technology components such as SAP Web Application Server	Master Guide	instguides
Sizing	Quick Sizer Tool	sizing
Technical configuration	Technical Infrastructure Guide	ti
Scalability	Technical Infrastructure Guide	ti
High availability	Technical Infrastructure Guide	ti
Security	Technical Infrastructure Guide	ti security

3 Monitoring of SAP Master Data Management 2.00

Monitoring of mySAP Technology is an essential task within the management of mySAP Technology. A chapter has therefore been devoted strictly to this subject.

You can find more information about the underlying technology in the Technical Operations Manual for mySAP Technology in the *SAP Library* under *mySAP Technology Components*.

3.1 Alert monitoring with CCMS

Proactive automatic monitoring is the basis to ensure reliable operations for your SAP system environment. SAP provides you the infrastructure and recommendations how to setup your alert monitoring to recognize critical situations for SAP Master Data Management 2.00 as fast as possible.

3.1.1 Component alert monitoring

Currently, there is no CCMS (Computer Center Management System) monitor template for the SAP Master Data Management 2.00 Solution. Therefore, you have to set up CCMS monitoring for each component individually. You can use existing monitors, such as XI 2.0 or the J2EE server for some components.

Please refer to the documentation *CCMS agents* under service.sap.com/monitoring on how to set up the CCMS monitoring agents.

In the Appendix to this chapter, you will find detailed descriptions on how to set up the CCMS monitoring for the different components.

3.1.1.1 Master Data Server 2.0

The Master Data Server 2.0 is based on Web Application Server 6.20. Please refer to the *Solution Management Guide for Web Application Server 6.20* for further information on CCMS Monitoring.

To enable CCMS monitoring, see Appendix – *Setting up Monitoring for Web Application Server 6.20 based components*.

Recommendations for monitoring are:

- Operating system monitors
- Database performance and growth
- File system performance and growth
- Performance and availability

3.1.1.2 User Management Engine 3.0 and Content Integrator 2.0

The User Management Engine (UME) and the Content Integrator 2.0 are running on a SAP J2EE Server 6.20. See section 3.3 *Appendix* on how to set up J2EE server monitoring for CCMS.

You can also use the J2EE monitoring template for J2EE monitoring.

In addition, the UME 3.0 and CI 2.0 have a GRMG (Generic Request and Message Generator) Heartbeat function. For setting up GRMG monitoring in CCMS, see the Appendix - *Setting up GRMG Availability Monitoring*.

You can also set up log file monitoring using the `sapccmsr` agent as described in SAP Note 535199 for the log files described in the next section.

3.1.1.3 Exchange Infrastructure 2.0

The Exchange Infrastructure 2.0 is a Web Application Server 6.20 based component. Please refer to the *Solution Management Guide for Web Application Server 6.20* for further information on CCMS Monitoring.

To enable CCMS monitoring, see Chapter 3.3 *Appendix – Setting up Monitoring for Web Application Server 6.20 based components*.

The XI 2.0 monitor template can be integrated into CCMS monitoring for the MDM solution landscape.

3.1.1.4 Enterprise Portal 5.0/6.0

The enterprise portal monitoring is accessed through the Administrator role in the Enterprise Portal. This allows administrators to view the content of loggers and to configure logging in the portal as well as to send data to CCMS.

3.1.1.5 Solution Manager 3.1

The Solution Manager 3.1 is based on Web Application Server 6.20. Please refer to the *Solution Management Guide for Web Application Server 6.20* for further information on CCMS Monitoring.

To enable CCMS monitoring, see Chapter 3.3 *Appendix – Setting up Monitoring for Web Application Server 6.20 based components*

3.1.1.6 Internet Transaction Server 6.20

See the Appendix on how to set up the CCMS monitoring for the Internet Transaction Server (ITS) 6.20 using the default ITS templates. You can also use the administrator instance for monitoring and administrating the ITS.

3.1.2 Scenario alert monitoring

In addition to required monitoring of each component some additional monitoring objects are designed to monitor cross component communication and other scenario specific critical situations.

3.1.2.1 Master Data Management 2.00

The processes of master data management are monitored with a very powerful monitoring framework. If you are logged on to the Master Data Server, use transaction code PC_D_MONI.

This monitoring framework allows you to monitor the various systems involved in the MDM scenario and enables you to keep track of the processed messages in the various integration servers.

Please refer to the documentation on *MDM 2.00 Process monitoring* under help.sap.com → *SAP NetWeaver* → *SAP Master Data Management (SAP MDM)* → *Master Data Exchange (Distribution)* → *Distribution Process Monitoring*.

3.2 Monitoring Details, Trace and Log Files

3.2.1 Master Data Server 2.0



For Master Data Server 2.0, please refer to help.sap.com → *SAP NetWeaver* → *SAP Master Data Management (SAP MDM)*.

3.2.2 User Management Engine 3.0

Detailed information can be found in the *Component Installation Guide – User Management Engine 3.0*.

In the following table, <J2EE Dir> stands for
/usr/sap/<SAPSID>/<instance_name>/j2ee/cluster/server.

<UM> stands for the UM installation directory.

Content	File	Path
Extended logging information Configuration file: <J2EE>/cluster/server /services/log/work /saplogging.config	default.trc system.log application.log	<J2EE dir>/log
Trace information Trace level set in <UM>/properties /mysap.properties, should be set to 4 in normal productive mode, up to 9 for troubleshooting Check content for: Java exceptions Error Warning	mysap.trace	<UM>/logs
Log information	mysap.log	<UM>/logs

The User Management Engine also supports the GRMG Heartbeat function.

You can check UME 3.0 using the following URLs:

Component	Source	Remarks
URL Check	http://<host>:<Port> /logon/PingUM	<ul style="list-style-type: none"> Returns an XML file containing the actual status of the User Management Can be integrated into CCMS or a third party monitoring tool
URL Check	http://<host>:<port> /logon/TestUM	<ul style="list-style-type: none"> Can be used to test login, to verify UM version, and so on Can be integrated into a third party monitoring tool

3.2.3 Content Integrator 2.0

Detailed information can be found in the *Component Installation Guide – Content Integrator 2.0*.

In the following table, <J2EE Dir> stands for
 /usr/sap/<SAPSID>/<instance_name>/j2ee/cluster/server.

<CI> stands for the directory
 usr/sap/<SAPSID>/<instance_name>global/config/ContentIntegrator.

Content	File	Path
Extended logging information Configuration file: <J2EE>/cluster/server /services/log/work /saplogging.config	default.trc system.log application.log	<J2EE dir>/log
Trace information Trace level set in <sapmarkets>/properties/mys ap.properties, or in <CI>/logging.properties depending on the distribution of UM and CI to different hosts should be set to 4 in normal productive mode, up to 9 for troubleshooting. Check content for <ul style="list-style-type: none"> • Java exceptions • Error • Warning 	ContentIntegrator.trace	<CI>/logs

The Content Integrator also supports the GRMG Heartbeat function. You can check CI 2.0 using the following URLs:

Component	Source	Remarks
URL Check	http://<host>:<j2ee-port>/ci/servlet/Heartbeat	<ul style="list-style-type: none"> • Returns an XML file containing the actual status of the Content Integrator. • Can be integrated into CCMS or a third party monitoring tool.

3.2.4 SAP J2EE Server 6.20

You can find a detailed description on monitoring the J2EE Server 6.20 in the standard Web Application Server 6.20 Guides (including the J2EE Engine). We have included the most important trace and log files in this guide:

In the following table, <J2EE Dir> stands for
 /usr/sap/<SAPSID>/<instance_name>/j2ee/cluster

Content	File	Path
Archived content of SAP J2EE	<YYYY>_<MM>_<DD>_at_<HH>	<J2EE

Engine console log	_ <mm>_<ss>_output.log< td=""> <td>dir>/server/console_logs or <J2EE dir>/dispatcher/console_logs</td> </mm>_<ss>_output.log<>	dir>/server/console_logs or <J2EE dir>/dispatcher/console_logs
Archived content of SAP J2EE Engine error log	<YYYY>_<MM>_<DD>_at_<HH>_<MM>_<SS>_error.log	<J2EE dir>/server/console_logs or <J2EE dir>/dispatcher/console_logs
Logging information from each J2EE Engine Service Trace levels can be set through the J2EE Engine's Admin UI	default.trc system.log application.log	<J2EE dir>/server/managers/log or <J2EE dir>/dispatcher/managers/log

3.2.5 Exchange Infrastructure

You will find detailed monitoring information in the standard logs and traces (see [3.2.4](#)) because the Exchange Infrastructure uses the J2EE server. Parts of the Solution Management Guide for XI 2.0 have been included in this guide.

3.2.5.1 System Landscape Directory

A System Landscape Directory memory log viewer is available under **<Integration Builder host>:<port>/sld**.

Choose *System Landscape Directory* → *Administration* → *Server: Server Log* to access the log viewer.

A file system log is also available on the System Landscape Directory host. It contains the log entries since the most recent restart of the SAP J2EE Engine. The log files can be safely deleted at any time.

In the following table, <J2EE dir> stands for

/usr/sap/<SAPSID>/<instance_name>/j2ee/cluster/server

on the System Landscape Directory host.

Content	File	Path
Corresponds to the content of the memory log	lcr_all.log	<J2EE dir>/managers/
Messages regarding starting/stopping the System Landscape Directory, including automatic start	lcrstart.log	<J2EE dir>/managers/

Trace level INFO is recommended for productive use. You set the trace level in the System Landscape Directory log viewer under **<Integration Builder host>:<port>/sld**.

Choose *System Landscape Directory* → *Administration* → *Server: Server Log* to access the log viewer.

3.2.5.2 Integration Builder

In the following table, <J2EE dir> stands for

/usr/sap/<SAPSID>/<instance_name>/j2ee/cluster/server

on the Integration Builder host.

Content	File	Path
Exceptions and errors that occurred when running the SAP J2EE Engine	error.log	<J2EE dir>/managers
Data about loading and starting of the managers and services of the SAP J2EE Engine	output.log	<J2EE dir>/managers

Trace level INFO is recommended for productive use. For more detailed information, refer to the *SAP J2EE 6.20 Engine Administration Manual* under *Configuration Tasks, Using the Log System and Monitoring*.

The following log files are written in addition to the log files mentioned above. They are usually not of major diagnostic importance and can safely be deleted at any time.

Content	File	Path
Information about Integration Builder components started using WebStart	jnlp.log	<J2EE dir>
Application-internal exceptions raised	Autolog.log	<J2EE dir>

3.2.5.3 Integration Engine

The Integration Engine does not usually persist message data in the file system. For diagnostic purposes, you may want to also write message trace information to a file. This can be configured in the Integration Server by choosing *Exchange Infrastructure: Administration* → *Integration Engine - Administration* → *Error Analysis Settings* from your SAP Easy Access user menu. The following files may be written:

Content	File	Path
Detailed information for each message <msgid> sent using the Integration Engine	TRC_<msgid>.txt	As defined in the SAP Web AS 6.20 profile parameter DIR_GLOBAL (see transaction AL11), typically

		/usr/sap/<SAPSID>/SYS/global
Versions of message <msgid> sent using the Integration Engine, with pipeline ID <pid> and logged message version <msgvs>	MSG_<msgid>_<pid>_<msgvs>.txt	As defined in the SAP Web AS 6.20 profile parameter DIR_GLOBAL (see transaction AL11), typically /usr/sap/<SAPSID>/SYS/global

Depending on the specific settings and size of documents sent using the Integration Engine, the number of files and the space occupied in the file system may become very large. Therefore, you should monitor the growth and remove trace information that is no longer required.

Trace level 1 is recommended for productive use. You can set the trace level on the Integration Server by choosing *Exchange Infrastructure: Administration* → *Integration Engine - Administration* → *Pipeline Settings* from your SAP Easy Access user menu.

3.2.5.4 Adapter Engine

The Adapter Engine includes the File, JMS, JDBC, and SOAP adapters as well as the Java part of the RFC adapter.

In the following table, <Java dir> stands for the directory where the Adapter Engine is installed.



Multiple Adapter Engines can be installed in an XI landscape.

Content	File	Path
Technical logging information for all installed adapters, except for the RFC adapter	adapter_1.log adapter_2.log adapter_3.log adapter_4.log adapter_5.log	<Java dir>/tech_adapter/LOGFILES
Technical logging information for the RFC adapter	Adapter_rfc.log	<Java dir>/tech_adapter/LOGFILES

The log can be viewed with the Adapter Engine that runs on the Integration Server under:

<Integration Builder host>:<port>/rep/start/index.jsp

Under *SAP Adapter on the Integration Server*, choose *Adapter Engine (RFC Adapter)*. Then, choose *Traces* from the main menu.

If the Adapter Engine is installed and running on another host, the log can be accessed by choosing *Traces* from the main menu under the following Internet address:

<Adapter Engine host>:<port>

Trace level *INFO* is recommended for productive use. You set the trace level under the following Internet address:

<Adapter Engine host>:<port>

Select the adapter in question under *Available Adapters* and then choose *Configure*.

The default logging settings produce a set of five trace files, each two MB in size. These files are used in rotation for logging, effectively limiting the file system space used for log files to 10 MB. The file names above represent the default logging settings.

The trace files can be viewed in the Adapter Engine under the same Internet address by choosing *Traces - Available Trace Files* from the main menu.

3.2.5.5 Market Set Adapter

In the following table, <J2EE dir> stands for

`/usr/sap/<SAPSID>/<instance_name>/j2ee/cluster/server`

on the Integration Server host.

Content	File	Path
Technical trace information	tracefile.txt	<J2EE dir>/services/servlet_jsp/work/jspTemp/MessagingSystem/root/admin/

The default trace level is *NONE*. Refer to the *SAP J2EE 6.20 Engine Administration Manual* under *Configuration Tasks, Using the Log System and Monitoring* for details.

3.2.6 Enterprise Portal

The log and file viewer component can be called by:

`<server>/irj/servlet/prt/portal/prtroot/com.sap.portal.runtime.admin.logviewer.default.`

3.2.7 Solution Manager 3.1

For SAP Solution Manager 3.1, please refer to help.sap.com → *SAP Netweaver* → *SAP Solution Manager*. You can also refer to the documentation under service.sap.com/rkt-solman → *SAP Solution Manager 3.1*.

3.2.8 Internet Transaction Server

The ITS 6.20 can also be monitored using a browser by connecting to the ITS administration instance.

Use the following URL:

`<its-host>:<port>/scripts/wgate/admin/`

In the following table, <ITS dir> is the ITS installation directory.

Content	File	Path
Statistical information on ITS	Access.log	<ITS dir>/<virtual

service usage		<i>instance>/logs</i>
Diagnostic information passed to a client	Diagnostic.log	<i><ITS dir>/<virtual instance>/logs</i>
Information on ITS and system performance	Performance.log	<i><ITS dir>/<virtual instance>/logs</i>
Information on the current Agate load	Loadstat.log	<i><ITS dir>/<virtual instance>/logs</i>

3.3 Appendix

In this Appendix, you can find some detailed information related to this chapter.

3.3.1 Setting up Monitoring for Web Application Server 6.20 based components

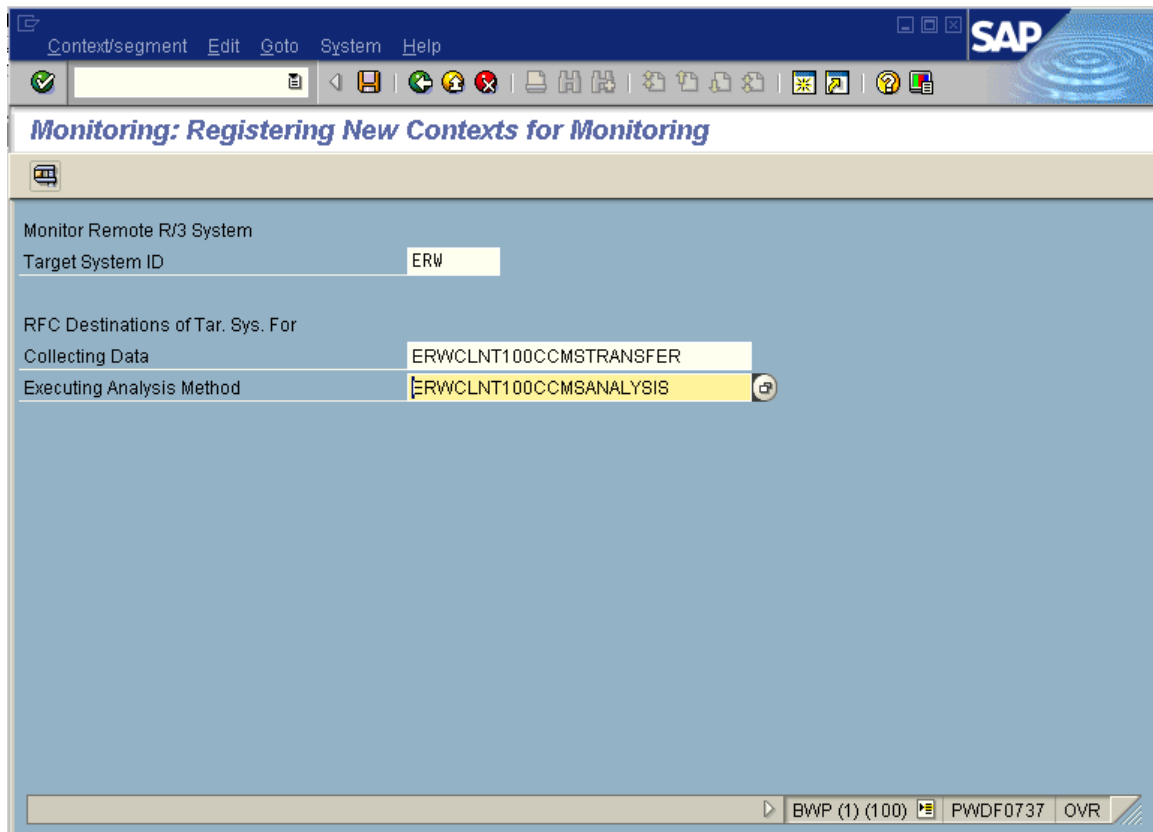
3.3.1.1 Setting up RFC Connections

Use SAP transaction SM59 to create two RFC connections from the central monitoring system to each remote SAP system:

- One for data transfer
 - Name of RFC destination: for example, <SID>CLNT<client>CCMSTRANSFER); <SID> is the SID of the remote SAP system, and <client> is the productive client of the remote SAP system.
 - Connection type: 3
 - Description: For example, data transfer from <SID> for CCMS
 - Target host: Host that runs remote SAP system
 - System number: Number of remote SAP system
 - Gateway host: Host of central monitoring
 - Gateway service: Service of central monitoring system
 - User name: CSMREG
 - Password: As set when creating the user
- One for remote analysis
 - Name of RFC destination: For example, <SID>CLNT<client>CCMSANALYSIS

All other settings are made according to RFC connection for data transfer, but without user entry; mark *current user*.

For each remote system, create a new monitoring segment in the central monitoring system using RZ21 → *Technical infrastructure* → *Create remote monitoring entry*.



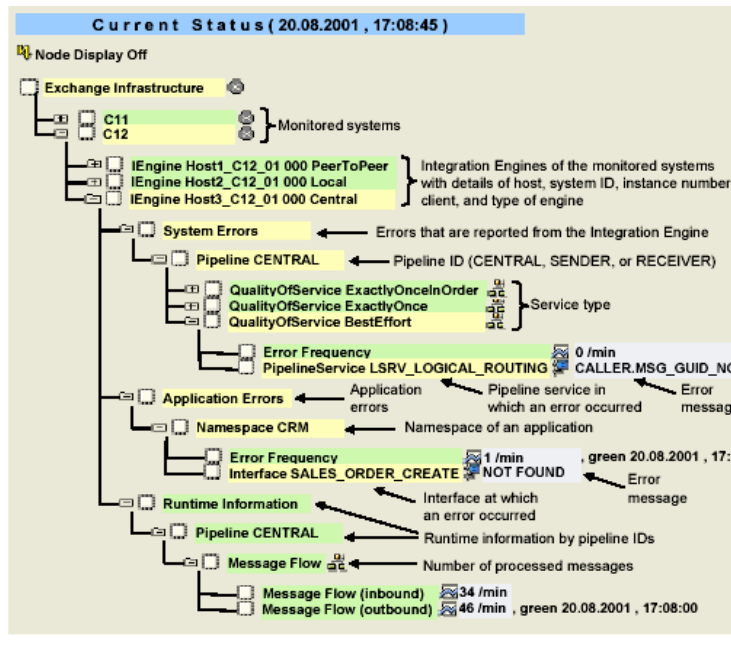
Now you are able to adapt monitors in SAP transaction RZ20 to include monitoring data from the remote SAP system.

3.3.1.2 Install Agents

This is described in 3.3.2.1.1 for the J2EE server.

3.3.1.3 Include MTE_CLASS to your monitors

This is described in 3.3.3.2 for ITS. You must include other MTE_CLASSES; for example, include the XI monitor template for monitoring the XI:



3.3.2 Setting up Monitoring for SAP J2EE Server

3.3.2.1 Preparation steps

You need at least InQMy 4.3.x. or the SAP J2EE Engine 6.20. Monitoring is also possible with InQMy 4.2.x, but the setup procedure is partially different. Only the monitoring starting with 4.3.x is supported for SAP Remote Services (EarlyWatch Alert, Going Live Checks, ...).

3.3.2.1.1 Install the sapccmsr agent

The `sapccmsr` agent is part of the SAP CCMS monitoring infrastructure. The `sapccmsr` agent must run on every host that runs a monitor server of the SAP J2EE Engine. The `sapccmsr` agent is also required if the monitor server runs on the same host as the SAP system which you are reporting to.



Please refer to SAP Note 371023 for instructions on where to obtain the agent and how to install it. Additional information is also available in the document *CCMS Agents: Features, Installation, and Usage*. You can obtain the document on the SAP Service Marketplace under service.sap.com/systemmanagement → *System Monitoring and Alert Management* → *Technical Information*.



We also recommend installing the `saposcol` agent on every host that runs elements of the SAP J2EE Engine. Installation of the `saposcol` agent is also described in SAP Note 371023.

3.3.2.1.2 Install saposcol

Install `saposcol` as described in SAP Note 19227. After successful installation, `saposcol` is able to report data of the operating system. Data is written to shared memory and read out by the agent. The agent provides this data to the CCMS of the monitoring SAP R/3 system.

3.3.2.2 Setup procedure

Monitoring of the SAP J2EE Engine is based on a monitor server that collects monitoring data from services and managers of the SAP J2EE Engine. The monitor server sends the monitoring data to different destinations: Visual Administrator, CCMS, or text files. The monitor server can run in a separate Java virtual machine or in the same VM as a server/single node.

3.3.2.2.1 Install the jmon native code CCMS library

The monitor server requires the native code library `jmon.dll` (or `libjmon.so` for Unix platforms), which must be downloaded from SAP.

Generic information on the Java Monitoring API for CCMS including installation instructions is provided in the document *Java Monitoring API: Properties and Installation*. You can obtain the document on the *SAP Service Marketplace* under service.sap.com/systemmanagement → *System Monitoring and Alert Management*.

For the SAP J2EE Engine, the installation of the library works as follows (the installation directory of the SAP J2EE Engine, for example, `C:\SAP_J2EEEngine6.10` or `C:\In-Q-MyAppServer4.3.5` is abbreviated by `<INSDIR>`):

- Download the native code library from service.sap.com/patches. Go to *SAP Web Application Server* → *SAP Web Application Server 6.20* → *Binary Patches* → *SAP KERNAL 6.20 64-BIT* → *<operating System>* → *Database independent*.
- Extract the `.sar` file with `sapcar` (see SAP Note 212876 for information on `sapcar`).
- [Windows:]
 - Copy the native code library into the Windows system directory `<windir>\system32`.
- [Unix:]
 - Copy the native code library into the directory `<INSDIR>/tools/lib`.
 - Edit the startup script for the monitor server `<INSDIR>/tools/monitor` and add the option `-Djava.library.path=./lib` to the command line of the Java command. This adds the subdirectory `lib` to the search path for native code libraries of the Java virtual machine. Configure and start the monitor server.

The monitor server can be run in two different modes:

1. In a separate Java VM (as separate operating system process)
2. In the same Java VM as a server node (or standalone node) of the J2EE Engine.

Mode 1 is recommended for testing the monitoring configuration as this mode provides a console.

Mode 2 is recommended for productive use as it provides automatic startup.

For configuring and testing the monitor server, create a text file `properties` in the directory `<INSDIR>/tools`.



The file must not have any suffixes like `.txt`.

The syntax of the configuration file is described in detail in the administration manual for the SAP J2EE Engine. If the file `properties` is not found, the monitor server asks for information to connect to the SAP J2EE Engine (dispatcher host, administrator account, and password). This data can be stored in the configuration file. In the following example, replace `<admin-account>` with

an Administrator account to connect to the cluster, `<admin-password>` with the password for the account, and `<monitor-context>` with a unique identifier such as `J2EE_myhost`:

```
java.naming.security.principal=<admin-account>
java.naming.security.credentials=<admin-password>
monitor.system.CCMS.mode=on
monitor.system.CCMS.root=<monitor-context>
monitor.system.CCMS.sessions.toplist.size=1
monitor.system.CCMS.threads.toplist.size=1
shell.autoexec.0=connect
shell.autoexec.1=include *
shell.autoexec.2=report
```

The configuration entry `monitor.system.CCMS.root` is extremely important if you want to connect more than one installations of the SAP J2EE Engine to the same CCMS. This statement defines the name of the monitor context, that is, the top level (root) node of the monitor tree for a SAP J2EE Engine installation. It must be unique system-wide. Therefore, change the default value (SAP J2EE Engine) to a unique identifier that includes, for example, the host name.



The entries `monitor.system.CCMS.sessions.toplist.size` and `monitor.system.CCMS.threads.toplist.size` are important for reducing the memory consumption in the `sapccmsr` agent.

If you run multiple installations of the SAP J2EE Engine on the same machine, you must set up a monitor server for each installation. To avoid conflicts, add the following two lines **to the beginning** of the configuration file `properties`. Replace `<p4port>` with the port you use to connect using the administrator (by default 3011, set by property `port` of the p4 service) and replace `<vaport>` with some free port):

```
java.naming.provider.url=localhost:<p4port>
monitor.system.va.port=<vaport>
```

Once you have created the proper configuration file and your cluster is running, start the monitor server with the shell script `<INSDIR>/tools/monitor.bat`. The console window will display error messages for any problems that occur. More detailed error messages may be contained in file `<INSDIR>/tools/dev_jmon`. If your setup Web Application Server is correct, the console of the monitor server will look similar to this screen:

```
C:\WINNT\System32\cmd.exe
Not connected or disconnected?

Monitor Server 4.3 started.

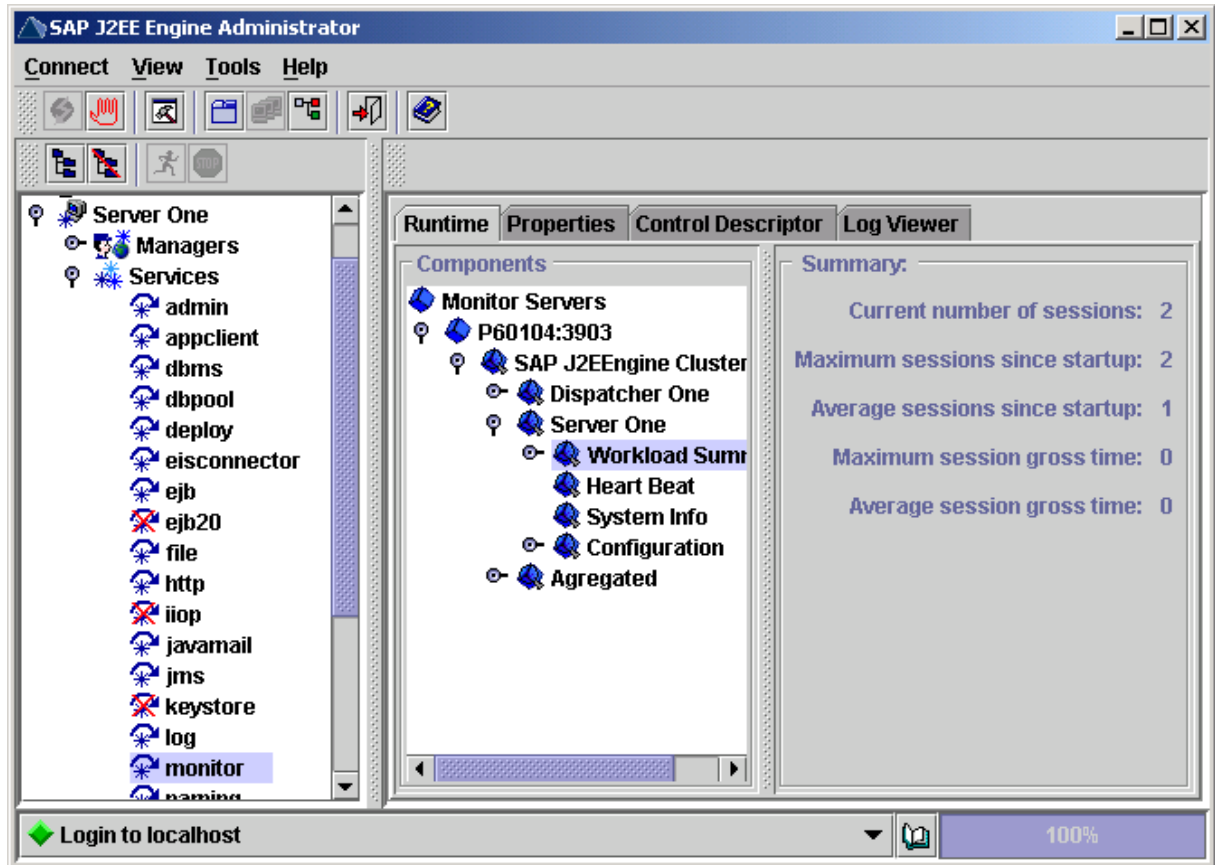
> [connect]
debug level is 0
Switch on monitor.system.UA.mode successful.
Switch on monitor.system.CCMS.mode successful.
> [include, *]
> [report]
>
```

3.3.2.2 Check the monitor data in the visual administrator

Once the monitor server and the SAP J2EE Engine are running, you should be able to see the monitor data in the administrator.

Launch the administrator and connect to your cluster/single installation. In the tree on the left-hand side, select the monitor service of a server node. The *Runtime* tab on the right-hand side shows all

monitor servers after double-clicking on *Monitor Servers*. Browse the tree to inspect the monitoring data.



3.3.2.2.3 Set up the monitor server for productive use

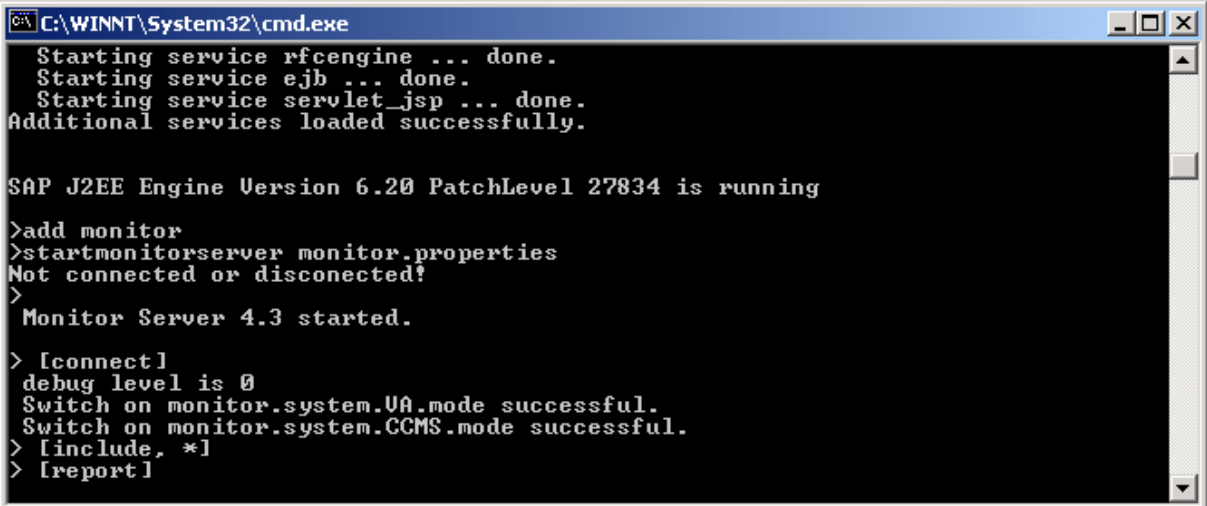
If you have found a satisfactory and validated configuration for the monitor, set up the monitor server to launch automatically in the server/single node, that is, run it in the above mentioned mode 2. Copy the configuration file to a server or single node:

```
copy <INSDIR>\tools\properties to <INSDIR>\alone\monitor.properties
or
copy <INSDIR>\tools\properties to
<INSDIR>\server\monitor.properties
```

Open a command line console of the server/single node that you decide to host the monitor server on. You get the console if you start the node interactively (using the start menu or go.bat) or, if it runs as service, by connecting to the node with the command `telnet localhost 2323` (2323 is the default value of property *Port* in the telnet service). Start the monitor server from the command line console with the following two commands:

```
add monitor
startmonitorserver monitor.properties
```

If the monitor server works after these commands, you should see lines similar to this screenshot:



```
C:\WINNT\System32\cmd.exe
Starting service rfcengine ... done.
Starting service ejb ... done.
Starting service servlet_jsp ... done.
Additional services loaded successfully.

SAP J2EE Engine Version 6.20 PatchLevel 27834 is running

>add monitor
>startmonitorserver monitor.properties
Not connected or disconnected!
>
Monitor Server 4.3 started.

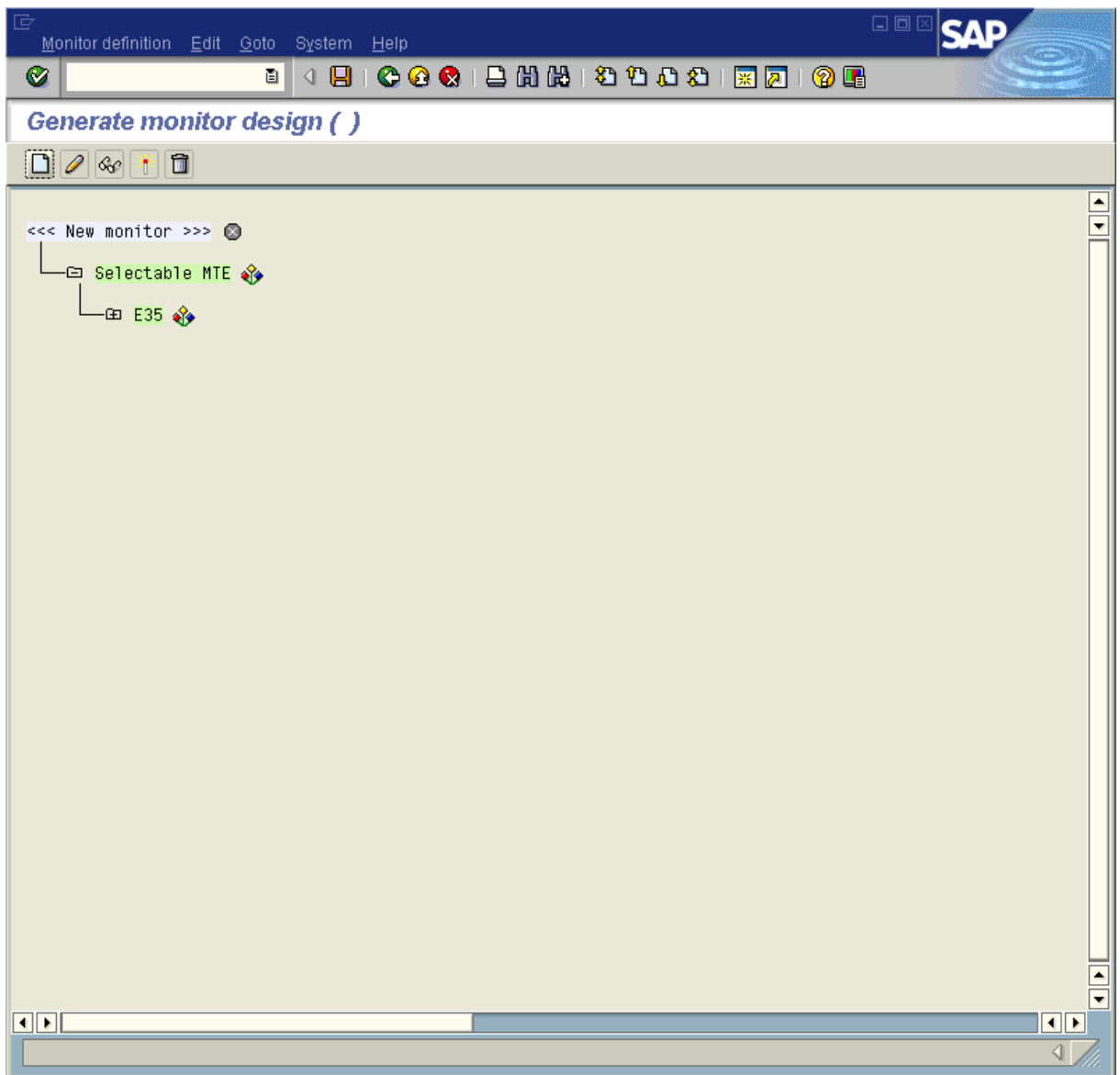
> [connect]
debug level is 0
Switch on monitor.system.UA.mode successful.
Switch on monitor.system.CCMS.mode successful.
> [include, *]
> [report]
```

Record the two commands to execute automatically on startup of the node. This is achieved by adding the two commands (**add monitor** and **startmonitorserver monitor.properties**) to the file `<alone or server>\services\shell\work\autorun.scr`. Restart your J2EE Engine and check if the monitor server launches automatically.

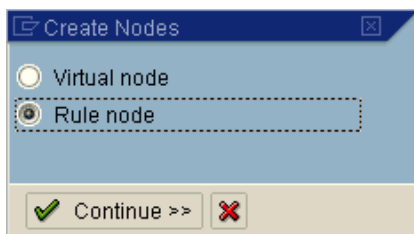
3.3.2.2.4 Define Monitor in RZ20

At this point, your monitoring is fully functional. The monitoring tree can be displayed in the SAP J2EE Engine Administrator (in the monitor service) or in transaction RZ20 of your SAP system. A monitor is included in all systems above Release 6.20; see *SAP CCMS Monitor Templates → J2EE Engine*. If the release of your monitoring system is lower than 6.20, or if you want Remote Services to check your SAP J2EE Engine, then proceed with the following steps to define a new monitor in RZ20:

1. Start transaction RZ20.
2. Activate the maintenance function by choosing the menu *Extras* and activate maintenance function.
3. Set the cursor on the monitor set MDM 2.00 and click *Create*.
4. Now create a new monitor in the new monitor set. Highlight the newly created monitor set and in menu *Monitor (set)* choose *Create*. Now create a new node by highlighting the `<<< New monitor >>>` entry and selecting *Edit, Create nodes*.



5. For Release 6.20 of the SAP J2EE Engine, create a new monitor by first choosing *Rule node* in the popup.



6. In the next popup, select the rule *CCMS_GET_MTE_BY_CLASS*.

You are now prompted to enter a value for the parameter *R3System*. Select the R/3 system and then enter the MTE class *SAP J2EE Engine* (for Release 6.20).

7. Save your changes and enter *EWA SAP J2EE Engine* as a name for the new monitor.



The monitor must have exactly this name for SAP Remote Services.

For Release 6.10 and 4.3.x of the SAP J2EE Engine, you create a new monitor as follows: From the tree *Selectable MTE*, select the top level node corresponding to the InQMy installation. The default label of the node is *In-Q-My Application Server*. Activate the check box in front of this node.

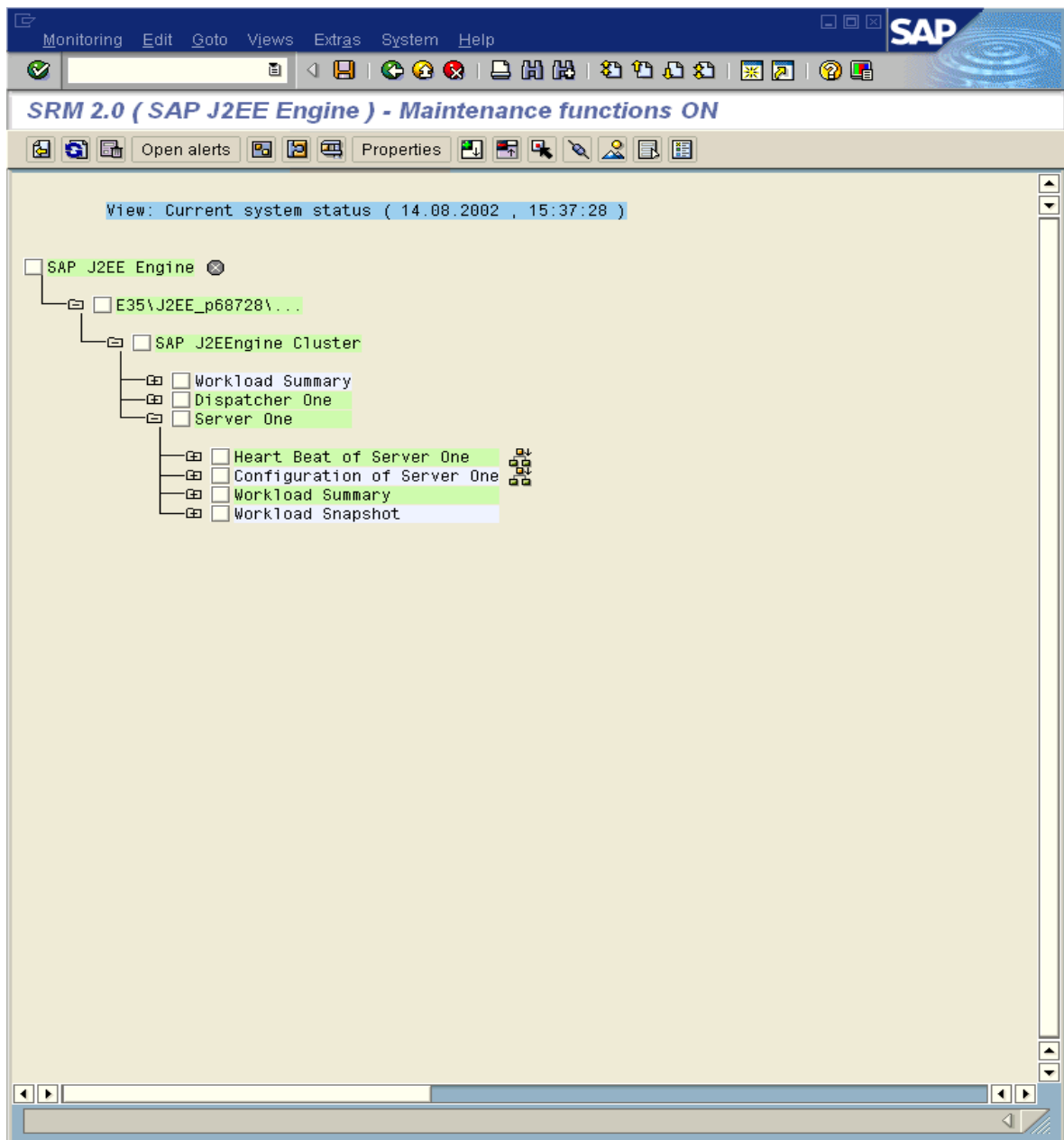
8. Save your changes and enter *EWA SAP J2EE Engine* as a name for the new monitor.



The name of the monitor is required.

9. If you did not define a monitor for the SAP J2EE Engine in the previous step: In transaction RZ20, choose *SAP CCMS Technical Expert Monitors* and *System / All Monitoring Segments / All Monitoring Contexts* to find your monitoring data.

If you double-click on the newly defined monitor, the monitor trees for all your installations of the SAP J2EE Engine that report to CCMS will appear, as shown below:



3.3.3 Setting up Monitoring for ITS 6.20

3.3.3.1 Installing the CCMS Agent (sapccmsr)

Create the directory `\\host\saploc\prfclog\sapccmsr`, if it does not exist.



`saploc` must be shared.

If you want to run an automatic installation, create a configuration file called `csconf`. This file is required for a dialog-free installation. Save the file in the working directory of the CCMS agent that you just created. Using a configuration file allows the installation to run unsupervised. The file is always the same when installing the CCMS agent on several servers. The content of the `csconf` should look as shown below. Make sure all parameters are set to match your configuration and system information. (For a detailed explanation, refer to the *CCMS Agent: Features, Installation, and Usage* document listed in the appendix. See also service.sap.com/monitoring).



Content of the `csconf` file

```
CEN_CONFIG
  CEN_SYSID=<SID of monitoring R/3 system>
CEN_ADMIN_USER
  CEN_ADMIN_CLIENT=<client>
  CEN_ADMIN_USERID=<valid R/3-user>
  CEN_ADMIN_LANG=<language>
  CEN_ADMIN_LOADBALANCING=n
  CEN_ADMIN_ASHOST=<hostname of application server>
  CEN_ADMIN_SYSNR=<instance no. of monitoring R/3 system>
  CEN_ADMIN_TRACE=0
  CEN_ADMIN_MSHOST=<hostname of message server>
  CEN_ADMIN_PASSWORD=<Password of the user>
CEN_GATEWAY
  CEN_GATEWAY_HOST=<hostname of gateway server>
  CEN_GATEWAY_SYSNR=<instance no. of the gateway of the monitoring R/3 system>
  CEN_GATEWAY_TRACE=0
CEN_CSMREG_USER
  CEN_CSMREG_CLIENT=<client>
  CEN_CSMREG_USERID=<valid user>
  CEN_CSMREG_LANG=<language>
  CEN_CSMREG_LOADBALANCING=n
  CEN_CSMREG_ASHOST=<hostname of application server>
  CEN_CSMREG_SYSNR=<instance no. of monitoring R/3 system>
  CEN_CSMREG_TRACE=0
  CEN_CSMREG_MSHOST=<hostname of message server>
  CEN_CSMREG_PASSWORD=<Password of the user>
```

Both ADMIN_USERID and CSMREG_USERID must be valid R/3 users in the Central Monitoring System with RFC privileges.

It is possible to install the agent without using a configuration file. All the information will be prompted for and should be answered interactively. This works similar as with the installation of the ccmsping service. After the installation is complete, a configuration file will be created in the agent's working directory according to the structure shown above.

1. Install / register the agent using the following command. During registration, the agent automatically creates an RFC connection to the central monitoring system.

```
cd <install drive>:\usr\sap<SID>\SYS\exe\run
```

```
sapccmsr -R -f <file name> to register
```

```
sapccmsr -U to unregister
```

<file name> is the name of the configuration file for the dialog-free installation. The default file name is *csmconf*.

Registration of the agent creates a log file (*sapccmsr<pid>.log*) in the working directory. Check the file for any errors and warnings. On Windows 2000, the agent will be configured as a service that will start automatically under the Local System Account. The service is called *SAPCCMSR.99*.

2. Adapt the sapccmsr.ini file in the CCMS agent directory by adding the line:

```
PlugIn <ITS program directory>\ITSMON.dll
```



The string has to be entered in the DOS format, for example, *PlugIn D:\PROGRA~1\SAP\ITS\2.0\programs\itsmon.dll*.

3. Save the file.
4. Add the path to the program directory of the ITS to the path environment variable by selecting: *Start → Settings → Control Panel → System*. Then switch to the *Advanced* tab and choose *Environment*. Now search the system variable *Path*. Add the path to the program directory. The program directory is usually located under <drive>:\Program Files\SAP\ITS\2.0\programs (so you add *D:\PROGRA~1\SAP\ITS\2.0\programs*).



The path has to be entered in the DOS format. You have to restart the server in order to activate the changes. Further information is found in SAP Note 418285.

Please refer also to SAP Note 418285 in order to set up the monitor in the CCMS environment (creation of MTE nodes).

3.3.3.2 Add the MTE_Classes to your monitor

1. Call transaction RZ20.
2. In menu *Extras*, choose *Activate maintenance function*.
3. In menu *Monitor (set)*, choose *Create*. Select *New monitor set* in the popup window and confirm. In the next popup windows, enter a name for the new monitor set, for example, *MDM 2.00 – ITS Monitor*.



Do not choose a name beginning with the letters *SAP*, as the CCMS would treat this as a pre-defined monitor provided by SAP. You will not be able to make any changes to or delete such a monitor set.

4. Set the modifiability to *Only for administrators and me*, select *Public* (visible for all users) and confirm. A new monitor set should appear within the tree *My favorites*.
5. If you need to create the ITS monitor nodes from scratch, select your created monitor set and choose *Create* from menu *Monitor (set)*.
6. Highlight the entry <<< *New monitor* >>> and then select *Create nodes* from menu *Edit*.
7. In the following popup window, select *Rule node* and press *Continue*. Choose *CCMS_GET_MTE_BY_CLASS* and press *Continue*.
8. In the upcoming popup windows, enter **CURRENT** as *R3System*.
9. In the field *MTEClass*, enter the value *ITSRootContext*.
10. In the section *Display options for MTE nodes from a rule*, activate the checkboxes *Display following parts of the MTE name* and *Context*. Choose *Continue*.

Edit Rule Nodes

Rule: CCMS_GET_MTE_BY_CLASS

Description: Determine MTE for a Specific MTE Class

Parameter values

R3System	<CURRENT>
MTEClass	ITSRootContext

Display options for virtual nodes from a rule

Display virtual summary nodes in the monitor

Display options for MTE nodes from a rule

Display long MTE name

Display following parts of MTE name:

System Context Object Short name

Continue >> << Back

Repeat the steps above; however, enter the value `ITSself` in field `MTEClass`. After activating the checkboxes as described above and choosing *Continue*, save the monitor. You will be prompted for a name – enter `EWA ITS`. According to SAP Note 418285, this name is required.

The new monitor should appear in your created monitor set. You have now included the ITS monitoring.

3.3.4 Setting up GRMG Availability Monitoring

3.3.4.1 Preparation

Here is what you will need to do to set up and start GRMG availability monitoring in your installation. You must have completed the installation of the SAP components in your landscape. In addition, all SAP components in your landscape should be up-to-date in Support Packages.

1. You must select an SAP System (an ABAP system) that you will use to monitor the availability and performance of the SAP components in your installation. This system may be the system at which the SAP Solution Manager is running or it can be a separate SAP System. If possible, you should dedicate a SAP System to monitoring and system management; in any case, avoid using one of your production SAP Systems for this task. Setting up a separate system has the advantage of allowing you to keep the SAP Basis Release and Support Package level at the system up-to-date, so that you can make use of the newest monitoring and management technologies. The monitoring and administration system does not require elaborate or expensive hardware to function correctly.
2. You must obtain the XML-format Customizing files for the GRMG monitoring scenarios of your applications. A GRMG Customizing file tells the monitoring system that you selected in step 1 to run a particular GRMG availability monitoring scenario to monitor the availability and condition of a particular component. The GRMG Customizing file(s) needed by an application are part of the application deliverables that you have installed. Check the application documentation for the location of the file(s). If you cannot find the GRMG Customizing file(s) in the application deliverables, then you can download the file(s) and accompanying documentation from the SAP Service Marketplace (service.sap.com/monitoring → *download area* → *GRMG Customizing files*). You will find the customizing files in *GRMG Customizing Files* under *Media Library*.
3. You will need to adjust the Customizing files. To do this, you will need to edit each .xml file using an XML editor or any normal text editor such as Windows WordPad, Linux KDE Kwrite, or any similar editor. You will find what you need to change in the application installation or operation documentation, *README*, or in a SAP Note. Typically, you will need to change the URL specified in each Customizing file to use the correct host name and port for your installation. You may also be asked to copy a Customizing template for each of the instances of a monitored component that you have installed.
4. You must upload each Customizing file into the monitoring system that you chose in step 1 as follows:
 - a. Log on to the monitoring system as a user with administrator authorizations. Make sure that you log on to the central application server. This is the server that offers the *Enqueue* service. You can determine which server is your central server with transaction SM51 or with transaction RZ03.
 - b. Start transaction GRMG by entering `grmg` in the *OK* field in the SAPGUI toolbar.
 - c. For each Customizing file that you wish to install, click on the button *Upload GRMG Customizing*. In the file selection dialog, navigate to the directory in which the Customizing file is located and select the file. When you select *Open* in the dialog window, the file will be uploaded. In the first production release of this transaction,

no confirmation message is issued; how to verify the correct Customizing and functioning of GRMG is described later.

5. After you have uploaded all of the Customizing files, start the availability monitoring. Please be sure that you are logged in on the central application server of the monitoring system before you carry out this step. The central server is the one that offers the *Enqueue* service. You can determine which server this is in transaction SM51 or transaction RZ03. To start the GRMG availability monitoring, click on the *Start all scenarios* button in transaction GRMG. The function displays no confirmation message that the availability monitoring has started; how to verify the successful start of monitoring is described later. Once you have started GRMG monitoring, the monitoring scenarios that you have installed run automatically. The CCMS monitoring architecture repeats each GRMG availability monitoring scenario automatically every five minutes (by default).

3.3.4.2 Displaying GRMG Monitoring Data

You use the CCMS Alert Monitor, transaction RZ20, to display the availability data and alerts for components monitored with GRMG. GRMG monitoring data is displayed as follows:

1. Log on to the SAP system that you are using for monitoring. You will need administrator authorizations.
2. Start transaction RZ20.
3. Look for and open the monitor collection for the application for which you wish to see GRMG data. If you cannot find the right monitor, there is a monitor collection for each major SAP product and component. The monitor definitions are delivered with upgrades and Support Packages of the SAP Basis component. If you do not find an appropriate monitor collection or monitor, then you should make sure that the monitoring system is up-to-date with respect to SAP Basis Support Packages. You can also define your own monitor collections and monitors; please see the CCMS documentation in RZ20 under *Help* → *Application help*. Finally, you can also download the newest versions of monitor definitions from the SAP Service Marketplace (service.sap.com/monitoring). You will find monitor definition transports in *GRMG Customizing Files* under *Media Library*. You can also use the global RZ20 monitor to find GRMG data, even if you do not find any appropriate application monitors, and you do not need to define a monitor yourself. To start the global monitor, double-click on the *SAP CCMS Technical Experts Monitors* collection to open it and open the *All Monitoring Contexts* monitor.
4. Double-click on the monitor for the component in which you are interested. GRMG data is usually presented in a subtree with the name *Heartbeat*. The monitor will look something like this:
 - The top node in the subtree contains the name of the GRMG scenario, which usually identifies the name of the application checked by the scenario.
 - For each component that is checked by the scenario, there is a separate component subtree. The subtree reveals the host or J2EE server node on which each instance of a component is running.
 - The *Availability* monitoring attribute reports the availability of the component in percent averaged over the last fifteen minutes.

The *Heartbeat* monitoring attribute contains a log of status messages reported by the component. You can display the log by marking the *Heartbeat* node and selecting *Details* from the toolbar.

4 Management of mySAP Technology

SAP provides you an infrastructure, which helps your technical support consultant and system administrators to effectively manage all SAP components and carry out all tasks related to middleware technology.

The aims of managing mySAP Technology are as follows:

- Provide a central interface to manage administrative tasks for middleware
- Improve the process of problem resolution for the entire solution
- Provide standardized administration of user profiles

You can find more information about the underlying technology in the Technical Operations Manual for mySAP Technology in the *SAP Library* under *mySAP Technology Components*.

4.1 Administration Tools of Software Components

Component	Detailed Description	Prerequisites
MDM Server based on Web Application Server	Please refer to Web Application Server Technical Operations Manual	

4.2 Starting and Stopping

4.2.1 Controlled starting and stopping of single components

Start and Stop Sequence and Tools

Software Component	Start Sequence and Tools (Stop sequence in reverse order)		
	Sequence	Tool	Detailed Description
Content Consolidation, Master Data Harmonization, Central Master Data Management			
CI 2.0	1	Start J2EE Engine	Wait until server has started and is connected.
	2	Start CI Proxy server	Steps 2, 3 and 4 can be started simultaneously.
	3	Start CI Job scheduler	
	4	Start RFC adapter	
	General remarks: Start CI 2.0 after the complete infrastructure (EP 5.0, MDM 2.00, UME 3.0, XI 2.0) is up.		
UME 3.0	1	Start J2EE Engine	Wait until server has started and is connected.
EP 5.0	See service.sap.com/ep50howtoguides , then <i>Operate SAP Enterprise Portal → Showcase and Software Logistics</i> .		
MDM 2.00	Standard Web Application Server procedure: see Technical Operations Manual		
XI 2.0	See SAP Exchange Infrastructure 2.0 Solution Management Guide at service.sap.com/instguides/ .		

MDM ID Mapping Framework servlet	Stopping and starting the MDM Web Application is like any other J2EE application. See administration manual of the SAP J2EE Engine: help.sap.com/saphelp_webas620/helpdata/ , and go to <i>Services Administration Reference</i> → <i>Deploy Service</i> → <i>Visual Administrator</i> .		
ITS	1	Start A-Gate Service	
	2	Start IIS Admin Service	
	3	Start World Wide Web Publishing Service	

4.2.2 Unplanned starting and stopping

Within SAP MDM, unplanned starting and stopping has major implications regarding the interaction between UME 3.0, CI 2.0 and MDM 2.00:

Stopped Component	Impact on Availability of Other Components	Restart Procedure
CI 2.0		Standard restart. When MDM 2.00 has stopped and needs to be restarted, CI 2.0 must be restarted as well.
UME 3.0	CI down	First, restart UME. Then, restart CI.
EP 5.0		Standard restart
MDM 2.00		Standard restart. Implies restart of CI 2.0.
XI 2.0		Standard restart
MDM ID Mapping Framework servlet		Standard restart
ITS		Standard restart

For possible implications on data consistency, see section 4.3 *Backup/Restore and Recovery*.

For possible impacts on MDM processes, see section 5.2 *High Availability Matrix for the Individual Components*.

4.3 Backup/Restore and Recovery

4.3.1 General remarks

In contrast to the traditional SAP R/3 system, mySAP solutions use several SAP component systems to implement cross system processes. Data is no longer held centrally in a single SAP R/3 system but is rather distributed between several SAP components.

Backup and Restore (B&R) concepts for mySAP solutions are discussed in detail in the SAP Best Practice document *Backup and Restore for mySAP.com*. A copy of this document can be found in the appendix of this Operations Manual. The latest version can be obtained through the SAP Solution Manager.

Due to the **non-transactional** character of the master data flow **between** the different landscape components involved within one MDM Business Scenario, it is almost impossible to find a common point of consistency across the whole MDM landscape.

The only backup type that can guarantee full *Physical and Logical Consistency* of a MDM landscape would be an offline backup of the whole landscape after all business users had logged off and the complete business workflow has ended.

Tools offering manageability and monitoring of these tasks do not yet exist.

Logical consistency involves the restoration to a consistent state of the **overall MDM landscape** (cross-system data consistency) on single data flow level at the time of the backup, including the successful roll-back of all open business transactions.

Physical consistency does guarantee the restore to a consistent state of **individual MDM components** followed by a successful startup of the restored components and a successful reconnect to other components. This state will provide for a working MDM runtime in which newly created master data objects can be exchanged. It is required to develop a transactional conduct on user level to react on broken workflows and outdated master data objects appearing after the restore.

For a more detailed discussion on logical consistency versus physical consistency, please refer to **section one** of the *SAP Best Practice* document *Backup and Restore for mySAP.com*. The need for a consistent backup of the whole landscape, as well as the question "What is a consistent backup of a system landscape?" are discussed in this document.

In distributed, business critical server landscapes, a well-elaborated B&R concept is needed. Besides backing up *business critical data (held in databases)* in these landscapes the *runtime infrastructure* itself should be backed up. Even if a loss of parts of the infrastructure can be afforded, it might take a long time to reinstall and reconfigure these components.

The downtime can be decreased tremendously when restoring the infrastructure together with the business data. Depending on the frequency of changes to the infrastructure, it should be backed up once after the initial installation and configuration and after each change applied to it (changes to the configuration, software upgrade of individual components, replacement of components).

In deciding which infrastructure components are worth backing up, factors such as the time needed for a full reinstallation plus additional configuration, and how critical the expected downtime of one or more infrastructure components would be with regard to the overall availability of the MDM landscape, need to be taken into account.



SAP generally recommends that you back up the runtime infrastructure of all components of a MDM landscape.

Finally, it is necessary to prove the concept with regular B&R tests. It is worth mentioning that a single test is not sufficient. It might be sufficient to prove the general concept with the initial landscape, but one should keep in mind that the MDM landscape is likely to change over time and that administrators need to be trained to react quickly should a restore be necessary.

In this document, we assume that the readers are familiar with database and server administration and therefore refrain from explaining how to back up a RDBMS or a file system. Please contact your IT staff on these questions and refer to your database and operating system vendors' operations manuals respectively.

Further reading and technical guidelines for B&R of individual SAP products based on SAP Web Application Server (SAP R/3, SAP BW, SAP CRM, and so on) are available in the SAP Online Help, and the books *System Administration Made Easy* ISBN 1-893570-44-4, *SAP Database Administration* ISBN 1592290051.

4.3.2 Backup of individual components in an MDM landscape

4.3.2.1 System components and data that need to be backed-up

The following table lists the technical components of an MDM landscape:

MDM Component	RDBMS involved	Running on J2EE Engine	Potential Loss of Configuration	Potential Loss of Data
SAP Enterprise Portal	No	Yes	Yes	Yes
SAP User Management Engine	Yes	Yes	Yes	Yes
SAP Master Data Engine	Yes	No	Yes	Yes
MDM ID Mapping Framework servlet	No	Yes	Yes	No
SAP Content Integrator	Uses RDBMS of Master Data Engine	Yes	Yes	Yes
SAP Exchange Infrastructure	Yes	Yes	Yes	Yes
ITS	No	No	Yes	No
Client Systems (R/3, SRM, CRM)	Yes	No	Yes	Yes
BW for Analytics	Yes	No	Yes	Yes

The following items should be considered when planning a B&R strategy for application data, software and configuration files:

- Operating system
- RDBMS data files
- RDBMS software
- SAP software and file systems
- Log files (SAP and other)
- Software of other system components (file systems and configuration files)



A component with application data (database, for example) usually also comprises application software and configuration files (runtime infrastructure) that need to be

backed up. A component holding no application data may comprise configuration files and the software that should be backed up.

B&R of Operating System, Software, and Configuration Data

Apart from business critical application data (generally held in databases), the system and application software (including configuration files) itself may be worth backing up. This prevents against a new installation being necessary, should all or part of the software become damaged.

While a new installation in principle will always be possible, a complete installation and configuration might take a long time. Thus, the restore time after a system failure may be significantly reduced if a backup of the software and configuration is available.

While data held in RDBMS can be backed up online, an online backup of the runtime infrastructure is not generally possible. Performing a backup of the operating system while the server itself is up and running may cause problems with open files not being backed up.

Keep in mind, that when we talk about online backups of the landscape, we mean online backups of the databases that hold the business critical application data, and not backups of the infrastructure components.



When discussing software backups, we distinguish between a **file system backup** and a **full system backup**. A file system backup only includes specific files or file systems, whereas a full system backup contains all files and file systems including the operation system itself.

After installing new software components, there are also some entries in configuration files of the operating system that cannot be found in the file systems in which the software installation took place. SAP therefore recommends that you take a full system backup after installation and that you backup the file systems of the installed software and the operating system on a regular basis, at least after applying changes to either one.

B&R of Databases

For the backup of databases, SAP generally recommends that you run the database in archive mode, in other words that all actions on the database that modify data are recorded by the database and written to a transaction log.

With regular full backups of your database (either offline or online) and a complete set of transaction logs since the last backup it is possible to restore a crashed database to any point in time before the database crashed.



SAP recommends backing up your database every day, with several backups of the log files during the day as the log files fill up.

B&R for SAP R/3 Application Server

Back up the file system to which the application software is installed. SAP recommends regular file system backups, at least after software changes and upgrades (for example, kernel upgrades, service packs). Take a full system backup after installation and upgrades of the operating system and the SAP software.

B&R for Java Applications running on SAP J2EE Engine

To back up an application that is running on a SAP J2EE Engine, you must back up the following components:

- File system directory, in which the SAP J2EE Engine is installed
 - For an installation on W2K, <drive>:\usr\sap\<Instance Name>\... is the installation directory of the SAP J2EE Engine
 - For an installation on Unix, /usr/sap/<Instance Name>/... is the installation directory
- File system directory that holds the properties and configuration data of the application
 - For an installation on W2K, <drive>:\sapmarkets is the directory for the properties and configuration files
 - For an installation on Unix, /sapmarkets/... is the directory for the properties and configuration files
 - RDBMS, if the Java application stores data in a database
 - Windows 2000 Registry

SAP suggests regular file system backups according to a fixed time schedule. An appropriate schedule could be:

- Full file system backup once a week (for example, on a weekend) and
- Incremental backup once a day.

If your operating system is Windows 2000 and your SAP J2EE Engine is installed as a Windows service, you must also back up the Windows registry. After the initial installation and configuration as well as after major changes, SAP recommends that you make full system backups of the server.

For those Java Applications that store data in a RDBMS backend system, you must back up the database.

4.3.3 B&R for individual system components

Enterprise Portal Server & Knowledge Management

Please refer to the *Exchange Infrastructure Solution Management Guide* under service.sap.com/instguides/, chapters *SAP Enterprise Portal Server* and *SAP Enterprise Portal Knowledge Management*.

User Management Engine

- Classification
 - Java Application installed on SAP J2EE Engine. Application data stored in RDBMS
- Software Backup
 - See *B&R for Java Applications running on SAP J2EE Engine*
 - Full system backup after software installation. Regular file system backup, either full or incremental of J2EE Engine, database software and configuration files
- Data Backup
 - Full database backup daily, log backups several times a day
- Restore
 - Restore host and database (software and configuration files) from full system backup and the latest file system backups
 - Recover the database data files from restoring the latest backup and applying database logs

MDM ID Mapping Framework servlet (ID Mapping Servlet for XI)

- Classification
Java servlet installed on SAP J2EE Engine. No Application data stored.
- Software Backup
See *B&R for Java Applications running on SAP J2EE Engine*
Full system backup after software installation. Regular file system backup, either full or incremental of J2EE Engine and configuration files
- Data Backup
Not necessary
- Restore
Restore host (software and configuration files) from full system backup and the latest file system backups

Master Data Engine

- Classification
ABAP Application installed on SAP Web Application Server 6.20 with installed BW Add-On. Application data stored in RDBMS
- Software Backup
The software of a SAP system is located in file systems on the host. There are also some entries in configuration files of the operating system; however, these cannot be found in the file systems created for the SAP system. It is recommended to take a full system backup after installation and to backup the file systems of the SAP system, the database system, and the operating system on a regular basis, at least after applying changes to either one.
Backup of Application Servers: If there are application servers on additional hosts connected to the database, their software and file systems should also be backed up regularly.
Type: File system backup, either full or incremental. Registry Backup on Windows platforms.
Interval: After installation and software changes, for example, kernel upgrade, applying patches to the operating system, modifying operating system configuration files. An incremental backup on a regular basis is also a good alternative if backups shall not be started on demand.
- Data Backup
The application data is kept in a database. Besides this, there is also information kept in file systems on the application servers (usually in file systems shared between all application servers). This includes, for example, job logs and batch input log files. This information can be very valuable so it should be included in a backup strategy as well. If files are used for data exchange with other systems, these files need to be included as well.
Type: Database backup, either full or incremental, depending on the database software. Log backup. File system backup, either full or incremental.
Interval: Database backup daily. Log backup several times a day or frequently, as logs are filled. File system backup regularly, frequency depends on importance of interface and log files.
- Restore

Restore of file systems. Database restore. Database recovery by applying logs.

Content Integrator

- Classification
Java Application installed on SAP J2EE Engine. Application data stored in RDBMS
- Software Backup
See *B&R for Java Applications running on SAP J2EE Engine*
Full system backup after software installation. Regular file system backup, either full or incremental of J2EE Engine, database software and configuration files
- Data Backup
CI uses the RDBMS of the Master Data Engine. Please refer to the chapter *Master Data Engine* for details.
- Restore
Restore host (software and configuration files) from full system backup and the latest file system backups
CI uses the RDBMS of the Master Data Engine. Please refer to the chapter *Master Data Engine* for details.

Exchange Infrastructure

Please refer to the *Exchange Infrastructure Solution Management Guide* under service.sap.com/instguides.

ITS

For ITS, please refer to section one of the *SAP Best Practice* document *Backup and Restore for mySAP.com*, chapter *SAP ITS*.

Client Systems

For SAP Client Systems, please refer to section one of the *SAP Best Practice* document *Backup and Restore for mySAP.com*.

BW for Analytics

For BW, please refer to section one of the *SAP Best Practice* document *Backup and Restore for mySAP.com* chapter *SAP BW/SAP SEM*.

4.3.4 Point-in-Time Recovery of single components

If one component of the MDM system landscape has to be restored to an older state (point-in-time (PIT) recovery), the logical consistency of the MDM system landscape can be affected. The following table gives an overview about potential cases, effects, and severity, but also shows how to analyze and work on the inconsistency.

Point-in-Time recovery for single components

	Result of PIT recovery	Severity	Analysis of inconsistency	Procedure
SAP Enterprise Portal	Documents/Links/Folders (CM) incorrect*	High	For loaded or distributed documents, analyze distribution logs	Manual rebuild necessary
	Index (TREX) incorrect	Low	Always after PIT	Rebuild index in CM
	User incorrect (corp. LDAP)*	Low	None	Manual rebuild necessary
	Roles incorrect (Portal LDAP)*	Low	None	Manual rebuild necessary
	Configuration/Patches lost	High	Continuous system documentation necessary	Reapply your changes
SAP User Management Engine	Role assignments (CI) incorrect*	Low	None	Manual rebuild necessary
	Configuration/Patches lost	High	Continuous system documentation necessary	Reapply your changes
SAP Master Data Engine				
	Objects created/changed by hand (not distributed) are lost	High	None	Manual rebuild necessary
	Objects created/changed by hand (distributed) are lost	High	Analyze distribution logs	Reload object from client
	Objects created/changed by load are lost	High	Analyze distribution logs	Reload objects
	Load/Distribution process (completed) lost	High	Analyze XI logs	Restart load/distribution
	Load/Distribution process (running) lost	High	Analyze XI logs	Restart load/distribution
	Configuration/Patches lost	High	Continuous system documentation necessary	Reapply your changes
SAP Content Integrator				
	Clearing list incorrect*	High	None	Work off clearing list

				after new load
	Key mapping incorrect*	High	None	Restart load/distribution
	Categories incorrect*	High	None	Reload or manual rebuild necessary
	Configuration/Patches lost	High	Continuous system documentation necessary	Reapply your changes
MDM ID Mapping Framework servlet	Configuration/Patches lost	Low	Continuous system documentation necessary	Reapply your changes
SAP Exchange Infrastructure				
	Messages Lost	High	Analyze local queues; (Asynchronous messages are stored in the local integration engine or the local ALE layer)	Restart load/distribution Check if the messages can be resent to XI.
	Configuration/Patches lost	High	Continuous system documentation necessary	Reapply your changes
ITS				
	Configuration/Patches lost	High	Continuous system documentation necessary	Reapply your changes
Client Systems (R/3, SRM, CRM)				
	Objects created/changed by hand (not sent or extracted) are lost	High	None	Manual rebuild necessary
	Objects created/changed by hand (sent or extracted) are lost	High	Analyze distribution logs	Reload object from server
	Object extraction not finished/partly finished	High	Analyze XI logs	Restart extraction
	Objects created/changed	High	Analyze XI logs	Restart

	by distribution are lost			distribution
	Configuration/Patches lost	High	Continuous system documentation necessary	Reapply your changes
BW for Analytics				
	MDM/CI Data not current	Low	None	New extraction
	Configuration/Patches lost	High	Continuous system documentation necessary	Reapply your changes
SAP Solution Manager				
	Configuration/Patches lost	High	Continuous system documentation necessary	Reapply your changes

* = "incorrect" can mean lost, not deleted, or unchanged

4.4 System Copy

The concept for system copy is still in the planning phase.

4.5 Periodical Tasks

4.5.1 Required periodical tasks (Components)

4.5.1.1 Master Data Server (MDS)

Required periodical tasks

Program name/Task	Short Description	Detailed description
Process Monitor (Transaction PC_D_MONI)	Delete process instances	Deletion can be triggered using dialog or periodically
Application Log (Transaction SLG2)	Delete application log	The application log objects PC_PROCESS with sub-objects PC_STEP and PC_VERSION are not deleted when deleting process instances (process container). Using this transaction, the mentioned application log objects can be deleted.
FOX Cache Persistency: (ReportFOX2_REQUEST_GARBAGE)	Delete obsolete FOX requests	The report deletes obsolete FOX requests physically or logically from the database.
CI Matching (Report MDM_RESTART_CI_PROCESSES)	Delete unsuccessful matching	The report searches the tables

MDM_RESTART_CI_PROCESSES)	matching	MDM_MATCH_HEADER and MDM_MATCH_ITEMS for defective CI updates. These updates will be restarted and the corresponding table entries deleted.
Process Chains (Transaction RSPC)	Delta download	In process chain maintenance, a chain for delta download from the master data clients (MDC) must be planned for the relevant objects.
Process Chains (Transaction RSPC)	Posting	In process chain maintenance, a chain for periodical inbound posting in staging (PIC, Periodical Inbound Collector) must be planned for the relevant objects, if no extraction is used.
Process Chains (Transaction RSPC)	Delta distribution	In process chain maintenance, a chain for delta distribution must be planned for the relevant objects.

4.5.1.2 Exchange Infrastructure (XI)

Required periodical tasks

Program name/Task	Short Description	Detailed description
XI Messages (Report RSXMB_RESTART_MESSAGES)	Periodical re-start	Plan/schedule report to restart incorrect messages. If messages cannot be restarted anymore, they need to be deleted manually. To avoid incorrect data, the corresponding object must be resent manually.

4.5.1.3 Master Data Clients (MDC)

Required periodical tasks

Program name/Task	Short Description	Detailed description
Especially relevant for client SAP R/3:		
Change Pointer (Report RBDPCCLR)	Clear processed change pointers	Plan/schedule report

4.5.2 General

4.5.2.1 Qrfc and tRFC Monitoring

The transactional RFC (tRFC) und queued RFC (qRFC) status must be monitored within the complete system landscape using the transactions SM58, SMQ1 and SMQ2. Unsuccessful processes need to be restarted.

The RFCs can contain the following:

- In the master data clients (MDC), RFCs can contain IDocs and XML messages.
- In XI, RFCs can contain XML message processing steps.
- In the master data server (MDS), RFCs can contain XML messages and application messages in process.

4.6 Logon and Load Balancing



Detailed descriptions of load balancing methods are provided in the guides for the following components used within Master Data Management:

Component	Detailed Description	Link
EP 5.0	See <i>Technical Infrastructure Guide EP (particularly Chapter 5)</i>	service.sap.com/
MDM 2.00	See <i>SAP Web Application Server 6.20 in Switchover Environments EP (particularly Chapter 7)</i>	service.sap.com/
XI 2.0	For SAP Exchange Infrastructure 2.0 components based on SAP Web Application Server 6.20 (including SAP J2EE engine), in other words, the System Landscape Directory, Integration Builder, Integration Engine, Market Set Adaptor, refer to the respective <i>SAP Web Application Server 6.20 documentation</i> . Since the Adaptor Engine component is based on J2SE, it does not provide any load balancing functions. See also the <i>Solution Management Guide for SAP Exchange Infrastructure 2.0</i>	service.sap.com/instguides/
CI 2.0	No load balancing concept for CI 2.0	
UME 3.0	No load balancing concept for UME 3.0	

MDM Web Application (Servlet)	The clustered version of the SAP J2EE Engine provides load balancing.	
ITS 6.20	See <i>SAP Internet Transaction Server - Technical Infrastructure Guide ITS (particularly Chapter 2)</i>	service.sap.com/

4.7 User Management

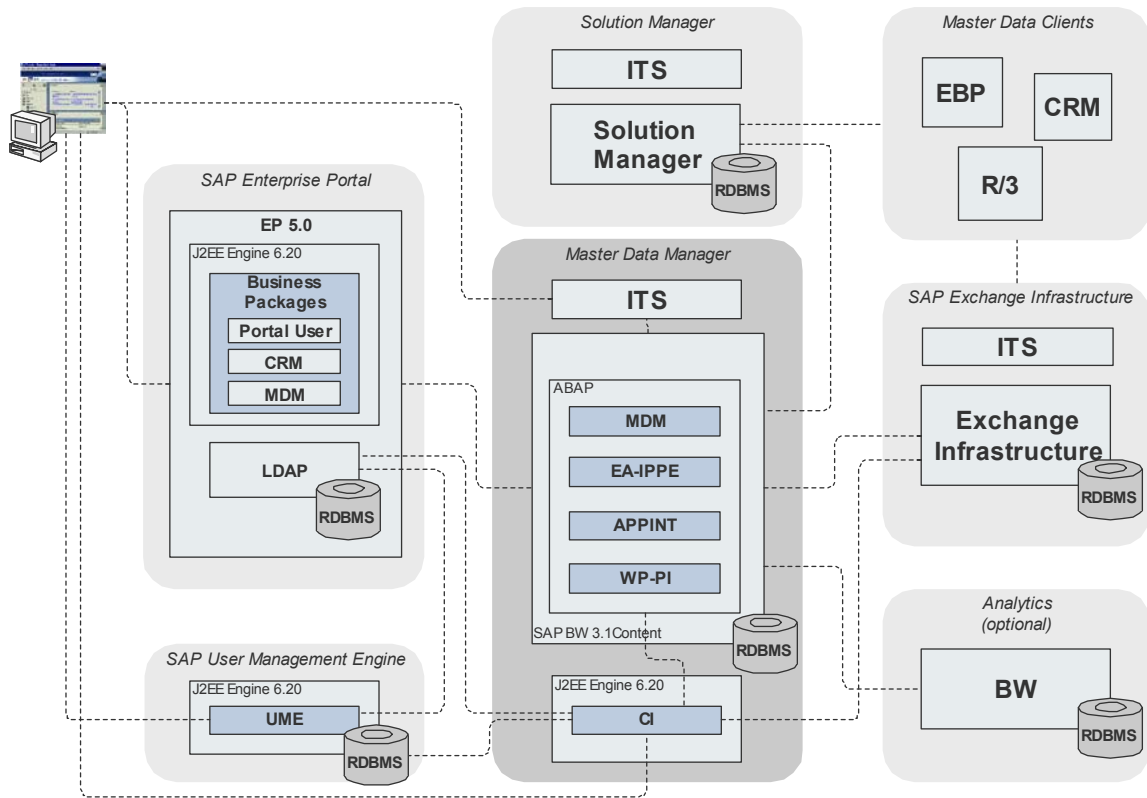
For detailed information about user management within SAP MDM, see *Master Data Harmonization and Central Master Data Management - Configuration Guide (particularly section 2.2)* under: service.sap.com/instguides/ → SAP MDM → SAP MDM 2.00.

4.8 Printing

Not relevant for SAP MDM 2.00.

5 High Availability

5.1 System Landscape of the Solution



An additional component (not illustrated here) is the MDM Web Application (MDM ID Mapping Framework servlet). It is used as a messaging interface between CI and XI for MDM key mapping.

5.2 High Availability Matrix for the Individual Components

Component	Single Point of Failure	Impact
EP 5.0	Yes	No processing possible MDM not accessible → MDM not operational
UME 3.0	Yes	CI breaks → MDM not operational
Solution Manager 3.1	No	If Customizing has been distributed successfully → no impact
MDM 2.00	Yes	No processing possible → MDM not operational
CI 2.0	Yes	No matching; no key mapping → MDM not

		operational
XI 2.0	Yes	No data load/distribution possible → MDM not operational
ITS 6.20	Yes	Some transactions cannot be accessed → MDM partially not operational
MDM Web Application	Yes	Distribution of Master Data will fail which could lead to data inconsistencies in the customer's system landscape. However, XI provides automatic and manual retry functionality for Master Data to be redistributed.
BW 3.1 Content	No	No analytics possible
Clients (for example, R/3 4.6C, R/3 Enterprise, CRM 4.0)	Yes	Exchange of master data information disturbed, local application not available

5.3 Relevant Documentation

Component	Documentation/Description	Link
EP 5.0	Technical Infrastructure Guide Enterprise Portal (particularly Chapters 5 and 6)	service.sap.com/epinstall , then <i>Enterprise Portal 5.0</i> → <i>Installation, Upgrade & Patches</i> → <i>EP 5.0 SP 05 Roadmap</i> → <i>System Requirements SP 05</i> → <i>Technical Infrastructure (EP 5.0 SP 05)</i>
UME 3.0	High Availability concept for UME 3.0 is not available yet.	
Solution Manager 3.1	Solution Manager 3.1 is based on CRM 3.1. Therefore, documentation about SAP Web Application Server 6.20 is applicable.	See entries under <i>MDM 2.00</i> .

MDM 2.00	<p>MDM 2.00 is based on BW 3.1 incl. SAP Web Application Server 6.20. Therefore, documentation about SAP Web Application Server 6.20 is applicable:</p> <ul style="list-style-type: none"> • SAP Web Application Server 6.20 - Product Documentation High Availability 	<p>help.sap.com/ → SAP NetWeaver → SAP Web Application Server → Release SAP Web Application Server 6.20 (→ set Language) → mySAP Technology components → SAP Web Application Server → Computing Center Management System (BC-CCM) → SAP High Availability (BC-CCM-HAV)</p>
	<ul style="list-style-type: none"> • SAP Web Application Server 6.20 in Switchover Environments 	<p>http://service.sap.com/~sapidb/011000358700008669802002E</p>
CI 2.0	High Availability concept for Content Integrator is not available yet.	
XI 2.0	<p>XI2.0 in High Availability Environments</p> <p>See also: <i>Solution Management Guide for SAP Exchange Infrastructure 2.0</i></p>	<p>http://service.sap.com/~sapidb/011000358700002352642003E</p> <p>service.sap.com/instguides/</p>
ITS 6.20	<p>SAP Internet Transaction Server - Technical Infrastructure Guide ITS (particularly Chapter 2)</p>	<p>http://service.sap.com/~sapidb/011000358700003678602001E</p>
MDM Web Application	<ul style="list-style-type: none"> • Component functionality can be distributed over several machines. • To achieve high availability, the customer must install the clustered version of the SAP J2EE Engine, which provides load balancing. • In the case of a machine crash, the updated or created Master Data object will not be distributed to the intended target systems. The distribution can be retried at a later date through the XI's retry functionality. • For further information, see <i>Chapter 6, Software Change Management</i>. 	

<p>BW 3.1 Content</p>	<p>BW 3.1 Content is based on SAP Web Application Server 6.20. Therefore, documentation about SAP Web Application Server 6.20 is applicable.</p>	<p>See entries under <i>MDM 2.00</i>.</p>
<p>Clients (e.g. R/3 4.6C, R/3 Enterprise, CRM 4.0)</p>	<p>If based on SAP Web Application Server 6.20, documentation about SAP Web Application Server 6.20 is applicable.</p>	<p>If so, see entries under <i>MDM 2.00</i>.</p>

6 Software Change Management

Software Change Management standardizes and automates software distribution, maintenance, and testing procedures for complex software landscapes and multiple software development platforms. These functions support your project teams, development teams, and application support teams.

The goal of software change management is to establish consistent, solution wide change management that allows for specific maintenance procedures, global rollouts, including localizations, and open integration with third-party products.

This section provides additional information about the most important software components.

The following topics are covered:

- Transport and Change Management
Enables and secures the distribution of software changes from the development environment to the quality assurance and productive environment.
- Support Packages and SAP Notes Implementation
Provides standardized software distribution and maintenance procedures.

6.1 SAP Master Data Management

6.1.1 Transport and Change Management

Component	Method for transport and change management
<p>EP 5.0</p>	<p>See documentation under service.sap.com/epinstall, then <i>Enterprise Portal 5.0 → Installation, Upgrade & Patches → EP 5.0 SP 05 Roadmap → Installation, Upgrade & Patches SP 5</i></p>
<p>UME 3.0</p>	<p>Standard JAVA transport and change</p>

	management procedures: Patched using Software Distribution Management (SDM). The patches are available on the Service Marketplace.
Solution Manager 3.1	Standard Web Application Server transport and change management procedures. See help.sap.com/ → <i>SAP NetWeaver</i> → <i>SAP Web Application Server</i> → <i>Release SAP Web Application Server 6.20</i> (→ set Language) → <i>mySAP Technology components</i> → <i>SAP Web Application Server</i> → <i>Computing Center Management System (BC-CCM)</i> → <i>SAP High Availability (BC-CCM-HAV)</i>
MDM 2.00	Standard Web Application Server transport and change management procedures. See <i>Web Application Server</i> → Technical Operations Manual → <i>Technical Operations Manual for mySAP Technology</i> → <i>Software Change Management</i>
CI 2.0	Standard JAVA transport and change management procedures: Patched using Software Distribution Management (SDM). The patches are available on the Service Marketplace.
XI 2.0	See SAP Note 588568 <i>SAP Exchange Infrastructure 2.0: Patch procedure</i> for instructions on how to patch SAP Exchange Infrastructure components.
ITS 6.20	See service.sap.com/patches → SAP ITS
MDM Web Application (Servlet)	Standard JAVA transport and change management procedures: See <i>SAP Note 651321</i> .
BW 3.1 Content	Standard Web Application Server transport and change management procedures

6.1.2 Support Packages and SAP Notes Implementation

For detailed information about the current status regarding Support Packages of single components, see the Master Guide under service.sap.com/instguides/ → *SAP MDM* → *SAP MDM 2.00*.



Please make sure not to implement relevant Support Packages during production operation of SAP MDM.

A SAP Note will be created to accommodate possible interdependencies between single components when implementing a higher Support Package or patch level.

Up-to-date information on SAP Notes, Support Package levels, and patches is published on the Service Marketplace. See service.sap.com/patches.

7 Troubleshooting

Troubleshooting instructions will be published in due time.

8 Services for SAP Master Data Management

Standard Remote Services are not available for SAP Master Data Management 2.0.

9 Appendix

9.1 Categories of System Components for Backup & Recovery

Categories of system components	Category Properties	Suggested Backup and Recovery Methods	Example
I	Only software, no configuration or application data	<ul style="list-style-type: none"> No backup, new installation in case of a restore or Initial software backup after installation and upgrade Backup of log files 	BDOC-modeler
II	Only software and configuration information, no application data	<ul style="list-style-type: none"> Backup after changes have been applied or No backup, New installation and configuration in case of a restore Backup of log files 	SAP Gateway Comm. Station SAP Business Connector SAP IPC (2.0C)
III	Only replicated application data, replication time is sufficiently small for a restore	Data: <ul style="list-style-type: none"> No data backup needed Backup of software, configuration, log files	SAP IMS / Search Engine * SAP IPC (2.0B) * Webserver * SAP ITS
IV	Only replicated application data, backup recommended because replication time is too long data not managed by a DBMS	Data: <ul style="list-style-type: none"> Application specific file system backup or Multiple instances Backup of software, configuration, log files 	SAP IMS / Search Engine * Webserver *
V	Only replicated application data, backup recommended because replication time is too long data managed by a DBMS	Data: <ul style="list-style-type: none"> Database and log backup or Multiple instances Backup of software, configuration, log files	SAP IPC (2.0B) * Catalog Server
VI	Original application data, standalone system, data not managed by a DBMS	Data: <ul style="list-style-type: none"> Application specific file system backup Backup of software, configuration, log files	Webserver *

VII	Original application data, standalone system, data managed by a DBMS, not based on SAP Web Application Server	Data: <ul style="list-style-type: none"> • Database and log backup Backup of software, configuration, log files	
VIII	Original application data, standalone system, based on SAP Web Application Server	Data: <ul style="list-style-type: none"> • Database and log backup, application log backup (e.g. job logs in file system) Backup of software, configuration, log files 	Standalone SAP R/3
IX	Original application data, data exchange with other systems, data not managed by a DBMS	Data: <ul style="list-style-type: none"> • Application specific file system backup, data consistency with other systems must be regarded Backup of software, configuration, log files	
X	Original application data, data exchange with other systems, data managed by a DBMS, not based on SAP Web Application Server	Data: <ul style="list-style-type: none"> • Database and log backup, data consistency with other systems must be regarded. Backup of software, configuration, log files	SAP liveCache SAP Mobile Workbench
XI	Original application data, data exchange with other systems, based on SAP Web Application Server	Data: <ul style="list-style-type: none"> • Database and log backup, application log backup (for example, job logs in file system), data consistency with other systems must be regarded Backup of software, configuration, log files	SAP R/3 SAP CRM SAP APO SAP BW

9.2 Related Guides

You can find more information about installation in the *Configuration Guides for SAP Master Data Management 2.00* in the *SAP Service Marketplace* under service.sap.com/instguides → *Installation and Upgrade Guides* → *SAP MDM*.

9.3 Related Information

The following table contains links to information relating to the Solution Management Guide.

Content	Quick Link to the SAP Service Marketplace (service.sap.com)
Master Guide, Installation Guide and Configuration Guide	service.sap.com/instguides
Related SAP Notes	service.sap.com/notes
Released platforms	service.sap.com/platforms
Network security	service.sap.com/securityguide network
Technical infrastructure	service.sap.com/ti
SAP Solution Manager	service.sap.com/solutionmanager