

OPTIMIZE

MERCURY BUSINESS AVAILABILITY CENTER™

Upgrading Mercury Business Availability Center

MERCURY™

BUSINESS TECHNOLOGY OPTIMIZATION

Mercury Business Availability Center

Upgrading Mercury Business Availability Center

Version 6.6

Document Release Date: May 7, 2007

MERCURY™

Mercury Business Availability Center, Version 6.6
Upgrading Mercury Business Availability Center

This document, and the accompanying software and other documentation, is protected by U.S. and international copyright laws, and may be used only in accordance with the accompanying license agreement. Features of the software, and of other products and services of Mercury Interactive Corporation, may be covered by one or more of the following patents: United States: 5,511,185; 5,657,438; 5,701,139; 5,870,559; 5,958,008; 5,974,572; 6,137,782; 6,138,157; 6,144,962; 6,205,122; 6,237,006; 6,341,310; 6,360,332; 6,449,739; 6,470,383; 6,477,483; 6,549,944; 6,560,564; 6,564,342; 6,587,969; 6,631,408; 6,631,411; 6,633,912; 6,694,288; 6,738,813; 6,738,933; 6,754,701; 6,792,460 and 6,810,494. Australia: 763468 and 762554. Other patents pending. All rights reserved.

U.S. GOVERNMENT RESTRICTED RIGHTS. This Software Documentation is a “commercial item” as defined at 48 C.F.R. 2.101 (October 1995). In accordance with 48 C.F.R. 12.212 (October 1995), 48 C.F.R. 27.401 through 27.404 and 52.227-14 (June 1987, as amended) and 48 C.F.R. 227.7201 through 227.7204 (June 1995), and any similar provisions in the supplements to Title 48 of the C.F.R. (the “Federal Acquisition Regulation”) of other entities of the U.S. Government, as applicable, all U.S. Government users acquire and may use this Documentation only in accordance with the restricted rights set forth in the license agreement applicable to the Computer Software to which this Documentation relates.

Mercury, Mercury Interactive, the Mercury logo, the Mercury Interactive logo, LoadRunner, WinRunner, SiteScope and TestDirector are trademarks of Mercury Interactive Corporation and may be registered in certain jurisdictions. The absence of a trademark from this list does not constitute a waiver of Mercury's intellectual property rights concerning that trademark.

All other company, brand and product names may be trademarks or registered trademarks of their respective holders. Mercury disclaims any responsibility for specifying which marks are owned by which companies or which organizations.

Mercury provides links to external third-party Web sites to help you find supplemental information. Site content and availability may change without notice. Mercury makes no representations or warranties whatsoever as to site content or availability.

Mercury Interactive Corporation
379 North Whisman Road
Mountain View, CA 94043
Tel: (650) 603-5200
Fax: (650) 603-5300
<http://www.mercury.com>

© 2005-2007 Mercury Interactive Corporation, All rights reserved

If you have any comments or suggestions regarding this document, please send them by e-mail to documentation@mercury.com.

Table of Contents

Welcome to Upgrading Mercury Business Availability Center 6.6.....	7
Using this Guide.....	8
Getting More Information	8

PART I: CHECKLISTS FOR UPGRADING TO MERCURY BUSINESS AVAILABILITY CENTER 6.6

Chapter 1: Introduction to Upgrade.....	11
Important Information About the Upgrade.....	12
Major Upgrade Steps	12
Chapter 2: Upgrade Checklist - from 4.5 to 6.6.....	13
Before You Begin	13
Upgrade Checklist	16
Chapter 3: Upgrade Checklist - from 5.x to 6.6.....	21
Before You Begin	21
Upgrade Checklist	22
Chapter 4: Upgrade Checklist - from 6.1.x to 6.6.....	29
Before You Begin	29
Upgrade Checklist	30
Chapter 5: Upgrade Checklist - from 6.2/6.3/6.4/6.5 to 6.6.....	37
Before You Begin	37
Upgrade Checklist	38

PART II: UPGRADE PROCEDURES

Chapter 6: Upgrading the Servers.....	47
Server Architecture for Mercury Business Availability Center	48
Upgrading Considerations	48
Installing Mercury Business Availability Center 6.1, the 6.2 Add-on, and the 6.6 Add-on on a Windows Platform	49

Installing Mercury Business Availability Center 6.2 and the 6.6 Add-on on a Solaris Platform.....	54
Chapter 7: Verifying and Upgrading the Database Schema.....	59
Introducing Upgrade Methodology	60
Using the Verify and Upgrade Utility	60
Verifying the Database Schema.....	63
Upgrading the Database Schema	68
Creating Database Users for the Upgrade Procedure	71
Troubleshooting Database Schema Verify and Upgrade Errors	72
Chapter 8: Retaining Monitor Administration	
Configuration Data	75
Overview of Retaining Monitor Administration	
Configuration Data	75
Backing Up Monitor Configuration Data Files	76
Copying Monitor Configuration Data Files to	
Mercury Business Availability Center	77
Upgrading the LDAP Database	78
Chapter 9: Configuration Upgrade.....	79
Upgrading Configuration Data	79
Chapter 10: Dashboard Views Upgrade	85
The Views Upgrade Page	86
Simulating a View Upgrade	88
Upgrading a View	89
Post-Upgrade Tasks.....	91
Displaying an Upgraded View.....	91
Troubleshooting	92
Notes and Limitations.....	93
Rollback.....	96
Chapter 11: Upgrading Repositories	97
Upgrading the Repositories from	
Mercury Business Availability Center 6.x	97
Upgrading the Repositories from	
Mercury Business Availability Center 5.x to 6.6	97
Chapter 12: Upgrading Source Adapters	115
Upgrading the Source Adapters from	
Mercury Business Availability Center 6.x	115
Upgrading the Source Adapters from	
Mercury Business Availability Center 5.x	116

Chapter 13: Upgrading Service Level Management	125
Prerequisites.....	126
Notes and Limitations.....	127
SLA Upgrade and the Business Process Monitor Source Adapter.....	128
SLA Upgrade and the SiteScope Source Adapter	130
Upgrading SLAs from 5.x to 6.6	132
Upgrading Custom Reports	135
Upgrading the Report Repository.....	136
Upgrading Rules Used For SLA Conversions	137
Upgrade Messages.....	145
Chapter 14: Switching Mercury Business Availability Center	
URL on the Data Collectors	151
Overview of Switching Data Collectors	151
Redirecting the Business Process Monitor URL.....	152
Redirecting the Client Monitor URL.....	153
Redirecting the SiteScope URL	154
Redirecting the Real User Monitor URL.....	156
Chapter 15: Upgrading Components	157
Business Process Monitor	158
Client Monitor	159
SiteScope.....	162
Real User Monitor.....	164
Virtual User Generator (VuGen)	169
Discovery Probe.....	172

PART III: MERCURY APPLICATION MAPPING

Chapter 16: Upgrading Mercury Application Mapping	
from Version 6.x to Version 6.6	175
Upgrading Mercury Application Mapping:	
Version 6.x – 6.6 with a Shared CMDB.....	176
Backing Up Configuration Files	180
Redeploying and Undeploying Packages	182
Index.....	185

Table of Contents

Welcome to Upgrading Mercury Business Availability Center 6.6

This guide provides detailed instructions on how to upgrade from the following versions to Mercury Business Availability Center 6.6:

- ▶ Topaz 4.5 FP2
- ▶ Mercury Business Availability Center 5.x
- ▶ Mercury Business Availability Center 6.x

Note to Mercury Managed Services customers: The information in this guide is not relevant to Mercury Managed Services customers.

Before starting the upgrade, refer to “Important Information About the Upgrade” on page 12.

Using this Guide

The guide contains the following parts:

Part I Checklists for Upgrading to Mercury Business Availability Center 6.6

Describes what actions to perform before and during the upgrade to Mercury Business Availability Center 6.6.

Part II Upgrade Procedures

Includes the various procedures to perform to upgrade from your current version of Topaz or Mercury Business Availability Center to Mercury Business Availability Center 6.6

Part III Mercury Application Mapping

Includes what actions to perform to upgrade from Mercury Application Mapping 6.x to version 6.6.

Getting More Information

For information on using and updating the Mercury Business Availability Center Documentation Library, reference information on additional documentation resources, typographical conventions used in the Documentation Library, and quick reference information on deploying, administering, and using Mercury Business Availability Center, refer to *Getting Started with Mercury Business Availability Center*.

Part I

Checklists for Upgrading to Mercury Business Availability Center 6.6

1

Introduction to Upgrade

This guide describes the methodology for upgrading your servers and database from various earlier versions to Mercury Business Availability Center 6.6. Mercury Business Availability Center supports direct schema and data upgrade from these earlier versions.

The aim of the procedures and recommendations provided in this guide is to enable you to upgrade your platform to Mercury Business Availability Center 6.6 with the minimum possible interruption to your system operation.

You can access this guide in PDF format (make sure you have Acrobat Reader 4.0 or later installed on the machine) from the following locations:

- From the Mercury Business Availability Center 6.6 release download area.
- From the Mercury Business Availability Center Documentation Portal area on the Mercury Customer Support Web site (support.mercury.com).

Important Information About the Upgrade

- ▶ Mercury Business Availability Center can be installed in a variety of configurations. The upgrade procedure depends on how Mercury Business Availability Center is configured in your environment. The steps detailed in this book are intended as a guide only.
- ▶ Throughout this document, **<Mercury Business Availability Center root directory>** refers to the full path of your installation directory.
 - ◆ In a Windows environment, the default for **<Mercury Business Availability Center root directory>** is C:\MercuryAM.
 - ◆ In a Solaris environment, the default for **<Mercury Business Availability Center root directory>** is /opt/MercuryAM.

<Mercury Business Availability Center root directory> can be the default installation path or you can change it to be a different path.

Major Upgrade Steps

Upgrading your platform to Mercury Business Availability Center 6.6 may involve the following major activities:

- ▶ Upgrading servers
- ▶ Upgrading the database schema
- ▶ Upgrading the data and completing the upgrade
- ▶ Upgrading Mercury Business Availability Center components

The complete upgrade process for upgrading from an earlier version to Mercury Business Availability Center 6.6 is described in Part I, “Checklists for Upgrading to Mercury Business Availability Center 6.6.” For each part of the upgrade process, the upgrade checklist directs you to the section of this guide that contains the relevant steps.

2

Upgrade Checklist - from 4.5 to 6.6

This chapter describes what actions to perform to upgrade from Mercury Business Availability Center 4.5 to 6.6.

This chapter describes:	On page:
Before You Begin	13
Upgrade Checklist	16

Before You Begin

You should be aware of the following information before you begin the upgrade.

- ▶ Direct upgrade from Topaz 4.5 FP2 on Solaris to Mercury Business Availability Center 6.6 on Solaris is not supported. If you require this upgrade scenario, contact Mercury Customer Support.
- ▶ The uninstall utility rolls Mercury Business Availability Center 6.6 back to the previous version. The database schema however, needs to be restored manually.
- ▶ In Mercury Business Availability Center 6.x, different server types are used than those in Topaz 4.5 FP2. For details, refer to “Server Architecture for Mercury Business Availability Center” on page 48.

- ▶ If you are upgrading from Topaz 4.5 FP2 and want to perform a “clean” installation and lose all existing data, uninstall all previous Topaz server installations and then install Mercury Business Availability Center 6.6, as for a first-time installation. For details, refer to *Deploying Servers*. You may want to make a list of your customized configuration settings before uninstalling, so that you can redefine them after the clean installation of Mercury Business Availability Center 6.6.
- ▶ Do not create any new databases between the database schema upgrade and the end of the full upgrade procedure. If you do so by mistake, contact Mercury Customer Support.
- ▶ Topaz 4.5 FP2 customers who require upgrade of views and repositories used with Topaz 4.5 FP2 must contact Mercury Customer Support for assistance in upgrading to Mercury Business Availability Center 6.6. This upgrade scenario involves the following major steps:
 - ◆ Upgrade Topaz 4.5 FP2 to Mercury Business Availability Center 5.1 SP1 (following the steps described in the upgrade documentation included with Mercury Business Availability Center 5.1 SP1).
 - ◆ Perform views and repositories upgrade in coordination with Mercury Customer Support.
 - ◆ Upgrade Mercury Business Availability Center 5.1 SP1 to Mercury Business Availability Center 6.1.
 - ◆ Upgrade Mercury Business Availability Center 6.1 to Mercury Business Availability Center 6.2.
 - ◆ Upgrade Mercury Business Availability Center 6.2 to Mercury Business Availability Center 6.6.
- ▶ If you have any private patches for your current installation, you will lose them when you upgrade. If you have private patches that you want to continue to use, contact Mercury Customer Support before beginning the upgrade process.

- ▶ During the upgrade process, SiteScope and Business Process Monitor downtime events are replicated. The scheduled downtime events will run as configured, and the replication of the downtime events has no impact on the system other than them being displayed in the Downtime/Event schedule in Mercury Business Availability Center. It is recommended that you do not remove the replicated entries unless necessary, and if so, you should contact your Mercury representative for assistance.

Upgrade Checklist

The following checklist should be used when upgrading from Topaz 4.5 FP2 to Mercury Business Availability Center 6.6:

Step	Description	Details
<p>1 Back up files.</p>	<p>Back up various files and directories that are required during the upgrade process, or as a precautionary measure.</p>	<p>Back up the following files and directories:</p> <ul style="list-style-type: none"> ▶ <Mercury Business Availability Center server root dir>\conf\TopazInfra.ini – file needed for upgrading the databases in step 6. For details on upgrading the databases, see “Verifying and Upgrading the Database Schema” on page 59. ▶ Any other files or directories you want to keep for security or historical purposes.
<p>2 Shut down existing Topaz 4.5 FP2 servers.</p>	<p>Stop the Topaz Supervisor service on each of the old Mercury Business Availability Center servers. Make sure there are no open connections to Mercury Business Availability Center databases.</p>	<ul style="list-style-type: none"> ▶ For Windows – Select Start > Programs > Topaz > Administration > Stop Topaz. ▶ For Solaris – Execute the command: <Mercury Business Availability Center server root dir>/scripts/run_topaz stop.

Step	Description	Details
<p>3 If upgrading to Mercury Business Availability Center 6.6 using the existing 4.5 FP2 server machines, uninstall Topaz 4.5 FP2.</p>	<p>Uninstall Mercury Business Availability Center 4.5 FP2 from all machines.</p> <p>You may need to run the uninstall procedure twice.</p> <p>After the uninstall procedure is finished, manually delete all files in the Mercury Business Availability Center directory.</p>	<ul style="list-style-type: none"> ▶ For Windows – Select Start > Programs > Topaz > Uninstall Topaz. ▶ For Solaris – Execute the commands: <pre style="margin-left: 20px;">cd <installation directory> /_uninst ./uninstall</pre>
<p>4 Install, in the following order, on all machines:</p> <ul style="list-style-type: none"> ▶ Mercury Business Availability Center 6.1 ▶ Mercury Business Availability Center 6.2 Add-on ▶ Mercury Business Availability Center 6.6 Add-on 	<p>Install each of the Mercury Business Availability Center versions on all machines, but do not connect to the database as part of the installation process.</p> <p>After each installation, do not start (enable) Mercury Business Availability Center.</p> <p>At the end of 6.6 Add-on installation, you can upgrade the database schema.</p>	<p>For details, see “Installing Mercury Business Availability Center 6.1, the 6.2 Add-on, and the 6.6 Add-on on a Windows Platform” on page 49.</p>
<p>5 Back up the databases.</p>	<p>Back up the existing management and profile databases.</p>	<p>For information on backing up your databases, refer to the database server documentation or to the Mercury Business Availability Center database administration document <i>Preparing the Database Environment</i>.</p>

Step	Description	Details
<p>6 If you did not upgrade the database schema automatically at the end of installing the 6.6 Add-on in step 4, run the database schema upgrade now.</p>	<p>Run dbupgrade from any one of the Mercury Business Availability Center 6.6 servers to verify and upgrade the management and profile databases to Mercury Business Availability Center 6.6 compatibility.</p> <p>Do not proceed to the next step until database upgrade has completed successfully.</p>	<p>See “Verifying and Upgrading the Database Schema” on page 59.</p>
<p>7 Update the database port in the management database.</p>	<p>Before connecting to the management database, manually update the database port in the upgraded management database.</p>	<p>Run the following query on the upgraded management database:</p> <pre>UPDATE SESSIONS SET SESSION_DB_PORT = '1433' WHERE SESSION_DBTYPE IN (2,4) AND SESSION_DB_PORT IS NULL</pre>
<p>8 Connect each Mercury Business Availability Center 6.6 machine to the management database.</p>	<p>On each Mercury Business Availability Center 6.6 machine, run Connect to Database to connect to the upgraded management database.</p> <p>The first server to be connected should be the Mercury Business Availability Center 6.6 Centers Server designated for running LDAP. For information on LDAP, refer to <i>Preparing the Database Environment</i>.</p>	<ul style="list-style-type: none"> ▶ In Windows, select Start Menu > Programs > Mercury Business Availability Center > Administration > Connect to Database. ▶ In Solaris, execute the command: <Mercury Business Availability Center server root dir>/scripts/setmngdbWizard.sh

Step	Description	Details
<p>9 Start Mercury Business Availability Center 6.6 on all machines.</p>	<p>Enable Mercury Business Availability Center 6.6 on all machines.</p> <p>It can take approximately 20-25 minutes for Mercury Business Availability Center to be available for login after starting all servers for the first time.</p>	<ul style="list-style-type: none"> ▶ For Windows – Select Start > Programs > Mercury Business Availability Center > Administration > Enable Business Availability Center. ▶ For Solaris – Execute the command: <Mercury Business Availability Center server root dir>/scripts/run_topaz start <p>Note: To verify that a server has successfully started – on the server in question, look in <Mercury Business Availability Center server root dir>\log\jboss_boot.log file for a line that includes INFO - JBoss and Started in.</p>
<p>10 Reenter the Mercury Business Availability Center 6.6 license key.</p>	<p>After starting Mercury Business Availability Center for the first time, and before proceeding with the steps for upgrading your data, reenter the Mercury Business Availability Center 6.6 license key.</p>	<p>Select Admin > Platform > Setup and Maintenance > License Management and click New License Key.</p> <p>For information on updating the license key, see <i>Platform Administration.</i></p>
<p>11 Check that data has been inserted into CMDB.</p>	<p>A few minutes after Mercury Business Availability Center 6.6 has been restarted, check that source adapters have inserted data in the CMDB.</p>	<p>From CMDB Administration, in the Source Manager tab, make sure that the Last Update column has a date for all the sources listed.</p>
<p>12 Upgrade configuration data.</p>	<p>Run all manual data upgrades.</p>	<p>See “Upgrading Configuration Data” on page 79.</p>

Part I • Checklists for Upgrading to Mercury Business Availability Center 6.5

Step	Description	Details
13 Upgrade SLAs.	Run the SLM upgrade process.	For details, see “Upgrading Service Level Management” on page 125.
14 Switch URLs on data collectors (only if upgrading to Mercury Business Availability Center 6.6 on new servers).	If you installed the Mercury Business Availability Center 6.6 on new machines with different URLs, switch the URLs on your data collectors to report to Mercury Business Availability Center 6.6 servers.	See “Switching Mercury Business Availability Center URL on the Data Collectors” on page 151.
15 Upgrade Mercury Business Availability Center components.	To benefit from the latest features, upgrade your Mercury Business Availability Center components to the most current version for Mercury Business Availability Center 6.6.	See “Upgrading Components” on page 157.

3

Upgrade Checklist - from 5.x to 6.6

This chapter describes what actions to perform to upgrade from Mercury Business Availability Center 5.x to 6.6.

This chapter describes:	On page:
Before You Begin	21
Upgrade Checklist	22

Before You Begin

You should be aware of the following information before you begin the upgrade:

- ▶ The uninstall utility rolls Mercury Business Availability Center 6.6 back to the previous version. The database schema however, needs to be restored manually.
- ▶ In Mercury Business Availability Center 6.x, different server types are used than those in Mercury Business Availability Center 5.x. For details, refer to *Deploying Servers*.
- ▶ If you are upgrading from Mercury Business Availability Center 5.x and want to perform a “clean” installation and lose all existing data, uninstall all previous Topaz server installations and then install Mercury Business Availability Center 6.6, as for a first-time installation. For details, refer to *Deploying Servers*. You may want to make a list of your customized configuration settings before uninstalling, so that you can redefine them after the clean installation of Mercury Business Availability Center 6.6.

- ▶ Do not create any new databases between the database schema upgrade and the end of the full upgrade procedure. If you do so by mistake, contact Mercury Customer Support.
- ▶ If you have any private patches for your current installation, you will lose them when you upgrade. If you have private patches that you want to continue to use, you should coordinate with Mercury Customer Support before beginning the upgrade process.

Upgrade Checklist

The following checklist should be used when upgrading from Mercury Business Availability Center 5.x to Mercury Business Availability Center 6.6:

Step	Description	Details
1 Shut down existing Mercury Business Availability Center 5.x servers.	Stop the Mercury Business Availability Center service on each of the old Mercury Business Availability Center servers. Make sure there are no open connections to Mercury Business Availability Center databases.	<ul style="list-style-type: none">▶ For Windows – Select Start > Programs > Mercury Business Availability Center > Administration > Disable Business Availability Center.▶ For Solaris – Execute the command: <code><Mercury Business Availability Center server root directory>/scripts/run_topaz stop.</code>

Step	Description	Details
2 Back up files.	Back up various files and directories that are required during the upgrade process, or as a precautionary measure.	<p>Back up the following files and directories:</p> <ul style="list-style-type: none"> ▶ <Mercury Business Availability Center server root directory>\conf\TopazInfra.ini – file needed for upgrading the databases in step 6. For details on upgrading the databases, see “Verifying and Upgrading the Database Schema” on page 59. ▶ <Mercury Business Availability Center Modeling Data Processing server root directory>\CMDDB – directory needed for upgrading Dashboard views in step 14. For details on upgrading Dashboard views, see “Dashboard Views Upgrade” on page 85. ▶ <Mercury Business Availability Center Centers server root directory>\openldap\bdb – directory needed for upgrading LDAP in step 8. For details on backing up LDAP, see “Backing Up Monitor Configuration Data Files” on page 76. <p>In addition, backup any other files or directories you want to keep for security or historical purposes.</p>

Step	Description	Details
<p>3 If upgrading to Mercury Business Availability Center 6.6 using the existing Mercury Business Availability Center 5.x server machines, uninstall Mercury Business Availability Center 5.x.</p>	<p>Uninstall Mercury Business Availability Center 5.x from all machines.</p>	<ul style="list-style-type: none"> ▶ For Windows, select Start > Settings > Control Panel > Add/Remove Programs > Mercury Business Availability Center ▶ For Solaris, execute the commands: <code>cd <installation directory> /_uninst ./uninstall</code>
<p>4 In a Windows environment, install, in the following order, on all machines:</p> <ul style="list-style-type: none"> ▶ Mercury Business Availability Center 6.1 ▶ Mercury Business Availability Center 6.2 Add-on ▶ Mercury Business Availability Center 6.6 Add-on 	<p>Install each Mercury Business Availability Center on all machines, but do not connect to the database as part of the installation process.</p> <p>After each installation, do not start (enable) Mercury Business Availability Center.</p>	<p>For details on installing Mercury Business Availability Center 6.1, 6.2 Add-on, and 6.6 Add-on in a Windows environment, see “Installing Mercury Business Availability Center 6.1, the 6.2 Add-on, and the 6.6 Add-on on a Windows Platform” on page 49.</p>
<p>5 In a Solaris environment, first install Mercury Business Availability Center 6.2 on all machines and then install Mercury Business Availability Center 6.6 Add-on on all machines.</p>	<p>Install each Mercury Business Availability Center on all machines, but do not connect to the database as part of the installation process.</p> <p>After each installation, do not start (enable) Mercury Business Availability Center.</p>	<p>For details on installing Mercury Business Availability Center 6.2 and the 6.6 Add-on in a Solaris environment, see “Installing Mercury Business Availability Center 6.2 and the 6.6 Add-on on a Solaris Platform” on page 54.</p>

Step	Description	Details
6 Back up the databases.	Back up the existing management and profile databases.	For information on backing up your databases, refer to the database server documentation or to the Mercury Business Availability Center database administration document <i>Preparing the Database Environment</i> .
7 If you did not upgrade the database schema automatically at the end of installing the 6.6 Add-on in step 4 (Windows) or in step 5 (Solaris), run the database schema upgrade now.	Run dbupgrade from any one of the Mercury Business Availability Center 6.6 servers to verify and upgrade the management and profile databases to Mercury Business Availability Center 6.6 compatibility. Do not proceed to the next step until database upgrade has completed successfully.	See “Verifying and Upgrading the Database Schema” on page 59.
8 Connect each Mercury Business Availability Center 6.6 machine to the management database.	On each Mercury Business Availability Center 6.6 machine, run Connect to Database to connect to the upgraded management database. The first server to be connected should be the Mercury Business Availability Center 6.6 Centers Server designated for running LDAP. For information on LDAP, refer to <i>Preparing the Database Environment</i> .	<ul style="list-style-type: none"> ➤ In Windows, select Start Menu > Programs > Mercury Business Availability Center > Administration > Connect to Database. ➤ In Solaris, execute the command: <code><Topaz_Home_Dir>/scripts/setmngdbWizard.sh</code>

Step	Description	Details
<p>9 Upgrade LDAP.</p>	<p>Upgrade LDAP (Lightweight Directory Access Protocol) which is used to store Monitor Administration configuration data.</p>	<p>See “Retaining Monitor Administration Configuration Data” on page 75.</p> <p>If you are installing Mercury Business Availability Center on a new machine, run the following queries against the 6.6 management database to set the LDAP-designated server:</p> <pre>UPDATE SETTING_PARAMETERS SET SP_VALUE= 'ldap://HOST_NAME:9389' WHERE SP_NAME='ldap.host.and.port'</pre>
<p>10 Start Mercury Business Availability Center 6.6 on all machines.</p>	<p>Enable Mercury Business Availability Center 6.6 on all machines.</p> <p>It can take approximately 20-25 minutes for Mercury Business Availability Center to be available for login after starting all servers for the first time.</p>	<ul style="list-style-type: none"> ▶ For Windows – Select Start > Programs > Mercury Business Availability Center > Administration > Enable Business Availability Center. ▶ For Solaris – Execute the command: <Mercury Business Availability Center server root dir>/scripts/run_topaz start <p>Note: To verify that a server has successfully started on the server in question, look in <Mercury Business Availability Center server root dir>\log\jboss_boot.log file for a line that includes INFO - JBoss and Started in.</p>

Step	Description	Details
11 Reenter the Mercury Business Availability Center 6.6 license key.	After starting Mercury Business Availability Center for the first time, and before proceeding with the steps for upgrading your data, reenter the Mercury Business Availability Center 6.6 license key.	Select Admin > Platform > Setup and Maintenance > License Management and click New License Key . For information on updating the license key, see <i>Platform Administration</i> .
12 Check that data has been inserted into CMDB.	A few minutes after Mercury Business Availability Center 6.6 has been restarted, check that Adapters have inserted data in the CMDB.	From CMDB Administration , in the Source Manager tab, make sure that the Last Update column has a date for all the sources listed.
13 Upgrade configuration data.	Run all manual data upgrades.	See “Upgrading Configuration Data” on page 79.
14 Upgrade Dashboard views.	Run the Dashboard upgrade process.	See “Dashboard Views Upgrade” on page 85.
15 Upgrade XML File Source Adapter.	If you have any XML File source adapters, they must be upgraded manually.	See “Upgrading the Source Adapters from Mercury Business Availability Center 5.x” on page 116.
16 Synchronize the information in the CMDB.	Perform a hard sync in CMDB Administration.	Select Admin > CMDB > Source Manager . Click Hard Sync in the Default source adapters pane.
17 Upgrade SLAs.	Run the SLM upgrade process.	For details, see “Upgrading Service Level Management” on page 125.
18 Switch URLs on data collectors (only if upgrading to Mercury Business Availability Center 6.6 on new servers).	If you installed the Mercury Business Availability Center 6.6 on new machines with different URLs, switch the URLs on your data collectors to report to Mercury Business Availability Center 6.6 servers.	See “Switching Mercury Business Availability Center URL on the Data Collectors” on page 151.

Part I • Checklists for Upgrading to Mercury Business Availability Center 6.5

Step	Description	Details
19 Upgrade Mercury Business Availability Center components.	To benefit from the latest features, upgrade your Mercury Business Availability Center components to the most current version for Mercury Business Availability Center 6.6.	See “Upgrading Components” on page 157.

4

Upgrade Checklist - from 6.1.x to 6.6

This chapter describes what actions you need to perform before and during the upgrade from Mercury Business Availability Center 6.1.x to 6.6.

This chapter describes:	On page:
Before You Begin	29
Upgrade Checklist	30

Before You Begin

You should be aware of the following information before you begin the upgrade:

- ▶ The uninstall utility enables complete removal of Mercury Business Availability Center or rollback to the previous version (6.5, 6.4, 6.3, or 6.2). The database schema however, needs to be restored manually. For details on uninstalling, see *Deploying Servers*.
- ▶ Do not create any new databases between the database schema upgrade and the end of the full upgrade procedure. If you do so by mistake, please contact Mercury Customer Support.
- ▶ If you have any private patches for your current installation, you will lose them when you upgrade. If you have private patches that you want to continue to use, you should coordinate with Mercury Customer Support before beginning the upgrade process.

Upgrade Checklist

The following checklist should be used when upgrading from Mercury Business Availability Center 6.1.x to Mercury Business Availability Center 6.6:

Step	Description	Details
<p>1 (Shared CMDB) Begin preliminary steps to upgrade Mercury Application Mapping.</p>	<p>If you are working with a shared CMDB, you must do several steps to begin upgrading Mercury Application Mapping to version 6.6 before you begin upgrading Mercury Business Availability Center to 6.6.</p>	<p>Follow the instructions in “Upgrading Mercury Application Mapping: Version 6.x – 6.6 with a Shared CMDB” on page 176 up to the instruction to upgrade Mercury Business Availability Center (step 5).</p>
<p>2 Shut down existing Mercury Business Availability Center 6.1.x servers.</p>	<p>Stop the Mercury Business Availability Center service on each of the old Mercury Business Availability Center servers. Make sure there are no open connections to Mercury Business Availability Center databases.</p>	<ul style="list-style-type: none"> ▶ In Windows, select Start > Programs > Mercury Business Availability Center > Administration > Disable Business Availability Center. ▶ In Solaris, execute the command: <Mercury Business Availability Center server root dir>/scripts/run_topaz stop

Step	Description	Details
3 Back up files.	Back up various files and directories that are required during the upgrade process, or as a precautionary measure.	Back up the following files and directories: <ul style="list-style-type: none"> ▶ <Mercury Business Availability Center server root directory>\conf\TopazInfra.ini ▶ <Mercury Business Availability Center Modeling Data Processing server root directory>\C MDB ▶ <Mercury Business Availability Center Centers server root directory>\openldap\bdb <p>In addition, backup any other files or directories you want to keep for security or historical purposes.</p>
4 Stop the Web server process on Mercury Business Availability Center servers.	Stop the IIS Admin Service for IIS, or Apache service for Apache Web Server, on all Mercury Business Availability Center servers.	For details, refer to your Web server documentation.
5 First install the Mercury Business Availability Center 6.2 Add-on on all machines. Next, install the Mercury Business Availability Center 6.6 Add-on on all machines.	Install the Mercury Business Availability Center 6.2 and then the 6.6 Add-on on all machines. After each installation, do not start (enable) Mercury Business Availability Center.	For additional details on installing Mercury Business Availability Center 6.6, see “Installing Mercury Business Availability Center 6.1, the 6.2 Add-on, and the 6.6 Add-on on a Windows Platform” on page 49 or “Installing Mercury Business Availability Center 6.2 and the 6.6 Add-on on a Solaris Platform” on page 54.

Step	Description	Details
<p>6 Restart the Web server process on Mercury Business Availability Center servers.</p>	<p>Restart the IIS Admin Service for IIS, or Apache service for Apache Web Server, on all Mercury Business Availability Center servers.</p>	<p>For details, refer to your Web server documentation.</p>
<p>7 Back up the databases.</p>	<p>Back up the existing management and profile databases.</p>	<p>For information on backing up your databases, refer to the database server documentation or to the Mercury Business Availability Center database administration document <i>Preparing the Database Environment</i>.</p>
<p>8 If you did not upgrade the database schema automatically at the end of installing the 6.6 Add-on in step 5, run the database schema upgrade.</p>	<p>Run dbupgrade from any one of the Mercury Business Availability Center 6.6 servers to verify and upgrade the management and profile databases to Mercury Business Availability Center 6.6 compatibility.</p> <p>Do not proceed to the next step until database upgrade has completed successfully.</p>	<p>See “Verifying and Upgrading the Database Schema” on page 59.</p>
<p>9 Connect each Mercury Business Availability Center 6.6 machine to the management database.</p>	<p>On each Mercury Business Availability Center 6.6 machine, run Connect to Database to connect to the upgraded management database.</p> <p>The first server to be connected should be the Mercury Business Availability Center 6.6 Centers Server designated for running LDAP. For information on LDAP, refer to <i>Preparing the Database Environment</i>.</p>	<ul style="list-style-type: none"> ▶ In Windows, select Start Menu > Programs > Mercury Business Availability Center > Administration > Connect to Database. ▶ In Solaris, execute the command: <Mercury Business Availability Center server root dir>/scripts/setmngdbWizard.sh

Step	Description	Details
10 Delete previously compiled .jsp files.	This is required to ensure proper functionality of Mercury Business Availability Center once servers are started.	Delete the contents of the directory <Mercury Business Availability Center root directory>\EJBContainer\server\mercury\work , if this directory exists.
11 Start Mercury Business Availability Center 6.6 on all machines.	<p>Enable Mercury Business Availability Center 6.6 on all machines.</p> <p>It can take approximately 20-25 minutes for Mercury Business Availability Center to be available for login after starting all servers for the first time.</p>	<ul style="list-style-type: none"> ▶ In Windows, select Start > Programs > Mercury Business Availability Center > Administration > Enable Business Availability Center ▶ In Solaris, execute the command: <Mercury Business Availability Center server root dir>/scripts/run_topaz start <p>In both Windows and Solaris, verify that the server has successfully started. On the server in question, look in <Mercury Business Availability Center root directory>\log\jboss_boot.log file for a line that includes INFO - JBoss and Started in.</p>
12 Reenter the Mercury Business Availability Center 6.6 license key.	After starting Mercury Business Availability Center for the first time, reenter the Mercury Business Availability Center 6.6 license key.	<p>Select Admin > Platform > Setup and Maintenance > License Management and click New License Key.</p> <p>For information on updating the license key, see <i>Platform Administration</i>.</p>

Step	Description	Details
<p>13 Check that data has been inserted into CMDB.</p>	<p>A few minutes after Mercury Business Availability Center 6.6 has been restarted, check that source adapters have inserted data in the CMDB.</p>	<p>From CMDB Administration, in the Source Manager tab, make sure that the Last Update column has a date for all the sources listed.</p>
<p>14 Upgrade source adapters.</p>	<p>Perform the manual procedure that upgrades 6.1 source adapters to 6.6 compatibility.</p>	<p>For details, see “Upgrading the Source Adapters from Mercury Business Availability Center 6.x” on page 115.</p>
<p>15 Restart Mercury Business Availability Center on the Data Processing Server.</p>	<p>Restart Mercury Business Availability Center on the Data Processing Server machine.</p> <p>In a distributed architecture, restart Mercury Business Availability Center on the Modeling Data Processing Server machine.</p>	<ul style="list-style-type: none"> ➤ In Windows: <ul style="list-style-type: none"> ◆ to stop Mercury Business Availability Center, select Start > Programs > Mercury Business Availability Center > Administration > Disable Business Availability Center. ◆ to restart, select Start > Programs > Mercury Business Availability Center > Administration > Enable Business Availability Center. ➤ In Solaris: <ul style="list-style-type: none"> ◆ to stop Mercury Business Availability Center, execute the command: <Mercury Business Availability Center server root dir>/scripts/run_topaz stop ◆ to restart, execute the command: <Mercury Business Availability Center server root dir>/scripts/run_topaz start

Step	Description	Details
16 (Shared CMDB) Upgrade Mercury Application Mapping to version 6.6.	Upgrade Mercury Application Mapping to version 6.6 (if you have not already done so).	Continue from step 5 in “Upgrading Mercury Application Mapping: Version 6.x – 6.6 with a Shared CMDB” on page 176. When you have finished all steps in the Mercury Application Mapping upgrade procedure, continue with the next step in this checklist.
17 Upgrade Mercury Business Availability Center components.	To benefit from the latest features, upgrade your Mercury Business Availability Center components to the most current version for Mercury Business Availability Center 6.6.	See “Upgrading Components” on page 157.
18 Verify that IIS topology view is not corrupted.	If your pre-version 6.6 CMDB included the IIS topology view, verify that it is not corrupted after the upgrade procedure. If it is, manually undeploy the IIS discovery package and then redeploy it.	For details, see “Redeploying and Undeploying Packages” on page 182.

Step	Description	Details
<p>19 Set KPI Over Time flag for existing CI Types configured in Problem Isolation.</p>	<p>To set the KPI Over Time flag, perform this procedure in http://<Data Processing Server machine name>:8080/jmx-console.</p>	<p>To upgrade the flag:</p> <ol style="list-style-type: none"> 1 In the JMX MBean View window, in the Topaz section, click service=CMDBClassModel Services. 2 In updateClassModel FromFolder operation pane, do the following: <ul style="list-style-type: none"> ◆ in customerID, enter 1 ◆ in folderPath, enter <Mercury Business Availability Center root directory>\CMDB\class model\deployment 3 Click Invoke. <p>An informational message is displayed when the KPI Over Time flag has been upgraded.</p>

5

Upgrade Checklist - from 6.2/6.3/6.4/6.5 to 6.6

This chapter describes what actions you must perform to upgrade from Mercury Business Availability Center 6.2/6.3/6.4/6.5 to Mercury Business Availability Center 6.6.

This chapter describes:	On page:
Before You Begin	37
Upgrade Checklist	38

Before You Begin

You should be aware of the following information before you begin the upgrade.

- ▶ The uninstall utility enables complete removal of Mercury Business Availability Center or rollback to the previous version (6.5, 6.4, 6.3, or 6.2). The database schema however, needs to be restored manually. For details on uninstalling, see *Deploying Servers*.
- ▶ Do not create any new databases between the database schema upgrade and the end of the full upgrade procedure. If you do so by mistake, please contact Mercury Customer Support.
- ▶ If you have any private patches for your current installation, you will lose them when you upgrade. If you have private patches that you want to continue to use, you should coordinate with Mercury Customer Support before beginning the upgrade process.

Upgrade Checklist

The following checklist should be used when upgrading from Mercury Business Availability Center 6.2/6.3/6.4/6.5 to Mercury Business Availability Center 6.6:

Step	Description	Details
<p>1 (Shared CMDB) Begin preliminary steps to upgrade Mercury Application Mapping.</p>	<p>If you are working with a shared CMDB, you must do several steps to begin upgrading Mercury Application Mapping to version 6.6 before you begin upgrading Mercury Business Availability Center to 6.6.</p>	<p>Follow the instructions in “Upgrading Mercury Application Mapping: Version 6.x – 6.6 with a Shared CMDB” on page 176 up to the instruction to upgrade Mercury Business Availability Center (step 5).</p>
<p>2 Shut down existing Mercury Business Availability Center 6.2/6.3/6.4/6.5 servers.</p>	<p>Stop the Mercury Business Availability Center service on each of the old Mercury Business Availability Center servers. Make sure there are no open connections to Mercury Business Availability Center databases.</p>	<ul style="list-style-type: none"> ▶ In Windows, select Start > Programs > Mercury Business Availability Center > Administration > Disable Business Availability Center ▶ In Solaris, execute the command: <code><Mercury Business Availability Center server root dir>/scripts/run_topaz stop</code>

Step	Description	Details
3 Back up files.	Back up various files and directories that are required during the upgrade process, or as a precautionary measure.	Back up the following files and directories: <ul style="list-style-type: none"> ▶ <Mercury Business Availability Center server root dir>\conf\ TopazInfra.ini ▶ <Mercury Business Availability Center Modeling Data Processing server root dir>\CMDB ▶ <Mercury Business Availability Center Centers server root directory>\ openldap\bdb <p>In addition, backup any other files or directories you want to keep for security or historical purposes.</p>
4 Stop the Web server process on Mercury Business Availability Center servers.	Stop the IIS Admin Service for IIS, or Apache service for Apache Web Server, on all Mercury Business Availability Center servers.	For details, refer to your Web server documentation.
5 Install the Mercury Business Availability Center 6.6 Add-on on all machines.	On a Windows platform, you are prompted to upgrade the database schema. After installation, do not start (enable) Mercury Business Availability Center 6.6.	
6 Restart the Web server process on Mercury Business Availability Center servers.	Restart the IIS Admin Service for IIS, or Apache service for Apache Web Server, on all Mercury Business Availability Center servers.	For details, refer to your Web server documentation.

Step	Description	Details
<p>7 Back up the databases.</p>	<p>Back up the existing management and profile databases.</p>	<p>For information on backing up your databases, refer to the database server documentation or to the Mercury Business Availability Center database administration document <i>Preparing the Database Environment</i>.</p>
<p>8 If you did not upgrade the database schema automatically at the end of installing the 6.6 Add-on in step 5, run the database schema upgrade now.</p>	<p>Run dbupgrade from any one of the Mercury Business Availability Center 6.6 servers to verify and upgrade the management and profile databases to Mercury Business Availability Center 6.6 compatibility.</p> <p>Do not proceed to the next step until database upgrade has completed successfully.</p>	<p>See “Verifying and Upgrading the Database Schema” on page 59.</p>
<p>9 Connect each Mercury Business Availability Center 6.6 machine to the management database.</p>	<p>On each Mercury Business Availability Center 6.6 machine, run Connect to Database to connect to the upgraded management database.</p> <p>The first server to be connected should be the Mercury Business Availability Center 6.6 Centers Server designated for running LDAP. For information on LDAP, refer to <i>Preparing the Database Environment</i>.</p>	<ul style="list-style-type: none"> ▶ In Windows, select Start Menu > Programs > Mercury Business Availability Center > Administration > Connect to Database. ▶ In Solaris, execute the command: <Mercury Business Availability Center server root dir>/scripts /setmngdbWizard.sh
<p>10 Delete previously compiled .jsp files.</p>	<p>This is required to ensure proper functionality of Mercury Business Availability Center once servers are started.</p>	<p>Delete the contents of the directory <Mercury Business Availability Center root directory>\EJBContainer\server\mercury\work, if this directory exists.</p>

Step	Description	Details
<p>11 Start Mercury Business Availability Center 6.6 on all machines.</p>	<p>Enable Mercury Business Availability Center 6.6 on all machines.</p> <p>It can take approximately 20-25 minutes for Mercury Business Availability Center to be available for login after starting all servers for the first time.</p>	<ul style="list-style-type: none"> ▶ In Windows, select Start > Programs > Mercury Business Availability Center > Administration > Enable Business Availability Center ▶ In Solaris, execute the command: <Mercury Business Availability Center server root dir>/scripts/run_topaz start <p>In both Windows and Solaris, verify that the server has successfully started. On the server in question, look in <Mercury Business Availability Center root directory>\log\jboss_boot.log file for a line that includes INFO - JBoss and Started in.</p>
<p>12 If needed, reenter the Mercury Business Availability Center 6.6 license key.</p>	<p>After starting Mercury Business Availability Center for the first time, you may need to reenter the Mercury Business Availability Center 6.6 license key.</p>	<p>Select Admin > Platform > Setup and Maintenance > License Management and click New License Key.</p> <p>For information on updating the license key, see <i>Platform Administration.</i></p>
<p>13 Check that data has been inserted into CMDB.</p>	<p>A few minutes after Mercury Business Availability Center 6.6 has been restarted, check that source adapters have inserted data in the CMDB.</p>	<p>From CMDB Administration, in the Source Manager tab, make sure that the Last Update column has a date for all the sources listed.</p>
<p>14 Upgrade source adapters.</p>	<p>Perform the manual procedure that upgrades 6.2, 6.3, 6.4, and 6.5 source adapters to 6.6 compatibility.</p>	<p>For details, see “Upgrading the Source Adapters from Mercury Business Availability Center 6.x” on page 115.</p>

Step	Description	Details
<p>15 Upgrade My BAC.</p>	<p>Upgrade My BAC 6.2/6.3/6.4/6.5 to My BAC 6.6 to provide support for SOA and CMDB portlets.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ Upgrading My BAC overrides the default module, Default Fallback Module, that was in BAC before the upgrade. Changes that you made to that module are lost when you upgrade to version 6.6. ▶ If you do not upgrade My BAC, SOA and CMDB portlets are not available in My BAC 6.6 portlet definitions. All other portlets are available. 	<p>For details on upgrading My BAC, see “Upgrading My BAC” in <i>My BAC Administration</i>.</p>

Step	Description	Details
<p>16 Restart Mercury Business Availability Center on the Data Processing Server.</p>	<p>Restart Mercury Business Availability Center on the Data Processing Server machine. In a distributed architecture, restart Mercury Business Availability Center on the Modeling Data Processing Server machine.</p>	<ul style="list-style-type: none"> ➤ In Windows: <ul style="list-style-type: none"> ◆ to stop Mercury Business Availability Center, select Start > Programs > Mercury Business Availability Center > Administration > Disable Business Availability Center ◆ to restart, select Start > Programs > Mercury Business Availability Center > Administration > Enable Business Availability Center ➤ In Solaris: <ul style="list-style-type: none"> ◆ to stop Mercury Business Availability Center, execute the command: <Mercury Business Availability Center server root dir>/scripts/run_topaz stop ◆ to restart, execute the command: <Mercury Business Availability Center server root dir>/scripts/run_topaz start
<p>17 (Shared CMDB) Upgrade Mercury Application Mapping to version 6.6</p>	<p>Upgrade Mercury Application Mapping to version 6.6 (if you have not already done so).</p>	<p>Continue with step 5 in “Upgrading Mercury Application Mapping: Version 6.x – 6.6 with a Shared CMDB” on page 176. When finished all steps in the Mercury Application Mapping upgrade procedure, continue with the next step in this checklist.</p>

Step	Description	Details
<p>18 Upgrade Mercury Business Availability Center components.</p>	<p>To benefit from the latest features, upgrade your Mercury Business Availability Center components to the most current version for Mercury Business Availability Center 6.6.</p>	<p>For details, see “Upgrading Components” on page 157.</p>
<p>19 Verify that IIS topology view is not corrupted.</p>	<p>If your pre-version 6.6 CMDB included the IIS topology view, verify that it is not corrupted after the upgrade procedure. If it is, manually undeploy the IIS discovery package and then redeploy it.</p>	<p>For details, see “Redeploying and Undeploying Packages” on page 182.</p>
<p>20 Set KPI Over Time flag for existing CI Types configured in Problem Isolation.</p>	<p>To set the KPI Over Time flag, perform this procedure in http://<Data Processing Server machine name>:8080/jmx-console.</p>	<p>To upgrade the flag:</p> <ol style="list-style-type: none"> 1 In the JMX MBean View window, in the Topaz section, click service=CMDBClassModel Services. 2 In updateClassModel FromFolder operation pane, do the following: <ul style="list-style-type: none"> ◆ in customerID, enter 1 ◆ in folderPath, enter <Mercury Business Availability Center root directory>\CMDB\classmodel\deployment 3 Click Invoke. <p>An informational message is displayed when the KPI Over Time flag has been upgraded.</p>

Part II

Upgrade Procedures

6

Upgrading the Servers

This chapter describes how to upgrade your servers to Mercury Business Availability Center 6.6.

This chapter describes:	On page:
Server Architecture for Mercury Business Availability Center	48
Upgrading Considerations	48
Installing Mercury Business Availability Center 6.1, the 6.2 Add-on, and the 6.6 Add-on on a Windows Platform	49
Installing Mercury Business Availability Center 6.2 and the 6.6 Add-on on a Solaris Platform	54

Note:

- ▶ If you are running Topaz 4.5 FP2 or Mercury Business Availability Center 5.x in a Windows environment, install Mercury Business Availability Center 6.1, on top of it install the 6.2 Add-on, and then install the 6.6 Add-on.
 - ▶ If you are running Topaz 4.5.2 in a Solaris environment, direct upgrade from Topaz 4.5 FP2 to Mercury Business Availability Center 6.6 on Solaris is not supported. If you require this upgrade scenario, contact Mercury Customer Support.
 - ▶ If you are running Mercury Business Availability Center 5.x in a Solaris environment, you need to install Mercury Business Availability Center 6.2 and then install the 6.6 Add-on.
-

Server Architecture for Mercury Business Availability Center

In Mercury Business Availability Center 6.x, the server types are:

- ▶ **Centers Server.** This server is mainly responsible for running the Mercury Business Availability Center applications, reporting and the Administration Console.
- ▶ **Core Server.** This server is mainly responsible for receiving data samples from the data collectors and distributing the data to the various Mercury Business Availability Center components.
- ▶ **Data Processing Server.** This server is mainly responsible for processing the data received from the data collectors.

The Mercury Business Availability Center servers can be deployed on a single machine, or in a distributed environment where each server (or multiple instances of each server) are deployed on separate machines.

When upgrading, you must consider how you want to migrate your existing architecture to suit the new server structure, keeping in mind requirements for a load balanced and/or high availability system. For more information, refer to *Deploying Servers*.

Upgrading Considerations

You can install Mercury Business Availability Center on new machines or on the same machine(s) on which your current system is running.

If installing Mercury Business Availability Center on existing servers, part of the upgrade process requires uninstalling your current system from all the servers. For details on uninstalling your current system, refer to the relevant system documentation. In addition, make sure your old machine(s) meet all current system requirements.

If installing Mercury Business Availability Center on new machines, bear in mind that the Data Processing Server is a new server as of Mercury Business Availability Center 6.0 and you may require an additional machine (for distributed environments). In addition, make sure your new machine(s) meet all current system requirements.

Note: During downtime, data collectors continue to collect data, but it is not sent to the database; alerts are not generated.

Installing Mercury Business Availability Center 6.1, the 6.2 Add-on, and the 6.6 Add-on on a Windows Platform

If you are installing on a machine previously used for a Topaz or Mercury Business Availability Center server, make sure that the previous installation has been fully removed. Refer to your system documentation for uninstall procedures.

For more information on installing Mercury Business Availability Center servers, refer to the chapters on installing servers on a Windows platform in *Deploying Servers*.

You install Mercury Business Availability Center 6.1 servers—the Centers Server, Core Server, and Data Processing Server—from the Mercury Business Availability Center 6.1 Setup CD-ROM provided with the Mercury Business Availability Center distribution package.

After upgrading to Mercury Business Availability Center 6.1, upgrade to Mercury Business Availability Center 6.2 from the Add-on CD-ROM.

Version 6.6 is available from the Mercury Business Availability Center 6.6 release download area.

Unless you install on a machine running IIS, Mercury Business Availability Center installs Apache HTTP Server (adapted for Mercury Business Availability Center) during the installation process.

You need administrative privileges for the machines on which you are installing Mercury Business Availability Center servers.

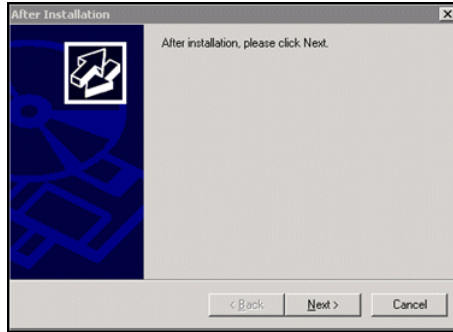
Note: For installation troubleshooting, refer to the Mercury Customer Support Knowledge Base, which can be accessed from the Mercury Business Availability Center Help menu or from the Mercury Customer Support Web site.

To install Mercury Business Availability Center servers on a Windows platform:

- 1** Insert the Mercury Business Availability Center 6.1 Windows Setup CD-ROM into the drive from which you want to install. If you are installing from a network drive, connect to it.
- 2** From the **Start** menu, select **Run**.
- 3** Type the location from which you are installing, followed by **setup.exe**. Note that the setup file for Mercury Business Availability Center servers is located in the CD-ROM root directory. For example, type `d:\setup.exe`.
- 4** Click **OK**. If Mercury Business Availability Center detects a previous Topaz or Mercury Business Availability Center installation on the machine, a message is displayed warning that any customized configuration data will be overwritten.
- 5** Setup begins. Follow the on-screen instructions for server installation.

Note the following during the server installation stage:

- ▶ **Installing on a Windows platform with remote services running in application server mode:**
 - ◆ The following window will appear if Windows detects a wrong user mode for the installation:



Click **Next** when the installation is complete and follow any other instructions that may appear in the window.

For more information on this subject, refer to Microsoft Knowledge Base Article – 252330.

- ▶ **Selecting the setup type:**
 - ◆ Select **Typical** setup type for a standard (Mercury Business Availability Center box) installation that installs the Core Server, Centers Server, and Data Processing Server on the machine, as well as MDAC.
 - ◆ Select **Custom** setup type to select the Mercury Business Availability Center features to be installed on the machine. For more information, refer to *Deploying Servers*.
- ▶ **Selecting the Web server type:**
 - ◆ If Mercury Business Availability Center does not detect an installation of Microsoft IIS on the machine, you are offered the **Apache HTTP Server** option only. If you want to run Mercury Business Availability Center with Microsoft IIS, click **Cancel** to exit Mercury Business Availability Center Setup. Install IIS and rerun the Mercury Business Availability Center installation.

► **Configuring connection settings:**

- ◆ For Apache HTTP Server – if port 80 (default port) is already in use by the existing Web server, Mercury Business Availability Center notifies you of this. Resolve the conflict by either entering a different port number (in which case, Mercury Business Availability Center configures Apache HTTP Server to use the defined port), or exiting Setup and changing the port number of the existing Web server, then rerunning the installation procedure. For more information, refer to *Deploying Servers*.
- ◆ For Microsoft IIS – if IIS is using a port other than port 80, enter the IIS port.

► **Specifying the SMTP mail server:**

- ◆ It is recommended that you specify the complete Internet address of your SMTP server. Use only alphanumeric characters.
- ◆ In the Sender name box, specify the name to appear in scheduled reports and on alert notices that Mercury Business Availability Center sends. Accept the default name (“MercuryAM_Alert_Manager”) or type another sender name.

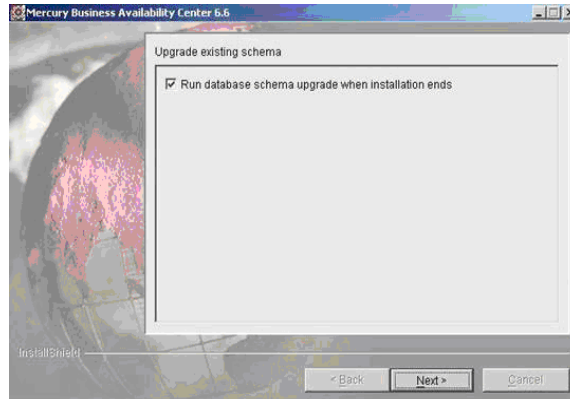
- 6** When Setup has completed the installation of the Mercury Business Availability Center server files, you are prompted as to whether you want to continue with the set management database stage immediately, or finish the server installation and set database parameters later.

Do not set the management database or restart servers at this stage. See the appropriate checklist for the correct sequence for connecting to the management database.

- 7** Install the Mercury Business Availability Center 6.2 Add-on from the Add-on CD-ROM.
- 8** Download the Mercury Business Availability Center 6.6 Add-on from the Mercury Business Availability Center 6.6 release download area.

9 Install the Mercury Business Availability Center 6.6 Add-on.

During the installation, you are asked about upgrading the existing database schema.



By default, the check box is checked. When the 6.6 Add-on installation ends, the database schema is automatically upgraded for Mercury Business Availability Center 6.6.

Important: It is highly recommended to keep the check box checked to enable automatic database schema upgrade. Failure to upgrade the database schema results in Mercury Business Availability Center not working properly.

If, for some reason, you do not want to automatically upgrade the database schema at this point, you can manually upgrade the schema later in the upgrade process with the dbupgrade utility. The upgrade check list directs you when to manually upgrade the schema.

Installing Mercury Business Availability Center 6.2 and the 6.6 Add-on on a Solaris Platform

Note: If you are running Mercury Business Availability Center 5.x in a Solaris environment, you upgrade your servers directly to Mercury Business Availability Center 6.2.

If you are installing on a machine previously used for a Topaz or Mercury Business Availability Center server, make sure that the previous installation has been fully removed. Refer to your system documentation for uninstall procedures.

For more information on installing Mercury Business Availability Center servers, refer to “Installing Mercury Business Availability Center Servers on a Solaris Platform” in *Deploying Servers*.

You install Mercury Business Availability Center 6.2 servers—the Centers Server, Core Server, and Data Processing Server—from the Mercury Business Availability Center 6.2 Solaris Setup CD-ROM provided with the Mercury Business Availability Center distribution package.

Version 6.6 is available from the Mercury Business Availability Center 6.6 release download area.

Unless you install on a machine running Sun Java System Web Server, Mercury Business Availability Center installs Apache HTTP Server (adapted for Mercury Business Availability Center) during the installation process.

You must be a root user to install Mercury Business Availability Center servers.

Note: For installation troubleshooting, refer to the Mercury Customer Support Knowledge Base, which can be accessed from the Mercury Business Availability Center Help menu or from the Mercury Customer Support Web site.

In addition, refer to the Mercury Business Availability Center readme file located in the Mercury Business Availability Center 6.2 Solaris Setup CD-ROM root directory for the latest technical and troubleshooting information.

To install Mercury Business Availability Center servers on a Solaris platform:

- 1** Log into the server as user **root**.
- 2** Insert **Mercury Business Availability Center 6.2 Solaris Setup Disk** CD-ROM into the drive from which you want to install. If you are installing from a network drive, mount it.
- 3** Move to the root directory of the CD-ROM drive.
- 4** Run one of the following scripts:
 - ◆ To install in UI mode:

```
./solv4_setup.sh
```

- ◆ To install in console mode:

```
./solv4_setup.sh -console
```

Select options by entering the option number. The selected option is marked with an [X].

- 5** The installation begins. Follow the on-screen instructions for server installation. Note the following during the server installation stage:

◆ **Selecting the setup type:**

- Select **Typical** for a standard (Mercury Business Availability Center box) installation that installs the Core Server, Centers Server, and Data Processing Server on the machine.
- Select **Custom** to select the Mercury Business Availability Center features installed on the machine.

◆ **Setting connection settings:**

- Apache HTTP Server – if port 80 (default port) is already in use, Mercury Business Availability Center notifies you of this.
- Sun Java System Web Server – if using a port other than port 80 (the default port), enter the number.

◆ **Specifying the SMTP mail server:**

- It is recommended that you specify the complete Internet address of your SMTP server. Use only alphanumeric characters.
- In the Sender name box, specify the name to appear in scheduled reports and on alert notices that Mercury Business Availability Center sends. Accept the default name **MercuryAM_Alert_Manager** or type another sender name.

◆ **Specifying user and group:**

If either the user or group that you specify are not found, choose one of the following options:

- **Exit installation.** Exits Setup so that you can create the user/group, and run Setup again.
- **Select a new user/group.** Enables you to enter a new user and/or group.
- **Allow Setup to create the user/group.** Setup creates a user and/or group on the local host.

- 6 When Setup has completed the installation of the Mercury Business Availability Center server files, you are prompted as to whether you want to continue with the set management database stage immediately, or finish the server installation and set database parameters later.

Do not set the management database at this stage. See the appropriate checklist for your version upgrade for the correct sequence to connect to the management database.

- 7** Download the Mercury Business Availability Center 6.6 Add-on from the Mercury Business Availability Center 6.6 release download area.
- 8** Install the Mercury Business Availability Center 6.6 Add-on.

7

Verifying and Upgrading the Database Schema

This chapter describes the methodology for upgrading your database schema to Mercury Business Availability Center 6.6.

This chapter describes:	On page:
Introducing Upgrade Methodology	60
Using the Verify and Upgrade Utility	60
Verifying the Database Schema	63
Upgrading the Database Schema	68
Creating Database Users for the Upgrade Procedure	71
Troubleshooting Database Schema Verify and Upgrade Errors	72

Introducing Upgrade Methodology

It is recommended that you upgrade the database schema in the correct sequence according to the upgrade checklists.

To access the database schema verify and upgrade utility in Mercury Business Availability Center, select **Start > Programs > Mercury Business Availability Center > Administration > Upgrade Database Schema**.

Important:

- ▶ Check that your current database server version is supported for Mercury Business Availability Center. For details on supported and recommended database servers, refer to *Preparing the Database Environment*.
 - ▶ Ensure that you have backed up your management and profile databases before running the database schema upgrade stage.
 - ▶ Once you run the database upgrade process, it is not possible to restore the databases to their pre-upgrade state. For details, refer to *Preparing the Database Environment*.
-

Using the Verify and Upgrade Utility

The database schema verify and upgrade utility runs the verify program and the upgrade program in two separate stages:

- ▶ **verify stage**. For details, see “Verify Stage” on page 61.
- ▶ **upgrade stage**. For details, see “Upgrade Stage” on page 62.

If errors occur during either stage, troubleshoot them, and then rerun the utility. For details, see “Troubleshooting Database Schema Verify and Upgrade Errors” on page 72.

Note:

- ▶ If you are running the database verify program on Oracle 10g schemas and use Oracle datapump utilities to import or export the target schemas, ensure that you do not have any active datapump jobs running against the target schemas.
 - ▶ If you do have datapump tables in the target schemas, they should be dropped prior to running the database schema verification program.
 - ▶ It is recommended to assign an administrator schema to perform datapump operations and not to use Mercury Business Availability Center schemas as the login. By assigning an administrator schema to perform datapump operations, you do not have to grant additional permissions to Mercury Business Availability Center schemas and the datapump tables will be created in the administrator schema.
-

If you want to verify the database after upgrading to Mercury Business Availability Center (for example, to debug database upgrade problems), see Appendix D, “Database Schema Verification” in *Preparing the Database Environment*.

Verify Stage

The utility first runs the database verify stage. This stage does not involve downtime for your system. The verify program checks that there are no problems with the existing databases, and that they can be upgraded.

For example, the program checks that there is no corruption and that there is sufficient storage space. The program also checks for possible lengthy operations that could slow down the upgrade process and notifies you of the estimated time they may take.

The verify program asks you for a user name and password that can access the master database; this is required for certain (read-only) tests to be performed. If you do not want to supply your DBA account user name and password, you can create a user name with the minimum privileges required for dbverify to operate. For details on how to create this user, see “Creating Database Users for the Upgrade Procedure” on page 71.

Notes

- ▶ During the verify stage, browse to the previous version of the **TopazInfra.ini** file from which you are upgrading.

In Mercury Business Availability Center versions 4.5.x, this file is in **<Topaz root directory>\conf** directory.

In Mercury Business Availability Center versions 5.x and later, this file is in **<Mercury Business Availability Center>\conf** directory.

Make sure you have a copy of this file accessible to the Mercury Business Availability Center machine on which you will be running the database verify utility.

- ▶ You will be prompted for a user name and password for each database server on which the management and profile databases reside.

Upgrade Stage

If the verification is successful, you are asked if you want to continue with the database schema upgrade program, which upgrades the management database and the profile databases to the latest version schema.

The upgrade stage necessitates a short amount of downtime for the Mercury Business Availability Center servers, unless lengthy operations have been detected. The verify stage preceding the upgrade should have informed you of the estimated time required for any lengthy operations it detects.

Note: There must be no open connections to the databases during the database schema upgrade.

Verifying the Database Schema

You run the database schema verify utility from a Mercury Business Availability Center server machine.

Announce system downtime, then stop all Mercury Business Availability Center servers by stopping the Mercury Business Availability Center service on each of the server machines. If you have any additional open connections to the databases (for example, additional connections that are not part of usual functioning or open connections from Mercury Application Mapping), close them.

On a Solaris platform, you must run the database schema verify utility **dbverify** from a machine that supports UI mode, and make sure that the DISPLAY environment variable is properly configured on the machine. For example:

```
setenv DISPLAY <terminal host name>:0.0
```

To verify databases:

- 1 From any of the Mercury Business Availability Center servers, select **Start > Programs > Mercury Business Availability Center > Administration > Upgrade Database Schema**. The database verify program starts.

Run the verify program according to your operating platform:

Copy the **dbverify** directory from the Mercury Business Availability Center Windows (or Solaris) Documentation & Utilities CD-ROM supplied with your package, (<**CD root directory**>\tools_and_utilities), to the local disk on your Mercury Business Availability Center server machine, or Core Server machine if you have a distributed deployment.

- ◆ If you are running dbverify from a Windows platform, open a command prompt (**Start > Programs > Accessories > Command Prompt**) and enter the path to the local copy of the **dbverify\bin** folder.

Enter the command:

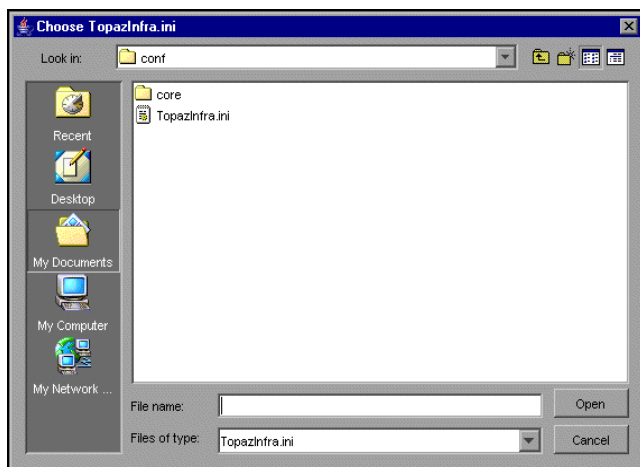
```
run_schema_upgrade.bat
```

- ◆ If you are running dbverify from a Solaris platform, make sure that the DISPLAY environment variable is set. Open an X-terminal window and move to the location of the local copy of the dbverify directory, then type:

```
./run_schema_upgrade.sh
```

The database verify program starts.

- 2 In the Choose TopazInfra.ini dialog box, browse to the **TopazInfra.ini** file that you copied from your previous version.



3 Specify the details required to connect to the appropriate database:

- ◆ In the SQL Master Connection dialog box, specify the details required to connect to the Master database.

In the **User** and **Password** boxes, type the user name and password of a user with permissions for the database. (The User box displays the default MS SQL Server administrator user name, **sa**. By default, there is no password.) Click **OK**.

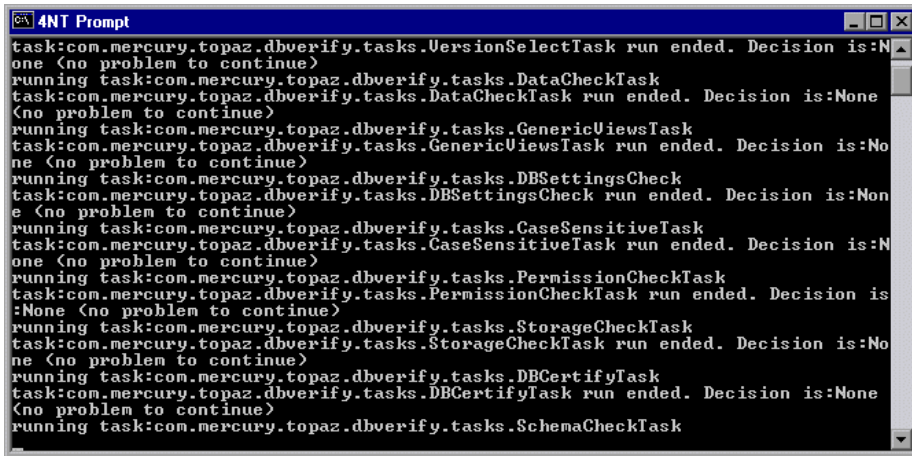
- ◆ In the Oracle Dictionary Connection dialog box, specify the details required to connect to the Oracle database.

In the **User** and **Password** text boxes, type the user name and password of a user with permissions for the database, and click **OK**.

Note:

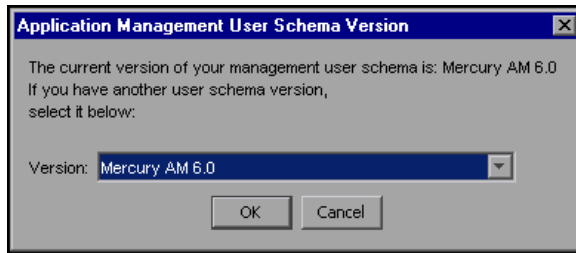
- ▶ You will be prompted for connection data for each different server on which your management and profile databases reside.
 - ▶ If you do not want to supply your database administrator account user name and password, you can create a user name with the minimum privileges required for the verify program to operate. For details on how to create this user, see “Creating Database Users for the Upgrade Procedure” on page 71.
-

- 4 The database verify program performs database verification. You can view the progress of the verify process in a command prompt window.



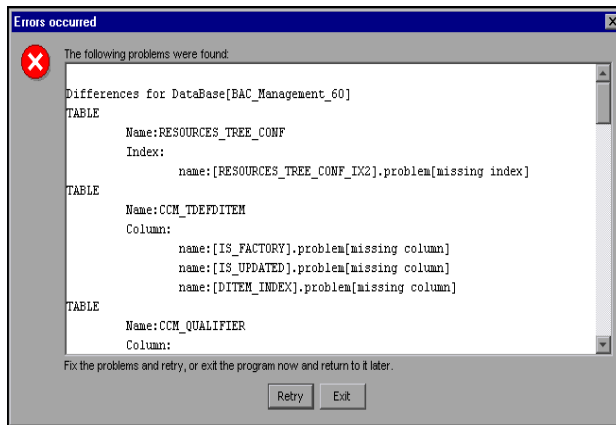
```
task:com.mercury.topaz.dbverify.tasks.VersionSelectTask run ended. Decision is:None (no problem to continue)
running task:com.mercury.topaz.dbverify.tasks.DataCheckTask
task:com.mercury.topaz.dbverify.tasks.DataCheckTask run ended. Decision is:None (no problem to continue)
running task:com.mercury.topaz.dbverify.tasks.GenericViewsTask
task:com.mercury.topaz.dbverify.tasks.GenericViewsTask run ended. Decision is:None (no problem to continue)
running task:com.mercury.topaz.dbverify.tasks.DBSettingsCheck
task:com.mercury.topaz.dbverify.tasks.DBSettingsCheck run ended. Decision is:None (no problem to continue)
running task:com.mercury.topaz.dbverify.tasks.CaseSensitiveTask
task:com.mercury.topaz.dbverify.tasks.CaseSensitiveTask run ended. Decision is:None (no problem to continue)
running task:com.mercury.topaz.dbverify.tasks.PermissionCheckTask
task:com.mercury.topaz.dbverify.tasks.PermissionCheckTask run ended. Decision is:None (no problem to continue)
running task:com.mercury.topaz.dbverify.tasks.StorageCheckTask
task:com.mercury.topaz.dbverify.tasks.StorageCheckTask run ended. Decision is:None (no problem to continue)
running task:com.mercury.topaz.dbverify.tasks.DBCertifyTask
task:com.mercury.topaz.dbverify.tasks.DBCertifyTask run ended. Decision is:None (no problem to continue)
running task:com.mercury.topaz.dbverify.tasks.SchemaCheckTask
```

- 5 Check that your schema version is displayed in the Application Management User Schema Version dialog box.



Click **OK** to use the listed version. Click **Cancel** to choose a different version.

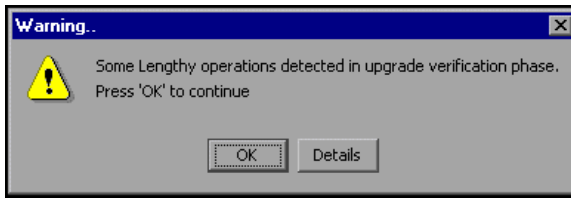
- 6 If problems occur during the database verification, a dialog box is displayed listing the errors.



Either fix the problems found and click **Retry**, or click **Exit** and rerun the database schema verify program at a later date.

You can view a log file of the errors in the **<Mercury Business Availability Center server root directory>\dbverify\log** directory. Under **\dbverify\tmp** you can find dedicated scripts for fixing the problems. The **dbverify** utility creates scripts automatically if mismatches are found and you need to run them on the relevant schema. If you are unable to fix the problems, contact Mercury Customer Support for assistance.

- 7 If the verification process detects lengthy operations that could slow down the upgrade process resulting in longer downtime, a dialog box is displayed.



Click **OK** to continue, or **Details** to display the estimated times that the lengthy operations detected could take during an upgrade.

- 8 If the database verification is successful, a confirmation message is displayed asking if you want to proceed with the database schema upgrade. Before proceeding, you should back up existing databases and shut down existing servers (see the checklist for details).
- 9 When this is done, proceed with the upgrade as described in “Upgrading the Database Schema” on page 68.

Note: During the database verification, the verify utility checks if the databases have sufficient disk space for a database rollback. If there is insufficient disk space, it does not continue with the verification.

Upgrading the Database Schema

After successfully verifying the database (for details, see “Verifying the Database Schema” on page 63), you can continue with the database upgrade stage.

Before proceeding with the upgrade, ensure that your management and profile databases are backed up.

Announce system downtime, then stop all Mercury Business Availability Center servers by stopping the Mercury Business Availability Center service on each of the server machines. If you have any additional open connections to the databases (for example, additional connections that are not part of usual functioning or open connections from Mercury Application Mapping), close them.

Note: Check that all processes have actually stopped after stopping the service. Stopping may take a few minutes. If necessary, stop the processes manually. There must be no open connections to the databases during the database schema upgrade.

To upgrade databases:

- 1** If you left the dbverify program open at the end of the database verification stage, click **Yes** to proceed with the database schema upgrade.
If you closed dbverify, rerun it according to the instructions on page 63. Note that the dbverify program will run through the verification stage again.
- 2** If there are still open connections to the database, a message is displayed giving details of the open connections. Make sure to close all connections.
- 3** The database schema upgrade program reviews all existing databases (management and profiles), and begins performing the required upgrade procedures for each database.
- 4** If lengthy operations are detected for a specific database, a message is displayed showing the estimated time that the upgrade will take, together with different options for continuing:
 - ◆ **Yes.** Continues with the upgrade for the specific database, including lengthy operations.
 - ◆ **No.** Aborts the upgrade for the specific database, but creates a script for upgrading the database that can be run at a later time.

Note: This script is only valid while Mercury Business Availability Center is disabled. Once Mercury Business Availability Center has been restarted, the script is no longer valid.

- ◆ **Details.** Displays details of the individual lengthy operations detected.
 - ◆ **Yes for All.** Continues with the upgrade for all the databases, including lengthy operations.
- 5** The database schema upgrade program runs until all existing MS SQL Server or Oracle Server databases are upgraded to the appropriate Mercury Business Availability Center format.

Note: During database upgrade, you can view log files in <**Mercury Business Availability Center_server_directory**>\log\dbupgrade.log. If errors occur, examine the dbupgrade.log file and troubleshoot the errors. For details, see “Troubleshooting Database Schema Verify and Upgrade Errors” on page 72.

- 6** Click **OK** to close the database schema upgrade utility.
- 7** Restart the Mercury Business Availability Center servers and processes (to work with the upgraded databases).

Creating Database Users for the Upgrade Procedure

When running the database schema verify and upgrade utility, you are prompted to supply a user name and password that can access the master database. You can create users with minimum privileges by running one of the following scripts.

For MS SQL Server

```
set nocount on
use master
GO
sp_addlogin @loginame = 'dbv_read', @passwd = '<pass>'
GO
sp_adduser @loginame = 'dbv_read', @name_in_db = 'dbv_read'
go
grant select on syslogins to dbv_read
go
set nocount off
```

Note: You must run this script as an **sa** user.

For Oracle Server

```
CREATE USER dbv_read IDENTIFIED BY admin;
GRANT SELECT_CATALOG_ROLE TO dbv_read;
GRANT CONNECT TO dbv_read;
```

Note: You must run this script as a system user.

Troubleshooting Database Schema Verify and Upgrade Errors

If errors occur during the database verify program, troubleshoot them by examining the log file located at **<Mercury Business Availability Center server root directory>\dbverify\log**. If errors occur during the database schema upgrade program, troubleshoot them by examining the **dbupgrade.log** file, located in the **<Mercury Business Availability Center server root directory>\log** directory.

After correcting errors, rerun the database schema verify and upgrade utility. If further errors occur, correct them as required, and rerun the utility.

For details on troubleshooting known issues, refer to the Mercury Business Availability Center Knowledge Base, accessed from the Mercury Customer Support Web site (support.mercury.com). (Only registered customers can access the resources on the Mercury Customer Support Web site. Customers who have not yet registered can do so from the site.)

Note: While running the database verify utility, if you receive an error that indexes are missing, this may be as a result of exporting and reimporting a profile database. For details, refer to the Mercury Business Availability Center Knowledge Base.

Modifying the mx Java Run-Time Parameter

If the database schema verify and upgrade utility (dbverify) fails, displaying a **java.lang.OutOfMemoryError** error, you need to modify the default value of the **mx** Java run-time parameter used by the dbverify Java application. The default value is approximately 64 MB, varying according to the platform and the Java virtual machine (JVM) version used.

When running a JVM using `java <app>`, the JVM extends a certain **HEAP_SIZE**. The **HEAP_SIZE** that is used grows and shrinks automatically according to the application code, varying between **ms** (minimum size) and **mx** (maximum size).

You change the default **mx** value to match your implementation size.

To change the mx value:

Open the appropriate file for your operating platform:

- 1** On a Windows platform on which you are running the database schema verify and upgrade utility, open the `\<Mercury Business Availability Center server root directory>\dbverify\bin\run_schema_upgrade.bat` file in a text editor.
 - ◆ On a Solaris platform, locate the `run_schema_upgrade.sh` script under the `dbverify` directory that you copied to your local disk (`../DbVerify/bin/run_schema_upgrade.sh`) and open it in a text editor.
- 2** Add the **mx** parameter to the Java command. The value of the parameter should be the upper limit of the memory size for your machine (frequently, this may mean a value as large as 200m). For example, the modified line may read as follows:

```
%JAVA_CMD% %OPTS% -Xmx200m -jar %TOPAZ_HOME%/lib/dbverifier.jar
```
- 3** Save the file and rerun the database schema verify and upgrade utility.

8

Retaining Monitor Administration Configuration Data

This chapter describes how to retain and reapply your Monitor configuration data when upgrading from Mercury Business Availability Center 5.x to Mercury Business Availability Center 6.6.

This chapter describes:	On page:
Overview of Retaining Monitor Administration Configuration Data	75
Backing Up Monitor Configuration Data Files	76
Copying Monitor Configuration Data Files to Mercury Business Availability Center	77
Upgrading the LDAP Database	78

Overview of Retaining Monitor Administration Configuration Data

Monitor Administration configuration data is stored in an LDAP (Lightweight Directory Access Protocol) database. This is for monitoring subsystems in Mercury Business Availability Center, such as SiteScope, Business Process Monitor, Client Monitor, and so forth.

When upgrading your Mercury Business Availability Center 5.x system to Mercury Business Availability Center 6.6, the Monitor Administration configuration data is overwritten.

In order to retain and reapply your Monitor Administration configuration data, you perform the following actions:

- ▶ Back up the Monitor Administration configuration data (stored in an LDAP database). For details, see “Backing Up Monitor Configuration Data Files” on page 76.
- ▶ Copy the saved Monitor Administration configuration data to the Mercury Business Availability Center 6.6 machine, or to the Centers Server in a distributed environment. For details, see “Copying Monitor Configuration Data Files to Mercury Business Availability Center” on page 77.
- ▶ Upgrade the LDAP database in Mercury Business Availability Center. For details, see “Upgrading the LDAP Database” on page 78.

Backing Up Monitor Configuration Data Files

Before beginning the upgrade to Mercury Business Availability Center 6.6, you should back up the files in the LDAP database.

By default this database resides in the <**Mercury Business Availability Center server root directory**>\openldap\bdb directory on the Centers Server. Any backup and restore processes should be performed on this directory.

You can determine on which server the LDAP database is installed by one of the following methods:

- ▶ Run the following query on the management database:

```
SELECT SP_VALUE, SP_VERSION, FROM SETTING_PARAMETERS WHERE  
SP_NAME LIKE 'ldap.host.and.port%'
```

- ▶ In **Admin > Platform > Infrastructure Settings**, look at the entry for **Monitor Administration Data Storage Location** in the **Monitor Administration** foundation.

Note: For additional information on LDAP database backup and recovery, refer to “Backing Up and Restoring Monitor Administration Configuration Data” in *Preparing the Database Environment*.

To manually back up the LDAP database:

- 1** If Mercury Business Availability Center is running, stop the LDAP service.
Edit <Mercury Business Availability Center root directory>\launch_service\dat\nanny\a_openldap.nanny and set **Enabled=False**.
- 2** Copy the <Mercury Business Availability Center server root directory>\openldap\bdb directory, and all its contents, to the backup media.
- 3** Start the LDAP service.
Edit <Mercury Business Availability Center root directory>\launch_service\dat\nanny\a_openldap.nanny and set **Enabled=True**.

Note: If you are backing up the LDAP database in the correct sequence, as detailed in the upgrade checklist, you do not have to restart Mercury Business Availability Center after copying the LDAP database.

Copying Monitor Configuration Data Files to Mercury Business Availability Center

After upgrading your Mercury Business Availability Center 5.x system to 6.6, you restore your Monitor Administration configuration data by copying the LDAP database to Mercury Business Availability Center 6.6.

To restore the LDAP database:

- 1** If Mercury Business Availability Center is running, stop the LDAP service.
Edit `<Mercury Business Availability Center root directory>\launch_service\dat\nanny\a_openldap.nanny` and set **Enabled=False**.
- 2** Copy the `<Mercury Business Availability Center server root directory>\openldap\bdb` directory that you saved from your Mercury Business Availability Center 5.x system, to `<Mercury Business Availability Center server root directory>\old_openldap\bdb` on the LDAP designated Centers Server on Mercury Business Availability Center 6.6.
- 3** Start the LDAP service.
Edit `<Mercury Business Availability Center root directory>\launch_service\dat\nanny\a_openldap.nanny` and set **Enabled=True**.

Note: The first Mercury Business Availability Center Centers Server installed contains the LDAP database.

You can determine on which server the LDAP database is installed by running the following query on the management database:

```
SELECT SP_VALUE, SP_VERSION, FROM SETTING_PARAMETERS WHERE  
SP_NAME LIKE 'ldap.host.and.port%'
```

Upgrading the LDAP Database

You must upgrade the old LDAP database to be compatible with Mercury Business Availability Center 6.6.

To upgrade the old LDAP database:

On the Mercury Business Availability Center 6.6 Centers Server on which you restored the old LDAP database, run `<Mercury Business Availability Center server root directory>\openldap\upgrade_ldap.bat`.

9

Configuration Upgrade

This chapter describes how to upgrade your configuration data.

Upgrading Configuration Data

You upgrade your configuration data to Mercury Business Availability Center 6.6 from the Manual Configuration Upgrade page in the Mercury Business Availability Center site.

Important: The list of entities on the Manual Data Upgrade page varies, depending on which version of Mercury Business Availability Center you are upgrading.

The following entities may be listed on the Manual Configuration Upgrade page:

Entities	Description
User Upgrade	Upgrades user and user roles to Mercury Business Availability Center 6.6.
Custom Reports Upgrade	<p>Upgrades custom and trend reports to Mercury Business Availability Center 6.6. There are two phases to the upgrade:</p> <ul style="list-style-type: none">▶ Phase 1 – The custom report (in 4.5) had a public flag. During upgrade the permissions are set according to this flag. If the flag is set to Private report, the owner gets full permissions and all the other users get no permission. If the flag is set to Public report, the owner gets full permissions and all other users get view permission on this report.▶ Phase 2 – Custom reports keep their JSPs in the database. During the upgrade, these JSPs are cleared so the next user who enters a report automatically creates a new JSP.

Entities	Description
Downtime Event Schedule Upgrade (4.5 to 6.6)	<p>Reconfigures the downtime/event schedules so that each schedule is event-based and can be assigned to multiple profiles.</p> <p>Downtime/events in Topaz 4.5 were defined per profile. If you were using the same downtime/event for different profiles you had to redefine it for each profile.</p> <p>When working in Mercury Business Availability Center 6.6, you can specify a specific downtime/event for a specific profile but you can also define a common downtime/event to which you can assign more than one profile.</p> <p>When you upgrade to Mercury Business Availability Center 6.6, you get a list of all downtime/events and their corresponding profiles. If a downtime/event appears in more than one profile, you can make it common by opening it and assigning to it all the profiles where it appears. For details, see “Downtime/Event Scheduling” in <i>Platform Administration</i>.</p> <p>Moves all downtime events for profiles to CMDB.</p>
Downtime Event Schedule Upgrade (5.x/6.x to 6.6)	Moves all downtime events for profiles to CMDB.
RUM Monitor Administration Upgrade (5.1 to 6.6)	Removes Real User Monitor entries from the Mercury Business Availability Center 6.6 LDAP.
Monitoring Upgrade	<p>Upgrades the monitoring administration. It includes:</p> <ul style="list-style-type: none"> ▶ Monitor Permissions Upgrade (this includes updating all the LDAP data) ▶ Licensing Upgrade

Entities	Description
Repositories Upgrade	Upgrades the repository definitions to Mercury Business Availability Center 6.6. For details of what is upgraded and how to redefine custom repository entities, see “Upgrading the Repositories from Mercury Business Availability Center 5.x to 6.6” on page 97.
Dashboard Filters Upgrade	Upgrades filter persistency to Mercury Business Availability Center 6.6. Also adds support for filter sharing between users and wildcards.

The system automatically upgrades global data and configures new data types for Mercury Business Availability Center 6.6 the first time that you access the Manual Configuration Upgrade page.

For a detailed explanation of the effects of data upgrade on certain components, see “Upgrading Components” on page 157.

To run a configuration upgrade:

- 1 Log into Mercury Business Availability Center.
- 2 Select **Admin > Platform > Setup and Maintenance > Configuration Upgrade**. The Manual Configuration Upgrade page opens.

Manual Configuration Upgrade

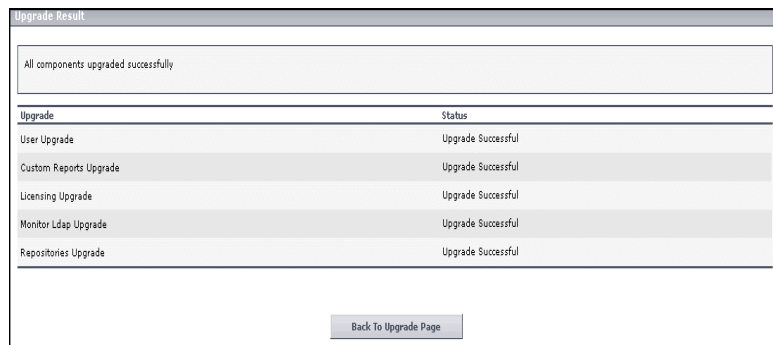
Note: If the Partition Manager was previously enabled for data purging, it was automatically disabled during the upgrade to Mercury Business Availability Center 6.1.0.0. If you wish to enable/re-enable the Partition Manager, please do so from the Data Purging page (Setup and Maintenance > Data Purging).

Upgrade	Status	Description
User Upgrade	Not Upgraded	Upgrades user and user roles to Application Management 6.0.
Custom Reports Upgrade	Not Upgraded	Upgrade custom and trend reports to BAC version 6.0
Downtime Event Schedule CMDB Upgrade	Not Upgraded	Inserts all downtime/event schedule definitions to the CMDB
RUM MA Upgrade (5.1 to 6.1)	Not Upgraded	removes RUM entries in LDAP of BAC 6.1
Monitoring Upgrade	Not Upgraded	
Repositories Upgrade	Not Upgraded	Upgrade all the custom repositories definitions to the new version.
Dashboard Filters Upgrade	Not Upgraded	Upgrades the filters persistency to support filter sharing (visibility) and wildcard filters.

Note: Only administrators with superuser permissions can view and use the Manual Configuration Upgrade page.

- 3 Click the **Upgrade All** button to perform an upgrade of the elements requiring upgrade (as indicated in the Status column).

The following page opens and displays information about the data upgrade taking place:



The screenshot shows a web interface titled "Upgrade Result". At the top, a message box states "All components upgraded successfully". Below this is a table with two columns: "Upgrade" and "Status". The table lists six upgrade categories, all of which are marked as "Upgrade Successful". At the bottom of the page, there is a button labeled "Back To Upgrade Page".

Upgrade	Status
User Upgrade	Upgrade Successful
Custom Reports Upgrade	Upgrade Successful
Licensing Upgrade	Upgrade Successful
Monitor Ldap Upgrade	Upgrade Successful
Repositories Upgrade	Upgrade Successful

When the data upgrade finishes, the table should show Upgrade Successful for the whole list of elements.

If some elements are marked as Upgrade Failed click the **Back to Upgrade Page** button and consult Mercury Customer Support, or try troubleshooting using the upgrade log in <Mercury Business Availability Center root directory>\log\topaz_all.ejb.log.

4 Click the **Back to Upgrade Page** button to confirm that all entities are upgraded.

Annual Configuration Upgrade

Note: If the Partition Manager was previously enabled for data purging, it was automatically disabled during the upgrade to Mercury Business Availability Center 6.5.0.0. If you wish to enable/re-enable the Partition Manager, please do so from the Data Purging page (Setup and Maintenance > Data Purging).

Upgrade	Status	Description
User Upgrade	Upgraded	Upgrades user and user roles to Application Management 6.0.
Custom Reports Upgrade	Upgraded	Upgrade custom and trend reports to BAC version 6.0
Downtime Event Schedule CMDB Upgrade	Upgraded	Inserts all downtime/event schedule definitions to the CMDB
RUM MA Upgrade (5.1 to 6.1) for MMS	Upgraded	removes RUM entries in LDAP of BAC 6.1
Monitoring Upgrade	Upgraded	
Repositories Upgrade	Upgraded	Upgrade all the custom repositories definitions to the new version.
Dashboard Filters Upgrade	Upgraded	Upgrades the filters persistency to support filter sharing (visibility) and wild

The configuration upgrade finished successfully. To complete the upgrade process, click Finish Upgrade.
Click Finish Upgrade to complete the upgrade of your system to Mercury Business Availability Center 6.5.0.0 .

Finish Upgrade

5 Click the **Finish Upgrade** button.

10

Dashboard Views Upgrade

This chapter describes how to upgrade your Mercury Business Availability Center 5.x Dashboard views to Mercury Business Availability Center 6.6 views.

This chapter describes:	On page:
The Views Upgrade Page	86
Simulating a View Upgrade	88
Upgrading a View	89
Post-Upgrade Tasks	91
Displaying an Upgraded View	91
Troubleshooting	92
Notes and Limitations	93
Rollback	96

The Views Upgrade Page

You upgrade your Mercury Business Availability Center 5.x Dashboard views to Mercury Business Availability Center 6.6 views from the Views Upgrade page in the Mercury Business Availability Center 6.6 site.

To access the Views Upgrade page, log in to Mercury Business Availability Center as an administrator with superuser permissions, and select **Admin > Platform > Setup and Maintenance > Views Upgrade**. The Views Upgrade page opens.

Upgrade Mercury Business Availability Center 5.x Dashboard Views

	View Name	Upgrade Status				
<input type="checkbox"/>	View1	Not Upgraded	Upgrade	Simulate Upgrade	View Log	Display Upgraded View
<input type="checkbox"/>	View2	Not Upgraded	Upgrade	Simulate Upgrade	View Log	Display Upgraded View
<input type="checkbox"/>	View3	Not Upgraded	Upgrade	Simulate Upgrade	View Log	Display Upgraded View
<input type="checkbox"/>	View4	Not Upgraded	Upgrade	Simulate Upgrade	View Log	Display Upgraded View
<input type="checkbox"/>	View5	Not Upgraded	Upgrade	Simulate Upgrade	View Log	Display Upgraded View
<input type="checkbox"/>	View6	Not Upgraded	Upgrade	Simulate Upgrade	View Log	Display Upgraded View
<input type="checkbox"/>	View7	Not Upgraded	Upgrade	Simulate Upgrade	View Log	Display Upgraded View

Upgrade Settings

Do not upgrade Dashboard 5.x items that are incompatible with the Mercury Universal CMDB.
Checking this option will cause the upgrade process to skip upgrading items if they are incompatible with the CMDB schema.

Hide this page once all views have been successfully upgraded.

Note: The mapping between Dashboard 5.x items and 6.0 CMDB configuration items can affect the success of the upgrade. It is recommended that you consult Mercury Customer Support prior to changing this mapping.
[To view and edit the current mapping click here.](#)

The top area of the page displays a list of all your Mercury Business Availability Center 5.x Dashboard views, showing their upgrade status, and has the following action buttons for each view:

- **Upgrade.** To perform the upgrade for the view. This option is only enabled if the view has not already been upgraded.

- ▶ **Simulate Upgrade.** To perform a simulation of the upgrade before actually upgrading the view, to check for errors. This option is only enabled if the view has not already been upgraded.
- ▶ **View Log.** To display a log of the upgrade process carried out. This option is only enabled after an upgrade has been performed.
- ▶ **Display Upgraded View.** To display how the upgraded view will appear in Mercury Business Availability Center 6.6. This option is only enabled after a successful upgrade has been performed.

The middle area of the page contains selection buttons, as well as buttons for upgrading multiple views and for rolling back (undoing) already completed upgrades.




To select a view for upgrading, you can either select the check box to the left of the view, or you can use the selection buttons for **Select All**, **Clear All**, and **Invert Selection**.

The bottom area of the page contains upgrade settings.

Upgrade Settings

There are two settings you can configure in the Views Upgrade page. To activate a setting, select the check box to the left of it, and to deactivate a setting, clear the check box. Click the **Save** button at the bottom of the Upgrade Settings section to save your setting selections.

 Upgrade Settings

Do not upgrade Dashboard 5.x items that are incompatible with the Mercury Universal CMDB.
Checking this option will cause the upgrade process to skip upgrading items if they are incompatible with the CMDB schema.

Hide this page once all views have been successfully upgraded.

Note: The mapping between Dashboard 5.x items and 6.0 CMDB configuration items can affect the success of the upgrade. It is recommended that you consult Mercury Customer Support prior to changing this mapping.
[To view and edit the current mapping click here.](#)

- ▶ The first setting determines how the upgrade relates to Mercury Business Availability Center 5.x Dashboard items that are incompatible with the Mercury Universal CMDB schema. Selecting this setting causes the upgrade process to ignore such incompatible items and to complete the upgrade for all the other items in the view. Not selecting this setting causes the upgrade process to fail if it encounters incompatible items.
- ▶ If you select the second setting, Mercury Business Availability Center hides the Views Upgrade page once you have upgraded all your Mercury Business Availability Center 5.1 Dashboard views to Mercury Business Availability Center 6.6.
- ▶ By clicking the link **To view and edit the current mapping click here**, you can view and edit the XML definition containing the mapping between Mercury Business Availability Center 5.x Dashboard items and Mercury Business Availability Center 6.6 CMDB configuration items.

Note: Changing any of the mappings can cause the views upgrade process to fail. It is recommended not to change any of these mappings.

Simulating a View Upgrade

To find out what errors the upgrade process will encounter during the upgrade of a specific view, you can run an upgrade simulation for the view.

To run an upgrade simulation for a view, click the **Simulate Upgrade** button for the appropriate view.

When the upgrade simulation process is complete, a log file is displayed showing details of items that can successfully be upgraded, as well as details of errors that will be encountered.

You can choose to ignore the errors during a real upgrade by activating the relevant upgrade setting (for details, see “Upgrade Settings” on page 87), or you can contact Mercury Customer Support for assistance in trying to correct the potential errors before upgrading the view.

Upgrading a View

Before starting the Dashboard views upgrade, perform the following:

- ▶ Copy <Mercury Business Availability Center root directory>\CMDB directory (from the 5.x Centers Server that ran the CDM service) to <Mercury Business Availability Center root dir>\CMDB\5.x in the 6.6 Offline Data Processing Server.
 - ◆ In order to find the 5.x Centers Server that ran the CDM service, execute the following SQL query from the Management database:


```
select bas_server from bac_available_servers where bas_subject_id=1
```
 - ◆ In order to find your Offline Data Processing Server, look in <Mercury Business Availability Center root directory>\conf\TopazSetup.ini for the line:


```
Processing_Server_Type=OFFLINE (or ALL)
```
- ▶ Increase the JVM heap size on the Data Processing servers to 1400 MB.

Edit the <Mercury Business Availability Center root directory>\conf\ProcessMemory.ini. file and increase the memory allocation. Make a note of the original value because you must reduce the memory allocation to its original value after the views have been upgraded.

For example, the Data Processing server currently allocates 780 MB of continuous memory, and you need to increase this amount to 1400 MB. Change the following line from:

```
Processing.2G.MercuryAS=780,80,196
```

to:

```
Processing.2G.MercuryAS=1400,80,196
```
- ▶ Restart the Offline Data Processing Server after the above steps have been done.

To upgrade views:

Note: Check that the source adapters are enabled and synchronized. If they are not, the Dashboard views will not be upgraded properly.

- 1 To upgrade an individual view, click the **Upgrade** button for the appropriate view.



Alternatively, to upgrade multiple views, select the check boxes for the views and click the **Upgrade** button under the Views table.

- 2 Check the view's status for success or failure.

When a view is successfully upgraded, its status changes from **Not Upgraded** to **Succeeded**, or **Succeeded with warnings**, and the check box for the view is disabled. The **Upgrade** and **Simulate Upgrade** buttons are disabled, and the **View Log** and **Display Upgraded View** buttons are enabled.

If a view upgrade fails, the view's status will change from **Not Upgraded** to **Failed (View Log)** and the **View Log** button is enabled.

To display a log of the upgrade process showing details of items that were successfully upgraded, warnings, and any errors encountered, click the **View Log** button for the appropriate view. A new window opens displaying the upgrade log.

Note: In rare cases, the upgrade view log states that the upgrade was successful even though the upgrade failed. In this case, it is recommended to check `<Mercury Business Availability Center root directory>\log\EJBContainer\bcu.log` on the Data Processing offline machine for further information.

If errors were encountered and the upgrade was unsuccessful, you can try to correct the errors and rerun the upgrade process. For assistance in trying to correct the errors, contact Mercury Customer Support.

- 3 Select **Admin > CMDB > Source Manager**. Click **Hard Sync** in the Default source adapters pane.

Post-Upgrade Tasks

After the views have been upgraded and verified, perform the following tasks:

- ▶ Change the name of the **CDM** directory in **<Mercury Business Availability Center root directory>\CMDB\5.x\CMDB** (on the 6.6 Offline Data Processing server) to **CDM.backup**. This prevents the JVM from trying to load old views and source adapter configurations after you have upgraded.
- ▶ Edit the **<Mercury Business Availability Center root directory>\conf\ProcessMemory.ini**. file and reduce the memory allocation to its original value.

For example, the Data Processing server currently allocates 1400 MB of continuous memory, and you need to reduce this amount to 780 MB. Change the following line from:

```
Processing.2G.MercuryAS=1400,80,196
```

to:

```
Processing.2G.MercuryAS=780,80,196
```

Displaying an Upgraded View

Once you have upgraded a view, you can display the upgraded view to see how it will look in Mercury Business Availability Center 6.6.

To display an upgraded view, click the **Display Upgraded View** button for the appropriate view. A new window opens displaying the upgraded view.



Expand the tree branches to see all configuration items.

Troubleshooting

For details about how repositories are upgraded from version 5.x to version 6.6, see “Upgrading Repositories” on page 97.

After upgrading views, it is possible that a KPI may have two sets of Threshold objectives, which is invalid for Mercury Business Availability Center.

Once all the views have been upgraded, and you can see views and status colors in Dashboard, check to see if there are any duplicate objectives for KPIs.

To check for duplicate objectives:

On the Online Data Processing Server, open the <Mercury Business Availability Center server root directory>\log\EJBContainer\bam.app.rules.log file and search for the following text:

ERROR - Too many Objectives For KPI

If the text is not found, continue with the upgrade process according to the steps in the upgrade checklist.

If the text is located in the **bam.app.rules.log** file, correct the duplicate objectives.

To correct duplicate objectives:

- 1** Log in to the Mercury Business Availability Center 6.6 system with administrator privileges.
- 2** In **Admin > CMDDB**, select the **Source Manager** tab.
- 3** Edit the **Business Process Monitor** adapter.
- 4** Click the **Edit Template** button to edit the Business Process Monitor adapter template.
- 5** In the template, locate the **customer** entity name:
`<entity id="customer"`
- 6** In this entity, change the value of the **logic id** to a different number (in the example below, the logic id number has been changed from 1 to 17):
`<logic><id>17</id></logic>`
- 7** Click **OK** to save the change and exit. The BPM source adapter automatically performs a hard sync when the process is finished.
- 8** Repeat steps 6 and 7 and change **logic id** back to its original number.

Notes and Limitations

- The following Mercury Business Availability Center 5.x Dashboard sources are not upgraded to Mercury Business Availability Center 6.6 and will cause errors in the views upgrade process:
 - ◆ CA
 - ◆ Generic EMS
 - ◆ HP OpenView
 - ◆ HP OpenView Service Navigator (if additional levels have been generated using node factory)
 - ◆ Tivoli Tec
 - ◆ XML File

Note: Configure new source adapters for these types in Mercury Business Availability Center 6.6.

- ▶ The following Mercury Business Availability Center 5.x Dashboard sources are not supported in Mercury Business Availability Center 6.6 and will cause errors in the views upgrade process:
 - ◆ Application Mapping
 - ◆ Remedy HelpDesk
 - ◆ dbAdapter
 - ◆ Siebel
 - ◆ Service Level Management
- ▶ Mercury Business Availability Center 6.6 includes the following default source adapters:
 - ◆ Business Process Monitor
 - ◆ Real User Monitor
 - ◆ SiteScope
- ▶ Mercury Business Availability Center 5.x source adapters of the same types are not upgraded. If you made any changes to the templates of these source adapters in Mercury Business Availability Center 5.x, and wish to have the same changes in Mercury Business Availability Center 6.6, manually change the Mercury Business Availability Center 6.6 default source adapter templates in **Admin > CMDB > Source Manager** prior to carrying out the views upgrade.
- ▶ Custom source adapters are not upgraded. If you made any changes to custom source adapter templates in Mercury Business Availability Center 5.x, and wish to have the same changes in Mercury Business Availability Center 6.6, configure a new source adapter in Mercury Business Availability Center 6.6 and manually change the source adapter template in **Admin > CMDB > Source Manager** prior to carrying out the views upgrade.
- ▶ Only Mercury Business Availability Center 5.x default properties are upgraded to 6.5; 5.x custom properties are not upgraded.

If a property of a CI generated by a source adapter was changed and you want to keep the current value, clear the **Allow CI Update** check box.

Note: When the **Allow CI Update** check box is not checked, none of the other properties are updated by the source adapter.

- ▶ In Mercury Business Availability Center 5.x, it is possible to have multiple Dashboard items with the same name, each appearing in a different view, and each with different properties.

When upgrading to Mercury Business Availability Center 6.5, all 5.x Dashboard items with the same name are combined into one CI. This CI is assigned the properties from the last 5.x view upgraded.

- ▶ If you are upgrading views that have link nodes, the views upgrade must be done in the following order:
 - a upgrade the view without link nodes
 - b upgrade the view with the link nodes

For example, ViewA has link nodes to ViewB. You must upgrade ViewB first and then upgrade ViewA.

- ▶ In Mercury Business Availability Center 5.x, regardless of the **Hierarchy structure** setting in the Business Process Monitor source adapter, transactions and locations at the bottom level of a Business Process Monitor tree are displayed using their configured name only. In Mercury Business Availability Center 6.6, setting the **Hierarchy structure** setting to **Transaction/Location** causes the transactions and locations at the bottom level of a Business Process Monitor tree to be displayed using an alternate format, which by default is set to **transaction name from location name**. You can change the format of the alternate display by editing the **BPM Transaction from Location** CIT from the **CI Type Manager** tab in CDMB Admin.

Rollback

You can rollback (undo) view upgrades and revert to the original Mercury Business Availability Center 5.x Dashboard views by clicking the **Rollback All Upgrades** button in the middle of the Views Upgrade page. However, Mercury Business Availability Center 5.x Dashboard views will not be visible in Mercury Business Availability Center 6.6 until they are upgraded.

Important: After doing a rollback, you must synchronize the source adapters. Select **Admin > CMDB > Source Manager**. Click **Hard Sync** in the Default source adapters pane.

Note: The rollback process will undo all completed view upgrades. You cannot roll back an individual upgraded view.

11

Upgrading Repositories

This chapter describes the repository upgrade.

This chapter describes:	On page:
Upgrading the Repositories from Mercury Business Availability Center 6.x	97
Upgrading the Repositories from Mercury Business Availability Center 5.x to 6.6	97

Upgrading the Repositories from Mercury Business Availability Center 6.x

All 6.x repository elements are automatically upgraded to version 6.6 during the general upgrade process.

Upgrading the Repositories from Mercury Business Availability Center 5.x to 6.6

You upgrade the repository elements from 5.x to 6.6 as part of the configuration data upgrade, which is run from the Manual Configuration Upgrade page (for details, see “Configuration Upgrade” on page 79).

Some factory 5.x repository elements are not upgraded (because they have no application in 6.6). Other repository elements are upgraded with certain changes or restrictions, as described in the following sections.

If you created custom repository elements in 5.x (by overriding or cloning, or by creating new elements), these still appear in the repositories after running the upgrade. It is recommended, however, that you delete the custom elements and redefine them in 6.6, using the upgrade log for guidance.

If necessary, it is possible in certain cases to update the 5.x custom elements (from the Edit dialog box for that element), and some guidance is given for this in the following sections. These changes should be made with caution.

The following sections describe the impact on repositories of upgrading from Mercury Business Availability Center 5.x to 6.6:

- “Upgrade Log” on page 98
- “Upgrading Entities/Items (CIs)” on page 99
- “Upgrading Dimensions (KPIs)” on page 99
- “Upgrading Rules” on page 105
- “Context Menus and Context Menu Items” on page 109
- “Upgrading Tooltips” on page 112

Upgrade Log

All the operations that are performed during the upgrade procedure are written in the following file:

`<Mercury_Business_Availability_Center_root_directory>\log\EJBContainer\repositories.upgrade.log`

Upgrading Entities/Items (CIs)

The Entities Repository in Mercury Business Availability Center 5.x is not upgraded. In 6.6, entities/items are replaced by Configuration Item Types (CITs), and the CIT repository is managed from the CI Type Manager. For more information, see *CI Type Manager Administration*.

Upgrading Dimensions (KPIs)

The upgrade procedure removes the dimensions that are obsolete in version 6.6 and modifies other dimensions. It also renames dimensions to **KPIs** (dimensions are referred to as KPIs in the following sections).

This section includes the following topics:

- “Removed KPIs” on page 99
- “New, Cloned, or Overridden KPIs” on page 100
- “Applicable Rules for a KPI” on page 103
- “Applicable Sections of a KPI” on page 104
- “KPI Parameters” on page 104

Removed KPIs

The following KPIs are removed during the upgrade:

- **Remedy.** The Remedy feature is not supported.
- **Change.** The Change feature is handled differently in this version – for details, see “Change Rule” in *Repositories Administration*.
- **Maps.** The Maps feature is handled differently in this version – for details, see “Configuring the Geographical Map” in *Application Administration*.
- **Abandon.** The feature is obsolete.
- **Diagnostics.** The Diagnostics feature is handled differently in this version – for details, see the Mercury diagnostic guide.

What you can do: if necessary, use the **Application** KPI instead – for details, see “Application” in *Repositories Administration*.

For example, the log entry corresponding to the Abandon KPI removed during upgrade because it is not supported is as follows:

```
*** Upgrading KPI [1051] [Abandon]
This KPI does not exist in 6.6 - will be removed from repositories
```

New, Cloned, or Overridden KPIs

Custom KPIs in 5.x are upgraded with the following restrictions:

- **Applicable rules.** For details, see below.
- **Applicable sections.** For details, see “Applicable Sections of a KPI” on page 104.
- **Parameters.** For details, see “KPI Parameters” on page 104.

For example, the log entry corresponding to the RT Impact KPI that was cloned is as follows:

```
*** Upgrading KPI [2000] [RT Impact Cloned]
This KPI was cloned or new - will be upgraded partially
The applicable rule [50] was removed
Setting Applicable Contexts from [events;dashboard] to [dashboard]
New parameter major
Changing parameter warning:
old key [good] new key [warning]
old color [339933;33cc33] new color [D8E57F;CCCC00]
old status range from [20] new from [15]
old status range to [20] new to [19]
```

For example, the log entry corresponding to the Availability KPI that was overridden is as follows:

```
*** Upgrading KPI [7] [Availability]
This KPI was overridden - will be upgraded
The applicable rule [21] was removed
The applicable rule [49] was added
Setting Applicable Contexts from [events;dashboard] to [dashboard]
New parameter major
Changing parameter warning:
old key [good] new key [warning]
old icon [ind6_grn.gif] new icon [ind6_grnyel.gif]
old color [339933;33cc33] new color [D8E57F;CCCC00]
old status range from [20] new from [15]
old status range to [20] new to [19]
```

For example, the log entry corresponding to upgrading the System KPI is as follows:

```
*** Upgrading KPI [1] [System]
This KPI was overridden - will be upgraded
The applicable rule [21] was removed
The applicable rule [50] was removed
The applicable rule [1010] was removed
The applicable rule [33] was added
The applicable rule [34] was added
Setting Applicable Contexts from [events;dashboard] to [dashboard]
Changing parameter downtime:
old color [dddddd;339933] new color [DDDDDD;66CC00]
Changing parameter stop:
old color [dddddd;339933] new color [DDDDDD;66CC00]
Changing parameter none:
old color [999999;dddddd] new color [DDDDDD;BBBBBB]
Changing parameter critical:
old key [error] new key [critical]
old color [cc3300;ff6666] new color [FF8787;FF3333]
ols status range to [5] new to [4]
New parameter major
Changing parameter minor:
old key [warning] new key [minor]
old color [cc9900;ffcc00] new color [FFE57F;FFCC00]
ols status range to [10] new to [14]
Changing parameter warning:
old key [good] new key [warning]
old icon [ind6_grn.gif] new icon [ind6_grnyel.gif]
old color [339933;33cc33] new color [D8E57F;CCCC00]
old status range from [20] new from [15]
ols status range to [20] new to [19]
New parameter ok
```


Applicable Rules for a KPI

Applicable rules for a KPI are upgraded in 6.6 as follows:

- ▶ Rules deleted from 5.x do not appear in the applicable rules list for the KPI in 6.6. For a list of those rules, see “Rules Removed During the Upgrade” on page 106.
- ▶ Rules added in 6.6 are automatically assigned to the appropriate overridden KPIs as follows:

Overridden KPIs	Rule
1-System	33-Sitescope Measurement Time-Based Rule
	34-Sitescope Monitor Time-Based Rule
6-Performance	60-RUM Page Monitor Performance Rule
	61-RUM Page Monitor Performance Rule
	62-RUM Session Monitor Performance Rule
	63-Average of Converted Performance Results in %
	64-Average Performance of Weighted Volume in %
	65-Average Performance of Weighted Volume in Seconds
7-Availability	49-RUM Page Monitor Availability Rule
	51-RUM Transaction Monitor Availability Rule
	52-RUM Session Monitor Availability Rule
	55-Average Availability of Weighted Volume
1050-Volume	2-Best Child Rule
	70-RUM Page Monitor Volume Rule
	71-RUM Transaction Monitor Volume Rule
	72-RUM Session Monitor Volume Rule
	73-RUM Event Monitor Volume Rule
	74-Sum of Volume

What you can do: check the rules that remain attached to each KPI (cloned or created in previous versions). If necessary, attach new rules. For details, see “Dashboard Business Rules Detailed Description” in *Repositories Administration*.

For example, the log entry corresponding to removing and adding applicable rules is as follows:

```
The applicable rule [21] was removed
The applicable rule [50] was removed
The applicable rule [1010] was removed
The applicable rule [33] was added
The applicable rule [34] was added
```

Applicable Sections of a KPI

Dashboard is automatically assigned to all upgraded KPIs in the Applicable Sections; all other sections are automatically removed.

The log entry corresponding to such an operation has the following syntax:

```
Setting Applicable Contexts from [events;dashboard] to [dashboard]
```

KPI Parameters

The KPI parameters are upgraded with the following restrictions:

- ▶ some of the parameters are renamed (**Good** is changed to **Informational**, **Warning** to **Minor**, and **Error** to **Critical**).
- ▶ two new parameters are automatically added: **Major** (bad) and **Warning** (good).
- ▶ the **From-To** fields will be translated to the new values (with 5 color statuses) as follows:

	From	To	Color
Critical	0	4	red
Major	5	9	orange
Minor	10	14	yellow

Warning	15	19	green-yellow
OK	20	20	green

- **Color** and **Icon** are converted to the new colors and icons.

What you can do: you may need to manually upgrade the parameters, especially the objectives.

For example, the log entry corresponding to adding a new parameter is as follows:

```
Changing parameter warning:
old key [good] new key [warning]
old icon [ind6_grn.gif] new icon [ind6_grnyel.gif]
old color [339933;33cc33] new color [D8E57F;CCCC00]
old status range from [20] new from [15]
ols status range to [20] new to [19]
New parameter ok
```

Upgrading Rules

The upgrade procedure removes the rules that are obsolete in version 6.6 and modifies other rules.

This section includes:

- “Rules Removed During the Upgrade” on page 106
- “New or Cloned Rules” on page 107
- “Overridden Rules” on page 108
- “Rule Parameters” on page 108
- “Rule Global Parameters” on page 109

Rules Removed During the Upgrade

If you attached one of the following rules to a dimension/KPI:

- ▶ **Any of the Real User Monitor rules.** New Real User Monitor rules are automatically added to the Business Rules Repositories during upgrade.

What you can do: select the appropriate new Real User Monitor rule and attach it to the relevant KPI. For details about the new Real User Monitor rules, see “Dashboard Business Rules Detailed Description” in *Application Administration*.

- ▶ **Link.** The internal Link rule has been removed.

What you can do: if you have been using the following class: **com.mercury.topaz.bam.application.rules.LinkRule**, create an instance view that performs the same function. For details about creating an instance view, see “Working with Instance Views” in *View Manager Administration*.

- ▶ **J2EE Avg Time, J2EE Max Time, J2EE Load, J2EE Exceptions, J2EE Time Outs, J2EE General, J2EE VU Avg Time.** For details, see *Mercury Diagnostics Installation and Configuration Guide*.

What you can do: use the new Diagnostics for J2EE/.Net General rule and customize it if necessary. For details, see “Deep Transaction Tracing Monitor Availability” in *Repositories Administration*.

- ▶ **Generic Sample Rule.**

What you can do: select one of the appropriate new generic rules and attach it to the relevant KPI. For details about the generic rules, see “Dashboard Business Rules Detailed Description” in *Application Administration*.

- ▶ **Worst Dashboard PNR, Worst Dashboard Text PNR, Dashboard Text PNR, Dashboard PNR.**

What you can do: use the new Dashboard PNR rule. For details, see “Dashboard PNR Rule” in *Repositories Administration*.

- ▶ **Change.** The Change feature has been improved and is handled differently. For details, see “Change Rule” in *Repositories Administration*.
- ▶ **Ticketing ETTR Rule, Ticketing Status Calculate Rule, Remedy Worst Child Rule.**

The log entry corresponding to such an operation has the following syntax:

```
*** Upgrading rule [50] [Link Rule]
This rule does not exists in 6.6 - will be removed from repositories
```

New or Cloned Rules

- ▶ The rules that were created or cloned in the previous version are not upgraded and remain as they were in the previous version.

What you can do: if necessary, you must manually upgrade the rules that were created or cloned in the previous version.

- ▶ If you created a class in the previous version, the old class name still appears in the **Class name** box, but the old class will not run.

What you can do: if necessary, rewrite the class in the new version.

- ▶ If you used an existing class, the behavior might be different.

What you can do: to use the default behavior of the original class you can copy the class name from the factory rule.

For example, the log entry corresponding to the Best Child Rule that was cloned and renamed Best Child Rule 2 is as follows:

```
*** Upgrading rule [2000] [Transaction Performance Rule Clone]
This rule was cloned or new - will not be upgraded
```

- ▶ The **Percentage** rule is updated, but the rule's **Number of Statuses**, **strip 1**, **strip 2**, and **strip 3** parameters are not converted into objectives; the new objectives are automatically added. The rule's strips had the following structure: **from Value, to Value, status Number**. This structure is no longer supported. Customization performed by the customer on those parameters in previous versions are also not upgraded.

What you can do: customize the new objectives. For details, see “Percentage Rule” in *Repositories Administration*.

Overridden Rules

- ▶ The rules that were overridden in the previous version are upgraded with some restrictions regarding the classes (for details, see below), the parameters (for details, see “Rule Parameters” on page 108), and the global parameters (for details, see “Rule Global Parameters” on page 109).
- ▶ If you created a class in the previous version and used it in overridden rules, the class is removed during upgrade.
- ▶ If you used an existing class, the class is automatically replaced by the new corresponding class during the upgrade procedure. Note that the behavior might be different.
- ▶ The parameters are also upgraded. For details, see “Rule Parameters” on page 108.

For example, the log entry corresponding to the upgrade of the Worst Child Rule that was overridden is as follows:

```
*** Upgrading rule [13] [Transaction Performance Rule]
This rule was overridden - will be upgraded
old class name com.mercury.topaz.bam.application.rules.TxPerformance
Parameter [UpperBound] on 6.6 will become Objective
Parameter [granularity] is not in use in 6.6 - will be removed
Parameter [szDecayTimeout] on 6.6 changed to [No data timeout]
Parameter [UpperBound] will become Objective [minor]
```

Rule Parameters

- ▶ **rule parameter names and values.** The names of the rule parameters are automatically replaced by the new names; the parameter values are not changed.
- ▶ **new parameters that were added to the rules.** The relevant new parameters are automatically added to the relevant rules during the upgrade procedure. The old parameters (except for **MUST**, **WEIGHT**, and **GRANULARITY** parameters that are automatically removed) are not upgraded.

What you can do: you might have to manually remove or upgrade the old parameters.

The parameters that were used for the objectives are translated by the upgrade procedure as follows:

Old name	New name	Rules
LowerBound	Minor	Transaction Availability Rule
	Informational	Transaction Performance Rule
UpperBound	Informational	Transaction Availability Rule
	Minor	Transaction Performance Rule
DollarImpact Threshold	Informational	Real time impact, Impact Over Time, and Sums values rules

The log entry corresponding to such an operation has the following syntax:

```
Parameter [UpperBound] on 6.6 will become Objective
```

Rule Global Parameters

The global parameters are automatically upgraded to 6.6. If you made a change to one of the global parameter's values in version 5.x, the change remains in 6.6.

Context Menus and Context Menu Items

The Context Menus Repository and the Context Menu Items Repository are not upgraded from version 5.x to version 6.6. In the earlier versions, the entries for these repositories were based on the element name; in the upgraded version, most of the context menus and context menu items have new names.

In 6.6, new context menus are automatically assigned to the CIs, according to the default context menu defined for the CIT.

Note: In version 6.6, IDs are added for context menus and context menu items.

If you created custom context menus or context menu items in version 5.x, an error is added to the log file

<Mercury_Business_Availability_Center_root_directory>\log\EJBContainer\repositories.upgrade.log.

What you can do: If the context menu is still relevant, add it manually to the repositories.

For example, the log entry corresponding to upgrading the BPM Group Menu context menu is as follows:

```
cannot perform upgrade for Context Menu, this element needs manual
upgrade
<menu DisplayName="BPM Group Menu" id="txGroupMenu">
ShowInUI="">
  <entity id="linkTo" appContexts="">
    <entity id="trendReport" appContexts=""/>
    <entity id="TxAnalysisReport" appContexts=""/>
  </entity>
  <entity id="showCustomerImpact" appContexts=""/>
  <entity id="customFilters" appContexts="">
    <entity id="subTree" appContexts=""/>
    <entity id="subTreeLeaves" appContexts=""/>
    <entity id="filterSubTree" appContexts=""/>
    <entity id="filterSubTreeLeaves" appContexts=""/>
  </entity>
  <entity id="ackDetail" appContexts=""/>
  <entity id="topView" appContexts="Dashboard - Business Console">
    <entity id="PathToRoot" appContexts=""/>
    <entity id="WorstPathToRoot" appContexts=""/>
    <entity id="Ancestors" appContexts=""/>
    <entity id="openCenter" appContexts=""/>
    <entity id="openSubTree" appContexts=""/>
  </entity>
</menu>
```


For example, the log entry corresponding to upgrading the 2000 Context Menu Item context menu item is as follows:

```
cannot perform upgrade for Context Menu Item, this element needs
manual upgrade
  <ContextMenuItem id="2000" DisplayName="2000 Context Menu Item"
multi="false" image="" imageOpen="">
  <PreProcessing
__class="com.mercury.topaz.bam.application.helpers.processors.preproc
essors.SiteScopePreprocess">
  <params>
    <param key="ROOT_PATH" value="http://www.cnn.com"
convert_to_key=""/>
    <param key="PROFILE_ID" value="NODE.PROPS.SESSION_ID"
convert_to_key=""/>
    <param key="POST_FIX" value=".html" convert_to_key=""/>
    <param key="GROUP_NODE_NAME"
value="NODE.PROPS.internal_name" convert_to_key=""/>
    <param key="HOST_BY" value="NAME" convert_to_key=""/>
    <param key="ROOT_POSTFIX" value="SiteScope.html"
convert_to_key=""/>
    <param key="PATH" value="SiteScope/htdocs/Detail"
convert_to_key=""/>
  </params>
  </PreProcessing>
  <PostProcessing
__class="com.mercury.topaz.bam.application.helpers.processors.postproc
essors.OpenWindowJSPostprocess">
  <params>
    <param key="SCROLL" value="1"/>
    <param key="HEIGHT" value="600"/>
    <param key="SLAVE_WIN" value="1"/>
    <param key="WIDTH" value="600"/>
    <param key="WIN_NAME" value="open_sitescope"/>
    <param key="RESIZE" value="1"/>
  </params>
  </PostProcessing>
</ContextMenuItem>
```

Upgrading Tooltips

The upgrade procedure removes the tooltips that are obsolete in version 6.6 and modifies other tooltips.

This section includes the following topics:

- “Removed Tooltips” on page 112
- “Cloned Tooltips” on page 113
- “Overridden Tooltips” on page 114
- “Tooltip Parameters” on page 114
- “Global Tooltip Parameters” on page 114

Removed Tooltips

- **Any of the Real User Monitor tooltips.** New Real User Monitor tooltips are automatically added to the Business Rules Repositories during upgrade.

What you can do: when you select the appropriate new Real User Monitor rule and attach it to the relevant KPI, the corresponding tooltip is automatically attached to the KPI. For details about the new Real User Monitor tooltips, see “Specifying the Tooltip Details” in *Repositories Administration*.

- **Link.** For details, see the Link rule in “Rules Removed During the Upgrade” on page 106.
- **J2EE Avg Time, J2EE Max Time, J2EE Load, J2EE Exceptions, J2EE Time Outs, J2EE General, J2EE VU Avg Time.** For details, see *Mercury Diagnostics Installation and Configuration Guide*.

What you can do: use the new Diagnostics for J2EE/.Net General tooltip and customize it if necessary. For details, see “Diagnostics for J2EE General Sentence” in *Repositories Administration*.

- **Worst Dashboard PNR, Worst Dashboard Text PNR, Dashboard Text PNR, Dashboard PNR.**

What you can do: when you assign the new Dashboard PNR rule to the KPI, the appropriate tooltip is automatically assigned to the KPI and you can then customize it. For details, see “PNR” in *Repositories Administration*.

- **Change.** The Change feature has been improved and is handled differently in this version. For details, see “Change Rule” in *Repositories Administration*.
- **Remedy ETTR sentence, Remedy status sentence, Remedy group sentence.**

The log entry corresponding to such an operation has the following syntax:

```
*** Upgrading tooltip [1076] [J2EE Average time]
This tooltip does not exist in 6.6 - will be removed from repositories
```

Cloned Tooltips

During the upgrade procedure, the **Calculation Rule** parameter is added to the tooltips that were cloned in 5.x; the rest of the parameters remain as they were in the previous version.

The tooltip parameters (for details, see “Tooltip Parameters” on page 114), and the global tooltip parameters (for details, see “Global Tooltip Parameters” on page 114) are upgraded.

What you can do: if necessary, you must manually upgrade them.

For example, the log entry corresponding to upgrading the New Rule tooltip that is cloned or new is as follows:

```
*** Upgrading tooltip [3.1] [SiteScope measurement sentence Cloned]
This tooltip was cloned or new - will be upgraded partially
Adding a new tooltip parameter [Calculation Rule]
  <param DisplayLabel="Calculation Rule" valuePrefix=""
valueSource="NODE.DIM.RULE.ID_CUST" valuePostfix=""
formattingMethod="ruleIDtoString"/>
```

Note: The **Percent sentence** tooltip’s **Number of Statuses**, **strip 1**, **strip 2**, and **strip 3** parameters are not converted into objectives. The new objectives are automatically added.

What you can do: customize the new objectives. For details, see “Understanding the Percentage Rule” in *Repositories Administration*.

Overridden Tooltips

The tooltips that were overridden in 5.x are upgraded with some restrictions regarding the tooltip parameters (for details, see “Tooltip Parameters” on page 114), and the global tooltip parameters (for details, see “Global Tooltip Parameters” on page 114).

For example, the Red threshold parameter has been removed from the overridden Dollar impact sentence tooltip, and the Informational parameter has been added:

```
*** Upgrading tooltip [19] [Dollar impact sentence]
Removing a tooltip parameter [Red threshold]
Adding a new tooltip parameter [Informational]
  <param DisplayLabel="Informational"
valuePrefix="[[NODE.DIM.OBJECTIVE_OP]] $"
valueSource="NODE.DIM.OBJECTIVE_TH.Informational" valuePostfix=""
formattingMethod=""/>
Switch PostFix [ Dollar] and PreFix [] to tooltip parameter [Business Loss]
```

Tooltip Parameters

The parameters are upgraded with the following restrictions:

- ▶ new parameters are added to the tooltips. For example, the **Calculation**, **Location**, and **Caused by** parameters are added to the relevant tooltips.
- ▶ obsolete parameters are removed: **Green threshold**, **Red threshold**, **Lower Bound**, and **Upper Bound**. They are replaced by the **Informational**, **Warning**, **Minor**, and **Major** objectives.
- ▶ unused parameters remain unchanged by the upgrade; you might have to manually upgrade those parameters.

For an example of the syntax used in such operations, see the example in “Overridden Tooltips” on page 114.

Global Tooltip Parameters

The global tooltip parameters are automatically upgraded to 6.6.

12

Upgrading Source Adapters

This chapter describes the process to upgrade source adapters to Mercury Business Availability Center version 6.6.

This chapter describes:	On page:
Upgrading the Source Adapters from Mercury Business Availability Center 6.x	115
Upgrading the Source Adapters from Mercury Business Availability Center 5.x	116

Upgrading the Source Adapters from Mercury Business Availability Center 6.x

Use the adapter upgrade utility to automatically upgrade the source adapters (including custom source adapters) from version 6.x to Mercury Business Availability Center version 6.6.

To upgrade source adapters from version 6.x to version 6.6:

- 1** In a Web browser, open:
<http://<Centers Server machine name>/topaz/adaptersUpgrade.jsp>.
The Adapter Upgrade Page dialog box opens.
- 2** Click **Upgrade**.
- 3** An informational message is displayed when the upgrade has completed.

Note: After upgrading source adapters, you must restart Mercury Business Availability Center on the Data Processing Server machine. In a distributed architecture, restart Mercury Business Availability Center on the Modeling Data Processing server machine.

Upgrading the Source Adapters from Mercury Business Availability Center 5.x

Upgrade of source adapters from 5.x is not supported with the exception of customized XML File source adapters. To upgrade customized XML File source adapters, you perform the manual upgrade procedures described below, including upgrading the customized XML File source adapter template and the corresponding Configuration File.

Note:

- ▶ You must upgrade the repositories before upgrading the customized XML File source adapter, otherwise the source adapter will not be correctly upgraded.
 - ▶ The customized XML File source adapter upgrade procedure can be performed during the general Mercury Business Availability Center upgrade procedure (at the point where it appears in the upgrade checklist) or at a later stage, after the general upgrade procedure is completed.
-

This section includes the following topics:

- ▶ “Update the XML File Template” on page 117
- ▶ “Upgrade the Configuration File” on page 122

Update the XML File Template

To upgrade the XML File template, you must change the version number, change the class path, map each basic entity to the appropriate new basic entity, and its rules as explained below.

To upgrade the XML File template:

For each customized XML File template proceed as explained in the following procedure.

- 1** Copy the <Mercury Business Availability Center root directory>\CMDB directory from the 5.1 server to the <Offline_Data_Processing_Server>\CMDB\5.x directory on the 6.6 machine.
- 2** In the <Offline_Data_Processing_Server>\CMDB\5.x directory, open the appropriate XML File template (named XML_File_<number>.config.xml) and make a backup copy. For details about the XML File template, see “XML File” in *Source Manager Administration*.
- 3** Open the XML File template (named XML_File_<number>.config.xml).
- 4** Change the version number from 5.1 to 6.6 in the following string:

```
<?xml version="1.0" encoding="UTF-8" ?>
  <Adapter bac-version="BAC 5.1">
```

- 5** Change the class path from **com.mercury.topaz.tdm.adapters.XMLFileAdapter.XMLFileAdapterImpl** to **com.mercury.am.adapters.xml.XmlEnhancedAdapterImpl** in the following string:

```
<classPath>com.mercury.topaz.tdm.adapters.XMLFileAdapter.XMLFileAd
  apterImpl</classPath>
```

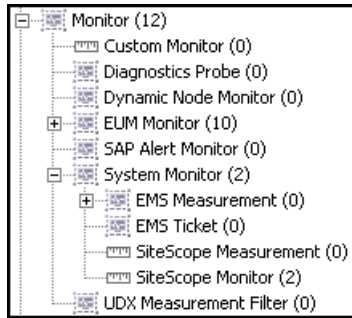
- 6** Map each basic entity in the XML File template to a basic entity in 6.6:
 - a** Use the following mapping table to select the appropriate corresponding basic entity or group of basic entities in 6.6:

Basic Entity in version 5.1	Basic Entity in Version 6.x
Group	Everything under Group except for Dynamic Node Group
NodeFactory	Dynamic Node Factory (Mercury:node_factory)
Custom	Business Unit (Mercury:business_unit)
Service	Business Service (Mercury:business_service_for_catalog)
SLA	No mapping
Application	Application (Mercury:logical_application) or everything under Software Element (inclusive)
Ticket	EMS Ticket (Mercury:ems_ticket)
Business Process	Business Process (Mercury:business_process)
Line of Business	Line of Business (Mercury:line_of_business)
Device	Everything under Host (inclusive) or under Network Resources
Link Node	No mapping
Customer	Business Unit (Mercury:business_unit)
Measurement	Everything under Monitor
Machine	Everything under Host (inclusive)
Owner	Business Unit (Mercury:business_unit)

If the basic entity in 5.1 (for example, **Business Process**) corresponds to a single basic entity in 6.6 (for example, **Business Process**), proceed to step **g**.

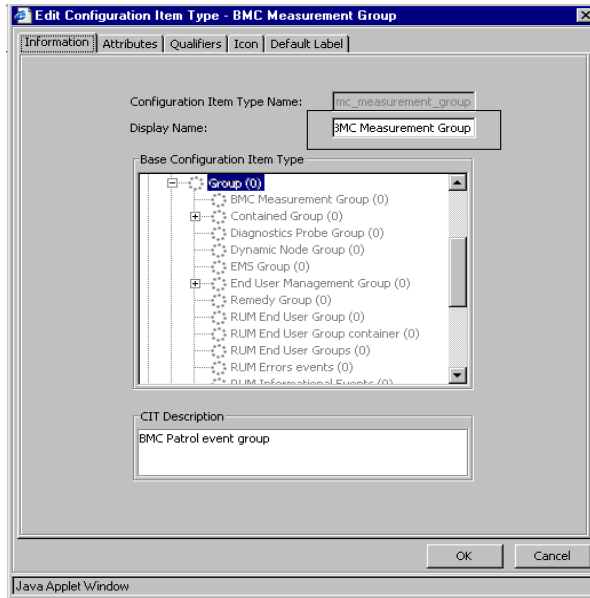
If the basic entity in 5.1 (for example, Measurement) corresponds to a group of basic entities in 6.6 (for example, everything under Monitor), you must select the CIT that matches your requirements. Proceed to step **b**.

- b** Open the CI Type Manager, search for the appropriate CIT. For example, expand Monitor to find SiteScope Measurement.



- c** Right-click the appropriate CIT and select **Edit CIT** to open the Edit Configuration Item Type dialog box.
- d** Click the **Qualifier** tab and check that the **RANDOM_GENERATED_ID_CLASS** qualifier is not listed in the **Configuration Item Type Qualifiers** area. If it is listed, you cannot use this CIT, and you must select another CIT in the group.
- e** Click the **Attributes** tab and check that there is at least one attribute that has been defined as a key of the CIT (indicated by a small keyin the left column). If none of the attributes has a key, you cannot use this CIT. You must select another CIT in the group.
- f** If the CIT has a key and does not have the **RANDOM_GENERATED_ID_CLASS** qualifier, check that the attributes are what you need to represent the basic entity you are mapping. If this is the correct CIT, look for the keys of the CIT (indicated by a small keyin the left column).

- g In the appropriate **basic Entity** string, change the name of the basic entity to the selected CIT name. Find the name of the basic entity in the Edit Configuration Item Type dialog box, in the Attributes tab, in the Configuration Item Type Name field, in the Configuration Item Type Name field.



For example, change Measurement to sitescope_measurement. An example of the original string is as follows:

```
<entity id="product">
  <basicEntity>Measurement</basicEntity>
```

- h Usually the context menu does not need to be updated. An example of the original string is as follows:

```
<contextmenu>txMeasurementMenu</contextmenu>
```

- i For each rule listed for the basic entity, select **Admin > Dashboard > Repositories > Business Rules**, open the rules description, select the rule, clone it, and click the **Edit** button to display the rule’s parameters.

- j** Select each rule's parameter and click the **Edit** button to display the parameters details.
- k** For each rule parameter, create a **param** string in the XML File template. An example of the original string is as follows:

```
<param dataType="Long" displayValue="LowerBound"
key="LowerBound" readOnly="false" reference="true"
referencedProperty="RANK_1_FROM" />
```

- Change the value of the **dataType** parameter to the **Type** of the rule parameter. For example, the **Type** of the **duration** parameter details is **Long**.
- Change the value of the **displayValue** parameter to the name of the rule parameter (for example, change LowerBound to duration)
- Change the value of the **key** parameter to the name of the rule parameter (for example, change LowerBound to duration)
- If the value of **reference** is true, make sure that the **referencedProperty** value exists in the configuration file that corresponds to the current XML File template. An example of the original string is as follows:

```
<properties>
  <property key="RANK_1_FROM" value="12" />
```

- l** Remove the old parameters.
- m** The selectors do not need to be changed. An example of the original code is as follows:

```
<selectors type="AND">
  <selector dataType="String" key="sampleType" operator="EQ"
readOnly="true" reference="false"
referencedProperty="sampleType" value="trans_t" />
</selectors>
```

- 7 Add links between the basic entities after the `</autoMappingEntities>` tag and before the `<displayNameMapping />` tag. Enter the appropriate `src_obj_type`, `dest_obj_type`, `type`, and `weight`. For example, the following code describes the relationship between the two basic entities:

```
</autoMappingEntities>
  <autoMappingLinks>
    <link src_obj_type="sitescope_measurement"
      dest_obj_type="sitescope_measurement"
      type="Mercury:depends_on" weight="1" />
  </autoMappingLinks>
</displayNameMapping />
```

For details, see “Automapping – Relationship Details” in *Source Manager Administration*.

- 8 After you have completed the upgrade of all the basic entities, rules, and you have added the appropriate relationships, save the XML File source adapter template in the appropriate directory.

Upgrade the Configuration File

Upgrade the Configuration File to match the XML File source adapter template, as explained below.

To upgrade the Configuration File:

- 1 Open the appropriate Configuration File and make a backup copy. For details about the Configuration File, see “XML File” in *Source Manager Administration*.

- 2** For each CIT that was mapped to a basic entity in the XML File source adapter template, make sure that each one of the CIT keys appears in a **property key** string. For example, the basic entity product is mapped to the sitescope_measurement basic entity which has the measurement_id and session_id keys, so the product entity must have two properties: measurement_id and session_id. In addition, you must provide a unique value for each one of those properties. For example, the original string is:

```
<entities>
  <entity type="product">
    <name>product1</name>
    <!-- The properties that combine the entity's id.The combination
    must be unique in the external system
    -->
    <idProperties>
      <property key="prop1" value="val1" />
      <property key="prop2" value="val2" />
    </idProperties>
```

- 3** Remove the old property lines.
- 4** Add the children description in each parent entity description according to the automapping links you defined in the XML File source adapter template. For example, the strings that represent the children in the parent entity description under the </properties> tag of the parent entity.

```
<children>
  <idProperties>
    <property key="measurement_id" value="3"/>
    <property key="session_id" value="4"/>
  </idProperties>
</children>
```

- 5 In the same way, add the parents entity description in each child description. For example, the strings that represent the parent in the child entity description under the `</properties>` tag of the parent entity are:

```
<parents>
  <idProperties>
    <property key="measurement_id" value="1"/>
    <property key="session_id" value="2"/>
  </idProperties>
</parents>
```

- 6 Make sure that the referenced properties also appear in the XML File source adapter template. For example, the original properties are:

```
<properties>
  <property key="RANK_1_FROM" value="12"/>
  <property key="RANK_1_TO" value="12"/>
  <property key="INIT_STATE" value="20"/>
  <property key="location" value="Israel"/>
  <property key="host" value="bravo"/>
</properties>
```

- 7 Save the Configuration File in the appropriate directory.

13

Upgrading Service Level Management

This chapter describes how to upgrade service level agreements (SLAs) to work with Mercury Business Availability Center 6.6. You can upgrade SLAs, Service Level Management custom reports, and reports saved to the report repository.

This chapter describes:	On page:
Prerequisites	126
Notes and Limitations	127
SLA Upgrade and the Business Process Monitor Source Adapter	128
SLA Upgrade and the SiteScope Source Adapter	130
Upgrading SLAs from 5.x to 6.6	132
Upgrading Custom Reports	135
Upgrading the Report Repository	136
Upgrading Rules Used For SLA Conversions	137
Upgrade Messages	145

Prerequisites

This section includes issues that should be considered before beginning the upgrade procedure:

- ▶ To verify version 5.x SLA configuration data, you can display the Service Level Panorama report to view the SLA configuration in its entirety, in report format. To access the report, select **Applications > Service Level Management > Offline Reports > Service Level Panorama**. This step is optional.
- ▶ The version 6.x default KPI definitions for the upgrade process are stored in an XML file in the Infrastructure Settings Manager (select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, click **Applications**, select **Service Level Management**, and locate the **Upgrade KPIs** entry in the Service Level Management – SLM Admin table). Prior to upgrade, it is recommended to view this file and make any necessary changes.
- ▶ The version 6.x default objectives are stored in an XML file in the Infrastructure Settings Manager (select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, click **Applications**, select **Service Level Management**, and locate the **Default KPIs** entry in the Service Level Management – SLM Admin table). Prior to upgrade, it is recommended to make yourself familiar with the objective values.
- ▶ Verify that the Monitor configuration item type (CIT) has been successfully upgraded. For details, refer to *Upgrading Mercury Business Availability Center*. Verify, too, that monitors, transactions, and measurements have been successfully upgraded by viewing them in IT Universe or Monitor Administration. For details, see *Working with Monitor Administration*.
- ▶ If you are upgrading from Mercury Business Availability Center version 5.x and no 5.x default profile database was defined, you must define a default profile database in version 6.x to be able to work with Service Level Management.

Notes and Limitations

- ▶ Before upgrading your SLAs, perform the following checks:
 - ▶ Determine whether the definition of time intervals **24x7** or **Business Hours** on the pre-upgrade system is different from the out-of-the-box definition of time intervals **24x7** or **Business Hours** in version 6.6 (**Business Hours** is defined as 8AM-5PM, Mon-Fri).
 - ▶ Determine whether time intervals whose definition is different have the exact same name in the pre-upgrade system and 6.6.

If both of the above checks are true, before upgrading your SLAs you must delete the time intervals whose definitions do not match (do so from the **Admin > Service Level Management > Repositories > Time Intervals** page).

- ▶ Because of differences in architecture between Mercury Business Availability Center versions 5.x and 6.x, Service Level Management calculations may not be identical in the two versions. An SLA will probably show the same result for monitor (leaf) data, but data attached to CIs nearer the root may not be the same in both versions. For details about how SLAs can differ between the two versions, see “Upgrading Rules Used For SLA Conversions” on page 137.
- ▶ Due to backward compatibility issues, an upgraded SLA configuration is different to the previous version. Before performing the upgrade procedure, it is recommended that you save important reports to the report repository.
- ▶ Run offline reports before doing the SLA upgrade to remove non-existent monitors from the SLA.
- ▶ You cannot roll back the custom report upgrade. Before upgrading custom reports, verify that you are satisfied with the upgraded SLAs. You can also back up the custom report tables before upgrading the SLAs.
- ▶ Service Level Management calculates the SLA for the past three months only.
- ▶ If a 5.x transaction is filtered by location, you can avoid losing data by configuring the Business Process Monitor source adapter (before performing the upgrade process) so that CIs include location information. For details, see “SLA Upgrade and the Business Process Monitor Source Adapter” on page 128.

- ▶ If a 5.x monitor is filtered by monitor and measurement, you can avoid losing data by configuring the SiteScope source adapter (before performing the upgrade process) so that CIs include measurement performance objectives—and not only monitor objectives. For details, see “SLA Upgrade and the SiteScope Source Adapter” on page 130.
- ▶ If the SLA has the same name as a version 6.6 SLA, Service Level Management does not perform the upgrade process. You must change the name of either of the SLAs. For details, see “Upgrading SLAs from 5.x to 6.6” on page 132.

SLA Upgrade and the Business Process Monitor Source Adapter

If a 5.x transaction is filtered by location, you can avoid losing data in version 6.x SLAs by configuring the Business Process Monitor source adapter (before performing the upgrade process) so that CIs include location information.

To configure the Business Process Monitor source adapter:

- 1** Display the Edit Source window: **Admin > CMDB > Source Manager**.
- 2** Click the **Edit** button for the Business Process Monitor source adapter.
- 3** Select **Transaction/Location** in the Hierarchy structure field:

The screenshot shows a dialog box titled "Edit Source: Business Process Monitoring". It contains the following fields and controls:

- Type: Business Process Monitoring
- Name: Business Process Monitoring
- Server URL: http://localhost:8080/topaz
- Include Client Monitor profiles
- Hierarchy structure: Transaction/Location (dropdown menu)
- Sync interval: 60 minutes
- Enable

At the bottom of the dialog are four buttons: OK, Cancel, Edit Template, and Help.

For details on the hierarchy structure, see “Business Process Monitor Hierarchies” in *Source Manager Administration*.

Tip: If most of the 5.x SLAs are filtered by location, set an adapter’s hierarchy structure to **Transaction/Location**. If most SLAs are not filtered by location, set the hierarchy structure to **Regular**.

Example of 6.x SLA Dependent on Adapter Mode

In 5.x, an SLA may or may not include location information. The upgrade process upgrades the SLA according to:

- ▶ whether the SLA includes location information
- ▶ how the Business Process Monitor source adapter is configured

The following table shows how the upgrade process configures the 6.x SLA:

Version 5.x	Version 6.x	
	Business Process Monitor Source Adapter Set at Transaction/Location	Business Process Monitor Source Adapter Set at Regular
Transaction (EverGreen) filtered by location (wall_050904): 	<p>EverGreen └─ wall_050904</p> <p>Upgrade process adds a CI of type BP Step and below it, a CI of type Transaction from Location, thereby replicating the 5.x SLA exactly.</p>	<p>EverGreen └─ EverGreen</p> <p>Upgrade process does not recognize location, so adds transaction only to the SLA.</p>
Transaction not filtered by location	<p>EverGreen ├─ wall ├─ wall_05 └─ wall_050904</p> <p>Upgrade process adds a CI of type BP Step and below it, a CI of type Transaction from Location for all 6.6 locations.</p>	<p>EverGreen └─ EverGreen</p> <p>Upgrade process replicates the 5.x SLA exactly.</p>

SLA Upgrade and the SiteScope Source Adapter

If a 5.x monitor is filtered by monitor and measurement, you can avoid losing data in version 6.x by configuring the SiteScope source adapter (before performing the upgrade process) so that CIs include measurement performance objectives—and not only monitor objectives.

To configure the SiteScope source adapter:

- 1** Display the Edit Source window: **Admin > CMDB > Source Manager.**
- 2** Click the **Edit** button for the SiteScope source adapter.

3 Select the **Include measurements** check box in the Edit Source window:

The screenshot shows a dialog box titled "Edit Source: SiteScope". It contains the following fields and options:

- Type: SiteScope
- Name: SiteScope
- Server URL: http://localhost:8080/topaz
- Exclude profiles: (empty text box)
- Include measurements
- Include machines
- Sync interval: 60 minutes
- Enable

At the bottom of the dialog are four buttons: OK, Cancel, Edit Template, and Help.

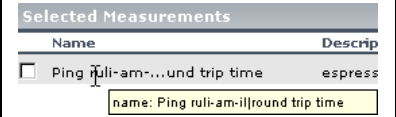
For details on editing the SiteScope source, see “SiteScope Hierarchies” in *Source Manager Administration*.

Example of 6.x SLA Dependent on Adapter Mode

In 5.x, an SLA may or may not include measurement information. The upgrade process upgrades the SLA according to:

- whether the SLA includes a SiteScope performance objective
- how the SiteScope source adapter is configured

The following table shows how the upgrade process configures the 6.x SLA:

Version 5.x	Version 6.x	
	SiteScope Source Adapter: Include Measurements Check Box Selected	SiteScope Source Adapter: Include Measurements Check Box Not Selected
Monitor (Ping ruli-am-il) filtered by measurement (round trip time): 	With measurements: Ping ruli-am-il └─ round trip time Upgrade process replicates the 5.x SLA exactly.	Monitor only: Ping ruli-am-il Upgrade process adds monitor only to the SLA. Note: You will lose SiteScope performance objectives data for this customer.

Upgrading SLAs from 5.x to 6.6

This section explains how to upgrade service level agreements from version 5.x to 6.6 and how to delete 5.x SLAs.

The SLA table includes the following components:

- **Name.** The name of the SLA
- **Description.** The description of the SLA
- **Status.** Shows whether the upgrade process has run

You can sort the list by name, description, or status: An arrow next to a title shows by which column the SLAs are sorted, and also the direction in which the column has been sorted (that is, ascending or descending).

Actions. These buttons show the actions that you can perform on the SLA: **Simulate**, **Upgrade**, **Roll Back**, and **View Log**.

To upgrade version 5.x SLAs to version 6.6:

- 1** Select **Admin > Platform > Setup and Maintenance** and click the **Service Level Management Upgrade** link to open the upgrade page. The page shows a list of SLAs that are not compatible with version 6.6, organized alphabetically.
- 2** Locate the SLA you want to upgrade.

Note: If the SLA has the same name as a version 6.6 SLA, Service Level Management does not perform the upgrade process. You must change the name of either of the SLAs.

- 3** To view upgrade results and identify configuration changes, click **Simulate**. This step is optional but highly recommended.

Service Level Management displays the Upgrade Warnings window. Read through the warnings. You can copy the information in this window to a text editor by copying and pasting.

During simulation, Service Level Management updates all components of an SLA apart from its associations with KPIs and objectives.

- 4** If you are satisfied with the results, return to the upgrade page and click **Upgrade**. The SLA's status changes to **Upgraded** and the **Upgrade** button changes to **Roll Back**.

At the end of the upgrade process, the Upgrade Warning window is displayed again. The first message informs you that the SLA has been upgraded successfully. The other messages are intended to help you decide whether you want to change the SLA in version 6.6 or to accept the upgraded version. Click **OK** to return to the Upgrade page.

- 5** To review the changes to the upgraded SLA in the Service Level Agreements page, click **Review 6.6 Configuration**. The SLA is now displayed in the list of SLAs that are compatible with version 6.6.

Note:

- ▶ An upgraded 6.6 SLA is not identical with the original 5.x version.
- ▶ It is highly recommended to use the SLA Wizard to check the SLA, make changes to the SLA (if necessary), and save it.

When checking an SLA, pay special attention to the default objectives, especially if they are replacing 5.x services and groups (in the cases where the 5.x SLA does not include overall objectives).

- ▶ You must start the SLA (that is, click the **Start** button) for Service Level Management to calculate the SLA. Service Level Management calculates the SLA for the past three months only.
-

- 6** Click **View Log** to view a chronological account of the upgrade process and the warning messages.

Logs are saved to the Data Processing Server.

- 7** Continue to upgrade the SLAs. Repeat steps 2 to 5 for each SLA.

To upgrade or roll back several SLAs simultaneously:

Note: This procedure is not recommended as it slows down performance and creates many warning notifications.

- 1** Select the check boxes of the SLAs you want to upgrade or roll back.
- 2** Click the **Upgrade** or **Roll Back** button below the list of SLAs.
- 3** Continue with the upgrade process, as described in the previous section.

The next step is to upgrade the custom reports. For details, see “Upgrading Custom Reports” on page 135.

To delete version 5.x SLAs:

You can upgrade custom reports to version 6.6 only after you have upgraded all 5.x SLAs. If there are SLAs that you do not wish to upgrade (for example, because they are no longer relevant to your system), you must delete them.

- 1 Select the check boxes of the SLAs you want to delete.
- 2 Click the **Delete** button below the list of SLAs.

Upgrading Custom Reports

You can upgrade Service Level Management custom reports only when all SLAs have been upgraded.

Important: You cannot roll back custom reports. Before performing the upgrade, verify that you are satisfied with the upgraded SLAs. You can also back up the custom report tables before upgrading the SLAs.

To upgrade custom reports:

- Click **Upgrade** to update existing Service Level Management custom reports.
- Click **Review 6.6 Configuration** to access the list of custom reports.

Version 5.x Reports	Version 6.6 Report
Executive Scorecard	SLAs Summary
Availability Snapshot Performance Snapshot	Time Range Comparison Note: If there are many SLAs in the 5.x Availability or Performance Snapshots, there will be one 6.6 Time Range Comparison report for each SLA.
Service Status	CI Status – only the service is saved to this version

Version 5.x Reports	Version 6.6 Report
Availability Over Time vs. SLA	CI Over Time vs. Target
Time Range Comparison	Time Range Comparison – only the service is saved to this version
Service Outages	Outages Summary – only the service is saved to this version. All outage categories are displayed.

- ▶ There is no Availability by Location/Group report. To produce a similar report, you must create an SLA to which you assign CIs for specific locations or groups.

Upgrading the Report Repository

Note: You can upgrade the Service Level Management report repository without upgrading the SLAs or custom reports.

- ▶ Click **Upgrade** to update the Service Level Management reports saved to the report repository.
- ▶ Click **Review 6.6 Configuration** to access the Report Repository page.

Upgrading Rules Used For SLA Conversions

Service Level Management uses a very complex algorithm to map SLAs from previous versions to version 6.6. However, due to backward compatibility issues (deriving from a difference in hierarchical structure), an upgraded 6.6 SLA is not identical with the 5.x SLA. The reasons for these differences are listed in this section.

Note: Transactions, measurements, and external data are collectively called data sources in this section.

For a note on the meaning of default objectives, see “Prerequisites” on page 126.

This section includes the following topics:

- “SLA Structure Issues” on page 137
- “Data Source and Objective Issues” on page 138
- “Downtime and Other Event Issues” on page 141
- “Service Level Management Report Issues” on page 142
- “Time Interval Issues” on page 143
- “Time Zone Issues” on page 144
- “Day of the Week Issues” on page 144
- “Notes” on page 144

SLA Structure Issues

- The upgraded SLA structure depends on the source adapter’s hierarchy structure. For details, see *Source Manager Administration*.
- The start date is set to three months prior to the date on which the SLA is upgraded. The end date is set at a year ahead of the upgrade date.
- For a previous version’s SLA groups and services, the upgrade process creates a CI for each group and service (to preserve the SLA’s structure).

- ▶ Any groups or services that do not have data sources are discarded.
- ▶ For a CI created from an SLA group, SLA, or service, the upgrade process gives default objectives to the CI. For SLA groups, however, if an overall objective was set in 5.x, the CI is given the 5.x overall objective and not the default objective.

Data Source and Objective Issues

- ▶ If a group includes data sources other than Business Process Monitor and SiteScope sources (that is, Real User Monitor data or external data), the data sources are discarded and are not included in the SLA.
- ▶ Previously, a data source was filtered by location. The upgrade process adds a CI of type BP Step to the SLA for each data source. Under this CI, the upgrade process adds a CI of type BP Transaction from Location for each previously-existing location.

If a 5.x transaction was not filtered by location and, before running the upgrade process, you set the adapter to a Transaction/Location hierarchy structure (for details, see “Prerequisites” on page 126), the upgrade process assigns each existing location to a transaction (with a CI of type BP Transaction from Location). This means that each SLA includes more information.

If the original SLA did not have a node equivalent to the CI of type BP Step and no objectives were defined for the SLA, the upgrade process assigns default objectives for the new CIs. For details on the default KPI definitions for the upgrade process, see “Prerequisites” on page 126.

- ▶ If a data source appears more than once in the original SLA, the upgrade process maps all instances of the data source to only one CI. The upgrade process selects the first occurrence of a KPI or objective. Furthermore, identical data sources running on the same location are also mapped to one CI and here, too, the first occurrence of a KPI or objective is selected.

To retain the original 5.x data, use one of the following options:

- ▶ Create an SLA (in version 6.6) for each service.

For example, a 5.x SLA includes one transaction and two services: Transaction A has an objective of 99% in Service 1, and 97% in Service 2. Create two SLAs, SLA 1 for Service 1 and SLA 2 for Service 2. Assign an objective of 99% to SLA 1 and an objective of 97% to SLA 2.

Tip: Clone the SLA, creating the same number of SLAs as there are services. Change each SLA according to one of the services. For details, refer to the SLM section of *Application Administration*.

- ▶ Configure the upgraded SLA so that it includes more than the Exceeded and Failed targets (for details, refer to the SLM section of *Application Administration*). Define an objective and set its 5.x higher value to the higher target and the lower value to the lower target.

For example, a 5.x SLA includes one transaction and two services: Transaction A had an objective of 99% in Service 1, and 97% in Service 2. Set the objectives for the 6.6 SLA so that **Exceeded** has an objective of 99% and **Met** has an objective of 97%.

- ▶ If an SLA previously included a service without any data sources, the upgrade process removes the service from the SLA's hierarchy.
- ▶ If an SLA previously included a service with data sources filtered by one or more locations, the upgrade process adds a CI of type BP Step to the SLA for each location.
- ▶ If an SLA did not previously include a performance percentile objective, the upgrade process cannot add a Six Sigma performance objective to the SLA, and the objective is discarded.

To support the Performance Six Sigma metric in version 6.6, the following objectives must have been defined for an SLA in version 5.x: percentile performance objectives and Six Sigma performance objectives.

- ▶ If the upgrade process cannot locate a Business Process Monitor or SiteScope monitor in version 6.6 that existed in version 5.x, the monitor is not added to the SLA.

- ▶ If the upgrade process cannot locate a Business Process Monitor transaction or a SiteScope measurement in version 6.6 that existed in version 5.x, the measurement is not added to the SLA.
- ▶ Before the upgrade process, if an adapter was not configured to support CIs per measurement, the upgrade process cannot upgrade the overall performance objectives for the SLA's groups.
- ▶ The definition of a data source in version 5.x is not the same as in 6.6: a data source in version 5.x can receive data from any location, whereas a data source in version 6.6 can receive data only from locations already defined in version 6.6.
- ▶ You cannot automatically filter Business Process Monitor transactions by group. This is because groups are not included in the IT Universe. You can, however, manually define a new configuration item (CI) with dedicated selectors and associate it with the SLA.
- ▶ If a data source was previously filtered by BPM group (that do not exist in version 6.6), the upgrade process removes the group filter from the SLA for that data source. Following the upgrade, the SLA includes only one instance of the data source which does not include any group filter. Also, the SLA's objective is taken from the first occurrence found by the upgrade process.

Example 1: a 5.x SLA contains two measurements, bloomberg ssl filtered on group wall_050409 and bloomberg ssl filtered on group wall_050409_2:

Selected Measurements			
Name	Description	Profile	Monitor Type
<input type="checkbox"/> bloomberg ssl 2		prfbpm	Business Process Monitor
<input type="checkbox"/> bloomberg ssl... wall_050409_1		prfbpm	Business Process Monitor
<input type="checkbox"/> bloomberg ssl... all_050409_2]	name: bloomberg ssl [Group: wall_050409]		Business Process Monitor
<input type="checkbox"/> bloomberg ssl... all_050409_2]		prfbpm	Business Process Monitor

The upgrade process creates an SLA with CI bloomberg ssl.

Example 2: a 5.x SLA contains a measurement, `bloomberg ssl`, filtered on two groups, `wall_050904` and `wall_050904_2`:

Selected Measurements			
Name	Description	Profile	Monitor Type
<input type="checkbox"/>	bloomberg ssl 2	prfbpm	Business Process Monitor
<input type="checkbox"/>	bloomberg ssl... wall_050904]	prfbpm	Business Process Monitor
<input type="checkbox"/>	bloomberg ssl...all_050904_2]	prfbpm	Business Process Monitor
<input type="checkbox"/>	bloomberg ssl...all_050904_2]	prfbpm	Business Process Monitor

name: bloomberg ssl [Group: wall_050904; wall_050904_2] Select All Delete Selected

The upgrade process creates an SLA with a CI named `bloomberg ssl`.

- ▶ Outlier trimming is not supported. Trimming is supported.

Previously, in version 5.x, you could import outlier thresholds from the transaction threshold configuration in Monitor Administration. In version 6.6, the outlier trimming setting is no longer supported. Trimming is now calculated by the trimming condition rule parameter.

Downtime and Other Event Issues

- ▶ If an event's end date has expired (that is, the end date falls before the 6.6 SLA's start date), the upgrade process discards the event.
- ▶ Downtime granularity was changed to 5 minutes in version 6.0. Following upgrade, you should check downtime durations.

During upgrade, event start times are rounded downwards and end times are rounded upwards. For example, the period 12:37 to 13:31 becomes 12:35 to 13:35.

- ▶ If an event is defined on a BPM group, the upgrade process discards the event (because BPM groups no longer exist in version 6.6).
- ▶ For event CIs of type BP Group Location, the upgrade process discards the event, due to a backward compatibility issue.
- ▶ If an event's name already exists in version 6.6, the upgrade process changes the current event name by appending the SLA name in brackets to the event name.
- ▶ If an event's CI of type BP Step is not found, the upgrade process discards the event.

- If an event's CI of type BP Location is not found, the upgrade process discards the event.
- If an event's CI of type BP Transaction from Location is not found, the upgrade process discards the event.
- If an event is defined as a BPM event on all SLAs and the event is not defined on a specific BPM item, it is upgraded as an SLA event on all SLAs.
- If an event is defined as a BPM event on a single SLA and the event is not defined on a specific BPM item, it is upgraded as an SLA event on a single SLA.

Service Level Management Report Issues

- The following reports take a different format in version 6.6:

Version 5.x Reports	Version 6.6 Report
Executive Scorecard	SLAs Summary
Availability Snapshot Performance Snapshot	Time Range Comparison Note: If there are many SLAs in the 5.x Availability or Performance Snapshots, there will be one 6.6 Time Range Comparison report for each SLA.
Service Status	CI Status – only the service is saved to this version
Availability Over Time vs. SLA	CIs Over Time vs. Target
Time Range Comparison	Time Range Comparison – only the service is saved to this version

- There is no Availability by Location/Group report. To produce a similar report, you must create an SLA to which you assign CIs for specific locations or groups.
- Report customizations are not upgraded.

- ▶ If the upgrade process does not succeed in upgrading one component of a custom report, you should use the Custom Report Manager to delete the component.
- ▶ The upgrade process calculates to-date reports till yesterday midnight.
- ▶ The upgrade process cannot upgrade reports that include active filters.
- ▶ The upgrade process can upgrade reports for predefined tracking periods only. For example, the process will not upgrade a report which includes a single value for the last three days.
- ▶ The upgrade process assigns calendar tracking periods only to reports. The minimum tracking period granularity is one hour.
- ▶ The upgrade process cannot assign headers or footers from version 5.x SLAs to version 6.6 SLAs Service Level Management reports. However, if the header and footer are part of a custom report, they are upgraded. You define headers and footers for reports in the Infrastructure Settings Manager.
- ▶ The upgrade process stores reports in the report repository in .pdf format only.

Time Interval Issues

- ▶ Before upgrading your SLAs, perform the following checks:
 - ▶ Determine whether the definition of time intervals **24x7** or **Business Hours** on the pre-upgrade system is different from the out-of-the-box definition of time intervals **24x7** or **Business Hours** in version 6.6 (**Business Hours** is defined as 8AM-5PM, Mon-Fri).
 - ▶ Determine whether time intervals whose definition is different have the exact same name in the pre-upgrade system and 6.6.

If both of the above checks are true, before upgrading your SLAs you must delete the time intervals whose definitions do not match (do so from the **Admin > Service Level Management > Repositories > Time Intervals** page).
- ▶ Time intervals can no longer be associated with a specific SLA, but are now global functions.
- ▶ If no objectives were associated with a time interval in version 5.x, the time interval is not added to the version 6.6 SLA.

- ▶ Time intervals no longer include calculation metrics, which are now incorporated in a KPI's business rule. Therefore, you cannot now define different metrics for a CI's time intervals (for example, you cannot define an average performance metric for the 24x7 time interval, and a percentile performance metric for Business Hours).
- ▶ In version 6.6, each time interval is unique and includes a specific schedule. During the upgrade process, if the schedule is the same, it is associated with the SLA. If the schedule is different, a time interval is created and it is associated with the SLA.

Time Zone Issues

If a version 5.x time zone is not supported in version 6.6, the upgrade process assigns to the SLA the first occurrence of a time zone with the same time difference as the 5.x time zone.

Day of the Week Issues

During upgrade, if the first day of the week has not been defined for the same day in versions 5.x and 6.6, you are asked to choose which definition to use as a default.

Notes

- ▶ Any changes you make to running 6.6 SLAs (configuration changes, time interval changes, or downtime event changes) do not affect the SLA retroactively, unless the changes are made before you start the SLA. To update the SLA for previous tracking periods, you must recalculate the data. For details, refer to the SLM section of *Application Administration*.
- ▶ Service Level Management can recalculate SLAs for the past three months only. (This parameter is configurable in the Infrastructure Settings Manager. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, click **Applications**, select **Service Level Management**, and locate the **Recalculation period limit** entry in the Service Level Management – SLM Admin table.)
- ▶ The upgrade process can fail if one of the following is exceeded: the CMDB object quota, the active TQL quota, the number of views.

Upgrade Messages

The following table includes the messages that Service Level Management displays following the successful upgrade of an SLA. The messages in this table follow the order in the Service Level Management application.

Message	Description
SLA end date is set to (<value>).	The start date is set to three months prior to the date on which the SLA is upgraded. The end date is set at a year ahead of the upgrade date. Note: The start date is configurable. For details, see the explanation in “Notes” on page 144.
Time zone <value> is not supported in 6.6. Assigning SLA to <value> time zone instead.	If a version 5.x time zone is not supported in version 6.6, the upgrade process assigns to the SLA the first occurrence of a time zone with the same time difference as the 5.x time zone.
SLA Owner name not found (User ID: <value>).	If a version 5.x does not include a user ID, the SLA owner name is ignored.
Time Interval (<value>) already exists and found to have the same schedule. Associating it with the SLA.	For version 6.6, each time interval is unique and includes a specific schedule. Check each SLA. If the schedule is the same, associate it with the SLA. Prior to version 6.6, it was possible to define different schedules for a time interval, depending on the SLA with which the time interval was associated.
Time Interval (<value>) was found but had a different schedule, creating a new time interval and associating it to SLA.	Check each SLA. If the schedule is different, create a time interval and associate it with the SLA.
Time Interval (<value>) has no objectives in 5.x, and therefore is not added to the 6.6 SLA.	If no objectives were associated with a time interval in version 5.x, the time interval is not added to the version 6.6 SLA.
Service (<value>) had no data sources, removed from SLA's hierarchy.	If an SLA previously included a service without any data sources, the upgrade process removes the service from the SLA's hierarchy.

Message	Description
<p>Group (<value>) contains Data Sources of type other than BPM and SiS. Those Data Sources are discarded.</p>	<p>The upgrade process upgrades Business Process Monitor and SiteScope data sources only. Other data sources, such as Real User Monitor and custom classes, are discarded.</p>
<p>Service Data Source (<value>) is filtered by several locations. Adding CI for each of the locations.</p>	<p>Previously, a data source was filtered by location. The upgrade process adds a CI of type BP Step to the SLA for each data source. Under this CI, the upgrade process adds a CI of type BP Transaction from Location for each previously-existing location.</p> <p>If the original SLA did not have a node equivalent to the CI of type BP Step and no objectives were defined for the SLA, the upgrade process assigns default objectives for the new CIs.</p>
<p>Service Data Source (<value>) is filtered by single location. Adding CI for the location.</p>	

Message	Description
<p>Service Data Source (<value>) ingredients already appear in the SLA. Please note that the objectives were already upgraded.</p>	<p>If a data source appears more than once in the original SLA, the upgrade process maps all instances of the data source to only one CI. The upgrade process selects the first occurrence of a KPI or objective. Furthermore, identical data sources running on the same location are also mapped to one CI and here, too, the first occurrence of a KPI or objective is selected.</p> <p>To retain the original 5.x data, use one of the following options:</p> <ul style="list-style-type: none"> ▶ Create an SLA (in version 6.6) for each service. For example, a 5.x SLA includes one transaction and two services: Transaction A has an objective of 99% in Service 1, and 97% in Service 2. Create two SLAs, SLA 1 for Service 1 and SLA 2 for Service 2. Assign an objective of 99% to SLA 1 and 97% to SLA 2. <p>Tip: Clone the SLA, creating the same number of SLAs as there are services. Change each SLA according to one of the services. For details, refer to the SLM section of <i>Application Administration</i>.</p> ▶ Configure the upgraded SLA so that it includes more than the Exceeded and Failed targets. For details, refer to the SLM section of <i>Application Administration</i>. Define an objective and set its 5.x higher value to the higher target and the lower value to the lower target. For example, a 5.x SLA includes one transaction and two services: Transaction A has an objective of 99% in Service 1, and 97% in Service 2. Set the objectives for the 6.6 SLA so that Exceeded has an objective of 99% and Met has an objective of 97%.
<p>Service Data Source (<value>) ingredients do not appear in 6.6, and therefore the data source is not added.</p>	<p>If the data source does not exist in the CMDB, the data source is not added to the 6.6 SLA.</p>
<p>Service Data Source (<value>) is filtered by Group(s). Adding CI for each of the locations.</p>	<p>If an SLA was previously filtered by BPM groups (that do not exist in version 6.6), the upgrade process adds a CI of type BP Step with a child for each location.</p>

Message	Description
<p>Service Data Source (<value>) is filtered by Location(s), but the model does not support by-location CIs.</p>	<p>If a 5.x SLA includes transactions filtered by one or more locations and the hierarchy structure is set to Regular, the upgrade process adds a CI of type BP Step to the SLA without any children.</p> <p>To include locations in the SLA, you must change the hierarchy structure. For details, see “SLA Upgrade and the Business Process Monitor Source Adapter” on page 128.</p>
<p>Service Data Source (<value>) is not filtered, but the model supports by-location CIs.</p>	<p>If a 5.x SLA includes transactions not filtered by location and the hierarchy structure is set to Transaction/Location, the upgrade process assigns all 6.6 locations to a transaction (with a CI of type BP Transaction from Location).</p> <p>Following the upgrade process, when you check the SLA, you can remove the unwanted locations.</p> <p>Note: Do not remove all locations from the transaction, otherwise the data is disabled. You must leave at least one location (as a data source) in the SLA.</p>
<p>Performance 6-Sigma Objective cannot be defined for group (<value>), because no performance objective defined.</p>	<p>If an SLA did not previously include an overall performance percentile objective, the upgrade process cannot add a Six Sigma performance objective to the SLA, and the objective is discarded.</p> <p>To support the Performance Six Sigma metric in version 6.6, the following objectives must have been defined for an SLA in version 5.x: percentile performance objectives and Six Sigma performance objectives.</p>
<p>The SiteScope monitor was not found in version 6.6 for the measurement (<value>).</p>	<p>If the upgrade process cannot locate a SiteScope monitor in version 6.6 that existed in version 5.x, the monitor is not added to the SLA.</p> <p>For a note on other reasons for a missing object, see “Prerequisites” on page 126.</p>
<p>The SiteScope measurement was not found in version 6.6 for the version 5.1 measurement (<value>).</p>	<p>If the upgrade process cannot locate a SiteScope measurement in version 6.6 that existed in version 5.x, the measurement is not added to the SLA.</p>

Message	Description
SiteScope has not been configured to support by-measurement CIs, so performance objectives cannot be upgraded for measurement (<value>).	If performance objectives have been defined for a version 5.x SLA that includes a service with System class (SiteScope) measurements, you can avoid losing the measurement data in version 6.6. Configure the SiteScope source adapter so that the upgrade process upgrades measurement performance objectives—and not only monitor objectives. This must be done before performing the upgrade process. For details, see “SLA Upgrade and the SiteScope Source Adapter” on page 130.
SiteScope has not been configured to support by-measurement CIs, so the overall performance objective cannot be upgraded for group (<value>).	
Cannot upgrade event defined on BPM group. Event name: (<value>).	If an event is defined on a BPM group, the upgrade process discards the event (because BPM groups no longer exist in version 6.6).
Events on location from profile are not supported. Event: (<value>).	Due to backward compatibility issues, the upgrade process cannot upgrade events based on a specific profile’s location.
Discarding event (<value>). Its end date has expired.	If an event’s end date has expired (that is, the end date falls before the 6.6 SLA’s start date), the upgrade process discards the event.
The event name (<value>) already exists. Changing name to (<value>).	If an event’s name already exists in version 6.6, the upgrade process changes the current event name by appending the SLA name in brackets to the event name.
Location CI (<value>) was not found for event (<value>). Discarding this event.	If an event’s location cannot be mapped to a 6.6 CI, the upgrade process discards the event. The reason that the event is not found in version 6.6 may be because the object on which the event is based no longer exists. For a note on other reasons for a missing object, see “Prerequisites” on page 126.
BP Group CI was not found for event (<value>). Discarding this event.	
BP Step CI was not found for event (<value>). Discarding this event.	
BP transaction from location CI was not found for event (<value>). Discarding this event.	

Part II • Upgrade Procedures

Message	Description
Changing event (<value>) scheduling. Previous scheduling: start limit date <value>, event range: <value> - <value>. Upgraded scheduling: start limit date <value>, event range: <value> - <value>.	<ul style="list-style-type: none">▶ Due to backward compatibility issues, the upgrade process concatenates the start limit date and hour to one value.▶ During upgrade, event start times are rounded downwards and end times are rounded upwards. For example, the period 12:37 – 13:31 becomes 12:35 – 13:35.▶ Downtime granularity was changed to 5 minutes in version 6.0. Following upgrade, you should check downtime duration periods.
Changing event (<value>) start limit time from <value> to <value>.	
Changing event (<value>) scheduling from <value> - <value> to <value> - <value>.	

14

Switching Mercury Business Availability Center URL on the Data Collectors

This chapter describes how to configure your data collectors to work with new Mercury Business Availability Center 6.6 servers.

This chapter describes:	On page:
Overview of Switching Data Collectors	151
Redirecting the Business Process Monitor URL	152
Redirecting the Client Monitor URL	153
Redirecting the SiteScope URL	154
Redirecting the Real User Monitor URL	156

Overview of Switching Data Collectors

If you install Mercury Business Availability Center 6.6 on a new machine or machines, you must update all the data collectors (Real User Monitor, Business Process Monitor, Client Monitor, and SiteScope) to report to the new Mercury Business Availability Center 6.6 servers.

Note: If you installed Mercury Business Availability Center 6.6 on new servers, but those servers are behind load balancers whose URL did not change, you do not need to update the data collectors that are using the load balancer's URL. You may, however, need to update the load balancer with the IPs of the new Mercury Business Availability Center server machines. For details on implementing a distributed deployment of Mercury Business Availability Center servers, refer to *Deploying Servers*.

Redirecting the Business Process Monitor URL

Use the following procedure if you need to update the Business Process Monitor data collector to report to the new Mercury Business Availability Center 6.6 server.

To redirect the Business Process Monitor URL:

- 1** On each Business Process Monitor host machine, open Business Process Monitor Admin.
- 2** For each Business Process Monitor instance, edit the URL for the Core Server to point to the new Mercury Business Availability Center 6.6 Core Server machine. For more details, refer to *Business Process Monitor Administration*.
- 3** Click **Save Changes and Restart Instance**. The Business Process Monitor restarts the instance.
- 4** Repeat for each Business Process Monitor instance.
- 5** Add scripts used for Topaz 4.5 FP2 (or for Mercury Business Availability Center 5.x) Business Process Transaction Monitors to the Mercury Business Availability Center 6.6 Script Repository. For details on adding scripts to the Script Repository from Monitor Administration, see "Managing Business Process Profiles" in *End User Management Data Collector Configuration*.

Redirecting the Client Monitor URL

Use the following procedure if you need to update the Client Monitor data collector to report to the new Mercury Business Availability Center 6.6 server.

To redirect the Client Monitor URL for version 5.0 FP1 Client Monitor Agents and later:

- 1 From the Start menu of a Client Monitor Agent machine, click **Programs > Mercury Client Monitor > Client Monitor Agent Settings**. Client Monitor opens the Client Monitor Agent Settings dialog box.

Note that if the Client Monitor Agent has not been configured to appear in the Start menu, you can open the Settings utility by running the following executable: \<MercuryClient Monitor root directory>\bin\OLConfig.exe.

- 2 Enter the new URL in the **AM Core URL** box.
- 3 Save the changes.
- 4 Restart Client Monitor.
- 5 Add scripts used for Topaz 4.5 FP2 (or for Mercury Business Availability Center 5.x) Client Monitor Transaction Monitors to the Mercury Business Availability Center 6.6 Script Repository. For details on adding scripts to the Script Repository from Monitor Administration, see “Creating and Managing Client Monitor Profiles” in *End User Management Data Collector Configuration*.

To redirect the Client Monitor URL for pre-version 5.0 FP1 Client Monitor Agents:

- 1 On the end-user machine, run the file \<MercuryClient Monitor root directory>\bin\OLConfig.exe.
The Client Monitor Agent Settings dialog box opens.
- 2 Enter the new URL in the **AM Core URL** box.
- 3 Click **Save & Exit**.
- 4 Restart Client Monitor.

- 5 Add scripts used for Topaz 4.5 FP2 (or for Mercury Business Availability Center 5.x) Client Monitor Transaction Monitors to the Mercury Business Availability Center 6.6 Script Repository. For details on adding scripts to the Script Repository from Monitor Administration, see “Creating and Managing Client Monitor Profiles” in *End User Management Data Collector Configuration*.

Redirecting the SiteScope URL

If Mercury Business Availability Center 6.6 is installed using the same machines as the previous Mercury Business Availability Center 5.x or Topaz 4.5 FP2 system, it is not necessary to redirect the SiteScope URL for SiteScope 8.x, but you must update the port number.

To redirect the port number for version 8.x if Mercury Business Availability Center 6.6 has been installed on existing Mercury Business Availability Center 5.x or Topaz 4.5 FP2 machines:

- 1 Before the upgrade, detach SiteScope from Mercury Business Availability Center.
- 2 After the upgrade, edit SiteScope in Monitor Administration and change the port to the port number of the new SiteScope interface. The default port number is 8080.
- 3 Attach SiteScope to Mercury Business Availability Center.

To redirect the SiteScope 8.0 SP1 and later URL:

- 1 Before the upgrade, detach SiteScope from Mercury Business Availability Center.
- 2 Using SiteScope classic interface, change the Mercury Business Availability Center Core Server name, user name, and user password.
- 3 Restart SiteScope.
- 4 In Monitor Administration, change the Mercury Business Availability Center Core Server, user name, and user password. Also, change the port number to the port number of the new SiteScope interface. The default port number is 8080.

- 5 Attach SiteScope. For details, see *SiteScope Administration*.

To redirect the SiteScope 8.0 URL:

- 1 Before the upgrade, detach SiteScope from Mercury Business Availability Center.
- 2 Stop SiteScope.
- 3 Export the SiteScope configuration.
- 4 Change all occurrences of the Mercury Business Availability Center Core Server name, user name, and user password.
- 5 Import the configuration.
- 6 Start SiteScope.
- 7 In Monitor Administration, change the Mercury Business Availability Center Core Server, user name, and user password. Also, change the port number to the port number of the new SiteScope interface. The default port number is 8080.
- 8 Attach SiteScope. For details, see *SiteScope Administration*.

To redirect the SiteScope 7.9.1.0/7.9.5 URL:

- 1 Before the upgrade, detach SiteScope from Mercury Business Availability Center.
- 2 Stop SiteScope.
- 3 Export the SiteScope configuration.
- 4 Change all occurrences of the Mercury Business Availability Center Core Server name, user name, and user password.
- 5 Import the configuration.
- 6 Start SiteScope.
- 7 In Monitor Administration, change the Mercury Business Availability Center Core Server, user name, and user password.
- 8 Attach SiteScope. For details, see *SiteScope Administration*.

Note:

- ▶ To import or export SiteScope configuration in versions 7.9.x, run the following command from the classes directory:
`..\java\bin\java COM.freshtech.TopazIntegration.AMSettingsManager import/export <filename>`
 - ▶ To import or export SiteScope configuration in version 8.0.0.1, run the following command from the WEB-INF/classes directory:
`..\java\bin\java COM.freshtech.TopazIntegration.AMSettingsManager import/export <filename>`
-

Redirecting the Real User Monitor URL

Use the following procedure if you need to update the Real User Monitor data collector to report to the new Mercury Business Availability Center 6.6 server.

To redirect the Real User Monitor URL:

- 1** Access the JMX console by entering the following URL in your Web browser:
`http://<Real User Monitor engine machine name>:8180/jmx-console`
- 2** In the JMX Agent View, scroll down to the **RUM.modules** section and click **service=ResolverURLMConfig**.
- 3** In the relevant parameter, change the setting to the required value.
- 4** Click the **Apply Changes** button.

For details, see “Configuring and Administering the Real User Monitor Engine” in *End User Management Data Collector Configuration*.

15

Upgrading Components

This chapter describes how to upgrade Mercury Business Availability Center components to work with Mercury Business Availability Center 6.6.

This chapter describes:	On page:
Business Process Monitor	158
Client Monitor	159
SiteScope	162
Real User Monitor	164
Virtual User Generator (VuGen)	169
Discovery Probe	172

Business Process Monitor

Mercury Business Availability Center 6.6 includes Business Process Monitor 6.6, but works with Business Process Monitor 4.5 FP2 and later. You do not need to upgrade Business Process Monitor unless you want to benefit from the enhanced functionality of later versions.

Note:

- ▶ Business Process Monitor 6.6 does not support versions of QuickTest Professional earlier than version 9.0.
 - ▶ Scripts recorded with VuGen 8.1 can only run on Business Process Monitor 6.1 and later. Scripts recorded with older versions of VuGen, however, can run on Business Process Monitor 6.6.
-

Business Process Monitor 6.6

Business Process Monitor 6.6 supports enhanced functionality from Mercury Virtual User Generator (VuGen). For details, see “Virtual User Generator (VuGen)” on page 169.

For details about other enhancements in Business Process Monitor prior to version 6.6, see the **What’s New?** file in:

- ▶ Mercury Business Availability Center Documentation Portal area on the Mercury Customer Support Web site (support.mercury.com)
- ▶ Business Process Monitor Admin Online Help menu

To upgrade Business Process Monitor to 6.6:

- 1** Uninstall the current version with the option to save the current configuration.
- 2** In Mercury Business Availability Center 6.6, select **Admin > Platform > Setup and Maintenance > Downloads**.
- 3** Click the **Mercury Business Process Monitor** link to access the Business Process Monitor 6.6 installation file.

- 4 Install Business Process Monitor 6.6. For details, see *Business Process Monitor Administration*.
- 5 Business Process Monitor scripts may need to be manually added to the Script Repository.

Do the following steps for each Business Process Monitor script in Monitor Administration:

- a Select the Business Process Monitor script in View Explorer. In Main Settings of the Property tab, the following message is displayed:

The script does not exist in the Script Repository and its settings cannot be edited. Edit the transaction monitor to add the script to the repository.
- b Click **Edit**. The following message is displayed:

The script does not exist in the Script Repository and its settings cannot be edited. Click OK to upload the script to the Script Repository. You can then continue editing the transaction monitor's settings.
- c Click **OK**. The Script Repository window opens.
- d Choose the folder where the Business Process Monitor script is to be uploaded. Click **OK** to add the script to the folder.

Client Monitor

Mercury Business Availability Center 6.6 includes Client Monitor 6.6, but works with Client Monitor 5.0 and later. You do not need to upgrade Client Monitor unless you want to benefit from the enhanced functionality of later versions.

Note: You can continue to work with Client Monitors already installed on end-user machines. Client Monitor scripts recorded in Client Monitor versions 4.5 FP2/5.x must be converted, using a converter tool, to be compatible with Client Monitor 6.6. For details, contact Mercury Customer Support.

To upgrade Client Monitor 4.5/5.x/6.x to 6.6:

- 1** Uninstall the previous version of Client Monitor.
- 2** In Mercury Business Availability Center 6.6, select **Admin > Platform > Setup and Maintenance > Downloads**.
- 3** Click the **Mercury Client Monitor** link to access the Client Monitor 6.6 installation file.
- 4** Install Client Monitor 6.6. For details, see *Client Monitor Administration*.

Client Monitor Upgrade from 4.5.x to 6.6

Note the following information regarding upgrading to Client Monitor 6.6:

Database Schema Upgrade

Database schema upgrade includes creating six new tables for Client Monitor large deployment:

- CM_GROUPS
- CM_GROUP_FILTERS
- CM_HOST_PROPERTIES
- CM_GROUP_HOSTS
- CM_GROUP_SCRIPTS
- CM_GROUP_TRACEROUTES

Configuration and Data Upgrade

During the upgrade, monitor data is kept in the database, but configuration data is lost. This means that if you upgrade to Mercury Business Availability Center 6.6 from an existing Mercury Business Availability Center with data, version 6.6 starts with the following initial configuration:

- **Platform/Data Collector Maintenance.**

You begin with no declared groups or containers, and with no Client Monitor host properties for a group's filters. Client Monitor hosts are automatically registered the first time you connect to Mercury Business Availability Center 6.6.

► **Client Monitor hosts.**

Job assignments for the Client Monitor hosts that were set before the upgrade are not kept. Note the following:

- ◆ In Monitor Administration, the old profiles and monitors do not have any assignment to the groups. Note that if you refresh the LDAP, you may lose the traceroutes monitors and will have to declare them again.
- ◆ In Dashboard, Client Monitor profiles appear empty.
- ◆ All CIs which appeared in Client Monitor 6.2 (for example, **Business Process Step, Business Process Monitor Transaction From Location, Location, Business Process Group Location**), are removed from CMDB in Mercury Business Availability Center 6.2. This means that all Service Level Agreements and thresholds that were defined using these CIs are also removed and must be redefined.
- ◆ The Client Monitor hosts that had jobs (transactions and traceroutes in profiles that are assigned to the Client Monitor) assigned to them before the upgrade and are now registered to Mercury Business Availability Center 6.2, do not have those jobs after the upgrade. This means that immediately after the upgrade, there are no registered jobs. You must assign the hosts to groups and then assign jobs to those groups.

Note: Job assignments made before the upgrade can be extracted from the database. They are not removed from the old tables until you delete the profile. You can extract the following tables: ACTIONS, GROUPS, EXT_GROUP_SCHEDULES, and TRACE_ROUTE_DEFINITION.

◆ **End User Management.**

All End User Management reports, both scripts and traceroutes, continue to work after the upgrade with historic data.

SiteScope

For a complete list of enhanced functionality provided by SiteScope 8.7, refer to the SiteScope release notes.

Note the following about SiteScope support in Mercury Business Availability Center 6.6:

- ▶ Mercury Business Availability Center 6.6 includes SiteScope 8.7, but supports SiteScope 7.9.5 and later. You must upgrade to SiteScope 8.2 to benefit from enhanced functionality and to be able to administer SiteScope from Monitor Administration.

For details of SiteScope versions and their compatibility with Mercury Business Availability Center 6.6, refer to the compatibility matrix in the readme file, available in the Mercury Business Availability Center Documentation Portal area on the Mercury Customer Support Web site (support.mercury.com).

- ▶ You must upgrade to SiteScope 8.7 if you want to do any of the following:
 - ◆ integrate your HP OVO system with Mercury Business Availability Center
 - ◆ use Mercury Business Availability Center Problem Isolation
- ▶ If you are using 7.9.0 and need to change the URL because Mercury Business Availability Center is installed on a new server machine, you must upgrade to SiteScope 7.9.5.0 (SiteScope 7.9.0 does not support changing the URL).
- ▶ If you want monitors to report custom data to Mercury Business Availability Center you must upgrade to SiteScope 7.9.5.0 or higher.
- ▶ If you currently have SiteScopes attached to Topaz Monitor Configuration in Topaz 4.5 FP2 or Monitor Administration in Mercury Business Availability Center 5.x (also known as Application Management 5.x), you must detach and upgrade them before upgrading the Topaz or Mercury Business Availability Center servers.
- ▶ If you want to administer SiteScope from the SiteScope machine and not from Mercury Business Availability Center, you do not need to upgrade to version 8.7.

- ◆ Previous SiteScope profiles created in Topaz are automatically upgraded when upgrading to Mercury Business Availability Center 6.6. You will be able to view SiteScope data in Mercury Business Availability Center. Additionally, all the features of those profiles are displayed but you are not able to change them using Monitor Administration (only by using SiteScope administration).
- ◆ You can create a new empty profile in Monitor Administration by entering the name of the profile in the **SiteScope Display Name** box and the name of the machine on which Mercury Business Availability Center is running in the **Host Name** box and by clearing **Import SiteScope Configuration**. Then you go to SiteScope administration and connect to the profile you created. This new profile allows you to view SiteScope data in Mercury Business Availability Center but you cannot control SiteScope through Mercury Business Availability Center (for example, adding features such as **Preferences**, **Health**, and so forth).

Note: If you are not sure how to proceed with your SiteScope under Mercury Business Availability Center 6.6, contact Mercury Customer Support.

To upgrade SiteScope from 7.9.x/8.x to 8.7:

- 1** In Mercury Business Availability Center 6.6, select **Admin > Platform > Setup and Maintenance > Downloads**.
- 2** Click the **SiteScope** link to access the SiteScope 8.7 installation file.
- 3** Install SiteScope 8.7. As part of the installation process, you upgrade SiteScope 7.9/8.x and can export data from your current SiteScope for later import into SiteScope version 8.7. For details, see *SiteScope Administration*.
- 4** Check that SiteScope is running with the correct configuration (the original groups).
- 5** In Mercury Business Availability Center, go to **Admin > Monitors** and attach each SiteScope. For details, refer to *Managing SiteScope*.

Real User Monitor

Mercury Business Availability Center 6.6 includes Real User Monitor 6.6 engine and Real User Monitor 6.6 probe.

Note: Real User Monitor Engine 6.6 is only supported in a Windows environment.

Mercury Real User Monitor 6.6 has the new functionality of resource caching. This functionality enables you to store all static resources, such as images and style sheets, on the Real User Monitor probe machine instead of requesting them from the monitored application. Caching makes snapshot viewing and replay more robust.

For details about other enhancements in Real User Monitor prior to version 6.6, see the **What's New?** file in:

- ▶ Mercury Business Availability Center Documentation Portal area on the Mercury Customer Support Web site (support.mercury.com)
- ▶ Real User Monitor Engine Online Help menu

Limitations

- ▶ The Real User Monitor 6.6 probe supports only Red Hat Enterprise Linux 4 (RHEL 4). Red Hat 9 is not supported.
- ▶ If you install Real User Monitor 6.6 probe on a different machine, make sure that you update the probe definitions (name, IP, user, and password). Mark the old probe as **disabled**. For details, refer to *Real User Monitor Administration*.
- ▶ Real User Monitor 6.6 engine does not support earlier versions of Real User Monitor probe.

Features of Previous Real User Monitor Versions

Mercury Real User Monitor 6.5 contains the following enhanced functionality:

- The Real User Monitor Probe can be configured directly from the Real User Monitor Web Console for the following options:
 - ◆ Keystore management for decrypted traffic
 - ◆ Interface connections to configure which of the Real User Monitor Probe's Ethernet devices to use for monitoring traffic
 - ◆ Collector Editor to specify ranges of servers and ports to be monitored
 - ◆ SSH Console for accessing the Real User Monitor Probe's console using secured channels
- Session ID detection identifies possible session keys in monitored traffic, to assist in configuring application sessions in Monitor Administration.
- Auto Discovery reports domains and servers accessed by end-users, to assist in configuring servers and applications in Monitor Administration.
- Current Sessions Report displays raw data of sessions that are still current in the Real User Monitor engine, which helps troubleshoot problems with session reporting in Mercury Business Availability Center.
- In the General Settings section, Session Reset Settings include a **By URL** configuration parameter. This parameter, if set, defines which Real User Monitor page to start the session and/or which Real User Monitor page to finish the session.

Mercury Real User Monitor 6.4 contains the following enhanced functionality:

- URLs configured for Real User Monitor in Monitor Administration do not have to be configured with a specific protocol, either HTTP or HTTPS. A URL can be configured with HTTP*, allowing it to be matched when used with either HTTP or HTTPS.

Mercury Real User Monitor 6.2 contains the following enhanced functionality:

- Meaningful names can be created for unconfigured pages. Siebel and PeopleSoft applications have predefined templates for meaningful names.
- Pages with errors are included in the Global Statistics report.
- Snapshot on error (SSOE) can be configured per application.

- Real User Monitor is included in the Mercury Self-Alert Monitor.
- System health reporting is improved in the Real User Monitor Web console.
- Open API for user name resolution is in place.
- General performance improvements are included.

Mercury Real User Monitor 6.1 contains the following enhanced functionality:

- Session tracking
- Response time for each page and each individual user
- Online user session replay
- Sharable offline replay via a zip file
- Drill down into Mercury Diagnostics for problem isolation
- Browser, host name, and header capture
- Real user name and login capture
- Improved handling of network address translation and proxies
- Content checking and content error/event capture
- Error/event reporting
- Page content capture and storage
- Production analysis reports to aid testing teams
- Mercury Virtual User Generator (VuGen) script generation from real user session
- SSL decryption onboard and non-proprietary
- New non-proprietary (x86) probe technology on Red Hat Linux
- Many security model improvements
- FIPS3 compliance capabilities
- Fault tolerance at every level via caching and TCP connections
- Scalability enhancements
- Numerous stability improvements

- Out-of-the-box dashboard views
- Windows 2000 and 2003 support for the Real User Monitor engine
- Solaris 10 support for the Real User Monitor engine

Note: This is the last version for Solaris support in the Real User Monitor engine.

To upgrade Real User Monitor from 6.2/6.3/6.4/6.5/6.5.1 to 6.6:

- 1** Back up the directory <Real User Monitor engine>\conf.

Important to Read Prior to Step 2:

- Do not delete the files in the Real User Monitor directory when prompted during the uninstall procedure in step 2.
 - If the uninstall procedure does delete the files in the Real User Monitor directory, recent data is lost.
-

- 2** Uninstall the Real User Monitor core engine and database engine. For details, see “Uninstalling Real User Monitor” in *Real User Monitor Administration*.
- 3** After uninstall, and before installing a new Real User Monitor version, navigate to the <Real User Monitor engine>\dat directory and do the following:
 - ◆ delete the files `mysql-ds.xml.bck` and `login-config.xml.bck`, if they exist
 - ◆ rename the file <Real User Monitor engine>\conf\`configurationmanager` to `\Beatbox_Default_Const_Configuration.xml`, if it exists, to `_Default_Const_Configuration.xml.bck`.

If `Beatbox_Default_Const_Configuration.xml` exists, it means that it was changed manually and you must change it again for the Real User Monitor 6.6 environment. (The default XML file should be changed only in rare cases. If you need to override the default settings, use the Real User Monitor Web console. For details, refer to *Real User Monitor Administration*.)

- 4 Navigate to the directory `<Real User Monitor engine>\persistence`. Delete the following:
 - ◆ Files and folders except the files beginning with `Remote_`.The folder should contain only those files beginning with `Remote_`.
- 5 Delete the directory `<Real User Monitor engine>\EJBContainer\server\mercury\data\hypersonic`.
- 6 In Mercury Business Availability Center 6.6, select **Admin > Platform > Setup and Maintenance > Downloads**.
- 7 Click the **Mercury Real User Monitor Engine** and **Mercury Real User Monitor probe** links to access the installation files.
- 8 Install Real User Monitor 6.6 engine.

Important:

- ▶ The engine must be installed in the same directory as the previous Real User Monitor engine. If the Real User Monitor database engine was installed on a separate machine, it must be installed on the same machine and in the same directory as the prior version. For details, see *Real User Monitor Administration*.
 - ▶ During the upgrade, you must connect to the same schema used by the earlier version of Real User Monitor. The length of time to upgrade depends on the amount of data in your database. A 1 GB, or 3 million row, schema takes about 5-10 minutes to upgrade. Schemas with more than 100 million rows may take several hours.
 - ▶ Interrupting the schema upgrade may result in loss of data.
-

- 9 Upgrade the Real User Monitor 6.6 probe. For details, see “Installing the Real User Monitor Probe” in *Real User Monitor Administration*.

To upgrade Real User Monitor from 6.1.x to 6.2:

- 1 Uninstall the Real User Monitor engine. For details, refer to *Real User Monitor Administration*. When prompted during the uninstall procedure, do not delete the files in the Real User Monitor directory.
- 2 Install Real User Monitor 6.2 engine in the same directory as the previous Real User Monitor engine. The Real User Monitor database must be installed on the same machine as the prior version.
- 3 Install the Real User Monitor 6.2 probe.

To upgrade Real User Monitor from pre-6.1:

Contact Mercury Customer Support for assistance in performing an upgrade from pre-6.1 versions of Real User Monitor to Real User Monitor 6.6.

Virtual User Generator (VuGen)

Mercury Business Availability Center 6.6 includes Mercury Virtual User Generator (VuGen) version 8.1 Service Pack 3. Upgrade VuGen to be compatible with the Business Process Monitor for Mercury Business Availability Center 6.6, and to benefit from the improved functionality.

Microsoft SQL Server 2005

The COM, ODBC, and MSSQL protocols are certified to support the MSSQL 2005 official release.

Web Services

Web Service Users support the .NET and Axis toolkits for services developed by .NET 1.1 Framework with WSE2 SP3 and Axis 1.3 Web Services Framework. Toolkit support provides greater compatibility for WSDL scanning, recording and replay.

For services that do not work with the .NET or Axis toolkits, LoadRunner provides a generic solution that emulates the Glue version 4.1.2, MS SOAP version 3.0, and other toolkits.

WAP

This feature pack provides the following enhancements to the WAP wireless protocol:

- ▶ Records any type of WAP application or simulator.
- ▶ Automatically recognizes the application or simulator settings.
- ▶ Supports WSP, HTTP proxy, and HTTP direct modes as configured in the application or simulator.

Web (Click and Script)

Web (Click and Script) is a new approach to Web load testing. It introduces a GUI-level scripting API, and a quick way to generate load testing scripts.

- ▶ Eliminates the need for correlation.
- ▶ Intuitive API functions describe user actions on Web objects (button, text link, and so forth).
- ▶ Groups steps according to their pages.
- ▶ Creates a Business Process Report in Microsoft Word format summarizing the VuGen script.
- ▶ The Business Process Report (in Microsoft Word format) summarizes the VuGen script.

AMF

This protocol provides the ability to record and replay AMF (Action Message Format), a Macromedia proprietary protocol that allows Flash Remoting binary data to be exchanged between a Flash application and an application server over HTTP.

Citrix

- ▶ New bitmap synchronization replay error management compares bitmap synchronization errors as they occur, and adds the necessary changes to the the script in a single click.
- ▶ Improved text trapping and text synchronization algorithm, including a function (**sync_on_text_ex**) that shows the area used for synchronization in the snapshot.
- ▶ Improved tree view, including replay snapshots and additional options in the context menu.
- ▶ Improved recording snapshots.
- ▶ New **CONTINUE_ON_ERROR** flag is available for each function that can potentially fail. Using this flag makes the script execution continue after the function returns the failure error code.
- ▶ Improved script replay stability and predictability.
- ▶ New **ctx_execute_on_window** function (replaces **ctx_set_exeption**) enables usage of wildcard characters (*) in the window caption.
- ▶ Supports script regeneration from the recording options and regenerate script dialog.

New MMS (Multimedia Messaging) Protocol

This protocol provides the ability to send and download MMS messages as well as receive notifications over SMPP transport. New functions were introduced for creating, sending, receiving, and downloading MMS messages.

Microsoft Visual Studio 2005 Add-In

Full support for creating, replaying, and debugging scripts from Microsoft Visual Studio 2005 in C#, VB.NET, or C++.

To upgrade VuGen to version 8.1:

- 1 If you are installing to the same machine running your existing Virtual User Generator, uninstall the existing version.

- 2 Select **Admin > Platform > Setup and Maintenance > Downloads > Mercury Virtual User Generator**. Install Mercury Virtual User Generator 8.1 Service Pack 3 according to the on-screen instructions.

If the Virtual User Generator setup file does not appear on the Downloads page, refer to *Deploying Servers* for details on installing components setup files on the Downloads page.

Note: Scripts recorded with VuGen 8.1 can only run on Business Process Monitor 6.1 and later. Scripts recorded with earlier versions of VuGen, however, can run on Business Process Monitor 6.2.

Discovery Probe

If you are upgrading to Mercury Business Availability Center 6.6 from Mercury Business Availability Center 6.x, you must uninstall the existing Discovery Probe and install Discovery Probe 6.6 before running the discovery process.

To upgrade Discovery Probe from 6.x to 6.6:

- 1 Uninstall all existing Discovery Probes.
- 2 In Mercury Business Availability Center 6.6, select **Admin > Platform > Setup and Maintenance > Downloads**.
- 3 Click the **Discovery Probe** link to access the Discovery Probe 6.6 installation file.
- 4 Install on machines as required.

Note: Active discovery patterns must be reactivated after the upgrade so that the newly installed Discovery Probes will receive the tasks they are assigned.

Part III

Mercury Application Mapping

16

Upgrading Mercury Application Mapping from Version 6.x to Version 6.6

This chapter explains how to upgrade Mercury Application Mapping from version 6.x to 6.6 when Mercury Application Mapping shares the CMDB with Mercury Business Availability Center.

This chapter describes:	On page:
Upgrading Mercury Application Mapping: Version 6.x – 6.6 with a Shared CMDB	176
Backing Up Configuration Files	180
Redeploying and Undeploying Packages	182

Upgrading Mercury Application Mapping: Version 6.x – 6.6 with a Shared CMDB

This section explains how to upgrade Mercury Application Mapping from version 6.x to 6.6 when Mercury Application Mapping shares the CMDB with Mercury Business Availability Center.

Note: As part of the upgrade procedure you are required to remove existing version 6.x **Process** and **Webservice** CIT instances from the CMDB. This is required because the definitions of these CI types change in version 6.6. After installing version 6.6, you must run Discovery for the webservices (UDDI module) and process (Host Resource) packages to recreate the instances in your version 6.6 CMDB.

To upgrade Mercury Application Mapping:

- 1** Back up all Mercury Application Mapping databases. For details, see *Preparing the Database Environment* included with Mercury Application Mapping.

Note: (Relevant for Windows installations only.) If you are installing version 6.6 on the same server as the previous version, you must rename the MAM shortcut to **MAM6.x**, where **x** is the current version number (**Start > Programs** (or **All Programs**) > **MAM**, right-click and select **Rename**).

- 2** Back up any Mercury Application Mapping 6.x configuration files that have been modified by users. For details, see “Backing Up Configuration Files” on page 180.
- 3** Verify the number of Process CIT instances in the system via the JMX console:

- a** Launch your Web browser and enter the following address:

```
http://<machine name or IP address>:8080
```

where **<machine name or IP address>** is the machine on which the Modeling Data Processing Server is installed.

- b** Click the JMX Console link. You may have to log in with the **admin** user and password.
- c** Click the **Topaz > service=CMDB Model Services** link.
- d** In the JMX MBEAN View page, locate the following operation:
retriveObjectCounts
- e** In the customerID field, enter **1**; in the type field, enter **process**; select **true** for isDerived.
- f** Click **Invoke**. A message is displayed showing the number of process CIT instances in the system. Record this number for later reference.

Tip: You can verify the number of processes also by accessing the CI Type Manager: Display the topology map organized by CI Types. Locate **Host Resources > Process**. The number of processes should be the same as the number in the JMX console. Next, log in to version 6.x and verify that the number is the same in that version.

- 4** Install the Mercury Application Mapping version 6.6 server. For details, see the relevant sections:
- ▶ **Windows:** Chapter 5, “Distributed Deployment Installation with a Shared CMDB” in *Mercury Application Mapping Installation Guide*
 - ▶ **Solaris:** Chapter 12, “Distributed Deployment Installation with a Shared CMDB” in *Mercury Application Mapping Installation Guide*
- 5** Upgrade Mercury Business Availability Center to version 6.6 according to the instructions in the relevant upgrade checklist. For details, see Part I, “Checklists for Upgrading to Mercury Business Availability Center 6.6.”

- 6 Stop all Mercury Business Availability Center 6.6 servers and run **BACMAMShareCMDDB.exe**. For details, see “Sharing the Mercury Business Availability Center CMDDB” in *Mercury Application Mapping Installation Guide*.
- 7 Using the modified configuration files that you backed up in step 2 as a reference, manually update the 6.6 configuration files similarly (if required). If a modified file appears in multiple locations, make the change to all instances of the file.

Caution: Do not overwrite any version 6.6 configuration files with configuration files from previous versions.

- 8 If the number of process CIT instances in the system, as calculated in step 3 above, is 10,000 or greater and an Oracle Server database is being used, remove all process CIT instances as follows:
 - ▶ Make sure the Modeling Data Processing Server is not running and ensure that **env_cmdb.bat** lists accurate database locations.
 - ▶ Run from the command line **66_upgrade.bat process**. The batch file is located in: **<Mercury Business Availability Center root directory>\cmdb\dbscripts\oracle** (version 6.6).

Note: Do not use the **66_upgrade.bat** script to remove any other type of CIT instance.

- 9 If the number of process CIT instances in the system, as calculated in step 3 above, is 9,999 or less, remove all process CIT instances as follows:
 - a Launch the Web browser and enter the following address:

```
http://<machine name or IP address>:8080
```

where **<machine name or IP address>** is the machine on which the Modeling Data Processing Server is installed.

- b Click the **JMX Console** link. You may have to log in with the **admin** user and password.
 - c Click the **Topaz > service=CMDB Model Services** link.
 - d In the JMX MBEAN View page, locate the following operation:
deleteByClassType()
 - e In the classType field, enter **process** as the type to be removed; in the chunkSize field, enter **500** (recommended); the isDerived parameter should be set to **true**; click **Invoke**. A message is displayed, signifying that the operation is successful.
- 10** Start all version 6.6 servers.
- 11** Remove **webservice** CIT instances:
- a Launch the Web browser and enter the following address:
- ```
http://<machine name or IP address>:8080
```
- b Click the **JMX Console** link. You may have to log in with the **admin** user and password.
  - c Click the **Topaz > service=CMDB Model Services** link.
  - d In the JMX MBEAN View page, locate the following operation:  
**deleteByClassType()**
  - e In the customerID field, enter **1**; in the classType field, enter **webservice** as the class type to be removed. The isDerived parameter should be set to **true**.
  - f Click **Invoke**. A message is displayed, signifying that the operation is successful.
- 12** Redeploy all packages. For details, see “Redeploying and Undeploying Packages” on page 182.

---

**Note:** If your pre-version 6.6 Mercury Application Mapping CMDB included the IIS topology view, verify that it is not corrupt after the upgrade procedure. If it is, manually undeploy the IIS discovery package before redeploying all packages. For details, see “Redeploying and Undeploying Packages” on page 182.

---

- 13 Reactivate the active Discovery patterns, so that newly installed probes receive their tasks.

## Backing Up Configuration Files

Before you install Mercury Application Mapping 6.6, back up the configuration files that you have modified to another directory.

If a change has been made to one of these files, repeat the change in the version 6.6 file.

---

**Tip:** Use a different backup mechanism to back up these files than the one you used for the full backup.

---

### CMDB Configuration Files

- ..\MAMServer\j2f\conf\cmdb.conf
- ..\MAMServer\j2f\conf\core\Tools\log4j\EJB\cmdb.properties
- .. \MAMServer\j2f\conf\core\Tools\log4j\PlainJava\cmdb.properties
- ..\MAMServer\scripts\install\J2F\conf\core\Tools\log4j\EJB\cmdb.properties
- ..\MAMServer\scripts\install\J2F\conf\core\Tools\log4j\PlainJava\cmdb.properties

### **Server Configuration Files**

- ..\MAMServer\root\lib\server\appilogConfig.properties
- ..\MAMServer\root\lib\server\backup.properties
- ..\MAMServer\root\lib\server\collectorsConfig.properties
- ..\MAMServer\root\lib\server\dbupgrade.properties
- ..\MAMServer\root\lib\server\icon.properties
- ..\MAMServer\root\lib\server\jms.properties
- ..\MAMServer\root\lib\server\mam4j-dbcreator.properties
- ..\MAMServer\root\lib\server\mam4j-scripts.properties
- ..\MAMServer\root\lib\server\mam4j-simulator.properties
- ..\MAMServer\root\lib\server\mam4j\_db.properties
- ..\MAMServer\root\lib\server\scripts\_db.properties
- ..\MAMServer\root\lib\server\shape.properties
- ..\MAMServer\root\lib\server\mam4bac4j.properties
- ..\MAMServer\root\lib\server\mam4j-debug.properties
- ..\MAMServer\root\lib\server\mam4j-non-debug.properties
- ..\MAMServer\root\lib\server\mam4j-stat.properties

### **Application Configuration Files**

- ..\MAMServer\j2f\EJBContainer\server\mercury\tmp\deploy\tmp<###>mam.war\appilog\gui\server.properties
- ..\MAMGUI\root\lib\gui\mam4j\_gui.properties
- ..\MAMServer\root\lib\web\gui.properties – located under a specific server

### **Discovery Probe Configuration Files**

- ..\MAMDiscoveryProbe\root\lib\collectors\appilog-remote.properties

## Redeploying and Undeploying Packages

Use the below procedures to redeploy or undeploy discovery packages:

### To redeploy packages:

- 1 Launch the Web browser and enter the following address:

```
http://<machine name or IP address>:8080
```

where **<machine name or IP address>** is the machine on which Mercury Application Mapping (or the Mercury Business Availability Center Modeling Data Processing Server, in the case of a shared CMDB environment) is installed.

- 2 Click the JMX Console link. You may have to log in with the admin user and password.
- 3 Click the **MAM > service=Package manager** link.
- 4 In the JMX MBEAN View page, locate the following operation:  
**deployPackages**
- 5 In the customerID field, enter **1**; in the packageNames field, enter the package name—to redeploy all packages, enter **\*.\***; ignoreTimestamp should be set to **true**.
- 6 Click **Invoke**. A message is displayed, signifying that the operation is successful.

### To undeploy packages:

- 1 Launch the Web browser and enter the following address:

```
http://<machine name or IP address>:8080
```

where **<machine name or IP address>** is the machine on which Mercury Application Mapping (or the Mercury Business Availability Center Modeling Data Processing Server, in the case of a shared CMDB environment) is installed.

- 2 Click the JMX Console link. You may have to log in with the admin user and password.



- 3** Click the **MAM > service=Package manager** link.
- 4** In the JMX MBEAN View page, locate the following operation:  
**undeployPackage**
- 5** In the customerID field, enter **1**; in the packageNames field, enter the name of the package to undeploy.  
  
To undeploy the IIS discovery package, enter **IIS.zip**.
- 6** Click **Invoke**. A message is displayed, signifying that the operation is successful.



---

# Index

## A

architecture (server) 48

## C

checklist

    upgrade 4.5 to 6.6 16

    upgrade 5.x to 6.6 22

    upgrade 6.1.x to 6.6 30

    upgrade 6.2/6.3/6.4/6.5 to 6.6 38

configuration, upgrading 79

## D

dashboard views

    display upgraded view 91

    notes and limitations 93

    troubleshooting 92

    upgrade rollback 96

    upgrade settings 87

    upgrade simulation 88

    upgrading 85, 89

data collectors

    changing URL 151

data files

    backing up 76

    copying 77

    retaining 75

    updating path to 78

database schema

    upgrading 59, 68

    verifying 59, 63

database users, creating for upgrade 71

dbverify 60

## J

Java run time, modifying mx parameter 72

## L

LDAP database

    backing up 76

    copying 77

    retaining 75

    updating path to 78

## M

monitor administration configuration data

    backing up 76

    copying 77

    retaining 75

    updating path to 78

## R

rollback, upgraded views 96

## S

server architecture 48

server installation

    Solaris platform 54

    Windows platform 49

servers, upgrading 47

service level agreements

    differences between 5.x and 6.x 137

    downtime events variations 141

    notes and limitations 127

    time interval variations 143

    transaction differences with  
        objectives 138

## Index

- upgrading from 5.x to 6.x 132
- Service Level Management
  - report variations 142
  - upgrading 125
  - upgrading custom reports 135
  - upgrading report repository 136
- SiteScope
  - upgrading 162
- Solaris platform
  - upgrading servers 54

## T

- troubleshooting
  - dashboard views 92
  - dbverify errors 72
  - views 92

## U

- upgrade
  - Business Process Monitor 158
  - checklist 4.5 to 6.6 16
  - checklist 5.x to 6.6 22
  - checklist 6.1.x to 6.6 30
  - checklist 6.2/6.3/6.4/6.5 to 6.6 38
  - Client Monitor 159
  - components 157
  - configuration 79
  - considerations 48
  - dashboard views 85, 89
  - data collectors 157
  - database schema 59
  - dbverify utility 60
  - getting started 13, 21, 29, 37
  - introduction 11
  - major steps 12
  - methodology 60
  - Real User Monitor 164
  - servers 47
  - views 85, 89
- upgrade settings, dashboard views 87
- upgrade simulation
  - dashboard views 88
  - views 88
- upgrade view, display 91

- upgrading
  - version 6.x to 6.6 175
- URL, changing on data collectors 151

## V

- verify utility 60
- verifying database schema 59
- views
  - display upgraded view 91
  - notes and limitations 93
  - troubleshooting 92
  - upgrade 89
  - upgrade rollback 96
  - upgrade settings 87
  - upgrade simulation 88
- Virtual User Generator, upgrading 169

## W

- Windows platform
  - upgrading servers 49