

OPTIMIZE

MERCURY BUSINESS AVAILABILITY CENTER™

Upgrading Mercury Business Availability Center 5.x - 6.2

MERCURY™

BUSINESS TECHNOLOGY OPTIMIZATION

Mercury Business Availability Center

Upgrading Mercury Business Availability Center

Version 5.x to Version 6.2

Document Release Date: July 18, 2006

MERCURY™

Mercury Business Availability Center, Version 6.2
Upgrading Mercury Business Availability Center 5.x-6.2

This manual, 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.

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
Toll Free: (800) TEST-911
Customer Support: (877) TEST-HLP
Fax: (650) 603-5300

© 2005-2006 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.....	v
Using this Guide.....	v
Getting More Information	vii
Chapter 1: Introduction to Upgrade.....	1
Important Information About the Upgrade Procedure	2
Major Upgrade Steps	2
Chapter 2: Upgrade Checklist	3
Before You Begin	3
Upgrade Checklist	5
Chapter 3: Upgrading the Servers	11
Server Architecture for Mercury Business Availability Center	12
Upgrading Considerations	12
Installing Mercury Business Availability Center 6.1 and the 6.2 Add-on on a Windows Platform	13
Installing Mercury Business Availability Center 6.2 on a Solaris Platform	17
Chapter 4: Verifying and Upgrading the Database Schema	21
Introducing Upgrade Methodology	22
Using the Verify and Upgrade Utility	22
Verifying the Database Schema.....	25
Upgrading the Database Schema.....	30
Creating Database Users for the Upgrade Procedure	33
Troubleshooting Database Schema Verify and Upgrade Errors	34
Chapter 5: Retaining Monitor Administration Configuration Data...37	37
Overview of Retaining Monitor Administration Configuration Data	37
Backing Up Monitor Configuration Data Files	38
Copying Monitor Configuration Data Files to Mercury Business Availability Center 6.2	39
Upgrading the LDAP Database	40
Chapter 6: Configuration Upgrade.....	41
Upgrading Configuration Data	41

Chapter 7: Dashboard Views Upgrade	47
The Views Upgrade Page	48
Simulating a View Upgrade	50
Upgrading a View	51
Displaying an Upgraded View	52
Troubleshooting	52
Notes and Limitations	53
Rollback	55
Chapter 8: Switching Mercury Business Availability Center URL on the Data Collectors	57
Overview of Switching Data Collectors	57
Redirecting the Business Process Monitor URL	58
Redirecting the Client Monitor URL	59
Redirecting the SiteScope URL	60
Chapter 9: Upgrading Components to Work with Mercury Business Availability Center 6.2	63
Upgrading Business Process Monitor	64
Client Monitor	65
SiteScope	68
Real User Monitor	70
Mercury Virtual User Generator	72
Chapter 10: Understanding Repository Upgrade from Version 5.x to Version 6.2	75
Upgrade Log	75
Upgrading Entities/CIs	76
Upgrading Dimensions/KPIs	76
Upgrading Rules	82
Upgrading Tooltips	89
Index	93

Welcome to Upgrading Mercury Business Availability Center

This guide provides detailed instructions on how to upgrade Mercury Business Availability Center 5.0 FP1 and Mercury Business Availability Center 5.1 SP1 to Mercury Business Availability Center 6.2.

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 Procedure” on page 2.

Using this Guide

The guide contains the following chapters:

Introduction to Upgrade

Introduces the methodology for upgrading your servers and database to Mercury Business Availability Center 6.2.

Upgrade Checklist

Describes what actions to perform before and during the upgrade to Mercury Business Availability Center 6.2.

Upgrading the Servers

Describes how to upgrade your servers to Mercury Business Availability Center 6.2.

Verifying and Upgrading the Database Schema

Describes the methodology for upgrading your database schema to Mercury Business Availability Center 6.2.

Retaining Monitor Administration Configuration Data

Describes how to retain and reapply your Monitor configuration data when upgrading to Mercury Business Availability Center 6.2.

Configuration Upgrade

Describes how to upgrade your data to Mercury Business Availability Center 6.2.

Dashboard Views Upgrade

Describes how to upgrade your Mercury Business Availability Center custom Dashboard views to Mercury Business Availability Center 6.2 views

Switching Mercury Business Availability Center URL on the Data Collectors

Describes how to configure your data collectors to work with new Mercury Business Availability Center 6.2 servers.

Upgrading Components to Work with Mercury Business Availability Center 6.2

Describes how to upgrade your components for Mercury Business Availability Center 6.2.

Understanding Repository Upgrade from Version 5.x to Version 6.2

Describes what happens to the repositories elements that have been customized by overriding, cloning, or that were created when you upgrade your site from version 5.x to version 6.2. This information may be useful in troubleshooting.

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*.

Welcome

1

Introduction to Upgrade

This guide describes the methodology for upgrading your servers and database to Mercury Business Availability Center 6.2. Mercury Business Availability Center supports direct schema and data upgrade from Mercury Business Availability Center 5.0 FP1 and Mercury Business Availability Center 5.1 SP1.

Note: Throughout this guide, versions of Mercury Business Availability Center for which upgrade is supported are referred to as **Mercury Business Availability Center 5.x**.

The aim of the procedures and recommendations provided in this guide is to enable you to upgrade your platform to Mercury Business Availability Center 6.2 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 **Deployment_Documentation** directory on the **Mercury Business Availability Center 6.2 (Windows or Solaris) Setup** CD-ROM.
- ▶ From the **Documentation\pdfs** directory on the **Mercury Business Availability Center 6.2 (Windows or Solaris) Documentation and Utilities** CD-ROM.
- ▶ From the Mercury Business Availability Center Documentation Portal area on the Mercury Customer Support Web site (support.mercury.com).

Important Information About the Upgrade Procedure

Mercury Business Availability Center can be installed in a variety of configurations. The upgrade procedure will depend on how Mercury Business Availability Center is configured in your environment. The steps detailed in this book are intended as a guide only.

Major Upgrade Steps

Upgrading your platform to Mercury Business Availability Center 6.2 requires 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 is described in Chapter 2, “Upgrade Checklist.” 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

This chapter describes what actions to perform before and during the upgrade to Mercury Business Availability Center 6.1.

This chapter describes:	On page:
Before You Begin	3
Upgrade Checklist	5

Before You Begin

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

- ▶ Uninstalling Mercury Business Availability Center 6.2 does not roll back to a previous version of Mercury Business Availability Center. It completely removes the software.
- ▶ 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 6.1, 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 6.1.

- ▶ 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.
- ▶ If you were working with Mercury Business Availability Center for Siebel 5.1 SP1 and wish to upgrade to Mercury Business Availability Center for Siebel 6.2, see “Upgrading from Mercury Business Availability Center for Siebel 5.1 SP1” in *Application Administration*.

Upgrade Checklist

The following checklist should be used when upgrading from Mercury Business Availability Center 5.x to Mercury Business Availability Center 6.1:

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"> ▶ MercuryAM\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 21. ▶ MercuryAM\CMDB – directory needed for upgrading Dashboard views in step 12. For details on upgrading Dashboard views, see “Dashboard Views Upgrade” on page 47. ▶ <Mercury Business Availability Center 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 38. <p>In addition, backup any other files or directories you want to keep for security or historical purposes.</p>

Step	Description	Details
<p>2 Shut down existing Mercury Business Availability Center 5.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"> ▶ 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>
<p>3 If upgrading to Mercury Business Availability Center 6.1 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</code> <code>./uninstall</code>
<p>4 In a Windows environment, install Mercury Business Availability Center 6.1 on all machines, and then install the Mercury Business Availability Center 6.2 Add-on on all machines</p>	<p>Install Mercury Business Availability Center 6.1 on all machines, but do not connect to the database as part of the installation process. After 6.1 installation, do not start (enable) Mercury Business Availability Center 6.1.</p> <p>Install the Mercury Business Availability Center 6.2 Add-on on all machines. After installation, do not start (enable) Mercury Business Availability Center 6.2.</p>	<p>For details on installing Mercury Business Availability Center 6.1 and the 6.2 Add-on in a Windows environment, see “Installing Mercury Business Availability Center 6.1 and the 6.2 Add-on on a Windows Platform” on page 13.</p>

Step	Description	Details
5 In a Solaris environment, install Mercury Business Availability Center 6.2 on all machines.	Install Mercury Business Availability Center 6.2 on all machines, but do not connect to the database as part of the installation process. After installation, do not start (enable) Mercury Business Availability Center 6.2.	For details on installing Mercury Business Availability Center 6.2 in a Solaris environment, see “Installing Mercury Business Availability Center 6.2 on a Solaris Platform” on page 17.
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 Run the database schema upgrade.	Run dbupgrade from any one of the Mercury Business Availability Center 6.2 servers to verify and upgrade the management and profile databases to Mercury Business Availability Center 6.2 compatibility. Do not proceed to the next step until database upgrade has completed successfully.	See “Verifying and Upgrading the Database Schema” on page 21.

Step	Description	Details
<p>8 Connect each Mercury Business Availability Center 6.2 machine to the management database.</p>	<p>On each Mercury Business Availability Center 6.2 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 6.2 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"> ▶ For Windows – Select Start Menu > Programs > Mercury Business Availability Center > Administration > Connect to Database. ▶ For Solaris – Execute the command: ./setmngdbWizard.sh
<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 37.</p>
<p>10 Start Mercury Business Availability Center 6.2 on all machines.</p>	<p>Enable Mercury Business Availability Center 6.2 on all machines. 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 ▶ To verify that a server has successfully started – on the server in question, look in MercuryAM\log\jboss_boot.log file for a line that includes INFO - JBoss and Started in.

Step	Description	Details
11 Reenter the Mercury Business Availability Center 6.2 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 6.2 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 6.2 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 41.
14 Upgrade Dashboard views.	Run the Dashboard upgrade process.	See “Dashboard Views Upgrade” on page 47
15 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. ► Click Hard Sync in the Custom source adapters pane.
16 Upgrade SLAs.	Run the SLM upgrade process.	For details, see “Upgrading Service Level Management to Mercury Business Availability Center 6.2” in <i>Application Administration</i> .

Step	Description	Details
<p>17 Switch URLs on data collectors (only if upgrading to Mercury Business Availability Center 6.2 on new servers).</p>	<p>If you installed the Mercury Business Availability Center 6.2 on new machines with different URLs, switch the URLs on your data collectors to report to Mercury Business Availability Center 6.2 servers.</p>	<p>See Chapter 8, “Switching Mercury Business Availability Center URL on the Data Collectors.”</p>
<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 6.2.</p>	<p>See Chapter 9, “Upgrading Components to Work with Mercury Business Availability Center 6.2.”.</p>

3

Upgrading the Servers

This chapter describes how to upgrade your servers to Mercury Business Availability Center 6.2. You upgrade your servers after performing the previous steps in the upgrade checklists, as described on page 3.

This chapter describes:	On page:
Server Architecture for Mercury Business Availability Center	12
Upgrading Considerations	12
Installing Mercury Business Availability Center 6.1 and the 6.2 Add-on on a Windows Platform	13
Installing Mercury Business Availability Center 6.2 on a Solaris Platform	17

Note:

- ▶ If running Mercury Business Availability Center 5.x in a Windows environment, you first upgrade your servers to Mercury Business Availability Center 6.1, and then install the 6.2 Add-on on top of the 6.1 servers.
 - ▶ If running Mercury Business Availability Center 5.x in a Solaris environment, you upgrade your servers directly to Mercury Business Availability Center 6.2.
-

Server Architecture for Mercury Business Availability Center

In Mercury Business Availability Center 6.x, the three 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 will continue to collect data, but it will not be sent to the database; alerts will not be generated.

Installing Mercury Business Availability Center 6.1 and the 6.2 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.

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 machine(s) 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.

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

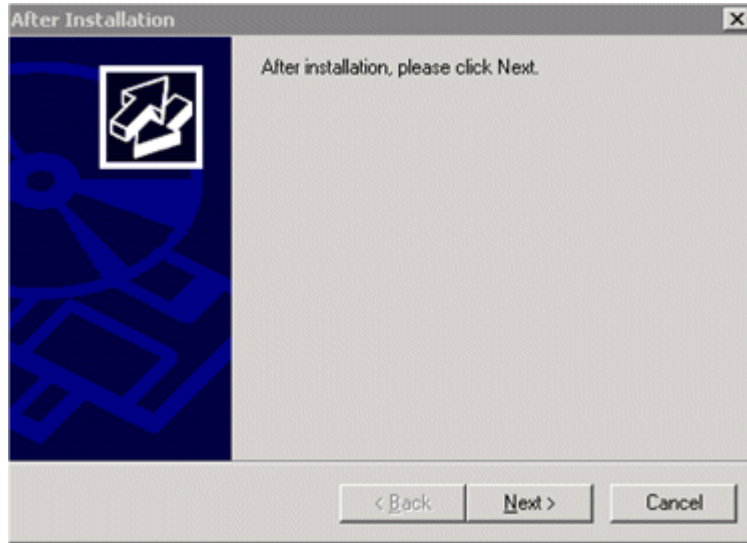
To install Mercury Business Availability Center servers on a Windows platform:

- 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 “Upgrade Checklist” on page 3 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.

For additional information on completing Mercury Business Availability Center server installation, refer to the section on completing server installation and launching Mercury Business Availability Center in *Deploying Servers*.

Installing Mercury Business Availability Center 6.2 on a Solaris 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 “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.

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 (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 “Upgrade Checklist” on page 3 for the correct sequence for connecting to the management database.

For additional information on completing Mercury Business Availability Center server installation, refer to the section on post-installation tasks in *Deploying Servers*.

Tip: When you are done, proceed with the next step in the checklist.

4

Verifying and Upgrading the Database Schema

This chapter describes the methodology for upgrading your database schema to Mercury Business Availability Center 6.2.

This chapter describes:	On page:
Introducing Upgrade Methodology	22
Using the Verify and Upgrade Utility	22
Verifying the Database Schema	25
Upgrading the Database Schema	30
Creating Database Users for the Upgrade Procedure	33
Troubleshooting Database Schema Verify and Upgrade Errors	34

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 6.2, select **Start > Programs > Mercury Business Availability Center > Administration > Upgrade Database Schema**.

Important: 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*.

Note: Check that your current database server version is supported for Mercury Business Availability Center 6.2. For details on supported and recommended database servers, 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: the verify stage (for details, see “Verify Stage” on page 23) and the upgrade stage (for details, see “Upgrade Stage” on page 24).

If errors occur during either stage, you troubleshoot them, and then rerun the utility. For details, see “Troubleshooting Database Schema Verify and Upgrade Errors” on page 34.

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 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.

Note: If you want to verify the database after upgrading to Mercury Business Availability Center 6.2 (for example, to debug database upgrade problems), refer to the Database Schema Verification chapter 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 33.

Note:

- ▶ During the verify stage, you must browse to the **TopazInfra.ini** file (<Mercury Business Availability Center root directory>\conf**TopazInfra.ini**) from the previous Mercury Business Availability Center version from which you are upgrading. Make sure you have a copy of this file accessible to the Mercury Business Availability Center 6.2 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.

Important: 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 6.2 server machine.

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 6.2 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 6.2 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:

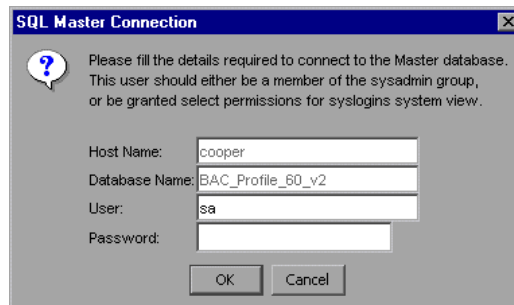
```
./run_schema_upgrade.sh
```

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 Mercury Business Availability Center version.

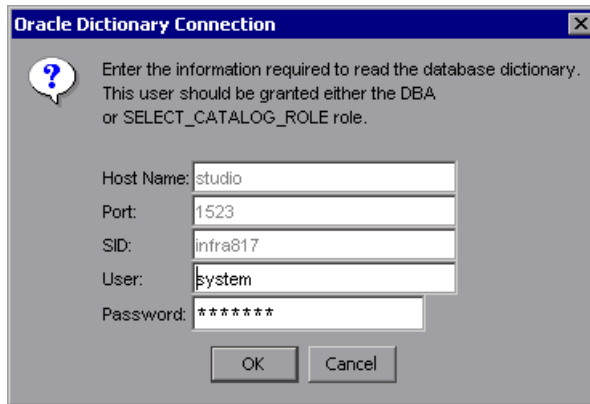


- 3 Specify the details required to connect to the appropriate database:
 - In the SQL Master Connection dialog box, specify the details required to connect to the Master database.



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.



Oracle Dictionary Connection

Enter the information required to read the database dictionary.
This user should be granted either the DBA
or SELECT_CATALOG_ROLE role.

Host Name: studio

Port: 1523

SID: infra817

User: system

Password: *****

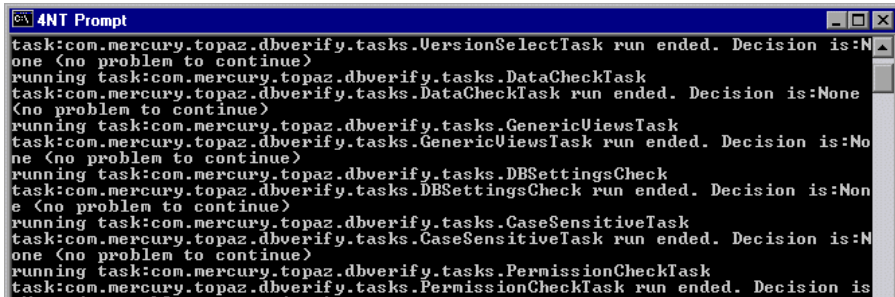
OK Cancel

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

Note:

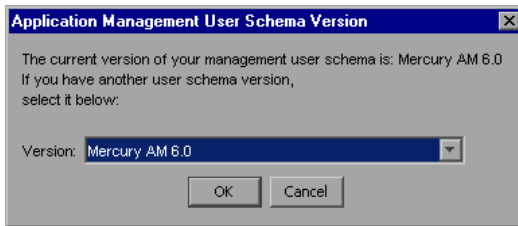
- ▶ You will be prompted for connection data for each different server on which your management and profile databases reside.
 - ▶ If you do not want to supply your database administrator account user name and password, you can create a user name with the minimum privileges required for the verify program to operate. For details on how to create this user, see “Creating Database Users for the Upgrade Procedure” on page 33.
-

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



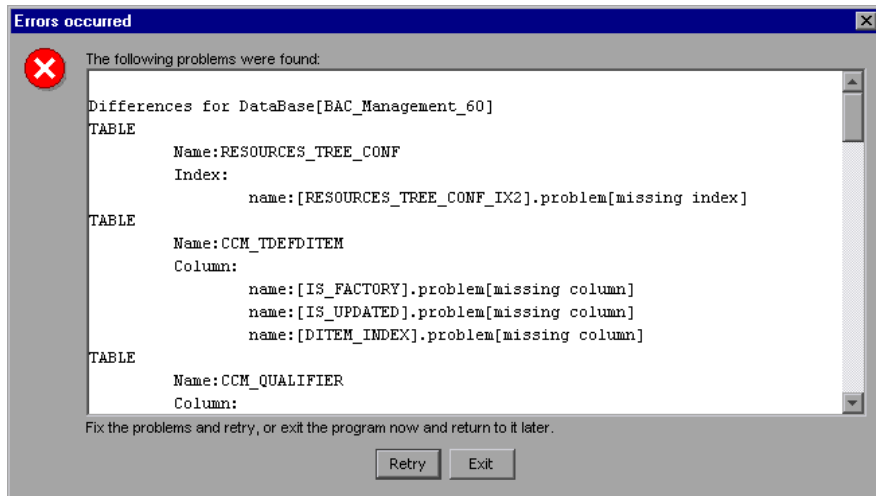
```
task:com.mercury.topaz.dbverify.tasks.VersionSelectTask run ended. Decision is:None (no problem to continue)
running task:com.mercury.topaz.dbverify.tasks.DataCheckTask
task:com.mercury.topaz.dbverify.tasks.DataCheckTask run ended. Decision is:None (no problem to continue)
running task:com.mercury.topaz.dbverify.tasks.GenericViewsTask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

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



Click **OK**.

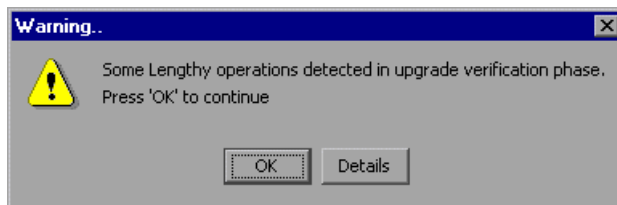
- 6 If problems occur during the database verification, a dialog box is displayed listing the errors.



Either fix the problems found and click **Retry**, or click **Exit** and rerun the database schema verify program at a later date. If you are unable to fix the problems, contact Mercury Customer Support for assistance.

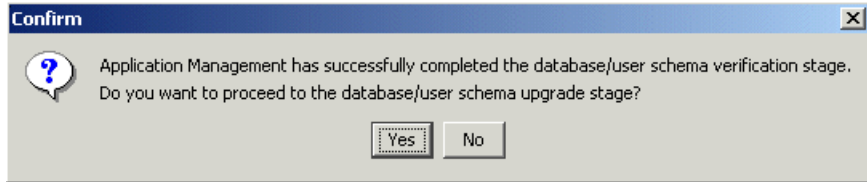
You can view a log file of the errors located in the **<Mercury Business Availability Center server root directory>\dbverify\log** directory.

- 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).



When this is done, proceed with the upgrade as described in “Upgrading the Database Schema” on page 30.

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 25), 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 Application Management 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), close them.

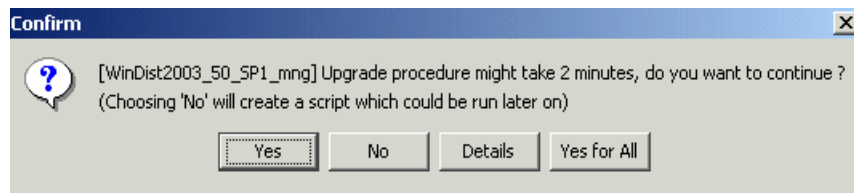
Note: Check that all processes have actually stopped after stopping the service. Stopping may take a few minutes. If necessary, stop the processes manually. There must be no open connections to the databases during the database schema upgrade.

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 25. 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:



The options for continuing are:

- ▶ **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 Mercury Business Availability Center 6.2 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 34.

- 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).

Tip: When you are done, proceed with the next step in the checklist.

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 `\MercuryAM\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.

5

Retaining Monitor Administration Configuration Data

This chapter describes how to retain and reapply your Monitor configuration data when upgrading to Mercury Business Availability Center 6.2 from Mercury Business Availability Center 5.x.

This chapter describes:	On page:
Overview of Retaining Monitor Administration Configuration Data	37
Backing Up Monitor Configuration Data Files	38
Copying Monitor Configuration Data Files to Mercury Business Availability Center 6.2	39
Upgrading the LDAP Database	40

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 6.2, 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 38.
- ▶ Copy the saved Monitor Administration configuration data to the Mercury Business Availability Center 6.2 machine, or to the Centers Server in a distributed environment. For details, see “Copying Monitor Configuration Data Files to Mercury Business Availability Center 6.2” on page 39
- ▶ Upgrade the LDAP database in Mercury Business Availability Center. For details, see “Upgrading the LDAP Database” on page 40

Backing Up Monitor Configuration Data Files

Before beginning the upgrade to Mercury Business Availability Center 6.2, 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** Stop the LDAP service by stopping Mercury Business Availability Center (**Start > Programs > Mercury Business Availability Center > Administration > Disable Business Availability Center**).
- 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 by restarting Mercury Business Availability Center (**Start > Programs > Mercury Business Availability Center > Administration > Enable Business Availability Center**).

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. For details, see the checklist on page 5.

Copying Monitor Configuration Data Files to Mercury Business Availability Center 6.2

After having upgraded your Mercury Business Availability Center 5.x system to Mercury Business Availability Center 6.2, you restore your Monitor Administration configuration data by copying the LDAP database to Mercury Business Availability Center 6.2.

To restore the LDAP database:

- 1** Stop Mercury Business Availability Center 6.2 (**Start > Programs > Mercury Business Availability Center > Administration > Disable Business Availability Center**).
- 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 6.2.

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 6.2.

To upgrade the old LDAP database:

On the Mercury Business Availability Center 6.2 Centers Server on which you restored the old LDAP database, run **MercuryAM\openldap\upgrade_ldap.bat**.

6

Configuration Upgrade

This chapter describes how to upgrade your configuration data.

Upgrading Configuration Data

You upgrade all your configuration data to Mercury Business Availability Center 6.2 from the Manual Configuration Upgrade page in the Mercury Business Availability Center site. Each of the entities listed below is upgraded independently.

The following entities are listed on the Manual Data Upgrade page:

User Upgrade	Upgrades user and user roles to Mercury Business Availability Center 6.2.
Custom Reports Upgrade	Upgrades custom and trend reports to Mercury Business Availability Center 6.2. There are two phases to the upgrade: <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.

Downtime Event Schedule Upgrade	Moves all downtime events for profiles to CMDB.
RUM MA Upgrade (5.1 to 6.2)	Removes Real User Monitor Monitor entries from the Mercury Business Availability Center 6.2 LDAP.
Monitoring Upgrade	Upgrades the monitoring administration. It includes: <ul style="list-style-type: none"> ▶ Monitor Permissions Upgrade (this includes updating all the LDAP data) ▶ Licensing Upgrade
Repositories Upgrade	Upgrades all the custom repositories definitions to Mercury Business Availability Center 6.2.
Dashboard Filters Upgrade	Upgrades filter persistency to Mercury Business Availability Center 6.2. 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 6.2 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 to Work with Mercury Business Availability Center 6.2” on page 63.

To run a configuration upgrade:

- 1** Wait until all source adapters have been inserted into the CMDB, otherwise the configuration upgrade will fail. From **CMDB Administration**, in the **Source Manager** tab, make sure that the **Last Update** column has a date for all the sources listed.
- 2** Log into Mercury Business Availability Center in the Web browser, enter the URL **http://<server_name>/MercuryAm** (**mercuryam** can also be used), where **server_name** is the name or IP address of a Mercury Business Availability Center server. If there are multiple servers or if Mercury Business Availability Center is deployed in a distributed architecture, specify the load balancer or Centers Server URL, as required.

- 3 Enter the login parameters (login name and password) of a user defined in the Mercury Business Availability Center system, and click **Log In**. After logging in, the user name appears at the top right, under the top menu bar.
- 4 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 6.0. 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) for MMS	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

Upgrade All

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

- 5 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.:

Upgrade Result	
All components upgraded successfully	
Upgrade	Status
User Upgrade	Upgrade Successful
Custom Reports Upgrade	Upgrade Successful
Licensing Upgrade	Upgrade Successful
Monitor Ldap Upgrade	Upgrade Successful
Repositories Upgrade	Upgrade Successful

[Back To Upgrade Page](#)

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`.

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

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	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 6.1.0.0 .

Finish Upgrade

7 Click the **Finish Upgrade** button.

Tip: When you are done, proceed with the next step in the checklist.

7

Dashboard Views Upgrade

This chapter describes how to upgrade your Mercury Business Availability Center 5.x custom Dashboard views to Mercury Business Availability Center 6.2 views.

This chapter describes:	On page:
The Views Upgrade Page	48
Simulating a View Upgrade	50
Upgrading a View	51
Displaying an Upgraded View	52
Troubleshooting	52
Notes and Limitations	53
Rollback	55

Important:

- ▶ Before starting the Dashboard views upgrade, you must first copy the **<Mercury Business Availability Center root directory>\CMDB** directory from your old Mercury Business Availability Center 5.x system that you saved in step 1 of the checklist to **<Mercury Business Availability Center root directory>\CMDB\5.x** in the Mercury Business Availability Center 6.2 system.
 - ▶ After upgrading all the views, refer to “Troubleshooting” on page 52 for additional steps.
-

The Views Upgrade Page

You upgrade your Mercury Business Availability Center 5.x custom Dashboard views to Mercury Business Availability Center 6.2 views from the Views Upgrade page in the Mercury Business Availability Center 6.2 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	Upgrade	Simulate Upgrade	View Log	Display Upgraded View
<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 5.1 custom 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 6.2. 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.](#)

Save

- ▶ 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 6.2.
- ▶ 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 6.2 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 49), or you can contact Mercury Customer Support for assistance in trying to correct the potential errors before upgrading the view.

Upgrading a View

You can choose to upgrade a single view, or multiple views.

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



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

When a view is successfully upgraded, its status will change 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.

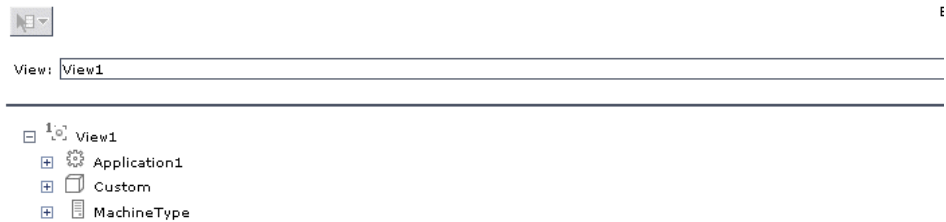
To display a log of the upgrade process showing details of items that were successfully upgraded, warnings, and any errors encountered, click the **View Log** button for the appropriate view. A new window opens displaying the upgrade log.

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.

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 6.2.

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 6.2, see Chapter 10, “Understanding Repository Upgrade from Version 5.x to Version 6.2.”

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 **MercuryAM\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 6.2 system with administrator privileges.
- 2** In **Admin > CMDB**, 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 Edit Source window.

Notes and Limitations

- The following Mercury Business Availability Center 5.x Dashboard sources are not upgraded to Mercury Business Availability Center 6.2 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 6.2.

- ▶ The following Mercury Business Availability Center 5.x Dashboard sources are not supported in Mercury Business Availability Center 6.2 and will cause errors in the views upgrade process:
 - ▶ Application Mapping
 - ▶ Remedy HelpDesk
 - ▶ dbAdapter
 - ▶ Siebel
 - ▶ Service Level Management
- ▶ Mercury Business Availability Center 6.2 includes the following default source adapters:
 - ▶ Business Process Monitor
 - ▶ Real User Monitor
 - ▶ SiteScope

The 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 6.2, manually change the Mercury Business Availability Center 6.2 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 6.2, configure a new source adapter in Mercury Business Availability Center 6.2 and manually change the source adapter template in **Admin > CMDB > Source Manager** prior to carrying out the views upgrade.

- ▶ Mercury Business Availability Center 6.2 uses default properties for CIs. If you made changes to Mercury Business Availability Center 5.x Dashboard item properties, and wish to have the same changes in Mercury Business Availability Center 6.2, manually make the changes in the **Admin > CMDB > IT Universe Manager > Properties** tab. To prevent your changes from being overridden in Mercury Business Availability Center 6.2, ensure that the **Allow CI Update** check box is not selected.
- ▶ 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.

In Mercury Business Availability Center 6.2, each CI in the CMDB must have a unique name; this CI can appear in multiple views, but each instance of the CI will have the same properties. Each 5.x Dashboard item with the same name will collectively create one equivalent CI in Mercury Business Availability Center 6.2, and this CI will be assigned the properties from the last 5.x item with that name that is upgraded as part of a view upgrade.

- ▶ 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 6.2, 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 CMDB 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 6.2 until they are upgraded.

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

8

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 6.2 servers.

This chapter describes:	On page:
Overview of Switching Data Collectors	57
Redirecting the Business Process Monitor URL	58
Redirecting the Client Monitor URL	59
Redirecting the SiteScope URL	60

Overview of Switching Data Collectors

If you install Mercury Business Availability Center 6.2 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 6.2 servers.

Note: If you installed Mercury Business Availability Center 6.2 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 6.2 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 6.2 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 Mercury Business Availability Center 5.x Business Process Transaction Monitors to the Mercury Business Availability Center 6.2 Script Repository. For details on adding scripts to the Script Repository from Monitor Administration, refer to *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 6.2 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 Mercury Business Availability Center 5.x Client Monitor Transaction Monitors to the Mercury Business Availability Center 6.2 Script Repository. For details on adding scripts to the Script Repository from Monitor Administration, refer to *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 Mercury Business Availability Center 5.x Client Monitor Transaction Monitors to the Mercury Business Availability Center 6.2 Script Repository. For details on adding scripts to the Script Repository from

Monitor Administration, refer to *End User Management Data Collector Configuration*.

Redirecting the SiteScope URL

If Mercury Business Availability Center 6.2 is installed using the same machines as the previous Mercury Business Availability Center 5.x 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 6.2 has been installed on existing Mercury Business Availability Center 5.x 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 the old SiteScope 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.AMServerSettings  
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.AMServerSettings  
import/export <filename>
```

9

Upgrading Components to Work with Mercury Business Availability Center 6.2

This chapter describes how to upgrade Mercury Business Availability Center components to work with Mercury Business Availability Center 6.2.

This chapter describes:	On page:
Upgrading Business Process Monitor	64
Client Monitor	65
SiteScope	68
Real User Monitor	70
Mercury Virtual User Generator	72

Upgrading Business Process Monitor

Mercury Business Availability Center 6.2 includes Business Process Monitor 6.2, 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 6.2 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 6.2.
-

Business Process Monitor 6.2

Business Process Monitor 6.2 includes the following enhanced functionality:

- ▶ Business Process Monitor can now color transactions for Diagnostics for any HTTP based protocol.
- ▶ Business Process Monitor reports to Mercury Business Availability Center failed transactions in scripts that did not end properly.

To upgrade Business Process Monitor to 6.2:

- 1 If you are using a version of Business Process Monitor prior to 5.0, the upgrade involves uninstalling the current version with the option to save the current configuration.

- 2 Access the Business Process Monitor 6.2 setup file for your operating system in Mercury Business Availability Center from **Admin > Platform > Setup and Maintenance > Downloads > Mercury Business Process Monitor**, and install Business Process Monitor 6.2 according to the instructions in *Business Process Monitor Administration*.

If the Business Process Monitor 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: You can remotely upgrade Business Process Monitor from within Mercury Business Availability Center 6.2. For details, refer to *Platform Administration*.

Client Monitor

Mercury Business Availability Center 6.2 includes Client Monitor 6.2, 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 6.2. For details, contact Mercury Customer Support.

Client Monitor 6.2 includes the following enhanced functionality:

- ▶ keyword support for host filtering in Mercury Business Availability Center
- ▶ Windows 2003 support for Client Monitor

- enhanced configuration for connecting to Mercury Business Availability Center
- improved persistency
- network optimization
- compatibility with the new Mercury Business Availability Center Client Monitor large deployment

Client Monitor Upgrade Notes

Note the following information regarding upgrading to Client Monitor 6.2:

Database Schema Upgrade

Database schema upgrade from Mercury Business Availability Center 6.1.x to 6.2 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

Database Data Upgrade

There is no support of data upgrade for version 6.2 in Client Monitor large deployment. This means that if you upgrade to Mercury Business Availability Center 6.2 from an existing Mercury Business Availability Center with data, version 6.2 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. In other words, the hosts that were registered before the upgrade are not included in the filters after the upgrade until you register them again in Mercury Business Availability Center 6.2.

► **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 6.1 (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 again.
- 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.

To upgrade Client Monitor 4.5/5.x to 6.2:

- 1** Uninstall the old Client Monitor.
- 2** Access the Client Monitor 6.2 setup file in Mercury Business Availability Center from **Admin > Platform > Setup and Maintenance > Downloads > Mercury Client Monitor**, and install Client Monitor 6.2 according to the instructions in *Client Monitor Administration*.

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

SiteScope

For a complete list of enhanced functionality provided by SiteScope 8.2, refer to the SiteScope release notes.

Note the following about SiteScope support in Mercury Business Availability Center 6.2:

- ▶ Mercury Business Availability Center 6.2 includes SiteScope 8.2, but supports SiteScope 7.9.0.0 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 6.2, refer to the compatibility matrix in the readme file, available in:

- ▶ From the **Deployment_Documentation** directory on the **Mercury Business Availability Center 6.2 (Windows or Solaris) Setup** CD-ROM.
- ▶ From the **Documentation\readme** directory on the **Mercury Business Availability Center 6.2 (Windows or Solaris) Documentation and Utilities** CD-ROM.
- ▶ From the Mercury Business Availability Center Documentation Portal area on the Mercury Customer Support Web site (support.mercury.com).
- ▶ 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 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 8.2.
 - ▶ Previous SiteScope profiles created in Topaz are automatically upgraded when upgrading to Mercury Business Availability Center 6.2. You will be able to view SiteScope data in Mercury Business Availability Center. Additionally, all the features of those profiles will be displayed but you will not be 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 add 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 6.2, contact Mercury Customer Support.

To upgrade SiteScope to 8.2:

- 1** Backup the <SiteScope_home>\cache directory
- 2** Backup the <SiteScope_home>\groups directory.

- 3 Access the SiteScope 8.2 setup file in Mercury Business Availability Center from **Admin > Platform > Setup and Maintenance > Downloads > SiteScope**, and install SiteScope according to the instructions in *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*.

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

Real User Monitor

Mercury Business Availability Center 6.2 includes Real User Monitor 6.2.

Note: Real User Monitor Engine 6.2 is only supported in a Windows environment.

Real User Monitor 6.2 includes the following enhanced functionality:

- ▶ Meaningful names can be created for pages that are not configured. Siebel and PeopleSoft applications have predefined templates for meaningful names.
- ▶ Global Statistics report now includes pages with errors.
- ▶ Snapshot on error (SSOE) can be configured per application.
- ▶ Real User Monitor is included in the Mercury Self-Alert Monitor.
- ▶ The system health reporting is improved in the Real User Monitor Web console.
- ▶ There is an open API for user name resolution.
- ▶ There are general performance improvements.

Contact Mercury Customer Support for assistance in performing an upgrade from pre-6.1 versions of Real User Monitor to Real User Monitor 6.2.

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.

Note:

- ▶ The Real User Monitor 6.2 probe supports only Red Hat Enterprise Linux 4 (RHEL 4). Red Hat 9 is not supported.
 - ▶ If you install Real User Monitor 6.2 probe on a different machine, you must configure it in Mercury Business Availability Center Monitor Administration just like a new probe. For details, refer to *Real User Monitor Administration*.
 - ▶ Real User Monitor 6.2 engine does not support earlier versions of Real User Monitor probe.
-

Limitation

A user custom report with an event summary component of Real User Monitor is not displayed after the upgrade. Delete the event summary component, create a new one, and set the desired filter.

Mercury Virtual User Generator

Mercury Business Availability Center 6.2 includes Mercury Virtual User Generator (VuGen) version 8.1. Upgrade VuGen to be compatible with the Business Process Monitor for Mercury Business Availability Center 6.2, and to benefit from the following improved functionality:

Note: The version of VuGen included with Mercury Business Availability Center 6.2 is the same as that included with Mercury Business Availability Center 6.1. Therefore, if you are upgrading from Mercury Business Availability Center 6.1 and installed the version of VuGen included with 6.1, you do not need to upgrade VuGen.

Workflow Wizard

The new Workflow Wizard guides you through the steps of creating a Vuser script. Each wizard screen presents an overview of the step with links to additional information or dialog boxes.

The wizard also provides summary reports for record and replay, along with links to the troubleshooting guide in the event of an error.

In conjunction with the wizard, VuGen features a new Task Pane with a list of all the tasks required for creating a script. An arrow in the task list, indicates the current task. You can move from one task to another by clicking on the desired task.

Thumbnails and Transaction Editor

VuGen now supports a thumbnail view of scripts for Web, SAPGUI, and Citrix-ICA Vusers. You can rename and annotate the thumbnails, and filter them to show only the primary thumbnails.

The Transaction editor gives you an visual overview of the script's transactions using thumbnails. You drag transaction brackets to mark the beginning and end of a transaction.

The Transaction editor also provides a filterable list of transactions, and allows you to rename and remove existing transactions.

Debugging Capabilities

VuGen features a new Run Time Data tab that lets you view run-time information during the script run. It shows the iteration number, the action name, the line number, and parameter values.

VuGen's Breakpoint Manager provides a single interface for managing breakpoints. Using the Breakpoint Manager, you can add, remove, enable, and disable breakpoints within your script.

VuGen lets you set bookmarks within your script. You can navigate between the bookmarks in each section of the script with a single key stroke.

Enhanced NTLM Authentication

VuGen has enhanced support for NTLM authentication. VuGen provides a user interface for entering NTLM login information, while automatically capturing the domain and user names. This eliminates the need to modify the script manually with the user name and password.

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** Access the Virtual User Generator setup file in Mercury Business Availability Center from **Admin > Platform > Setup and Maintenance > Downloads > Mercury Virtual User Generator**, and install the Mercury Virtual User Generator 8.1 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 older versions of VuGen, however, can run on Business Process Monitor 6.2.

10

Understanding Repository Upgrade from Version 5.x to Version 6.2

This chapter describes what happens to the repositories elements that have been customized by overriding, cloning, or that were created when you upgrade your site from Mercury Business Availability Center version 5.x to Mercury Business Availability Center version 6.2.

This chapter describes:	On page:
Upgrade Log	75
Upgrading Entities/CIs	76
Upgrading Dimensions/KPIs	76
Upgrading Rules	82
Upgrading Tooltips	89

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/CIs

The CIs are not part of the Repositories in version 6.2. The CIs are not upgraded from version 5.x to version 6.2. For details about how to handle CIs, see “Working with CIs in IT Universe Manager” in *IT Universe Manager Administration*.

Upgrading Dimensions/KPIs

The upgrade procedure removes the KPIs that are obsolete in version 6.2 and modifies other KPIs.

This section includes:

- ▶ “KPIs Removed in Version 6.2” on page 76
- ▶ “New, Cloned, or Overridden KPIs” on page 77
- ▶ “Applicable Rules” on page 79
- ▶ “Applicable Sections” on page 81
- ▶ “KPI Parameters” on page 81

KPIs Removed in Version 6.2

The following KPIs are removed during upgrade to version 6.2:

- ▶ **Remedy.** The Remedy feature is not supported in version 6.2.
- ▶ **Change.** The Change feature is handled differently in this version – for details, see “Change Report” 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 in version 6.2.
- ▶ **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 that is removed by the upgrade procedure as it is not supported in version 6.2 is as follows:

```
*** Upgrading KPI [1051] [Abandon]
This KPI does not exist in 6.2 - will be removed from repositories
```

New, Cloned, or Overridden KPIs

KPIs that were cloned or created in a previous version are upgraded to version 6.2 with the following restrictions:

- **Applicable rules.** For details, see below.
- **Applicable sections.** For details, see “Applicable Sections”.
- **Parameters.** For details, see “KPI Parameters”.

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

```
*** 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

The applicable rules for a KPI are upgraded to version 6.2 as follows:

- all rules that were deleted in version 6.2 will not be added to the applicable rules – for a list of those rules, see “Rules Removed in Version 6.2” on page 83

- all rules that were added in version 6.2 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

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 might have to manually upgrade the parameters, specially regarding 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 6.2 and modifies other rules.

This section includes:

- ▶ “Rules Removed in Version 6.2” on page 83
- ▶ “New or Cloned Rules” on page 84

- “Overridden Rules” on page 85
- “Rule Parameters” on page 85
- “Global Parameters” on page 86

Rules Removed in Version 6.2

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

- **Any of the Real User Monitor rules** – removed during upgrade. 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*.

- the **Link rule** – removed during upgrade.

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*. The internal Link rule has been removed from version 6.2.

- the **J2EE Avg Time, J2EE Max Time, J2EE Load, J2EE Exceptions, J2EE Time Outs, J2EE General, and J2EE VU Avg Time** rules are removed during upgrade – for details, see *Mercury Diagnostics Installation and User’s 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*.

- the **Generic Sample Rule** rule – removed during upgrade.

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*.

- the **Worst Dashboard PNR, Worst Dashboard Text PNR, Dashboard Text PNR, and Worst Dashboard PNR** rules – removed during upgrade.

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

- ▶ the **Change** rule – removed during upgrade. The Change feature has been improved and is handled differently in this version – for details, see “Change Report” in *Repositories Administration*.
- ▶ the **Ticketing ETTR Rule**, **Ticketing Status Calculate Rule**, and **Remedy Worst Child Rule** – removed during upgrade; they are not supported in version 6.2.

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

```
*** Upgrading rule [50] [Link Rule]
This rule does not exists in 6.2 - 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 – Note that 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 not supported in version 6.2. Customization performed by the customer on those parameters in previous version 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 85), and the global parameters (for details, see “Global Parameters” on page 86).
- ▶ 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 will automatically be 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 below.

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 6.2 will become Objective
Parameter [granularity] is not in use in 6.2 - will be removed
Parameter [szDecayTimeOut] on 6.2 changed to [No data timeout]
Parameter [UpperBound] will become Objective [minor]
```

Rule Parameters

During upgrade procedure:

- ▶ **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 in version 6.2** – 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	in Transaction Availability Rule
	Informational	in Transaction Performance Rule
UpperBound	Informational	in Transaction Availability Rule
	Minor	in Transaction Performance Rule
DollarImpact Threshold	Informational	in 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 6.2 will become Objective
```

Global Parameters

The global parameters were not modified in the new version. They are not automatically upgraded and do not need to be upgraded manually.

If you made a change to one of the global parameter’s values in any version 5.x, the change is upgraded as is and is available in version 6.2.

Upgrading Context Menus and Context Menu Items

The Context Menus and Context Menu Items are not upgraded from version 5.x to version 6.2, because they do not have IDs. The corresponding repository entry is based on their name, and most of the Context Menus and Context Menu Items have new names from version 6.0.

If you had created custom Context Menus or Context Menu Items in version 5.x, an error will be added to the log.

What you can do: If the context menu is still relevant in 6.2, 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.preprocessors.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.postprocessors.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 6.2 and modifies other tooltips.

This section includes the following topics:

- “Tooltips Removed in Version 6.2” on page 89
- “Cloned Tooltips” on page 90
- “Overridden Tooltips” on page 91
- “Tooltip Parameters” on page 91
- “Global Tooltip Parameters” on page 92

Tooltips Removed in Version 6.2

The following tooltips are removed during upgrade:

- **Any of the Real User Monitor tooltips** – removed during upgrade. 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 Parameter Details” in *Repositories Administration*.

- the **Link** tooltip – removed during upgrade. For details, see the Link rule in “Rules Removed in Version 6.2” on page 83.
- the **J2EE Avg Time, J2EE Max Time, J2EE Load, J2EE Exceptions, J2EE Time Outs, J2EE General, and J2EE VU Avg Time** tooltips are removed during upgrade. For details, see *Mercury Diagnostics Installation and User’s 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/.Net General” in *Repositories Administration*.

- the **Worst Dashboard PNR, Worst Dashboard Text PNR, Dashboard Text PNR, and Worst Dashboard PNR** tooltips – removed during upgrade.

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*.

- ▶ the **Change** tooltip – removed during upgrade. The Change feature has been improved and is handled differently in this version. For details, see “Change Report” in *Repositories Administration*.
- ▶ the **Remedy ETTR sentence**, **Remedy status sentence**, and **Remedy group sentence** tooltips – removed during upgrade; they are not supported in version 6.2.

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

```
*** Upgrading tooltip [1076] [J2EE Average time]
This tooltip does not exist in 6.2 - will be removed from repositories
```

Cloned Tooltips

The **Calculation Rule** parameter is added to the tooltips that were cloned in previous versions during the upgrade procedure, the rest of the parameters remain as they were in the previous version.

The tooltip parameters (for details, see “Tooltip Parameters” on page 91), and the global tooltip parameters (for details, see “Global Tooltip Parameters” on page 92) 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="" value-
Source="NODE.DIM.RULE.ID_CUST" valuePostfix="" formatting-
Method="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 previous versions are upgraded with some restrictions regarding the tooltip parameters (for details, see “Tooltip Parameters” on page 91), and the global tooltip parameters (for details, see “Global Tooltip Parameters” on page 92).

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" valuePre-
fix="[[NODE.DIM.OBJECTIVE_OP]] $" value-
Source="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 91.

Global Tooltip Parameters

The global parameters were not modified in the new version. They are not automatically upgraded and do not need to be upgraded manually.

Index

A

architecture (server) 12

B

Business Process Monitor
upgrading 64

C

checklist, upgrade 5
Client Monitor, upgrading 65
components, upgrading 63
configuration, upgrading 41

D

dashboard views
 display upgraded view 52
 notes and limitations 53
 troubleshooting 52
 upgrade rollback 55
 upgrade settings 49
 upgrade simulation 50
 upgrading 47, 51
data collectors
 changing URL 57
 upgrading 63
data files
 backing up 38
 copying 39
 retaining 37
 updating path to 40
database schema
 upgrading 21, 30
 verifying 21, 25
database users, creating for upgrade 33

dbverify 22

J

Java run time, modifying mx parameter 34

L

LDAP database
 backing up 38
 copying 39
 retaining 37
 updating path to 40

M

monitor administration configuration data
 backing up 38
 copying 39
 retaining 37
 updating path to 40

R

Real User Monitor, upgrading 70
rollback, upgraded views 55

S

server architecture 12
server installation
 Solaris platform 17
 Windows platform 13
servers, upgrading 11
SiteScope
 upgrading 68
Solaris platform
 upgrading servers 17

T

- troubleshooting
 - dashboard views 52
 - dbverify errors 34
 - views 52

U

- upgrade
 - checklist 5
 - components 63
 - configuration 41
 - considerations 12
 - dashboard views 47, 51
 - database schema 21
 - dbverify utility 22
 - getting started 3
 - introduction 1
 - major steps 2
 - methodology 22
 - servers 11
 - views 47, 51
- upgrade settings, dashboard views 49
- upgrade simulation
 - dashboard views 50
 - views 50
- upgrade view, display 52
- URL, changing on data collectors 57

V

- verify utility 22
- verifying database schema 21
- views
 - display upgraded view 52
 - notes and limitations 53
 - troubleshooting 52
 - upgrade 51
 - upgrade rollback 55
 - upgrade settings 49
 - upgrade simulation 50
 - upgrading 47
- Virtual User Generator, upgrading 72

W

- Windows platform, upgrading servers 13