Mercury Business Availability Center 6.6 Readme

Last revised: March 20, 2006

This file provides the following information about Mercury Business Availability Center 6.6:

Mercury Business Availability Center 6.6 Files

Mercury Business Availability Center 6.6 includes the following files:

- **Mercury Business Availability Center 6.6 setup file**
  - Setup.exe (Windows installation)
  - Setup.bin (Solaris installation)

- **Component setup files**
  - Real User Monitor Probe (Linux)
  - Real User Monitor Engine (Windows)
  - Mercury Client Monitor 6.5.3 (Windows)
  - Mercury Business Process Monitor 6.6 (Windows, Solaris, Linux)
  - Virtual User Generator (VuGen) files and related patches required for Business Process Monitor:
    - VuGen 8.1 (no change from the one released in Mercury Business Availability Center 6.2)
    - LoadRunner 8.1 Feature Pack 3 (for installation on top of VuGen 8.1 to upgrade to VuGen 8.1 FP3)
    - Microsoft .Net Framework 1.1 Package
    - Microsoft WSE 2.0 SP3 Runtime
  - Mercury Discovery Probe (Windows)
  - Mercury Dashboard Ticker 6.2 (no change from the one released in Mercury Business Availability Center 6.2)
  - SiteScope 8.7 (Windows, Solaris, Linux)
    Note: If you downloaded Mercury Business Availability Center 6.6 from the Mercury Web site, you should download SiteScope 8.7 separately.

- **Additional files**
  - sis_for_pi_v6_6.zip – file needed for Problem Isolation application
  - tzupdater.jar – file needed for DST update (see Appendix 2)

- **Documentation files**
  - whatsnew.html
  - readme66.doc
  - readme65.html (for reference)
  - readme64.html (for reference)
  - readme63.html (for reference)
  - readme62.html (for reference)
  - Deploy_docs.zip – includes the following deployment documentation:
    GettingStarted.pdf – Getting Started with Mercury Business Availability Center
    PrepDatabase.pdf – Preparing the Database Environment
    Deploy.pdf – Deploying Servers
    Hardening.pdf – Hardening the Platform
    Upgrade.pdf – Upgrading Mercury Business Availability Center
    MAMInstall.pdf – Mercury Application Mapping Installation Guide
  - BAC_HPOVO.pdf – Mercury Business Availability Center-HP OVO Integration Document

Note: Updated PDF documents included with Business Availability Center 6.6 are labeled as version 6.6. PDF documents labeled as version 6.5 are still relevant with version 6.6.

Mercury Business Availability Center 6.6 Prerequisites

Mercury Business Availability Center 6.6 can be installed on top of the following versions:

- Mercury Business Availability Center 6.5
- Mercury Business Availability Center 6.4
- Mercury Business Availability Center 6.3
- Mercury Business Availability Center 6.2

Notes:

- New customers should install Mercury Business Availability Center **6.1**, then install the Mercury Business Availability Center **6.2** add-on, and then install the Mercury Business Availability Center **6.6** add-on.
- Mercury Business Availability Center 6.6 includes the content of Mercury Business Availability Center 6.3, 6.4, and 6.5. Version 6.6 can be installed directly on top of 6.2 (it is not necessary to install 6.3 / 6.4 / 6.5).
- For upgrade from 4.5.x or 5.1.x, contact Mercury Customer Support.

Mercury Business Availability Center 6.6 Installation

- For new installation instructions, see *Deploying Servers* (Deploy.pdf).
- For upgrade instructions, see *Upgrading Mercury Business Availability Center* (Upgrade.pdf).
- After the installation, it is recommended to activate the new LRDT monitor. For details, see Appendix 1. The new LRDT monitor may solve certain bus issues.
  It is mandatory to switch to the new LRDT monitor if your SiteScope is sending data to Mercury Business Availability Center and Mercury Self-Alert Monitor is active.
- After the installation, read and apply the DST procedure described in Appendix 2.
- Perform the following steps if upgrading from Business Availability Center 6.5 running in a shared CMDB architecture to Business Availability Center 6.6 running in a shared CMDB architecture:
  1. Before starting the upgrade process, redeploy the PM.zip package while Mercury Application Mapping is running.
  2. After completing the upgrade process, redeploy the PM.zip package while Mercury Application Mapping is running.

  Note: For instructions on package deployment, see Redeploying and Undeploying Packages in *Upgrading Mercury Business Availability Center* (Upgrade.pdf).
- Perform the following steps if upgrading from Business Availability Center 6.5 without a shared CMDB to Business Availability Center 6.6 running in a shared CMDB architecture:
  1. Undeploy the PM.zip package.
  2. In Mercury Application Mapping:
     a. In the Correlation Manager tab, delete the PM folder and all its contents.
     b. In the TQL Builder tab, delete the PM folder and all its contents.
     c. If there is a corrupted correlation rule that cannot be deleted from the Correlation Manager tab:
        - Create a new view based on the existing TQL correlation_view.
        - Use the Topology View tab to find the corrupted correlation rule and delete it.
        - Restart Mercury Application Mapping.

  Note: For instructions on package undeployment, see Redeploying and Undeploying Packages in *Upgrading Mercury Business Availability Center* (Upgrade.pdf).

Mercury Business Availability Center 6.6 Uninstallation

- For uninstall instructions, see *Deploying Servers* (Deploy.pdf).

Mercury Business Availability Center 6.6 Content

- **Problem Isolation** – a significant improvement to and rebranding of the Problem Management application released in Business Availability Center 6.5. The Problem Isolation application enables users to more quickly isolate the causes of problems and incidents occurring throughout their services, applications, and infrastructure to shorten mean time to resolution.
- **Real User Management 6.6** – improves on the existing Real User Monitor solution by providing a much richer, user-session replay interface and adding new alerting capabilities.
- **HP OVO Integration** – the HP OVO Event Monitor integrates OVO data into Business Availability Center. The monitor supports integration with Business Availability Center 6.6. A new automated Integration Add-on configures the mapping between OVO data and Business Availability Center applications and enables:
  - forwarding events from the OVO system to Business Availability Center
  - automatically building the relevant topology of host or host and application
  - retrieving data for the applicable KPIs
- **SiteScope 8.7**

- **Bug fixes:**
  - Fixed: Business Process Monitor scheduled by local time worked incorrectly after Daylight Saving Time shift (SR# 1-526204863).
  - Fixed: Adapter deleted all CIs from CMDB, causing loss of custom KPIs, CIs, views, and so on (SR# 1-562378693).
  - Fixed: Error occurred while assigning WebTrace and single URL monitors to public POPs in MMS (eSAR # 29615).
  - Fixed: Problem in Business Process Monitor replay of Web protocol scripts (SR# 1-247F9T).
  - Fixed: Business Process Monitor received incorrect downtime status (SR# 31265, SR# 1-496730273).
  - Fixed: If Client Monitor runs and breakdown option is enabled, IE crashed in specific cases (1-24AJJH).
  - Fixed: Error occurred in log if user generates a KPI Over Time report on values, and there are no values (eSAR# 30872).
  - Fixed: Empty End User reports on stopped Business Process Monitor profiles on data more than 3 months old (SR# 30024).
  - Fixed: Cannot export CSV report for SiteScope Cross-Performance report if custom report contains the Cross-Performance report component (SR# 1-587984565).
  - Fixed: Business Process Monitor Page Component Breakdown failed in some cases (SR# 29289).
  - Fixed: Cannot define Business Process Monitor downtime on location in Service Level Management (SR# 1B-1Q4PCK).
  - Fixed: Cannot attach SiteScope to Business Availability Center when the SiteScope contains a Weblogic monitor with a secure connection (SR# 1-2454PL).
  - Fixed: On specific configuration of distributed Monitor Administration (which includes load balancer), when creating new empty profile, string error exception occured (eSAR# 28657).
  - Fixed: JavaScript exception when trying to open calendar from some reports (SR# 29504).
  - Fixed: Some reports are not displayed if connection to bus failed (SR# 29757).
  - Fixed: Connection leak in Bus and clustering component on Solaris (SR# 1-24HHP1).
- Internal bugs fixes

- **6.5 content:** See readme65.html for details.
- **6.4 content:** See readme64.html for details.
- **6.3 content:** See readme63.html for details.

Updated Components

The following updated components are included with Mercury Business Availability Center 6.6:

- **Client Monitor 6.5.3** (Build 187)
  - Bug fixes

- **Business Process Monitor 6.6** (Build 881)
  - Bug fixes

- **Discovery Probe**
  - Bug fixes

- **Real User Monitor 6.6** (engine build 6.6.94; probe build 6.6.50)
  - Added resource caching ability, which enables storing of all static resources (such as images and style sheets) on the Real User Monitor probe machine, instead of requesting them from the monitored application. This makes the viewing and replaying of snapshots more robust.

  Note: Newer versions of the Real User Monitor engine and probe might be released after Mercury Business Availability Center 6.6. Contact Mercury Customer Support to check whether there are newer versions of these components available for installation.

- **SiteScope 8.7**
  - OVO Integration into Business Availability Center 6.6 (see details in Content section above)
  - New SSH client allows running multiple SSH-based monitors under heavy load
  - Fixes for customers escalations
  - Bugs fixes

Limitations and Issues

General

- When working with Business Availability Center, it is highly recommended to avoid using the short time zone abbreviations such as EST and MST. Use the long names instead, for example, America/New_York.
- When navigating to Mercury Business Availability Center 6.6 pages for the first time after installation, the pages may take some time to load due to .jsp compilation.

Real User Monitor- Session Replay Limitations

- There must be a network connection between the client machine that runs the session replay applet and Real User Monitor engine.
- In some non-standard sites, the page layout might seem wrong in the snapshot view.
- There can be only one replay window opened at a time. Opening more than one might lead to data getting mixed between windows.
- When a long string is passed in post parameters, the replay applet does not show any parameters in the GUI.
- The timeout between the session replay applet and Real User Monitor engine is 20 minutes. Leaving it open with no change for longer will cause it to lose the connection.
- Certain content types may not be displayed properly.

HP OVO Integration

- After adapter change, new samples do not create full hierarchy. Wait 20 minutes. Only samples that arrive after 20 minutes will create a full hierarchy.
- Restarting Business Availability Center will cause all event colors to be deleted from the OVO view.
- Changing the OVO adapter from two-KPI to four-KPI mode or vice versa ("Include Network and Security KPIs") deletes all CI hierarchies previously created by the adapter.
- Deleting host CI from HP OVO view leaves the EMS monitor. Subsequent host recreation will not connect the host to the existing monitor. The workaround is deleting the EMS monitor manually. In this case, both the host and EMS monitor are recreated.

Adapters and Views

- When editing the SiteScope source adapter in Source Manager, if you change the **Include measurements** value to None, the previous SiteScope monitor configurations are deleted from the CMDB. This may affect, for example, SLAs in Service Level Management that are based on SiteScope measurements.
- When synchronizing a SiteScope source adapter in Source Manager, if the adapter includes a large number of objects, then adapter performance might be slow, taking several minutes.
- When editing the SiteScope source adapter in Source Manager, if you select the **Include machines** option, then the hierarchy in the Monitors View and System Monitors View (as shown in View Explorer) includes CIs for the monitored host machines. However, for each appearance of a host in the view, the child CIs for the host include all monitors monitoring that host. This means that: a) monitor CIs may be duplicated, appearing under multiple instances of a host CI. b) monitor CIs may appear under SiteScopes or SiteScope groups to which they do not belong.
- If you have a large number of CIs in the Monitors View (over the 50,000 limit), when you access the view, it may be empty. Use one of the following workarounds:
  a. Work instead with the End User Monitors View or the System Monitors View (which together contain all CIs that are in the Monitors View).
  b. In View Manager, create new pattern views that define TQLs only for specific monitoring areas. For example, you can create a different pattern view for each SiteScope, by adding conditions to the TQL node definitions.
- If you are upgrading the HP Systems Insight Manager (SIM) source adapter to Mercury Business Availability Center 6.6, some machine and device items that do not have an IPAddress property may not pass the upgrade. If you receive a warning about this, rollback the upgrade, define the IPAddress property for each relevant item in the previous version, and run the upgrade again.
- Specific words included in an event sample field's value (being sent to Mercury Business Availability Center) can cause events to be omitted from the EMS Event Log. The problem occurs when EMS configuration file keys are used as field values. Therefore, do not use EMS fields such as "object," "instance," or "subject" (for example, data_source="instance") as values. These words can cause a problem in the mechanism that retrieves data from the Mercury Business Availability Center database.

Monitor Administration

- Copying items within the monitor tree from a SiteScope object running on SiteScope version 8.0 or higher to another SiteScope object running on a previous version of SiteScope may cause unexpected errors.
- Copying items within the monitor tree from a SiteScope object running on one operating system (for example, Windows) to another SiteScope object running on a different operating system (for example, Linux) is not supported.
- Pasting a container into another container in the monitor tree is not supported.
- Monitor Administration does not support Dynamic Update preferences for SiteScope. Dynamic Update preferences are supported only when working in a standalone SiteScope. If you work with Dynamic Update preferences, you can add a SiteScope to Monitor Administration for reporting purposes only but do not import configurations when adding the SiteScope.
- If a SiteScope has been detached from Monitor Administration and unregistered from Mercury Business Availability Center, it is possible to add another SiteScope to Monitor Administration with the same host name. If a second SiteScope has been added with the same host name, it is highly recommended to work only with the new SiteScope and not reattach the old SiteScope. Only one SiteScope profile can report data to Mercury Business Availability Center from a SiteScope server and working with the old SiteScope may cause unexpected errors.
- If you use a very long string for the name field when adding a SiteScope to Monitor Administration, your browser may get stuck.
- SiteScope cannot report data to a Mercury Business Availability Center whose user name or password uses Japanese characters.

Updated Mercury Business Availability Center Support Matrixes

SiteScope Support Matrix

The following table enables you to compare SiteScope support for the current and previous Mercury Business Availability Center and Topaz versions (√=supported; X=not supported):

Compatibility Matrix	**BAC 6.6**	**BAC 6.0-6.5**	**BAC 5.x**	**Topaz Managed Services 4.5 FP2**	**Topaz 4.5 FP2**
SiteScope 8.7	√ (Recommended)	√	√	X	X
SiteScope 8.6, 8.5, 8.2.1	√	√	√	X	X
SiteScope 8.1.1, 8.1.2, 8.0 SP3, 8.0 SP3	√	√	√	√	√
SiteScope 7.9.5.0, 7.9.1.0, 7.9	√	√	√	√	√
SiteScope 7.8.1.0, 7.8.1.2 ,7.8.1.3	X	X	√	√	√

SiteScope/Mercury Business Availability Center Compatibility Matrix

There are two main aspects of compatibility between SiteScope and Mercury Business Availability Center. The first is **data logging** which is the process of logging data collected by SiteScope to Mercury Business Availability Center for the purposes of real-time status, reporting, Service Level Management, and so forth. The second aspect of compatibility is **Monitor Administration** which refers to configuring SiteScope (including deploying monitors) from within Mercury Business Availability Center. The following table contains compatibility information regarding these two aspects and the various combinations of SiteScope and Topaz/Mercury Business Availability Center releases.

1 = Data logging support
2 = Monitor Administration support

SiteScope Version	**BAC Version**			
	6.x	**5.1**	**5.0**	**Topaz 4.5SP1–4.5SP3**
SiteScope 8.7, 8.6, 8.5	1,2	1,2	1	X
SiteScope 8.2.1	1,2	1,2	1	X
SiteScope 8.1, 8.1.1, 8.0 SP3, 8.0 SP2	1,2	1,2	1	1
SiteScope 8.0, 8.0 SP1	1	1,2	1	1
SiteScope 7.9.5.x	1,2	1,2	1	1
SiteScope 7.9.1.0	1	1	1,2	1
SiteScope 7.9.0.0	1	1	1	1
SiteScope 7.8.1.0, 7.8.1.2	X	1	1	1

Real User Monitor Support Matrix

- Real User Monitor 6.6 (probe and engine) works only with Business Availability Center 6.6.

Business Process Monitor Changes

Business Process Monitor Version	**Changes**
6.6	Bug fixes
6.5	Moved to use LoadRunner 8.1 FP3 replay and support three new protocols (WebGUI, Citrix, WSE). Scripts in the new protocols are supported from this version and up only.
6.4.1	EA version of the functionality introduced in Business Process Monitor 6.5
6.4	Fix for Siebel transaction coloring
6.3	Changes and fixes in NTLM and authentication

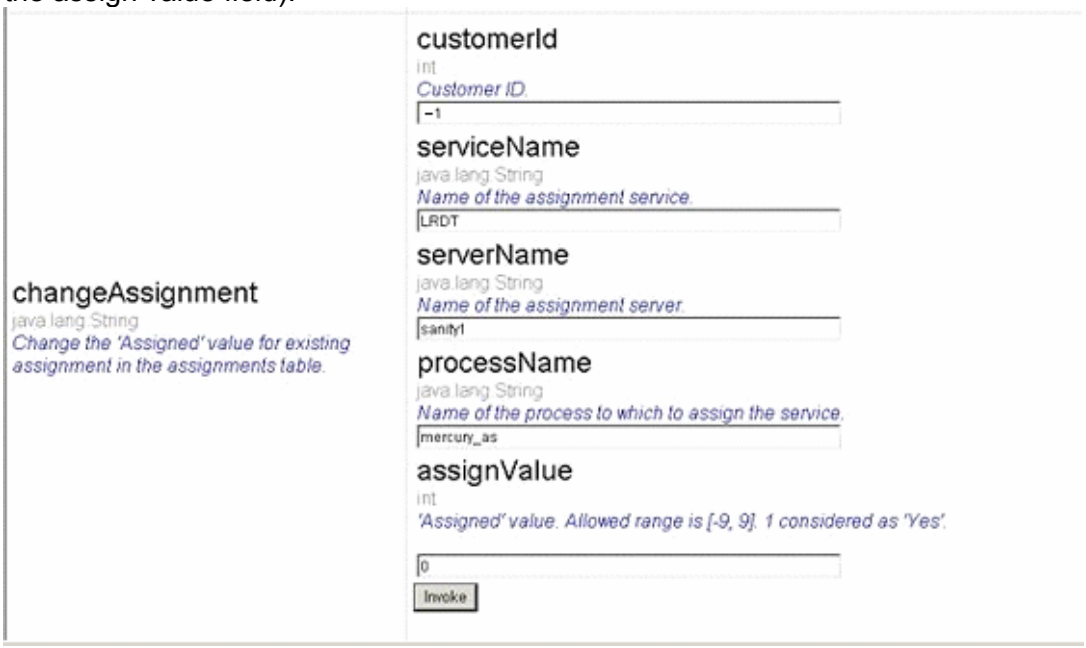
Other Notes

- If burning Solaris or Linux components onto a CD-ROM for installation purposes, make sure to select a non-Joliet ISO setting.
- If burning Mercury Business Availability Center 6.6 files onto a CD-ROM, keep in mind that the complete release will not fit onto one CD-ROM. Divide the files between two CD-ROMs according to your requirements.

Appendix 1: Activating the New LRDT Monitor

Starting from Mercury Business Availability Center 6.4, there is a new implementation of the LRDT (last reported data time) monitor. This monitor extracts the last reported data time of Business Process Monitor, Client Monitor, and SiteScope data collectors, and its results are displayed in SiteScope. The new LRDT monitor solves one of the causes of Mercury Business Availability Center BUS failure. By default, the old LRDT monitor is operational. To switch to the new implementation (recommended), follow the steps below:

1. Disable the old LRDT monitor:
   - Open the Mercury Business Availability Center JMX console: **http://<server_name>:8080/jmx-console**
   - In the **Topaz** section, click **service=LastReportedDataTime**.
   - Invoke the **Stop** method.
2. Disable LRDT in the HAC Manager:
   - Go to JMX console HAC Mbean: http://< server_name >:8080/jmx-console/HtmlAdaptor?action=inspectMBean&name=Topaz%3Aservice%3Dhac-manager
   - Go to changeAssignment and change LRDT assignment to 0 (see in the picture below the assign value field).



3. Configure Mercury Business Availability Center to work with the new LRDT monitor:
   - Run the following query against the Mercury Business Availability Center management database:

     MS SQL Server:

     insert into SYSTEM (SYS_NAME,SYS_VALUE) values ('LRDTProviderType', 'LRDTSQLImplementation')

     ORACLE Server:

     insert into "SYSTEM" ("SYS_NAME", "SYS_VALUE") values ('LRDTProviderType', 'LRDTSQLImplementation')
   - Restart Mercury Business Availability Center.
4. Configure the timeframe. By default, the LRDT monitor searches for last reported data within the last 24 hours. Because it affects the monitor performance, this timeframe can be expanded/narrowed, depending on the database and its performance. The change can be done using the following procedure:
   - Add a key to the SYSTEM table:

     MS SQL Server:

     insert into SYSTEM (SYS_NAME,SYS_VALUE) values ('LRDT_TIMEFRAME', <value in seconds>)

     ORACLE Server:

     insert into "SYSTEM" ("SYS_NAME", "SYS_VALUE") values ('LRDT_TIMEFRAME', <value in seconds>)
   - Restart Mercury Business Availability Center.

Appendix 2: Daylight Savings Time Update Procedure

General

In August 2005, the United States Congress passed the Energy Policy Act, which changes the dates of both the start and end of Daylight Saving Time (DST). When this law goes into effect in 2007, DST will start three weeks earlier (2:00 A.M. on the second Sunday in March) and will end one week later (2:00 A.M. on the first Sunday in November) than it had previously.
This appendix explains how to ensure that Business Availability Center is compliant with the DST change. For more information see:

- http://java.sun.com/developer/technicalArticles/Intl/FAQ_appendix.html
- http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=6466476

Note: A separate Business Availability Center patch was already released to handle the new DST policy.

- If you already updated the operating system, you do not need to update it again.
- Business Availability Center 6.6 already contains the correct JODA files.
- Updating of the JRE of BAC 6.6 servers is done automatically after the installation.

Updating Business Availability Center Servers and Databases

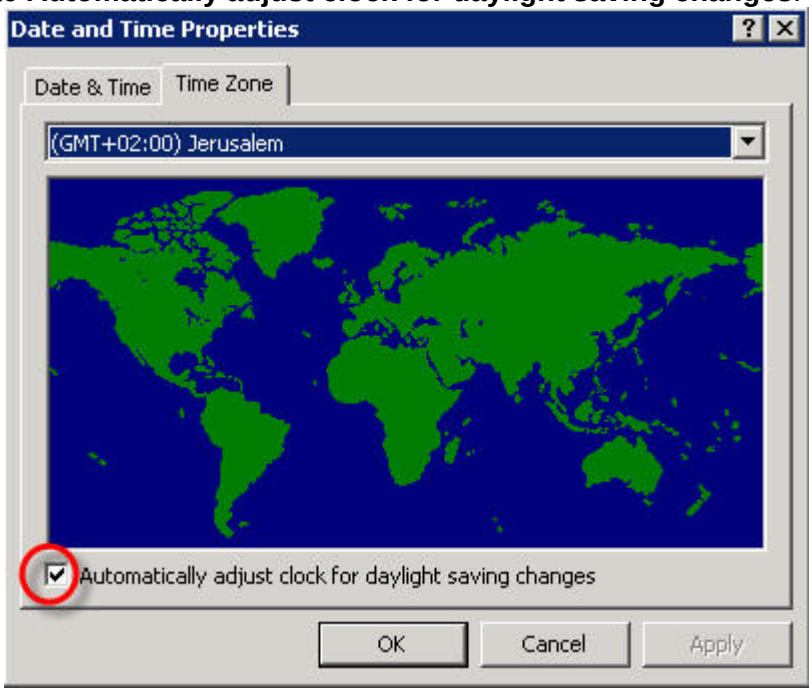
- Update the operating system on all server machines on which Business Availability Center is installed. (See instructions below.)
- Update the operating system on all Business Availability Center database machines. (See instructions below.)

Updating Components (Data Collectors)

Note: It is recommended that you update the operating system for all data collectors, even if not outlined as mandatory below.

Business Process Monitor (BPM)

- It is recommended that you update both the operating system and the JRE for all Business Process Monitor machines. If you decide to update the JRE for Business Process Monitor, note that the Business Process Monitor supplied with Business Availability Center 6.6 (and available from the Downloads page) uses the "non-updated" JRE and should be updated.
- It is mandatory to update the operating system for Business Process Monitor machines that are set to **Automatically adjust clock for daylight saving changes**:



- Updating the JRE is optional, however, if it is not updated, the Business Process Monitor Admin GUI might show times with one hour offset.

Client Monitor

No fix is required.

Real User Monitor

No fix is required (for both Engine and Probe).

SiteScope

- **SiteScope 8.2 and higher:** No fix is required. However, it is recommended that you update the operating system as a best practice (see instructions below).
- **Older versions of SiteScope:** It is recommended that you upgrade previous versions of SiteScope to SiteScope 8.7. If it is not feasible, you can update SiteScope 7.9.5.17 by updating the JRE (see instructions below).

Discovery Probe

It is not mandatory to update the Discovery probe. However, it is recommended that you update the operating system and the JRE.

Updating the Operating System

Consult the following links:

Microsoft Windows
Microsoft Windows update: http://support.microsoft.com/kb/928388/
General Information: http://www.microsoft.com/windows/timezone/dst2007.mspx
Windows 2000: If you still use Windows 2000, note that Microsoft's Web site indicates that Windows 2000 has passed the end of mainstream support and will not be receiving an update without an Extended Support Hotfix Agreement. See also: http://support.microsoft.com/kb/914387/

SUN Solaris
SUN Solaris update: http://sunsolve.sun.com/search/document.do?assetkey=1-26-102775-1
General Information:

- http://www.sun.com/bigadmin/features/techtips/dst_changes.html
- http://java.sun.com/developer/technicalArticles/Intl/USDST/

Redhat Linux
Redhat Linux update: http://kbase.redhat.com/faq/FAQ_80_7909.shtm

Updating the Java Runtime Environment (JRE)

Updating Business Process Monitor (BPM)

1. Navigate to the Business Process Monitor installation directory and copy **tzupdater.jar** to **<Business Process Monitor Home>\JRE\bin**. (You can also find this folder by entering **%topaz_agent_home%** in the **Start > Run** command box).
2. Open a Command Prompt window (DOS shell).
3. Change directory to **<Business Process Monitor Home>\JRE\bin**.
4. Run the following command to check whether the update is required: **java –jar tzupdater.jar –t**
5. If an update is required, the command returns a long list of messages. If nothing is returned, no further action is necessary.
6. Stop the Business Process Monitor service.
7. Close all Business Process Monitor Admin windows.
8. Run the following command to install the patch: **java –jar tzupdater.jar –u -bc**
9. Verify that the patch has been correctly applied. Run the same command specified in step 4. If nothing is returned, the patch has been successfully applied.
10. Restart the Business Process Monitor service.

Updating SiteScope

1. Navigate to the SiteScope installation directory and copy **tzupdater.jar** to **<SiteScope Home>\java\bin**.
2. Open a Command Prompt window (DOS shell).
3. Change directory to **<SiteScope Home>\java\bin**.
4. Run the following command to check whether the update is required: **java –jar tzupdater.jar –t**
5. If an update is required, the command returns a long list of messages. If nothing is returned, no further action is necessary.
6. Stop the SiteScope service.
7. Close all SiteScope GUI windows.
8. Run the following command to install the patch: **java –jar tzupdater.jar –u -bc**
9. Verify that the patch has been correctly applied. Run the same command specified in step 4. If nothing is returned, the patch has been successfully applied.
10. Restart the SiteScope service.

Updating Discovery Probe

1. Navigate to the Discovery Probe installation directory and copy **tzupdater.jar** to **<Discovery Probe Home>\jre\bin**.
2. Open a Command Prompt window (DOS shell).
3. Change directory to **<Discovery Probe Home>\jre\bin**.
4. Run the following command to check whether the update is required: **java –jar tzupdater.jar –t**
5. If an update is required, the command returns a long list of messages. If nothing is returned, no further action is necessary.
6. Stop the Discovery Probe.
7. Run the following command to install the patch: **java –jar tzupdater.jar –u -bc**
8. Verify that the patch has been correctly applied. Run the same command specified in step 4. If nothing is returned, the patch has been successfully applied.
9. Restart the Discovery Probe.

For more information about the JRE update, see:
http://java.sun.com/javase/tzupdater_README.html