Mercury Business Availability Center 6.7 Readme

Last revised: June 24, 2007

This file provides the following information about Mercury Business Availability Center 6.7:

Mercury Business Availability Center 6.7 Files

Mercury Business Availability Center 6.7 includes the following files:

- **Mercury Business Availability Center 6.7 setup file**
  - Setup.exe (Windows installation)
  - Setup.bin (Solaris installation)

- **Component setup files**
  - Real User Monitor Probe 6.6 (Linux)
  - Real User Monitor Engine 6.6 (Windows)
  - **New**: Mercury Client Monitor 6.5.4 (Windows)
  - **New**: Mercury Business Process Monitor 6.6.1 (Windows, Solaris, Linux)
  - Virtual User Generator (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 6.6
  - Mercury Dashboard Ticker 6.2
  - SiteScope 8.8 (Windows, Solaris, Linux)
    Note: If you downloaded Mercury Business Availability Center 6.7 from the Mercury Web site, you need to separately download SiteScope 8.8.

- **Documentation files**
  - whatsnew.html
  - readme67.doc
  - readme66.doc (for reference)
  - 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 (**Updated**)
    MAMInstall.pdf – Mercury Application Mapping Installation Guide
  - BAC_HPOVO.pdf – Mercury Business Availability Center-HP OVO Integration Document

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

Mercury Business Availability Center 6.7 Prerequisites

- Mercury Business Availability Center 6.7 can be installed on top of the following versions:
  - Mercury Business Availability Center 6.6
  - 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 **6.7** add-on.
- Mercury Business Availability Center 6.7 includes the content of Mercury Business Availability Center 6.3, 6.4, 6.5 and 6.6, so 6.7 can be installed directly on top of 6.2 (it is not necessary to install 6.3 / 6.4 / 6.5 / 6.6).
- For upgrade from 4.5.x or 5.1.x, contact Mercury Customer Support.

Mercury Business Availability Center 6.7 Installation

- For new installation instructions, see Deploying Servers (Deploy.pdf).
- For upgrade instructions, see Upgrading Mercury Business Availability Center (Upgrade.pdf).
  If you are using a Business Availability Center-Mercury Application Mapping shared CMDB architecture, you **must** contact Customer Support before the installation.
  If you are using Discovery Probe 6.6, you must update it:
  - Copy the following .jar files from MercuryAM/lib on the Data Processing Server:
    cmdb_server.jar
    cmdb shared.jar
  - Paste these two .jar files into the following directory on Mercury Application Mapping 6.6 Probe machine**:**
    Root/ext/cmdb
- If you are upgrading from Business Availability Center 6.6, at the end of the installation you can clear the "Perform schema upgrade after Setup" option (since there is no schema change between 6.6 and 6.7).
- 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.

- **Problem Isolation**
  - Perform the following steps if upgrading from Business Availability Center 6.5 running in a shared CMDB architecture to Business Availability Center 6.7 running in a shared CMDB architecture:
    - Before starting the upgrade process, redeploy the PM.zip package while Mercury Application Mapping is running.
    - 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 6.7 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).

- Perform the following steps if upgrading from Business Availability Center 6.6 without a shared CMDB to Business Availability Center 6.7 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).

- If you are planning to use Real User Monitor session replay bypass, you must do the following after Business Availability Center installation but before starting Business Availability Center. Change the Web server configuration as following:
  - **IIS**
    Add to **WebServer\conf\workers2.properties** the following two lines and restart IIS (in Services, stop IIS Admin and then start the WWW service):

    ```
    [uri:/rumproxy/*]
    worker=ajp13:localhost:8009
    ```
  - **Apache**
    Add to **WebServer\conf\workers2.properties** the following two lines and restart Tomcat (WebServer\bin\Apache2Stop.bat, WebServer\bin\Apache2Start.bat):

    ```
    [uri:/rumproxy/*]
    worker=ajp13:localhost:8009
    ```
  - **IPlanet**
    Add into the **Iplanet's obj.conf** file the following line and then restart IPlanet:

    ```
    NameTrans fn="assign-name" from="/dashboard/*" name="J2FRedirect"
    ```

  Restart Business Availability Center.

Mercury Business Availability Center 6.7 Uninstallation

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

Mercury Business Availability Center 6.7 Content

- Bugs fixes – see table below for details:

Description of Bug Fixes	Area	SR/E-Sar Number
Sort by default the KPI Over Time "View as Graph" view according to CI and KPI names	BAC_Applications	1-582122246
Fixed: Apache Tomcat Error when trying to remove alert recipient	BAC_Applications	31947
Fixed: Adapters are duplicated when the adapters home directory is not accessible	BAC_Applications	33228
Hide BPM script download links if the user is a viewer	BAC_BPM_CM	1-27GKSD
Fixed: Citrix transaction times are reported incorrectly	BAC_BPM_CM	1-626287150
Fixed: Some Siebel transactions finish with 'stopped' status while they should finish with 'succeeded' status	BAC_BPM_CM	1B-1QYKHQ
Enable drilldown in KPI Over Time Report	BAC_Dashboard	
Fixed: Changing SiteScope monitor name in Monitor Administration not reflected in model	BAC_Dashboard	1-586684873
Fixed: In KPI Over Time report, Apache error when generating report on monitor CIs after drilldown	BAC_Dashboard	1-601581986
Fixed: Adapters are duplicated when Settings Manager is not available	BAC_Dashboard	32516
Fixed: When changing a transaction schedule in Monitor Administration, the rule parameter "no data timeout" is not updated in BLE model	BAC_Dashboard	32826
Fixed: Doubling of RUM summary data in reports	BAC_DataRetrieval	1-601330883
Fixed: Shifting of summary data to the following day in RUM reports	BAC_DataRetrieval	1-643474323
Fixed: Application freezes when large amounts of BPM and/or SiteScope reports are generated simultaneously	BAC_DataRetrieval	32394
Fixed: Triage report Apache error when generating the report for deleted locations	BAC_EUM	1-586306751
Enable viewing Triage report portlets even if the previous selected location was deleted	BAC_EUM	32348
Enable viewing Triage report portlets even if the user has no permissions to see the previous selected profile	BAC_EUM	33252
Setting "Max trend report measurements" in Infrastructure Settings Manager affects Trend Report Manager	BAC_Platform	32077
Fixed: Report for last 24 hours that comes from the scheduler contains only 12 hours of data	BAC_PlatformAdmin	1-582730128

Fixed: Trend Reports with SiteScope measurements for past day timeframe go to the aggregated tables instead of raw data tables resulting in missing data	BAC_SiteScope	1-582730128
Enable exporting CSV report for SiteScope cross-performance report	BAC_SiteScope	1-587984565
Fixed: Ignore time out samples in BPM outage is not working	BAC_SLM	1-26P7U1
Fixed: Siebel SARM - mouseover data is incorrect	BAC_Verticals	1-624846231

- Internal bugs fixes
- **6.6 Content:** See readme66.doc for details.
- **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 6.7:

- **Client Monitor 6.5.4** (Build 189)
    - Bug fixes

- **Business Process Monitor 6.6.1** (Build 883)
    - Bug fixes

- **SiteScope 8.8**
    - Bug fixes

Limitations and Issues

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 6.7, 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.

Business Availability Center for Siebel and Business Availability Center for SAP Solutions

- Business Availability Center for Siebel and Business Availability Center for SAP solutions require SiteScope 8.8 or higher.
- To use SiteScope 8.7 or lower, contact Mercury Customer Support for a SiteScope patch.

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, 6.7**	**BAC 6.0-6.5**	**BAC 5.1 SP1, 5.0 FP1**	**BAC 5.0**	**Topaz Managed Services 4.5 FP2**	**Topaz 4.5 FP2**
SiteScope 8.8	√	√	√	√	X	X
SiteScope 8.7	√	√	√	√	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	√	√	√ (1)	√	√	√
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	√	√	√	√

Comments:
(1) Mercury Business Availability Center 5.1 SP1 needs a patch to work with SiteScope 8. To obtain this patch, contact Customer Support.

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	**Business Availability Center Version**			
	6.x	**5.1**	**5.0**	**Topaz 4.5SP1–4.5SP3**
SiteScope 8.8 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	1	1	1,2	1

7.9.1.0				
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, and 6.7.

Business Process Monitor Changes

Business Process Monitor Version	**Changes**
6.6, 6.6.1	Bug fixes. Support QTP 9.1, 9.2 (in addition to QTP 9.0)
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

- Starting from BPM 6.6, the following versions of QTP are supported: 9.0, 9.1, 9.2
- Supported protocols:

Web
QuickTest Professional Oracle Add-in (Web-based & Java-based Oracle applications)
QuickTest Professional Add-in for SAP Solutions (Windows-based & Web-based SAP solutions)
QuickTest Professional Siebel Add-in
QuickTest Professional Web Services Add-in
QuickTest Professional PeopleSoft Add-in
QuickTest Professional Java Add-in
QuickTest Professional .NET Add-in
QuickTest Professional Terminal Emulator Add-in
QuickTest Professional Stingray Add-in
QuickTest Professional VisualAge Smalltalk Add-in

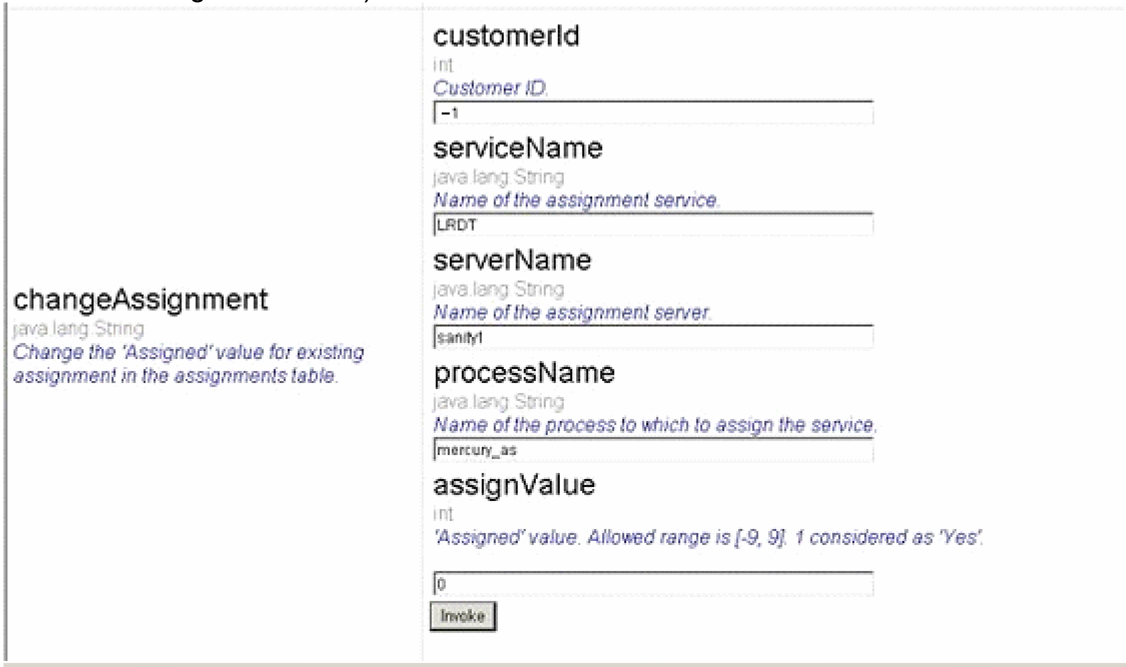
Other Notes

- 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 6.7 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.
- **Important:** When navigating to Mercury Business Availability Center 6.7 pages for the first time after installation, the pages may take some time to load due to .jsp compilation.

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



changeAssignment
java.lang.String
Change the 'Assigned' value for existing assignment in the assignments table.

customerId
int
Customer ID.
-1

serviceName
java.lang.String
Name of the assignment service.
LRDT

serverName
java.lang.String
Name of the assignment server.
sanity1

processName
java.lang.String
Name of the process to which to assign the service.
mercury_as

assignValue
int
'Assigned' value. Allowed range is [-9, 9]. 1 considered as 'Yes'.
0

3. Configure Mercury Business Availability Center to work with the new LRDT monitor:

    a. 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')

    b. 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:

    a. 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>)

    b. 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 6.7 already contains the correct JODA files.
- Updating of the JRE of Business Availability Center 6.7 servers is done automatically after the installation.

Updating Business Availability Center Servers and Databases

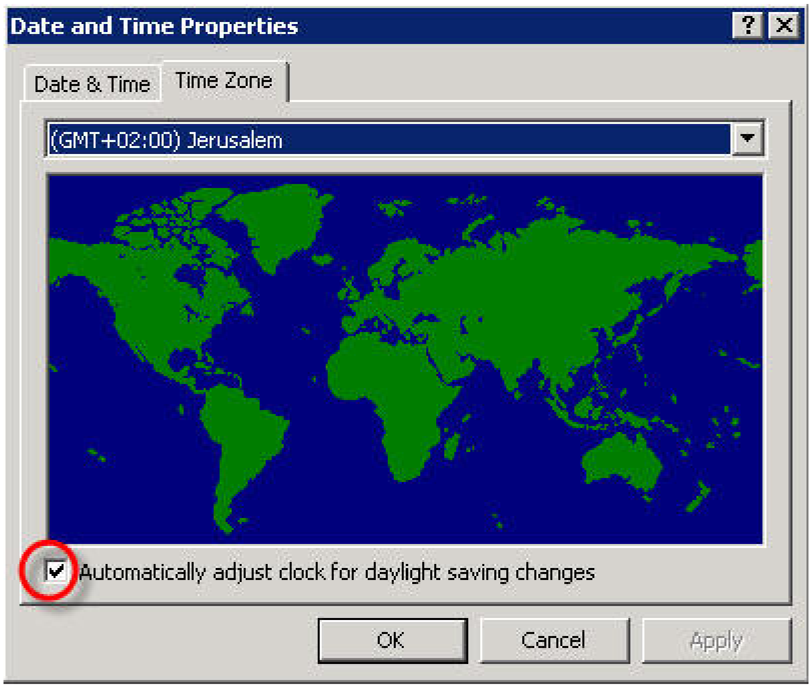
- Update the operating system on all server machines on which Business Availability Center is installed. (See instructions below.)
- Update the operating system on all Business Availability Center database machines. (See instructions below.)

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 6.7 (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**:



(GMT+02:00) Jerusalem

☑ 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 8.8. 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 will return 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

- Navigate to the SiteScope installation directory and copy **tzupdater.jar** to **<SiteScope Home>\java\bin\**.

11. Open a Command Prompt window (DOS shell).
12. Change directory to **<SiteScope Home>\java\bin\**.
13. Run the following command to check whether the update is required: **java –jar tzupdater.jar –t**
14. If an update is required, the command will return a long list of messages. If nothing is returned, no further action is necessary.
15. Stop the SiteScope service.
16. Close all SiteScope GUI windows.
17. Run the following command to install the patch: **java –jar tzupdater.jar –u -bc**
18. 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.
19. Restart the SiteScope service.

Updating Discovery Probe

- Navigate to the Discovery Probe installation directory and copy **tzupdater.jar** to **<Discovery Probe Home>\jre\bin\**.

20. Open a Command Prompt window (DOS shell).
21. Change directory to **<Discovery Probe Home>\jre\bin\**.
22. Run the following command to check whether the update is required: **java –jar tzupdater.jar –t**
23. If an update is required, the command will return a long list of messages. If nothing is returned, no further action is necessary.
24. Stop the Discovery Probe.
25. Run the following command to install the patch: **java –jar tzupdater.jar –u -bc**
26. 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.
27. Restart the Discovery Probe.

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