HP Business Service Management

for the Windows and Linux operating systems

Software Version: 8.07

Pre-Upgrade Tool Guide

Document Release Date: July 2011
Software Release Date: July 2011

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

AMD and the AMD Arrow symbol are trademarks of Advanced Micro Devices, Inc.

Google™ and Google Maps™ are trademarks of Google Inc.

Intel®, Itanium®, Pentium®, and Intel® Xeon® are trademarks of Intel Corporation in the U.S. and other countries.

iPod is a trademark of Apple Computer, Inc.

Java is a registered trademark of Oracle and/or its affiliates.

Microsoft®, Windows®, Windows NT®, Windows® XP, and Windows Vista® are U.S. registered trademarks of Microsoft Corporation.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Acknowledgements

This product includes software developed by the Apache Software Foundation (**http://www.apache.org**).

This product includes software developed by the JDOM Project (**http://www.jdom.org**).

This product includes software developed by the MX4J project (**http://mx4j.sourceforge.net**).

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support web site at:

http://www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

1

Pre-Upgrade Tool

This guide contains information about using the pre-upgrade tool and understanding the customized pre-upgrade tool reports.

This chapter includes:

Pre-Upgrade Tool Overview

The pre-upgrade tool is designed to help you plan your upgrade to BSM 9.10. It scans your BAC 8.07 system for settings and configurations which may need your attention during the upgrade and generates a custom report. The tool detects most of the common issues that will need your attention during the upgrade. The complete list of issues can be found in "Pre-Upgrade Tool Messages" on page 13.

The tool can be run using the JMX console or using the command line interface (details below). The reports are in html format. You can export the reports to Microsoft Excel by opening them in a web browser and right-clicking the table.

The pre-upgrade tool reports are created on the machine that runs the pre-upgrade tool. A blank table means that the pre-upgrade tool was run successfully, but no problematic items were detected.

Note: Only one instance of the pre-upgrade tool should be run at one time.

Running the Pre-Upgrade Tool - Command Line Interface

The primary way to use the pre-upgrade tool is through the command line interface. The client is run on any BAC 8.07 server via the following script:

Windows:

```
C:/<HPBAC>/tools/preupgrade/preupgrade.bat
```

Solaris:

```
/opt/<HPBAC>/tools/preupgrade/preupgrade.sh
```

Note: For Solaris environments, the pre-upgrade directory must be owned by the owner of the <HPBAC> direcory. The pre-upgrade tool must be run by this user as well.

Use the arguments below to run the tool. We recommend including the -dep argument when running the script and executing the -undep command once after you have completed running the pre-upgrade tool.

Argument	Description
-show	Show the list of all applications along with their statuses.
-all	Runs all installed applications (on distributed systems this runs applications on the Gateway and Data Processing servers).
-a <application names>	Runs the analysis only on specified applications. The application names should be separated with commas, with no spaces between the names. The check for application name is Case sensitive.
-dep	This argument is appended to the -a or -all commands. It deploys the Pre-Upgrade CMDB views. On distributed deployments this deployment runs on the data processing server. All the pre-upgrade views will be deployed even if the analysis run on specified applications. This argument (if it's present at all) should be the last one.
-undep [data processing machine name]	Undeploys the Pre Upgrade CMDB views. On distributed deployments the views undeployment will run on data processing server. All relevant views will be undeployed.

Argument	Description
-gw <gateway machine name>	Relevant only on distributed deployments, in which case it is required. Specifies the machine name on which one of the BAC's Gateway servers is installed. If you have more than one Gateway server, only one server should be specified. This argument is appended to the -a or -all commands and should come first. Use only the following characters for the machine name: a-z, A-Z, 0-9, . , - , _.
-dps <data processing machine name>	Relevant only on distributed deployments, in which case it is required. Specifies the machine name on which one of the BAC's Data Processing servers is installed. If you have more than one Data Processing server, only one server should be specified. This argument is appended to the -a or -all commands and should come right after the -gw argument. Use only the following characters for the machine name: a-z, A-Z, 0-9, . , - , _.

Examples:

```
C:\<HPBAC>\tools\preupgrade>preupgrade -gw <GW server name> -dps <DPS server name> -show
```

Show the statuses of all applications available on the specified Gateway and Data Processing server.

```
C:\<HPBAC>\tools\preupgrade>preupgrade -gw <GW server name> -dps <DPS server name> -all
```

Runs the pre-upgrade tool on all available applications on the specified Gateway and Data Processing servers.

```
C:\<HPBAC>\tools\preupgrade>preupgrade -gw <GW server name> -dps <DPS server name> -a Application1,Application2
```

Runs the pre-upgrade tool on applications Application1 and Application2 on the specified Gateway and Data processing servers (each application will be run on its home machine.)

```
C:\<HPBAC>\tools\preupgrade>preupgrade -gw <GW server name> -dps <DPS server name> -all -dep
```

Runs the pre-upgrade tool on all available applications on the specified Gateway and Data Processing servers as well as deploy Pre Upgrade CMDB views.

```
C:\<HPBAC>\tools\preupgrade>preupgrade -undep <server name>
```

Undeploys the pre-upgrade CMDB views on the specified server.

Running the Pre-Upgrade Tool - JMX Console

The pre-upgrade tool can be run through the JMX console. To obtain complete results when running the pre-upgrade tool in a distributed BAC environment using the JMX console, it must be run once on each server type (Gateway and Data Processing Server).

1. Run the following command to open the JMX console: **http://<machine_name>:8080/jmx-console.**
2. In the Topaz section, select **Service=Pre Upgrade JMX Client**.
3. In the **DeployCMDBPackage** section, select **Invoke**.
4. In the **ShowApplicationStatuses** section, select **Invoke**.

5 Check the boxes corresponding to the applications you want to analyze, and select **Analyze**. This runs the pre-upgrade tool on the specified applications. They may take some time to complete. Refresh the browser or use the **showApplicationStatuses** command to view the progress.

JMX MBean Operation Result

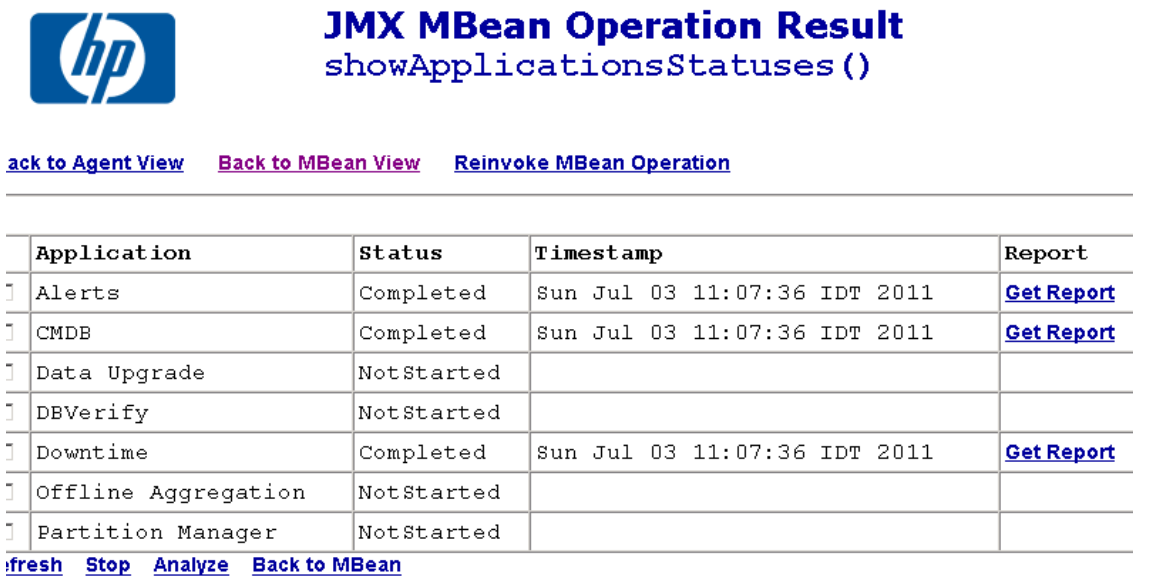
showApplicationsStatuses()

Back to Agent View Back to MBean View Reinvoke MBean Operation

	Application	Status	Timestamp
☐	Alerts	NotStarted	
☐	CMDB	NotStarted	
☐	Data Upgrade	NotStarted	
☐	DBVerify	NotStarted	
☐	Downtime	NotStarted	
☐	Offline Aggregation	NotStarted	
☐	Partition Manager	NotStarted	

Refresh Stop Analyze Back to MBean

6 When the pre-upgrade tool has finished running, select the **Get Report** links to view the output.



JMX MBean Operation Result
showApplicationsStatuses()

ack to Agent View Back to MBean View Reinvoke MBean Operation

	Application	Status	Timestamp	Report
	Alerts	Completed	Sun Jul 03 11:07:36 IDT 2011	Get Report
	CMDB	Completed	Sun Jul 03 11:07:36 IDT 2011	Get Report
	Data Upgrade	NotStarted		
	DBVerify	NotStarted		
	Downtime	Completed	Sun Jul 03 11:07:36 IDT 2011	Get Report
	Offline Aggregation	NotStarted		
	Partition Manager	NotStarted		

efresh Stop Analyze Back to MBean

Alternatively, you can view the files in **<HPBAC>\tools\preupgrade**

7 When you are finished viewing the reports, in the **UndeployCMDBPackage** section, select **Invoke**.

Pre-Upgrade Tool Messages

The following table lists the messages you may receive after running the pre-upgrade tool.

Message ID	Description
100	
100	Schema and data upgrade will take a long time.
101	Schema and data upgrade will take a long time.

Message ID	Description
102	This environment will not be supported in BSM 9.x. In BSM 9.0 and higher, the only method used by the Partition and Purging Manager to partition historical data (of the profile databases) is the Native Partitioning method. In an Oracle database, the **Oracle Partitioning** option must be enabled. If the Oracle Partitioning option is not available, the Partition and Purging Manager will not partition or purge data, which may result in major performance issues. In an SQL database, make sure the **Compatibility Level** database setting is set to reflect the version of SQL server that you are using in each of the BSM 9.10 database schemas. For example if you are using SQL SERVER 2005, the compatibility level should be 90. This will ensure the activation of the native partitioning option.
103	Schema and data upgrade will take a long time.
104	Schema and data upgrade will take a long time. Modify the purging policy for the tables.
105	Schema and data uprade will fail.
106	Schema and data upgrade will fail.
107	Profile Database not ready for data upgrade.
108	Load database contexts.
109	Session table inconsistency.
110	Delete Optional Views.
111	Read only error.
112	Case sensitivity detected.
113	Missing database statistics.
114	Schema validation error.

Message ID	Description
160	Action parameter <<**SubAlerts**>> will be automatically renamed to <<**Alert XML**>>. The structure of the XML file was changed. For details, see "BPM Alerts" on page 94.
161	The values of action parameter <<**TriggerTypeMessage**>> were changed. For details, see "BPM Alerts" on page 94.
162	Action parameters with extensions must be manually upgraded. For details, see "Action Parameters Manual Upgrade" on page 98.
163	The SNMP trap structure of the EUM alerts was changed. There is only one trap type: eventAlert. The OIDs 4.9 , 4.10 , 4.11.1.1.2 - 4.11.1.1.8 have changed. For details, see "SNMP Trap Structure Changes" on page 93.
164	RUM alerts are related to applications instead of RUM engines. Alerts might be duplicated to several applications. For details, see "Alerts Pre-Upgrade Documenation References" on page 87.
165	The ability to group performance data by group is no longer supported in BSM 9.x.
166	Filter by group is no longer supported in BSM.
167	Command line quote substitution will be restored to the default value. For details, see "Infrastructure Settings" on page 88.
170	Detected CI alerts Service Manager Integration is configured. This integration requires manual changes after the upgrade.
180	Updated to downtime timezone model.
190	Abnormal tasks have been detected in your system.
200-206	See "Dashboard and SLM Pre-Upgrade Details" on page 21
220	The following KPIs no longer exist in 9.x: User [0], Customer [2], HP System [12], Component Availability [53], Bandwidth [54], AppAggr (internal) [1000], Latency [1077], Operations Performance KPI [10002], Operations Availability KPI [10003].

Message ID	Description
221	There are Business Rules that no longer exist in 9.x; KPIs with these rules are deleted.
222	OMi KPIs Unresolved Events and Unassigned Events are deleted if they have leaf rules.
223	KPIs with group rules on CIs monitored by SiteScope are deleted.
224	KPIs on CIs monitored by a SiteScope monitor or measurement, which monitors one or more other CIs as well, might be deleted.
225	KPIs on obsolete CI types are deleted.
226	KPIs on BPM Transaction from Location CIs are deleted when the BPM adapter is in Transaction/Location mode.
227	KPI instances that do not have a KPI type in the 8.x KPI repository are not upgraded.
228	KPIs with rules that do not have a rule definition in the business rules repository are not upgraded.
229	SiteScope Availability KPIs are replaced with SiteScope Health KPIs.
230	Duration KPIs with TransactionVision Duration Rule (Completed Transactions) are replaced with Application Performance KPIs.
231-260	See "Dashboard and SLM Pre-Upgrade Details" on page 21
301	Profile configuration will not be fully upgraded.
302	Group value will not be upgraded as BPM agent property.
303	Script version will not be upgraded in CRS. Only the most updated script version was recovered from the EUM repository.
304	Script was not found in the CRS, but the most updated version will be recovered from the EUM repository.
305	Process Group name will be upgraded to its corresponding profile name.

Message ID	Description
306	Business Process Group description will be replaced by the profile description.
307	Business Process Step name will be upgraded to its corresponding transaction name.
308	Business Process Step description will be replaced by the profile transaction description configured in the EUM Admin.
309	Profile and all its related data will not be upgraded.
310	RUM application and all its related data will not be upgraded.
311	RUM end user group and all its related data will not be upgraded.
312	RUM event and all its related data will not be upgraded.
313	RUM page and all its related data will not be upgraded.
314	RUM transaction and all its related data will not be upgraded.
315	RUM transaction and all its related data will not be upgraded.
316	RUM end user group will not be upgraded.
317	RUM end user group will be merged with another group on a different engine.
318	RUM application does not have a unique name in the system and will be renamed during the upgrade.
319	RUM page folder has a description text which will not be upgraded.
320	Script will not be upgraded.
321	Link to EUM CI will not be upgraded.
322	Location does not exist in the upgraded system.
323	CI status alert will not be upgraded.

Message ID	Description
324	CI status alert will not be upgraded.
325	View will not display a breakdown by location topology of EUM CIs after the upgrade.
326	View will not display correct results after the upgrade.
327	View will not display correct results after the upgrade.
328	View may display incorrect results after the upgrade.
329	View may display incorrect results after the upgrade.
330	View will not display correct results after the upgrade.
331	View will not display a breakdown by location topology of EUM CIs after the upgrade.
332	BaseLine configuration for EUM profile will not be upgraded. Static transaction thresholds will be used for the upgrade.
333	Custom changes made to the adapter template will not be upgraded. Note that user defined CI types are not upgraded, and some of the changes to KPIs and selectors may not be upgraded if they do not comply with the new model or status calculation logic.
334	The .usr file name in the zip file does not match the zip file name.
335	The .usr file for the script is missing from the zip file.
336	The script is a Client-Monitor type script, which is not supported in BSM 9.x.
339	Some RUM page samples will not be upgraded as they refer to non-existent pages.
341	Some RUM transaction samples will not be upgraded as it refers to non-existing transactions.
343	Some RUM event samples will not be upgraded as they refer to non-existent RUM events.

Message ID	Description
345	Some RUM event samples will not be upgraded as they refer to non-existent RUM pages.
400	Configuration of SiteScope monitors/measurements connected to more than one CI is not supported. For details, see "SiteScope Monitors Connected to Multiple CIs" on page 45.
401	DNode CIs were deleted.
402	KPIs manually defined on SiteScope monitors and measurements do not influence CIs in the impact chain from the monitor/measurement. Reconfigure your logical changes for BSM 9.x. For details, see "SiteScope Dynamic HI Assignment" on page 47.
403	Configuration of SiteScope monitors/measurements connected to a non-default CI type is not supported. For details, see "SiteScope Monitors Associated with Non-default CIs or Multiple CIs" on page 49 and "Monitors Not Reporting Topology Data By Default" on page 52.
404	Alerts defined on specific manual KPIs on CIs monitored by SiteScope monitors/measurements might not be triggered. The KPI types on which alerts might not be triggered are: System/SAP/Siebel/Siebel Sessions/ Siebel Tasks in Error.Reconfigure your logical changes for BSM 9.x. For details, see "SiteScope Dynamic HI Assignment" on page 47.
405	Topology changes where SiteScope monitor/measurement connected to SiteScope Group/Measurement Group CI by "Monitored By" link is not supported.
406	SiteScopes versions earlier than 10.10 are not supported when integrated with BSM 9.1.

Message ID	Description
407	Alerts defined on KPIs that propagated from SiteScope monitors or measurements are not configured on KPIs, or the alert's behavior might change if the KPI is of a type other than System, SAP, Siebel, Siebel Sessions, and Siebel Tasks In Error. The alert is either configured on all KPIs, or on selected KPIs before the propagation. For more information, see"SiteScope KPI Assignments Associated With Custom KPIs" on page 48.
408	Downtime behavior changed in SiteScope 11.x versions connected to BSM 9.x from "Stop reporting" to one of two options: "Stop monitoring" or "Stop sending alerts". For details, see "CI Downtime" on page 54 and "Downtime Management — Overview" on page 56.
409	In custom views, the monitored CIs are not influenced by the KPIs of SiteScope monitors/measurements that are connected to them.
410	Inconsistencies were found between the RTSM and DB which might cause the upgrade to run with warnings.
412	The KPIs created by custom assignments on SiteScope monitors or measurements do not influence CIs in the impact chain from the monitor or measurement. The change also affects alerts configured on these KPIs. For more information, see "SiteScope KPI Assignments Associated With Custom KPIs" on page 48.
500	User classes will be renamed.
501	The upgrade process will fail because of unsupported enum-to-list conversion.
502	The upgrade process will fail because of unsupported list-to-enum conversion.

2

Dashboard and SLM Pre-Upgrade Details

This chapter provides information about upgrading Dashboard and Service Level Management. It includes information about the pre-upgrade tool messages 200-260 as well as background information.

This chapter includes:

Pre-Upgrade Tool Messages

The following table contains informaiton about the pre-upgrade tool messages 200-260.

Message ID	Description
200-206	For general information on messages 200-206 see: ➤ "Monitor CI Removal" on page 32 ➤ "Health Indicators and KPIs" on page 32 ➤ "Monitors CITs Which Are Not Removed" on page 33 ➤ "View Upgrade and Monitor Removal" on page 39
200	Custom template-based views are not upgraded. After upgrade, fix template views according to the new 9.x concepts. Remove monitor CIs from your view definitions, and add the **monitored_by** attribute to their parent CIs (for example, monitored by RUM or BPM). For more details refer to "View Upgrade and Monitor Removal" on page 39.
201	In general, the upgrade process removes monitor nodes from view definitions as described in "View Upgrade and Monitor Removal" on page 39. If a monitor node includes a property condition, the node is removed together with its property condition; the property condition is lost because the upgrader does not know how you want the condition converted, and leaves the conversion to the user. Note that this applies only to **removable** monitors (see "Monitors CITs Which Are Not Removed" on page 33). Before upgrading, edit TQL definitions so that monitor nodes do not contain property conditions. To preserve the requested TQL results, find a parallel condition on another node or link in the TQL.
202	A **removable** monitor CI (see "Monitors CITs Which Are Not Removed" on page 33) is only upgraded if it has a single parent CI, with an incoming monitored_by or impact_link relationship. If there is more than one parent CI (or none), or a different link, the monitor CI is not upgraded because its content cannot be placed on a single specific parent CI. Before upgrading, edit TQL definitions so that each monitor node has exactly one parent node, related with an incoming monitored_by or impact_link relationship.
203	For details, see "Message 203" on page 27.

Message ID	Description
204	For details, see "Message 204" on page 29.
205	For details refer to the explanation and examples for 203; where 203 discusses subgraphs, 205 describes compound links.
206	When a monitor node has an incoming compound link, the monitor cannot be upgraded. Due to the complexity of compound links, the upgrader does not handle these nodes; you must decide how you want to handle the compound link related to removable or SiteScope monitors. The upgrader does not handle the following (for details refer to the examples for 204): ➤ The monitor node is a subtype of a removable monitor CIT. ➤ The monitor node is a subtype of an impact detached monitor (for example SiteScope Monitor), and the compound link contains a triplet with an impact link to one of the SiteScope impact detached monitor CITs (for example SiteScope Monitor linked with an impact link to a CIT other than SiteScope Group). An incoming compound link related to a SiteScope monitor with invalid triplets will result in unexpected view results, due to the new impact removal model. In these cases, edit the compound link before upgrading as follows: ➤ In the case of removable monitors, turn the leaf triplet into a pattern node by extracting it from the compound link definition, and relating it to the removable monitor node. ➤ In the case of SiteScope monitors, align the impact links to the BSM 9.x model.
231	PNR KPI instances configured on removable monitors CIs are not upgraded. For details, see "Monitors CITs Which Are Not Removed" on page 33 and "KPI Upgrade" on page 33. The pre-upgrade tool creates a view where these removable monitors CIs are listed. Access **Admin** > **Dashboard** > **KPIs**, select **bsmAppsPnrKpiOnMonitors_pupg** in the view explorer, and check where you have monitor CIs with PNR KPI instance customizations.

Message ID	Description
240	In SLM 8.0, you use BPM events when adding an event affecting Business Process Monitor data in agreements, and SLA events when adding an event that affects specific agreements. In BSM 9.x there is no longer a BPM downtime event mechanism, and these downtimes have no effect on calculations. Before upgrading, create SLA downtime events to replace the BPM downtime events. The replacement needs to consider the following: ➤ If a BPM event is configured for a specific SLA with specific CIs, create a matching SLA event for the SLA and selected CIs. ➤ If a BPM downtime event is configured for All SLAs with selected CIs, create an SLA event for each SLA which contains these CIs. ➤ In breakdown mode, BPM downtime event is configured with selected location CIs; create a matching SLA downtime event for each SLA which is configured with CIs affected by this location.
250-256	For general information about messages 25--256 see: ➤ "KPI Upgrade" on page 33 ➤ "SiteScope and EMS KPI Assignment Upgrade" on page 37
250-251	The following KPI assignments are **not** upgraded, and are overwritten by pre-defined 9.x HI and KPI assignments, due to changes in the assignment logic: ➤ SLM assignments. ➤ Default (out-of-the-box) Dashboard assignments that have not been modified. ➤ Customized Dashboard assignments other than SiteScope and EMS. In this case, reproduce customizations in 9.x according to the new (9.x) concepts.

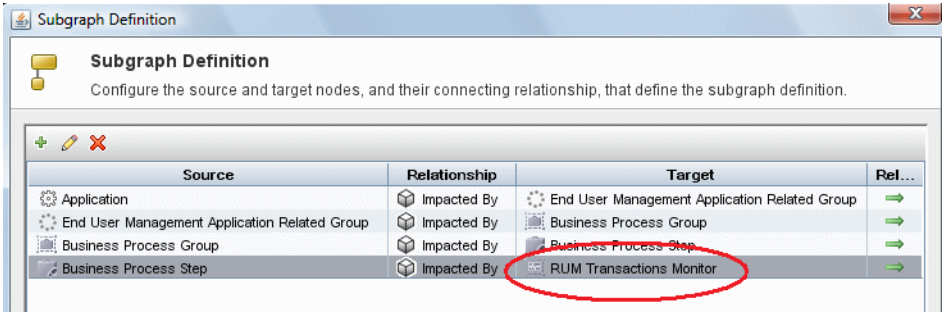
Message ID	Description
252	Out-of-the-box KPI assignments that belong to supported domains (SiteScope or EMS) that are stopped in 8.x, will not affect the 9.x related out-of-the-box HI assignment. If you created or edited SiteScope or EMS KPI assignments in Dashboard administration, they are upgraded within Service Health 9.x. Regarding these "upgradable" assignments, note that only significantly customized assignments are upgraded. These include assignments where KPIs were added, removed, or edited, or where context menus were edited. If an out-of-the-box assignment is stopped prior to upgrade, this is not considered a customization. The post-upgrade HI assignment will therefore be running. In this case, after upgrade stop the matching HI assignment. If a significantly customized assignment (as listed above) is stopped before upgrade, the post-upgrade will be stopped.
253	Due to the reorganization of content that was done in BSM 9.x, a number of domain-specific KPIs are removed, and are replaced with more general KPIs. Following upgrade, assignments with these KPIs are invalid. The following KPIs are removed: User (0), Customer (2), HP System (12), Component Availability (53), Bandwidth (54), AppAgr (1000), Latency (1077), Operations Performance KPI (10002), Operations Availability KPI (10003). For details, see "KPI Upgrade" on page 33. Before upgrading, review the KPIs on the affected assignments. If you want to keep a KPI after upgrade, change the assignment to use a different KPI; note that this can be a clone of the original KPI.
255	In BSM 9.x, a list of applicable CI types was added to each of the calculation rules. As a result, an assignment that was valid in 8.x may become invalid in 9.x, if it uses a rule and CI type that do not match. After upgrade, edit the rule in the rule repository to be applicable to the CI type, or change the assignment to use a different (applicable) rule.

Message ID	Description
256	Within the objective area of a KPI assignment in 8.x, you can use the default setting for some parts of the objective (thresholds or operator) and custom values for other parts, within a single KPI. In BSM 9.x assignments, the thresholds and operator for an HI must be defined either as all default, or all custom. If your 8.x assignment has some KPI thresholds or operator as default and some as custom for a specific KPI, the post-upgrade 9.x HI assignment is invalid. Before upgrade, edit the assignment and modify the objective as needed.
257	If you have customized an assignment on the SiteScope Web Service Monitor CIT, this assignment is upgraded to the Web Service Operation CIT. As a result, the upgraded HI assignment on 9.x might become invalid (for example, due to an invalid RefProp). After upgrade, fix the assignments as needed.
258	For details refer to the explanation for 252; where 252 discusses stopped out-of-the-box KPI assignments belonging to supported domains, 258 discusses stopped out-of-the-box KPI assignments belonging to unsupported domains (not SiteScope or EMS).
260	This analyzer lists all customized (new or edited) propagation rules, even if the customization is minor (for example if you edited the rule name). After upgrade, customized propagation rules are not removed; you should take the following into consideration: **1** A propagation rule which contains any of the following is not valid: ➤ A CI type that does not exist. ➤ A calculation rule that no longer exists or is not applicable for the CIT. ➤ A KPI that no longer exists. **2** Both the customized 8.x propagation rules and the 9.x out-of-the-box rules will be running following upgrade; you should decide if you want to keep both the customized and the matching 9.x rules, or to merge them.

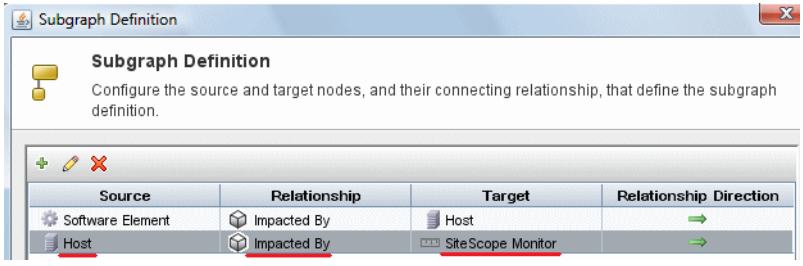
Message 203

Subgraph nodes and compound links are entities composed of triplets. Due to the complexity of subgraph or compound link structures, the upgrader does not handle these nodes; you must decide how you want to handle the subgraph related to removable monitors. The upgrader does not handle the following:

- A triplet whose source or target is a subtype of a removable monitor CIT (for example BPM or RUM monitor). For example, suppose you have an Application node with subgraph definition:

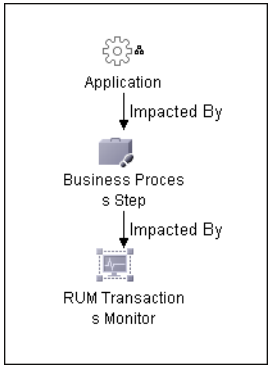


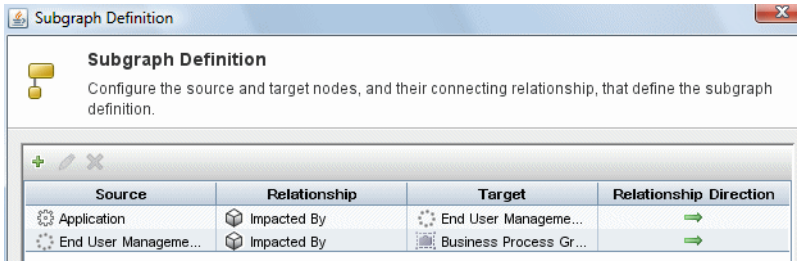
- A triplet with an impact link to one of the SiteScope impact detached monitor CITs (for example SiteScope Monitor linked with an impact link to a CIT other than SiteScope Group). For example, suppose you have an Software Element node with subgraph definition:



In these cases, edit the triplet before upgrading as follows:

➤ In the case of removable monitors, remove the triplet from the subgraph, and move the monitor node outside the subgraph:



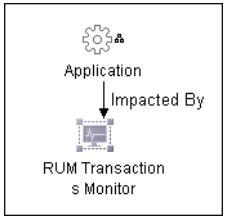


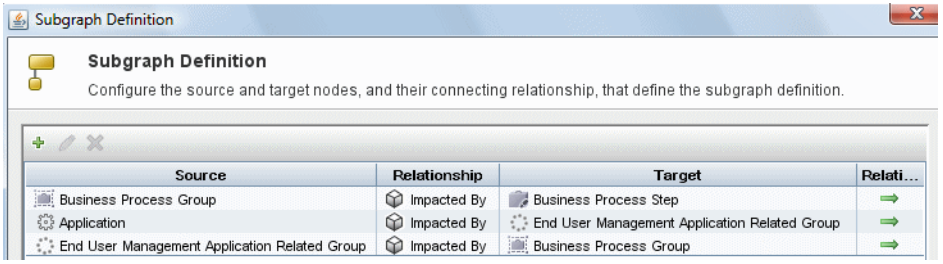
➤ In the case of SiteScope monitors, align the impact links to the BSM 9.x model.

Message 204

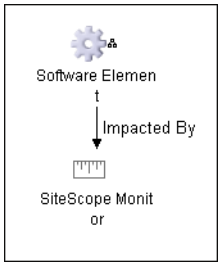
When a monitor node has a parent CI which is a subgraph, the upgrader does not handle these nodes. Due to the complexity of subgraph or compound structures, the upgrader cannot predict the implications of removing the monitor node; you must decide how you want to handle the subgraph related to removable or SiteScope monitors. The monitor cannot be upgraded in either of the following cases:

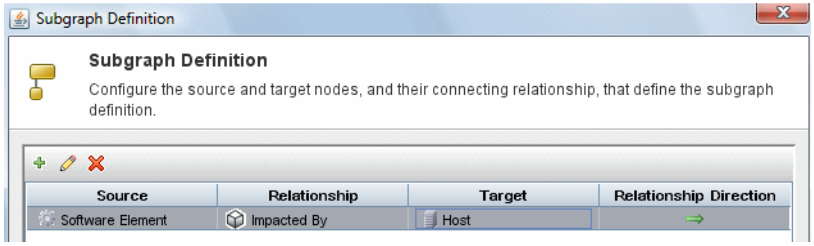
- The monitor node is a subtype of a removable monitor CIT (for example BPM or RUM monitor). For example, suppose you have a monitor node with an Application parent CI which is a subgraph node:





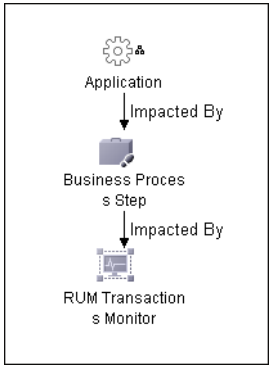
➤ The monitor node is a subtype of an impact detached monitor (for example SiteScope Monitor), and there is an incoming impact link from the subgraph node to the monitor CIT. Subgraphs related to SiteScope monitors with an impact link may result in unwanted view results, according to the new impact removal model. For example, suppose you have a SiteScope Monitor, and there is an incoming impact link from the subgraph node (Software Element) to the monitor:

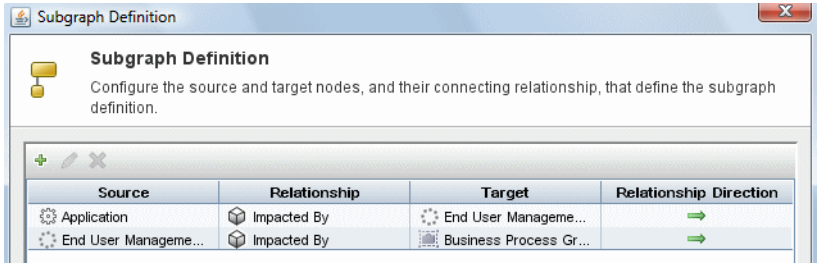




In these cases, edit the subgraph triplet before upgrading as follows:

➤ In the case of removable monitors, turn the leaf triplet into a pattern node by extracting it from the subgraph definition, and relating it to the removable monitor node.





➤ In the case of SiteScope monitors, align the impact links to the BSM 9.x model. Edit the link type, or turn the leaf triplet into a pattern node by extracting it from the subgraph definition, and relating it to the SiteScope monitor node according to the new model concepts.

Monitor CI Removal

In BAC 8.x, each monitored CI had a child CI which was called a **monitor CI.** KPIs which provided information on the monitored CI were assigned to its child CI - the monitor CI.

For example, if you wanted to monitor CPU load on a computer, the computer CI (representing an actual computer) had a monitor CI as its child, and the System KPI monitoring CPU load was assigned to the monitor CI.

In the BSM 9.x topology, the layer of monitor CIs has been removed, and KPIs are now assigned directly to the monitored CIs.

For example, to monitor CPU load on a computer, the relevant KPI is assigned to the computer CI itself.

Note: SiteScope and EMS monitor CIs were not removed in BSM 9.x.

Health Indicators and KPIs

In BSM 9.x, an additional layer of information was added to the monitored CIs: **health indicators** (HIs).

- HIs provide fine-grained monitoring of CIs, with far more detail than KPIs. Some HIs provides business metrics, while others monitor aspects of performance and availability. For example, a Windows CI type includes the following HIs: CPU load, memory utilization, and disk space, as well as other HIs that reflect the status of other Windows metrics.
- KPIs are now higher level indicators than HIs, and they represent a more general aspect of domain health, such as System Performance, System Availability, Application Performance, Application Availability, and so on.

  KPIs apply calculation rules to the data provided by HIs to determine CI status; A KPI can be calculated using data from HIs, from other KPIs, or a combination of these.

Monitors CITs Which Are Not Removed

The following monitor CITs are not removed during upgrade:

- Dynamic Node Monitor
- EMS Measurement
- EMS Monitor
- EMS Ticket
- SAP Alert Monitor
- SiteScope Profile Monitor

In addition, certain SiteScope monitors and their subtypes (such as SiteScope Web Service Monitor) are not removed during upgrade. However, the impact links in BSM between these monitors and their monitored CIs are detached:

- SiteScope Measurement
- SiteScope Monitor

Note: The impact within the SiteScope model remains unchanged: SiteScope Monitor impacts SiteScope Group, and SiteScope Measurement impacts SiteScope Measurement Group.

KPI Upgrade

If your monitored environment contains default KPIs which have not been modified prior to upgrade, they are replaced by the corresponding KPIs and HIs, as defined by the Service Health 9.x pre-defined assignments.

If you modified any KPIs in your pre-upgrade environment, the upgrade handles these KPIs as described in the following section.

This section includes the following topics:

Monitor CIs removed and health indicators added

The two major changes related to KPIs in Service Health 9.x are **monitor removal**, and the addition of **health indicators**.

- As a result of monitor removal, if a customized KPI was assigned to a monitor CI, the upgrade moves this KPI up one level in the hierarchy to the monitored CI (because the monitor CI is removed).
- In addition, a health indicator is assigned to the monitored CI; the status and value of the KPI are calculated based on this HI.
- If you have customized a KPI on a non-monitor CI, the customization is still in effect following upgrade, within the limitations described below.

Note: SiteScope monitors are not removed; for details see "KPIs and HIs on CIs monitored by SiteScope and EMS" on page 35.

Domain-specific KPIs removed

Due to the reorganization of Service Health content that was done in BSM 9.x, the following KPIs are removed (KPI ID appears in parentheses):

User (0), Customer (2), HP System (12), Component Availability (53), Bandwidth (54), and Latency (1077).

These domain-specific KPIs have been replaced with more general KPIs.

OMi KPIs and rules removed or replaced

The following OMi KPIs and rules are removed or replaced following upgrade (IDs appear in parentheses):

BAC 8.x	BSM 9.x
➤ Operations Performance KPI (10002) ➤ Operations Availability KPI (10003)	These KPIs are removed.
➤ Unresolved Events KPI (10004) ➤ Unassigned Events KPI (10005)	These KPIs are removed if they were assigned to leaf (monitor) CIs in 8.x.
➤ OprSampleRule (10000) ➤ OprSampleRule (unresolved) (10004) ➤ OprSampleRule (unassigned) (10005)	The KPIs which used these calculation rules in 8.x are removed.
➤ Convert OprWorstChildGroupRule (10001) ➤ Convert IncidentLifecycleGroupRule (10002)	These rules are replaced with Worst Child Rule (1).

KPIs and HIs on CIs monitored by SiteScope and EMS

Unlike other CIs monitored by Service Health, SiteScope and EMS monitor CIs are not removed in BSM 9.x. If a customized KPI is assigned to a SiteScope or EMS monitor CI, an HI is added to the monitor CI, and the KPI is calculated based on this HI.

On CIs monitored by SiteScope, the System Availability KPI is replaced with the Legacy System KPI.

Manual KPI upgrade limitations

The upgrade of manual (customized) KPIs has the following limitations:

BAC 8.x	BSM 9.x limitation
EUM adapter configured to monitor transactions by location	Customized KPIs on the transaction by location monitor CI are no longer supported. For example, if you are monitoring a business transaction from New York, this CI is no longer modeled the same way in BSM 9.x. The CIs are assigned KPIs and HIs using the Service Health 9.x assignment and propagation mechanism. For details on how to set up transaction by location monitoring in Service Health 9.x, refer to "Breakdowns" in *Using Service Health*.
Manual KPIs on the following CI types (and their descendant CITs): ➤ RUM Errors ➤ RUM Information Events ➤ RUM Servers ➤ RUM Event Monitor ➤ RUM Server Monitor	In the BSM 9.x topology, a number of CITs were removed. As a result, these KPIs are not upgraded.
If you created a KPI calculation rule using the Rules API (Groovy script)	Verify that the rule is still valid for the post-upgrade KPI and CI. In some cases you may need to modify the script to match your post-upgrade environment.
If you created a KPI calculation rule using the Rules API on a monitor CI	The rule script is transferred to the HI on the monitored CI; verify that the rule is still valid for your post-upgrade CI.
If a KPI on a monitor CI is calculated using a sibling rule (based on the values of sibling KPIs)	Verify that the sibling KPIs exist on the post-upgrade monitored CI.

SiteScope and EMS KPI Assignment Upgrade

If you created or edited SiteScope or EMS KPI assignments in Dashboard administration, they are upgraded within Service Health 9.x.

The following KPI assignments are **not** upgraded, and are overwritten by pre-defined BSM 9.x KPIs due to changes in the KPI assignment logic:

- SLM assignments.
- Default Dashboard assignments that have not been modified.
- Dashboard assignments other than SiteScope and EMS.

Each pre-upgrade KPI assignment is upgraded to two assignments: a KPI assignment, and a health indicator assignment, using the following guidelines.

Note: Context menus are copied directly from the old KPI assignments to the new ones.

This section includes the following topics:

- "On which CI types are assignments upgraded?" on page 37
- "Limitations in the assignment upgrade process" on page 38

On which CI types are assignments upgraded?

Assignments defined on the following CI types (and their descendant CITs) are upgraded:

- EMS Monitor
- SiteScope Measurement
- SiteScope Monitor
- SiteScope Profile Monitor
- SiteScope Web Service Monitor

Limitations in the assignment upgrade process

- **SiteScope Monitored CI.** When a SiteScope KPI assignment is upgraded and it assigns HIs and KPIs to a monitor CI, the KPI does **not** propagate from the monitor CI to the parent (monitored) CI. The KPI **does** propagate to the Sitescope group related to the monitor CI.
- **Stopped Default Assignments.** If you have stopped a default assignment in 8.x, it is not upgraded in 9.x.
- **Identical Conditions.** If a new default assignment has the same condition as an upgraded custom assignment, the new assignment is stopped, and the upgraded assignment is active.
- **Default Objectives.** Within the objective area of a KPI assignment in 8.x, you could use the default setting for some parts of the objective (thresholds or operator) and custom values for other parts, within a single KPI.

  In BSM 9.x assignments, the thresholds and operator for an HI must be defined either as all default, or all custom. If your 8.x assignment had some KPI thresholds or operator as default and some as custom for a specific KPI, the post-upgrade 9.x HI assignment is invalid. You can edit the assignment and modify the HI objective as needed.
- **Applicable CITs for Rules.** In 9.x, a list of applicable CI types was added to each of the calculation rules. As a result, an assignment that was valid in 8.x may become invalid in 9.x, if it uses a rule and CI type that do not match.

  To fix this, open **Admin** > **Service Health** > **Repositories** > **Business Rules** and edit the relevant rule to be applicable to the CI type, or change the assignment to use a different (applicable) rule.
- **SOA Assignments.** If you have customized an assignment on the SiteScope Web Service Monitor CIT, this assignment is upgraded to the Web Service Operation CIT. As a result, the upgraded HI assignment on 9.x might become invalid due to an invalid RefProp, for example.

Propagation Rule Upgrade

The upgrade of propagation rules automatically deals with BDM changes, meaning that CI types which changed from 8.x to 9.x (for example it_world > configuration_item) are updated within the propagation rule definitions.

After upgrade, a propagation rule which contains any of the following is not valid:

- A CI type that does not exist.
- A calculation rule that no longer exists.
- A KPI that no longer exists.

Within the Propagation Rules tab, if a propagation rule is invalid after upgrade because its CIT no longer exists, you can create a new rule or clone the rule to replace the invalid one, and delete the invalid rule.

If a propagation rule is invalid because it contains a calculation rule or KPI that no longer exists, you can edit the invalid propagation rule and fix the problem.

View Upgrade and Monitor Removal

The upgrade removes monitor CIs from your view definitions, and adds the **monitored_by** attribute to their parent CIs (for example, monitored by RUM or BPM).

View upgrade and monitor removal are done using the settings described in the following sections. You can modify these settings using the file **conf\views_upgrade\bsm_views_upgrade_configuration.properties**.

This section includes the following topics:

➤ "Views which are not upgraded" on page 41

➤ "SiteScope monitor CIs in 9.x" on page 43

Links defining monitor CITs for removal

The BSM upgrade process removes monitor CIs that fill the following conditions:

➤ **monitored_by** (and its descendant links)

➤ **impact_link** (and its descendant links)

If a monitor CI is attached using a compound link, it is not removed.

Removed monitor CITs and their corresponding monitored_by attribute

The following is a list of monitor CITs which are removed (if their link is monitor_by or Impacted By), and their corresponding **monitored_by** attribute.

For example, if a **bpi_monitor** CI is removed, its parent CI is assigned a monitored_by attribute of **BPI**.

➤ BPI Monitor > BPI

➤ BPI Business Process Monitor > BPI

➤ BPI Business Process Step Monitor > BPI

➤ BPM Transaction From Location > BPM

➤ BPM Transaction Monitor > BPM

➤ BPM Web Service Monitor > BPM

➤ Diagnostics Probe > Diagnostics

➤ Diagnostics Web Service Monitor > Diagnostics

➤ EUM Monitor > BPM,RUM

➤ OPR Monitor > OM

➤ RUM Sessions Monitor > RUM

➤ RUM Event Monitor > RUM

- RUM Location Monitor > RUM
- RUM Page Monitor > RUM
- RUM Server Monitor > RUM
- RUM Trans Monitor > RUM
- RUM Transactions Monitor > RUM
- SiteScope Measurement > SiteScope
- SiteScope Monitor > SiteScope
- SiteScope Profile Monitor > SiteScope
- SOA Monitor > Diagnostics, BPM
- System Monitor > SiteScope, EMS
- TV Monitor > TV

Monitor CIs which are not removed

If a monitor CI has more than one parent CI, it is not removed.

The following CITs are not removed:

- Dynamic Node Monitor
- EMS Measurement
- EMS Monitor
- SAP Alert Monitor
- SiteScope Measurement
- SiteScope Monitor
- SiteScope Profile Monitor

Views which are not upgraded

Only pattern-based and perspective based views are upgraded; template-based views are not upgraded.

If a view contains a subgraph, the subgraph is not upgraded.

Note: We recommend that you review the view definitions that contain monitor CIs or CI types, and replace them with the relevant parent CI type (for example Oracle, Windows, and so on).

In addition, the following views are not upgraded:

- AD_Logical_View
- AD_Physical_View
- CPU_Infrastructure
- End User MonitorsAdmin
- EndUserLocations
- EndUserMonitors
- Exchange_Mail_View
- Exchange_Org_View
- Exchange_Site_View
- Filesystem_Infrastructure
- HACluster_Infrastructure
- Infrastructure_Common
- J2EE_Deployment
- MSSQL_Deployment
- NetworkInterface_Infrastructure
- ORA_Deployment
- RealUserApplications
- RealUserEndUsers
- RealUserLocations
- RealUserMonitors
- RealUserServers

- Systems_Infrastructure
- Virtualization_Infrastructure
- vMA_Infrastructure

SiteScope monitor CIs in 9.x

- SiteScope monitor CIs have been removed from the **System Hardware Monitoring** and **System Software Monitoring** views. In addition, these views now show CIs monitored by all domains and not only by SiteScope.
- Monitors have also been removed from the **System Monitors Only** perspective. Any custom views which were build using this perspective will no longer include monitors; they will only show CIs monitored by SiteScope.
- Monitors are not removed from custom patterns views (views created by users). Since there is no direct impact between monitors and monitored CIs in BSM 9.x, you can remove the monitors from the views themselves. If you do not use monitor CIs for drill downs, Go to Report, or other options, we recommend removing them from the custom views.

3

SiteScope Pre-Upgrade Documentation References

This chapter includes:

SiteScope Monitors Connected to Multiple CIs

In BSM 9.x, each SiteScope monitor can only be associated with a single CI instance. However, you may have manually associated a monitor with more than one CI before upgrading to BSM 9.x. For example, a CPU monitor may be associated by default with a Computer, and manually with a Running Software.

To see if you have any monitors associated with more than one CI, open **RTSM Administration** > **IT Universe Manager**, and drill down to **Monitors** > **SiteScope** > **SiteScope Monitors Connected to Multiple CIs**. If you have monitors associated with multiple CIs, the **SiteScope Monitors Connected to Multiple CIs** view contains these monitors, and their associated CIs. To enable BSM to receive data from a monitor for a CI, you must associate the monitor with a single CI only. The procedure you must follow depends on which CI you want the monitor to link to, as follows:

To create a relationship from a monitor to its default CI:

1 Within RTSM, delete the relationships between the monitor and the non-default CIs.

2 Within SiteScope, access the monitor's properties page.

- For SiteScope 10.x, within the **HP BAC Integration Settings** panel, verify that **Include topology data when reporting to BAC** is selected.
- For SiteScope 11.x, within the **HP Integration Settings** panel, verify that **Report Monitor and Related CI Topology** is selected, and CI Type is not **None**.

To create a relationship from a monitor to a non-default CI:

1 Within RTSM, delete the relationships between the monitor and all CIs except the preferred non-default CI.

2 Within SiteScope, access the monitor's properties page. In SiteScope 11.x, within the **HP Integration Settings** panel, select the **Report Monitor and Related CI Topology** option. Select the CI type for the monitor, and enter values for the CI type key attributes (they depend on the CI type selected).

This enables you to associate the monitor with a non-default CI, rather than with its default CI.

3 To enable BSM to receive health indicator data from a monitor after associating it with a CI of a non-default CIT, perform the following:

If necessary, create new health indicators for the non-default CIT within the Indicator Repository.

Map the indicators that you want to associate with the monitor, to the monitor metrics. This step depends on your version of SiteScope:

- For SiteScope 10.x, access **Admin** > **System Availability Management**, and select the **Metrics and Indicators** tab. Manually map the metrics from the monitor to the required indicators on the CI, by selecting the appropriate CIT and the indicators that you want to associate with the monitor. For details, refer to the "Metrics and Indicators Tab" section in *Using SiteScope*.
- For SiteScope 11.x, within the monitor's properties page in SiteScope, within the **HP Integration Settings** panel, check the **Report monitor and related CI topology** checkbox. In the **CI Type** dropdown select the relevant CI type, and fill in the details of the CI to which the monitor is linked. In the same panel, under **Indicator Settings**, map metrics of the monitor to the relevant indicators for the CI.

SiteScope Dynamic HI Assignment

Service Level Management contains a default assignment named **SiteScope Dynamic Health Indicator Assignment**, which assigns HIs to the CIs monitored by SiteScope. This assignment dynamically assigns HIs to these CIs based on the metrics you have chosen to monitor within SiteScope. If you change the definitions of what is monitored on a CI within SiteScope, the assignment engine will determine the HIs dynamically in run time.

You **cannot** perform the following:

- Create another dynamic assignment.
- Delete this assignment.
- Add HIs to this dynamic assignment, or remove HIs from the assignment.
- Modify the condition or selector defined for an HI in this assignment.

You **can** make the following changes within the dynamic assignment:

- Change the HI calculation rule. Note that the new rule is used to calculate *all* of the HIs assigned via this assignment.
- Change the rule parameters and rule thresholds (where relevant).
- Stop the assignment if necessary.

SiteScope KPI Assignments Associated With Custom KPIs

If you created a KPI in BAC 8.x or earlier using the **Clone** option in the Dashboard KPI repository (KPI ID 2000 and higher), KPI assignments using this KPI are upgraded. However, since there is no impact from SiteScope monitors to CIs in 9.x, the assignments will not create an impact as they used to. The following section describes two options for handling this within Service Health 9.x.

Note: The following section is also applicable if you used any non-SiteScope KPIs in KPI assignments for SiteScope Monitors.

Use default HIs to calculate the custom KPI

Within the KPI Assignments tab, you can create a KPI assignment which uses default HIs to calculate your custom KPI. The relevant CIs will then have your custom KPI assigned, calculated by the values of default HIs.

Use custom HIs to calculate the custom KPI

1. If you have an assignment with a custom KPI, the upgrade creates an HI in the indicator repository, for the CIT defined in the assignment condition, using the syntax **<CIT>_<KPI Name>_Auto_Generated**.

   You can use this HI to calculate your KPI, or you can create a new HI in the indicator repository.

2. Map the relevant monitor metrics to the custom HI.

   Access **Admin** > **System Availability Management**, and select the **Metrics and Indicators** tab. Manually map the metrics from the monitor to the required indicators on the CI, by selecting the appropriate CIT and the indicators that you want to associate with the monitor. For details, refer to the "Metrics and Indicators Tab" section in *Using SiteScope*.

3. If you created a new HI, create a KPI assignment in the KPI Assignments tab which uses this new HI to calculate your custom KPI. The relevant CIs will then have your custom KPI assigned, calculated by the values of your custom HIs.

SiteScope Monitors Associated with Non-default CIs or Multiple CIs

If you have manually associated SiteScope monitors to CIs of non-default CIT, or multiple CIs in earlier versions of BAC, the upgrade to BSM 9.x may result in two types of configuration issues. This can occur if you created relationships from CIs to monitors either using the Link Monitor to CI option in SiteScope, using UCMDB Administration in BAC, or using the Monitor Deployment Wizard (MDW).

Since SiteScope is not aware of these relationships, the CIs will not have the correct health indicators defined. In addition, a monitor may be connected to more than one CI following manual creation of relationships, and this cannot be handled properly by the CI Resolution process. For details on CI Resolution, refer to "Advanced Event Automation" in *Using Operations Management*.

Two new views have been created in RTSM to help you identify and resolve these problems.

SiteScope Monitors Connected to Multiple CIs

In BSM 9.x, each SiteScope monitor can only be associated with a single CI instance. However, you may have manually associated a monitor with more than one CI before upgrading to BSM 9.x. For example, a CPU monitor may be associated by default with a Computer, and manually with a Running Software.

To see if you have any monitors associated with more than one CI, open **RTSM Administration** > **IT Universe Manager**, and drill down to **Monitors** > **SiteScope** > **SiteScope Monitors Connected to Multiple CIs**. If you have monitors associated with multiple CIs, the **SiteScope Monitors Connected to Multiple CIs** view contains these monitors, and their associated CIs. To enable BSM to receive data from a monitor for a CI, you must associate the monitor with a single CI only. The procedure you must follow depends on which CI you want the monitor to link to, as follows:

To create a relationship from a monitor to its default CI:

1 Within RTSM, delete the relationships between the monitor and the non-default CIs.

2 Within SiteScope, access the monitor's properties page.

- For SiteScope 10.x, within the **HP BAC Integration Settings** panel, verify that **Include topology data when reporting to BAC** is selected.
- For SiteScope 11.x, within the **HP Integration Settings** panel, verify that **Report Monitor and Related CI Topology** is selected, and CI Type is not **None**.

To create a relationship from a monitor to a non-default CI:

1 Within RTSM, delete the relationships between the monitor and all CIs except the preferred non-default CI.

2 Within SiteScope, access the monitor's properties page. In SiteScope 11.x, within the **HP Integration Settings** panel, select the **Report Monitor and Related CI Topology** option. Select the CI type for the monitor, and enter values for the CI type key attributes (they depend on the CI type selected).

This enables you to associate the monitor with a non-default CI, rather than with its default CI.

3 To enable BSM to receive health indicator data from a monitor after associating it with a CI of a non-default CIT, perform the following:

If necessary, create new health indicators for the non-default CIT within the Indicator Repository.

Map the indicators that you want to associate with the monitor, to the monitor metrics. This step depends on your version of SiteScope:

- For SiteScope 10.x, access **Admin** > **System Availability Management**, and select the **Metrics and Indicators** tab. Manually map the metrics from the monitor to the required indicators on the CI, by selecting the appropriate CIT and the indicators that you want to associate with the monitor. For details, refer to the "Metrics and Indicators Tab" section in *Using SiteScope*.
- For SiteScope 11.x, within the monitor's properties page in SiteScope, within the **HP Integration Settings** panel, check the **Report monitor and related CI topology** checkbox. In the **CI Type** dropdown select the relevant CI type, and fill in the details of the CI to which the monitor is linked. In the same panel, under **Indicator Settings**, map metrics of the monitor to the relevant indicators for the CI.

SiteScope Monitors with Missing Health Indicators

In BSM 9.x, each CI type has a default set of health indicators defined in the Indicator Repository, which represents what is monitored on CIs of that CI type. If you have manually associated a monitor with a CI of a non-default CIT, you may need to configure the mappings between the metrics of the monitor, and the indicators.

For example, if you have manually associated a CPU monitor with a Running Software CI (and not with a Computer CI), the Running Software CIT will not have the CPU-related indicators defined, and the Running Software CI will therefore not show CPU data.

To identify CIs and monitors with missing health indicators

Open **RTSM Administration** > **IT Universe Manager**, and drill down to **Monitors** > **SiteScope** > **SiteScope Monitors with Missing Health Indicators**. If you have CIs that are missing health indicators, the **SiteScope Monitors with Missing Health Indicators** view displays these CIs and their associated monitors.

To enable BSM to receive health indicator data from a monitor after associating it with a CI of a non-default CIT

1 If necessary, create new health indicators for the non-default CIT within the Indicator Repository.

2 Map the indicators that you want to associate with the monitor, to the monitor metrics. This step depends on your version of SiteScope:

- For SiteScope 10.x, access **Admin** > **System Availability Management**, and select the **Metrics and Indicators** tab. Manually map the metrics from the monitor to the required indicators on the CI, by selecting the appropriate CIT and the indicators that you want to associate with the monitor. For details, refer to the "Metrics and Indicators Tab" section in *Using SiteScope*.
- For SiteScope 11.x, within the monitor's properties page in SiteScope, within the **HP Integration Settings** panel, check the **Report monitor and related CI topology** checkbox. In the **CI Type** dropdown select the relevant CI type, and fill in the details of the CI to which the monitor is linked. In the same panel, under **Indicator Settings**, map metrics of the monitor to the relevant indicators for the CI.

Monitors Not Reporting Topology Data By Default

The following is a list of monitors that do not monitor the status of a host or server.

Note: For these monitors to report CI information to BSM, you must select the CI type, enter the required CI key attributes, and select an indicator relevant for the CI type linked to the monitor.

- Composite Monitor
- Directory Monitor
- e-Business Transaction Monitor
- File Monitor
- Formula Composite Monitor

- HP NonStop Event Log Monitor
- JMX Monitor (when not monitoring WebLogic)
- Link Check Transaction Monitor
- Log File Monitor
- Microsoft Windows Dial-up Monitor
- Microsoft Windows Media Player Monitor
- Multi Log File Monitor
- Network Bandwidth Monitor
- Real Media Player Monitor
- Script Monitor
- SNMP Trap Monitor
- URL Monitor
- URL Content Monitor
- URL List Monitor
- URL Sequence Monitor
- XML Metrics Monitor

CI Downtime

Note: This section is relevant only to those users connecting SiteScope with BSM 9.00 or later.

Downtimes are defined and managed in BSM using the Downtime Management page in Platform Administration. For details about configuring downtime, refer to "Downtime Management — Overview" on page 56.

SiteScope is affected by downtime if a SiteScope monitor, measurement, or group CI is directly linked to a CI that BSM detects is in downtime.

Monitors affected by a CI that is currently in downtime do not go into downtime immediately. The time that it takes for the monitors to go into downtime is affected by two configuration parameters:

- The interval between SiteScope queries to BSM for downtime requests (the default downtime retrieval frequency value is 15 minutes). This can be modified in SiteScope in **Preferences** > **Infrastructure Preferences** > **General Settings** > **BSM downtime retrieval frequency (minutes)**.
- The interval between the updates of the SiteScope downtime cache in BSM (the default value is 5 minutes). This can be modified in BSM in **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**:
  - Select **Applications**.
  - Select **End User/System Availability Management**.
  - In the **Downtime** table, locate **SiteScope Downtime Cache Update Interval**. Change the value to the required cache update interval.

The action that is taken in SiteScope during the downtime depends on the downtime configuration in BSM. Downtime can be enforced on the following:

- Alerts. No alerts are sent for any of the CIs associated with the downtime.
- Reports. Reports are not updated and display the downtime for the CI.
- KPIs. KPIs attached to the CI are not updated and display the downtime for the CI in Service Health.

➤ Monitoring. SiteScope monitoring stops for any of the CIs associated with the downtime.

A monitor that is in downtime is indicated in the SiteScope Dashboard **Summary** column by "disabled by <Downtime Name> from BSM". Details of downtimes that are associated with the monitor and are currently taking place are displayed in the **Monitor Downtime** table in the **Enable/Disable Monitor** panel.

If the monitor is affected by a CI that is currently in downtime and the downtime applies to associated alerts of the monitor, downtime details are displayed in the **Associated Alerts Downtime** table in the **Enable/Disable Associated Alerts** panel.

Notes and Limitations

➤ When SiteScope queries BSM for downtime requests, it gets the downtimes for the downtime period (up to a maximum of 24 hours). A record is written to the **audit.log** in the **<SiteScope root directory>\logs** directory which includes new downtimes, changes to existing downtimes, and deleted downtimes.

➤ When SiteScope 11.00 or later is connected to BSM, the downtime mechanism is enabled by default. To change the default setting, clear the **Enable downtime mechanism** check box in SiteScope's **Preferences** > **Infrastructure Preferences** > **General Settings**.

➤ Downtime is not supported for SAP, Siebel, or SOA topologies (regardless of whether the Application Management for Siebel/SAP license is installed).

➤ For monitors that report the CI per metric, when a CI connected to a metric is in downtime, this sends the monitor to which the metric belongs into downtime. This is applicable to the "VMware Performance Monitor" and "Solaris Zones Monitor"

➤ Downtime information is not available in System Availability Management reports.

➤ When SiteScope is connected to BSM 9.10, downtime on the SiteScope profile is upgraded to downtime on the hosts and software elements that are monitored by the SiteScope profile monitors and measurements.

Downtime Management — Overview

Downtime or other scheduled events can skew CI data. You may want to exclude these periods of time from being calculated for events, alerts, reports, views, or SLAs. Downtimes are configured based on associated CIs. For example, you might want to exclude a recurring maintenance event or a holiday for a specific host CI whose physical host you know will be down for that period of time.

You define and manage downtimes using the Downtime Management page in Platform Admin. BSM enables you to:

- Configure the downtime to occur once or to recur weekly or monthly.
- Select multiple CIs to be affected by the downtime.

When configuring a downtime, you select specific instances of CIs from the available views. You can select CIs of the following CI types for the downtime:

- node
- running software
- business process
- business application
- ci collection
- infrastructure service
- business service

Downtime Actions

You can select what action is taken during the downtime on the CIs specified in the downtime configuration. Downtime can impact the following:

- **Alerts and Events**. Events are suppressed and no CI Status alerts, EUM alerts, or notifications are sent for any of the CIs associated with the downtime.

- **KPIs**. KPIs attached to the CI and impacted CIs are not updated and display the downtime for the CI in Service Health. For details on how downtime configurations affect Service Health, see "KPI Status Colors and Definitions" in *Using Service Health*.
- **Reports**. End User Management Reports are not updated and display the downtime for the CI. For details on how downtime configurations affect reports, see "Downtime Information in Reports" in *Reports*.
- **SLAs**. Selected SLAs that are attached to the CI are not updated. You can select which SLAs to include in the downtime. For details on how downtime configurations affect SLAs, see "Adjusting SLA Data - Overview" in *Using Service Level Management*.
- **Monitoring**. Business Process Monitor and SiteScope monitoring stops for any of the CIs associated with the downtime. For details on how downtime configurations affect SiteScope monitoring, see "CI Downtime" in *Using System Availability Management*.

The options you select in the downtime wizard are combinations of the above actions, grouped in this order. This means that each option includes the previous options listed. The actions that are taken in BSM during the downtime depends on the option selected during downtime configuration.

Events in Operations Management

When you select an action option that includes suppressing events in a downtime on a selected CI, the result in the Operations Management application depends on how the downtime behavior is configured in Operations Management. For details, see "Downtime Configuration" on page 545 in *Using Operations Management*.

Downtime REST Service

You can retrieve, update, create, and delete downtimes through a RESTful Web service running on the Gateway Server. For details, see "Downtime REST Service" on page 60.

How to Create and Manage Downtimes for CIs

This task describes how to create and manage downtimes for the CIs in your system.

1 Prerequisites

Plan how you want the downtime to affect the CIs in your system. Before working in the wizard:

- When determining which CIs may need downtimes, take into consideration CIs whose status is impacted by other CIs. If a CI's status is impacted by a CI you selected for the downtime, that CI is also affected by the downtime. You can select only CIs from the following CI types:
  - node
  - running_software
  - business_process
  - business_application
  - ci_collection
  - infrastructure_service
  - business_service
- Determine which actions should be applied to which CIs. The options for what happens during downtime are to:
  - Suppress events, alerts and notifications
  - Enforce downtime on KPI calculations; and suppress events, alerts and notifications
  - Enforce downtime on Reports and KPI calculations; and suppress events, alerts and notifications
  - Stop monitoring for Business Process Monitors and SiteScope; enforce downtime on Reports and KPI calculations; and suppress events, alerts and notifications

2 Configure how events are handled in Operations Management - optional

You can manage how events associated with CIs that are in downtime are handled. You do this in **Admin** > **Operations Management** > **Tune Operations Management** > **Downtime Behavior.**

For details on this topic, see "Downtime Configuration" in *Using Operations Management*.

3 Run the Create Downtime wizard

Go to **Admin** > **Platform** > **Downtime** and click the **Add Downtime** button.

For user interface details, see "New Downtime Wizard" on page 69.

4 Results

After running the wizard, the details of the downtime are displayed in the Downtime Manager page. You can export the details of the downtimes to a .pdf or Excel file.

For user interface details, see "Downtime Management Page" on page 65.

Tip: To limit the downtimes in the exported file to a specified selection, you can filter the visible downtimes in the Downtime Manager and then export to a .pdf or Excel file. You can filter by any combination of one or more columns, including: Name, CIs, Status, Action, Scheduling, Next Occurrence, Modified By, Approved By, Planned, and Category.

Downtime REST Service

You can use a RESTful Web service running on the Gateway Server to retrieve, update, create, and delete downtimes. HTTP requests can be entered in your browser, and combinations of HTTP requests and XML commands in a REST client. Service authentication is based on basic authentication.

Supported HTTP Requests

The downtime REST service supports the following HTTP requests:

Note: CustomerID is always 1 except in the case of HP SaaS customers.

Action	HTTP Command
Retrieve all downtimes	http://<HPBSM server>/topaz/bsmservices/customers/[customerId]/downtimes
Retrieve a specific downtime	http://<HPBSM server>/topaz/bsmservices/customers/[customerId]/downtimes/[downtimeId]
Update a downtime using http PUT	http://<HPBSM server>/topaz/bsmservices/customers/[customerId]/downtimes/[downtimeId] + XML of the downtime (see "Downtime XML Example" on page 62)
Create downtime using http POST	http://<HPBSM server>/topaz/bsmservices/customers/[customerId]/downtimes + XML of the downtime (see "Downtime XML Example" on page 62) **Note:** Successful creation of the downtime causes a return of the newly created downtime in XML format, including the downtime ID.
Delete downtime using http DELETE	http://<HPBSM server>/topaz/bsmservices/customers/[customerId]/downtimes/[downtimeId]

Allowed Downtime Actions

Use the XML commands listed for the following downtime actions:

Action Description	XML Command
Take no action	<action name="REMINDER"/>
Suppress events, alerts and notifications (continue monitoring, calculating and displaying data)	<action name="SUPPRESS_NOTIFICATIONS"/>
Enforce downtime on KPI calculations; suppress events, alerts and notifications (continue monitoring)	<action name="ENFORCE_ON_KPI_CALCULATION"/>
Enforce downtime on Reports and KPI calculations; suppress events, alerts and notifications (continue monitoring)	<action name="ENFORCE_ON_REPORTS"/>
Enforce downtime on Reports and KPI calculations; suppress events, alerts and notifications (continue monitoring), including all SLAs	<action name="ENFORCE_ON_REPORTS"> <propGroup name="SLM" value="ALL"/> </action>

Action Description	XML Command
Enforce downtime on Reports and KPI calculations; suppress events, alerts and notifications (continue monitoring), including specific SLA	<action name="ENFORCE_ON_REPORTS"> <propGroup name="SLM" value="SELECTED"> <prop>dda3fb0b20c0d83e078035ee1c005201 </prop> </propGroup> </action>
Stop active monitoring (BPM and SiteScope); enforce downtime on Reports and KPI calculations, suppress events, alerts and notifications	<action name="STOP_MONITORING"/>

Downtime XML Example

The following fields may not exceed the maximum lengths specified:

- Name: 200 characters
- Description: 2000 characters
- Approver: 50 characters

```
<downtime userId="1" planned="true"
id="8898e5a5dbcdc953e04037104bf5737c">

    <name>The name of the downtime</name>
    <action name="ENFORCE_ON_REPORTS">
    </action>
    <approver>The approver name</approver>
    <category>1</category>
    <notification>
        <recipients>
            <recipient id="24"/>
            <recipient id="22"/>
            <recipient id="21"/>
        </recipients>
    </notification>
    <selectedCIs>
```

```
        <ci>
            <id>ac700345b47064ed4fbb476f21f95a76</id>
            <viewName>End User Monitors</viewName>
        </ci>
    </selectedCIs>
    <schedule xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="WeeklyScheduleType">
        <type>WEEKLY</type>
        <startDate>2010-06-10T15:40:00+03:00</startDate>
        <timeZone>Europe/Zurich</timeZone>
        <days>
            <selectedDays>WEDNESDAY</selectedDays>
            <selectedDays>THURSDAY</selectedDays>
            <selectedDays>FRIDAY</selectedDays>
            <selectedDays>SATURDAY</selectedDays>
        </days>
        <startTimeInSecs>52800</startTimeInSecs>
        <durationInSecs>300</durationInSecs>
    </schedule>
</downtime>
```

Scheduling

Keep the following in mind when setting the downtime schedule:

- Retroactive downtime is not supported. You cannot:
  - Create a downtime that is scheduled in the past.
  - Delete a downtime that has started or that occurred in the past.
  - Modify a downtime that has started or that occurred in the past.
- The date format of startDate/endDate is: **yyyy-MM-dd'T'HH:mm:ssZ**
- For weekly and monthly downtimes, the startDate and endDate should be defined at midnight. For example:
  - <startDate>2010-07-24T00:00:00+03:00</startDate>
  - <endDate>2010-09-04T00:00:00+03:00</endDate>

Example of a Downtime Schedule with One Occurance

```
<schedule xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="OnceScheduleType">
    <type>ONCE</type>
    <startDate>2010-06-08T14:40:00+03:00</startDate>
```

```
    <endDate>2010-06-08T14:45:00+03:00</endDate>
    <timeZone>Asia/Tokyo </timeZone>
</schedule>
```

Example of a Weekly Downtime Schedule

```
<schedule xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="WeeklyScheduleType">
    <type>WEEKLY</type>
    <startDate>2010-06-10T15:40:00+03:00</startDate>
    <timeZone>Europe/Zurich</timeZone>
    <days>
        <selectedDays>WEDNESDAY</selectedDays>
        <selectedDays>THURSDAY</selectedDays>
        <selectedDays>FRIDAY</selectedDays>
        <selectedDays>SATURDAY</selectedDays>
    </days>
    <startTimeInSecs>52800</startTimeInSecs>
    <durationInSecs>300</durationInSecs>
</schedule>
```

Example of a Monthly Downtime Schedule

```
<schedule xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="WeeklyScheduleType">
    <type>WEEKLY</type>
    <startDate>2010-06-10T14:40:00+03:00</startDate>
     <timeZone>America/Montevideo</timeZone>
     <days>
        <selectedDays>WEDNESDAY</selectedDays>
        <selectedDays>THURSDAY</selectedDays>
        <selectedDays>FRIDAY</selectedDays>
        <selectedDays>SATURDAY</selectedDays>
    </days>
    <startTimeInSecs>52800</startTimeInSecs>
    <durationInSecs>300</durationInSecs>
</schedule>
```

Downtime Management User Interface

This section includes:

Downtime Management Page

Displays the list of scheduled downtimes configured for the associated CIs.

To access:	Select **Admin** > **Platform** > **Downtime Management**
Important information	➤ To add, edit or delete downtimes, you must have Full permission on the Downtime resource. In addition, you should have View permission on the Views to which CIs in the downtime belong. For details on permissions, see "Permissions Overview" on page 405. ➤ The values you see in this page are view only. To edit any of the values for a downtime, highlight the downtime and click **Edit**. The Downtime Wizard opens and you can edit the value in the page in which it appears. ➤ For downtimes that have already occurred, only the following fields are editable: ➤ Properties page - all fields ➤ Scheduling page - **End by** date in **Range of recurrence** ➤ Notification page - **Selected Recipients** ➤ Each column includes the option of filtering the list by the contents of the column. For example, you can select a category type in the category column and see only those downtimes configured with that category.
Relevant tasks	"How to Create and Manage Downtimes for CIs" on page 58
See also	"Downtime Management — Overview" on page 56

User interface elements are described below

UI Element (A–Z)	Description
	**Create new downtime.** Opens the New Downtime wizard where you configure a new downtime. For details, see "New Downtime Wizard" on page 69.
	**Edit downtime.** Opens the Edit Dowtime wizard, which enables to you edit the configuration of an existing downtime. This wizard presents the same screens as the New Downtime wizard. For details, see "New Downtime Wizard" on page 69.
	**Duplicate downtime.** Clones the settings of an existing downtime to a new downtime.
	**Delete downtime(s).** Deletes selected downtime(s).
	**Export to Excel.** Exports the table of configured downtimes to a file in Excel format.
	**Export to PDF.** Exports the table of configured downtimes to a PDF file.
Action	The action that takes place when the downtime is in active status. You configure the action for the downtime in the New Downtime wizard. For details about the possible actions, see "Action Page" on page 74.
CIs	The CIs associated with the downtime. These are the CIs that are impacted when the downtime is in active status.
Modified by	The user who last created or modified the downtime configuration.
Name	The name of the downtime as configured in the Downtime wizard.
Next Occurrence	The date and time of the next occurrence of the downtime. This field is updated automatically.

UI Element (A–Z)	Description
Scheduling	Displays the: ➤ Date, time, time zone, and duration For recurring downtimes, also displays: ➤ What day of the week or month the downtime is scheduled to recur ➤ Range of recurrence
Status	Displays whether the downtime is currently: ➤ **Active.** The CIs are currently in downtime and the action selected for the downtime is now taking place. ➤ **Inactive.** The downtime is configured but it is currently not the time for the downtime to take place. ➤ **Completed**. The time for the downtime has passed and the actions configured for the downtime have occurred.
Optional Columns	
Approved by	Indicates if there was an approval for the downtime and who approved it.

UI Element (A–Z)	Description
Category	The category assigned to the downtime. Options include: ➤ Application installation ➤ Application maintenance ➤ Hardware installation ➤ Hardware maintenance ➤ Network maintenance ➤ Operating system reconfiguration ➤ Other ➤ Security issue You can also create your own customized categories using Infrastructure Settings. To add a custom downtime category, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**: ➤ Select **Foundations**. ➤ Select **Downtime**. ➤ In the **Downtime - General settings** table, edit the **Downtime categories** value to the name you want to use as a customized category for the downtime. The name you enter appears as an option in the list of available downtime categories.
Planned	Indicates whether the downtime is planned or not.

New Downtime Wizard

This wizard enables you to create and edit downtimes for the CIs in your model.

To access	**Admin** > **Platform** > **Downtime** > click the **Create new downtime** button, or select existing downtime and click the **Edit downtime** button.
Relevant tasks	"How to Create and Manage Downtimes for CIs" on page 58
Wizard map	This New Downtime Wizard contains: Properties Page > Select CIs Page > Scheduling Page > Action Page > Notification Page > Preview Page
See also	"Downtime Management — Overview" on page 56

Properties Page

This wizard page enables you to configure the general properties of the downtime.

Important information	For downtimes that have already occurred, all of the fields in the Properties page are editable.
Wizard map	This New Downtime Wizard contains: Properties Page > Select CIs Page > Scheduling Page > Action Page > Notification Page > Preview Page
See also	"Downtime Management — Overview" on page 56

User interface elements are described below:

UI Element	Description
Downtime Name	Cannot exceed 200 characters.
Downtime Description	This description also appears in the "Downtime Information Area" in *Reports*.

UI Element	Description
Approved by	You can enter the person or department who approved this downtime. Cannot exceed 50 characters.
Planned	Select if you want this downtime marked as planned. You can create downtimes that are unplanned. This is for information purposes only.
Downtime Category	Select a category from the drop-down menu. This category describes the reason for the downtime. You can also create your own customized categories using Infrastructure Settings. To add a custom downtime category, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**: ➤ Select **Foundations**. ➤ Select **Downtime**. ➤ In the **Downtime - General settings** table, edit the **Downtime category** value to the name you want to use as a customized category for the downtime. The name you enter appears as an option in the list of available downtime categories after you restart BSM.

Select CIs Page

This wizard page enables you to select the CIs that are affected by the downtime.

Important information	For downtimes that have already occurred, you cannot edit the selected CIs in this page.
Wizard map	This New Downtime Wizard contains: Properties Page > Select CIs Page > Scheduling Page > Action Page > Notification Page > Preview Page
See also	"Downtime Management — Overview" on page 56

User interface elements are described below:

UI Element (A-Z)	Description
Available CIs	Select from the list the view that contains the CIs to be affected by this downtime. You can use the  button to browse and perform a search among the available views. Highlight a CI from the view to move it to the Selected CIs list. Hold the Ctrl key for selecting multiple CIs. All views that the user has permission to see may be selected. You can select CIs only of the following CI types: ➤ node ➤ running software ➤ business process ➤ business application ➤ ci collection ➤ infrastructure service ➤ business service
Selected CIs	Once CIs are selected, they appear in the Selected CIs list. To remove a CI from a downtime, select the CI in the Selected CIs and click the back arrow to move it back to the Available CIs list.

Scheduling Page

This wizard page enables you to configure the schedule for the downtime.

Important information	➤ You cannot schedule a downtime in the past. ➤ For downtimes that have already occurred, only the following field is editable in the Scheduling page: **End by** date in **Range of recurrence** To cancel a recurring downtime that has already occured at least once, edit the downtime and modify this field.
Wizard map	This New Downtime Wizard contains: Properties Page > Select CIs Page > Scheduling Page > Action Page > Notification Page > Preview Page
See also	"Downtime Management — Overview" on page 56

User interface elements are described below:

UI Element	Description
Time of occurrence	➤ **Start**. The dropdown list includes times set for every half hour on the hour and half hour. To select a different time of day, select the closest half hour and edit the field to enter the actual time you want the downtime to start. For example, for 2:10 am, select 2:00 am and edit the minutes to indicate 2:10 am. ➤ **End**. You can select an end time and the duration automatically updates. Or select the duration and the end time automatically updates. ➤ **Duration.** Includes options from 5 minutes to one week. The downtime duration must be in increments of 5 minutes and be defined in lengths of minutes, hours, days, or weeks. If the length of time you want to specify does not appear, for example 1 1/2 hours, then enter the end time and the duration automatically updates. To select a time greater than 1 week, select 1 week and edit the field to the correct number of weeks.
Recurrence pattern	Select one of the following: ➤ **Once.** The downtime happens only once as scheduled and does not recur. Select the calendar date for the occurrence. ➤ **Weekly.** Select the day of the week for the scheduled weekly recurrence. ➤ **Monthly.** Select a day in the month from the dropdown list for the scheduled monthly recurrence.
Range of recurrence	If you selected **Weekly** or **Monthly**: ➤ You must define a **Start** date. ➤ Select either an **End by** date or **No end date**.
Time zone	All time zones are displayed in relation to GMT.

Action Page

This wizard page enables you to define the set of actions taken during the downtime.

Important information	For downtimes that have already occurred, no fields in the Action page are editable.
Wizard map	This New Downtime Wizard contains: Properties Page > Select CIs Page > Scheduling Page > Action Page > Notification Page > Preview Page
See also	"Downtime Management — Overview" on page 56

User interface elements are described below:

UI Element	Description
Take no actions	There is no action taken on the associated CIs or the CI monitoring, alerts, reports, or SLAs. **Note:** During this downtime, the affected CI doesn't change its status to **Downtime**. CI Status Alerts configured to be triggered if the CI changes its status.
Suppress alerts and close events	➤ No alerts or their associated notifications or actions are sent for any of the CIs associated with the downtime. ➤ By default, events are submitted as closed. If OMi is installed, event handling in downtime can be configured in Event Management, and overrides the setting here. ➤ Monitoring continues, and reports, status in Service Health, and SLAs are updated. **Note:** During the downtime period, the affected CI may change its status, and the status change may trigger the relevant CI Status alert.

UI Element	Description
Enforce downtime on KPI calculations; suppress alerts and close events	➤ KPI calculations are not run and status in Service Health is not updated, and instead display the downtime for the CI. ➤ No alerts or their associated notifications or actions are sent for any of the CIs associated with the downtime. ➤ By default, events are submitted as closed. If OMi is installed, event handling in downtime can be configured in Event Management, and overrides the setting here. ➤ Reporting and monitoring continue. SLAs are updated.

UI Element	Description
Enforce downtime on Reports and KPI calculations; suppress alerts and close events	➤ Report data is not updated and the downtime is displayed for the associated CIs. ➤ Selected SLAs are not updated for those SLAs affected by CIs associated with the downtime. ➤ KPI calculations are not run and status in Service Health is not updated, and instead display the downtime for the CI. ➤ No alerts or their associated notifications or actions are sent for any of the CIs associated with the downtime. ➤ By default, events are submitted as closed. If OMi is installed, event handling in downtime can be configured in Event Management, and overrides the setting here. ➤ Monitoring continues.

UI Element	Description
Stop active monitoring (BPM & SiteScope); enforce downtime on Reports & KPI calculations; suppress alerts and close events (affects all related SLAs)	➤ Business Process Monitor and SiteScope monitoring stops. ➤ Report data is not updated and the downtime is displayed for the associated CIs. ➤ Selected SLAs are not updated for those SLAs affected by CIs associated with the downtime. ➤ KPI calculations are not run and status in Service Health is not updated, and instead display the downtime for the CI. ➤ No alerts or their associated notifications or actions are sent for any of the CIs associated with the downtime. ➤ By default, events are submitted as closed. If OMi is installed, event handling in downtime can be configured in Event Management, and overrides the setting here. **Note:** If you configure a downtime period for an Application CI (whose data is updated by BPM monitoring), Downtime Manager automatically sends an event to the BPM Agent when the downtime period starts. The agent stops sending samples to BSM. The samples that are suppressed are the BPM samples that correspond to the Transaction CIs, which are child CIs of the Application CIs on which the downtime is configured. There is one sample per transaction.

Notification Page

This wizard page enables you to select recipients to receive notification of the downtime. Notifications are sent by email at the time of downtime occurrence and immediately after it completes. You can select only those recipients with an email address defined.

Important information	For downtimes that have already occurred, you can edit the **Selected Recipients** in the Notification page.
Wizard map	This New Downtime Wizard contains: Properties Page > Select CIs Page > Scheduling Page > Action Page > Notification Page > Preview Page
See also	"Downtime Management — Overview" on page 56

User interface elements are described below:

UI Element	Description
	Opens the **New recipient** dialog box to create a recipient that is not yet in the list of available recipients. The recipients you create are available as recipients in all of BSM. For details on creating recipients, see "How to Configure and Manage Recipients" on page 519.
Available Recipients	Lists the available recipients for downtime notification by means of either email, SMS, or pager.
Selected Recipients	Lists the selected recipients for downtime notification by means of either Email, SMS, or Pager. Either one, two or all three means of notification may be selected.

Preview Page

This wizard page enables you to preview a summary of your Downtime settings.

Wizard map	This New Downtime Wizard contains: Properties Page > Select CIs Page > Scheduling Page > Action Page > Notification Page > Preview Page
See also	"Downtime Management — Overview" on page 56

User interface elements are described below:

UI Element	Description
Preview table	Table listing all the values configured for this downtime. Gives you the opportunity to click the **Back** button to return to a page that has a value that should be modified or deleted. Once you click **Finish** on this page, the downtime is added to the system and displayed in the Downtime Manager page.

Troubleshooting and Limitations

This section describes troubleshooting and limitations for the Downtime Manager.

Editing Downtimes

- If while editing a downtime in the Downtime wizard its status changes from **Idle** to **Active**, the downtime cannot be saved.
- If you want to cancel a recurring downtime that has already occured at least once, edit the downtime's **End by** date in the Scheduling page.

Downtime and Daylight Saving Time

In time zones that observe Daylight Saving Time (DST), downtime calculations take into account the transitions between Standard and Daylight Time, using the following rules:

Note: The examples that follow use the daylight saving changes observed throughout most of the United States.

- March 14 2010 -- when 2:00 am arrives, the clock moves forward to 3:00 am. Thus, the period 2:00-2:59 am does not exist.
- November 7 2010 -- when 2:00 am arrives, the clock moves back to 1:00 am. Thus, the period 1:00-1:59 am appears twice.

In other time zones, the behavior is the same, but the transition dates and times may vary.

These examples are summarized in the table "DST Changes Affecting Downtime - Example Summary" on page 83.

Spring (Standard to Daylight Time)

- When downtime starts before the DST change and ends the day after the change, its end time is as expected, but the duration is 1 hour less than defined.

  Example 1:

  Monthly downtime starting 14th day of month at 1:30 am and ending on 15th day of month at 2:40 am. Duration is 1 day, 1 hour, and 10 minutes.

  No DST change: Downtime starts on 14th at 1:30 am and ends on 15th at 2:40 am. Duration is 1 day, 1 hour, 10 minutes.

  DST change on March 14 2010: Downtime starts on 14th at 1:30 am and ends on 15th on 2:40 am, but the duration is 1 day, 0 hours, 10 minutes (1 hour less than defined).

- When downtime starts before the DST change and ends the same day as the change, but after the change, its end time is 1 hour more than defined, but its duration is as defined.

  Example 2:

  Monthly downtime on 13th day of month, starting at 11 pm (23:00), for a duration of 5 hours.

  No DST change: Downtime starts on 13th at 11:00 pm and ends on 14th at 4:00 am.

  DST change on March 14 2010: Downtime starts on 13th at 11:00 pm and ends on 14th at 5:00 am, and the duration remains 5 hours.

- When downtime is defined to start during the skipped hour, the start time shifts 1 hour forward and keeps the defined duration.

  Example 3:

  Monthly downtime on 14th day of month, starting at 2:30 am, for a duration of 2 hours.

  No DST change: Downtime starts on 14th at 2:30 am and ends on 14th at 4:30 am.

  DST change on March 14 2010: Downtime starts on 14th at 3:30 am and ends on 14th at 5:30 am, and the duration remains 2 hours.

- When downtime is defined to start before the DST change and end during the skipped hour, the end time shifts 1 hour forward and keeps the defined duration.

  Example 4:

  Monthly downtime on 13th day of month, starting at 1:30 am, for a duration of 1 day, 1 hour, and 10 minutes.

  No DST change: Downtime starts on 13th at 1:30 am and ends on 14th at 2:40 am. The duration is 1 day, 1 hour, and 10 minutes.

  DST change on March 14 2010: Downtime starts on 13th at 1:30 am and ends on 14th at 3:40 am, and the duration remains as defined -- 1 day, 1 hour, and 10 minutes.

- When downtime is defined to start and end during the skipped hour, downtime takes place one hour later than defined.

Example 5:

Monthly downtime on 14th day of month, starting at 2:00 am, for a duration of 1 hour.

No DST change: Downtime starts on 14th at 2:00 am and ends on 14th at 3:00 am.

DST change on March 14 2010: Downtime starts on 14th at 3:00 am and ends on 14th at 4:00 am, and the duration remains as defined -- 1 hour.

Fall (Daylight Time to Standard Time)

- When downtime starts and ends after the DST change, its end time and duration are as defined.
- When downtime starts before the DST change (same day as change or day before) and ends after the change during the day of the change, the end time is 1 hour less than expected, and duration is as defined.

Example 6:

Two monthly downtimes, both starting on the 7th day of month at midnight. The first downtime duration is 1 hour, and the second is 2 hours.

No DST change: The first downtime is on 7th from 0:00 to 1:00 am (1 hour duration), and the second on 7th from 0:00 to 2:00 am (2 hours duration).

DST change on November 7 2010: The first downtime starts on 7th at 0:00 Daylight Time and ends on 7th at 1:00 am Daylight Time, with a duration of 1 hour. The second downtime starts on 7th at 0:00 Daylight Time and ends on 7th at 1:00 am Standard Time, and the duration remains 2 hours.

Example 7:

Monthly downtime on 7th day of month, starting at midnight, for a duration of 4 hours.

No DST change: Downtime starts on 7th at 0:00 and ends on 7th at 4:00 am.

DST change on November 7 2010: Downtime starts on 7th at 0:00 and ends on 7th at 3:00 am, and the duration remains as defined -- 4 hours.

Example 8:

Monthly downtime on 6th day of month, starting at 8:00 pm (20:00), for a duration of 7 hours.

No DST change: Downtime starts on 6th at 8:00 pm and ends on 7th at 3:00 am.

DST change on November 7 2010: Downtime starts on 6th at 8:00 pm and ends on 7th at 2:00 am, and the duration remains as defined -- 7 hours.

➤ When downtime starts before the DST change and ends the day after the change, the end time is as expected, and duration is 1 hour more than defined.

Example 9:

Monthly downtime on 7th day of month, starting at midnight (0:00), for a duration of 1 day, 1 hour (25 hours).

No DST change: Downtime starts on 7th at 0:00 and ends on 8th at 1:00 am.

DST change on November 7 2010: Downtime starts on 7th at 0:00 and ends on 8th at 1:00 am, but the duration is 26 hours.

DST Changes Affecting Downtime - Example Summary

Example	Downtime as Set/With DST Change	Start Time	End Time	Duration
1	Set	14th at 1:30 am	15th at 2:40 am	1 day, 1 hour, 10 minutes
	With DST Change	14th at 1:30 am	15th at 2:40 am	1 day, 0 hours, 10 minutes
2	Set	13th at 11:00 pm	14th at 4:00 am	5 hours
	With DST Change	13th at 11:00 pm	14th at 5:00 am	5 hours

Example	Downtime as Set/With DST Change		Start Time	End Time	Duration
3	**Set**		14th at 2:30 am	14th at 4:30 am	2 hours
	With DST Change		14th at 3:30 am	14th at 5:30 am	2 hours
4	**Set**		13th at 1:30 am	14th at 2:40 am	1 day, 1 hour, and 10 minutes
	With DST Change		13th at 1:30 am	14th at 3:40 am	1 day, 1 hour, and 10 minutes
5	**Set**		14th at 2:00 am	14th at 3:00 am	1 hour
	With DST Change		14th at 3:00 am	14th at 4:00 am	1 hour
6	**1st**	**Set**	7th at 0:00	7th at 1:00 am	1 hour
		With DST Change	7th at 0:00	7th at 1:00 am	1 hour
	2nd	**Set**	7th at 0:00	7th at 2:00 am	2 hours
		With DST Change	7th at 0:00	7th at 1:00 am Standard Time	2 hours
7	**Set**		7th at 0:00	7th at 4:00 am	4 hours
	With DST Change		7th at 0:00	7th at 3:00 am	4 hours
8	**Set**		6th at 8:00 pm	7th at 3:00 am	7 hours
	With DST Change		6th at 8:00 pm	7th at 2:00 am	7 hours

Example	Downtime as Set/With DST Change	Start Time	End Time	Duration
9	**Set**	7th at 0:00	8th at 1:00 am	25 hours
	With DST Change	7th at 0:00	8th at 1:00 am	26 hours

4

Alerts Pre-Upgrade Documenation References

In BSM 9.10, the alert applications have been moved to their own domains: CI Status Alerts to Service Health (formerly Dashboard), SLA Alerts to the Service Level Management application, and EUM alerts (formerly event-based alerts) to the End User Management application.

To define CI Status alerts in version 9.x, see "How to Create a CI Status Alert Scheme and Attach it to a CI" in the *Using Service Health* PDF.

To define your EUM alerts in version 9.x, see "How to Create EUM Alert Schemes" in the *Using End User Management* PDF.

To define SLA alerts in version 9.x, see "How to Define an SLA Alert Scheme" in the *Using Service Level Management* PDF.

This chapter includes:

Infrastructure Settings

This sections describes upgrade limitations for alert infrastructure settings.

This section includes:

Setting Substitution for Quote in Command Line Parameters

The setting **Substitution for quote in command line parameters** under **Foundations - alerting** that was available in version 8.06 is no longer available in version 9.10. If the value of the parameter was customized in version 8.06, that change will not be available after upgrade. To set it manually after the upgrade, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**:

➤ Select **Foundation**.

➤ Select **Alerting**.

➤ In the **Foundation - Alerting table**, locate and update the **Command line substitution pairs**.

Parameters in Default Exe and Default URL Infrastructure Settings

Parameters used in the **Default Exe path** and **Default URL** infrastructure settings for alerts triggering defaults in version 8.07, are not upgraded to the new parameters for version 9.10. To set them manually after the upgrade, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**:

➤ Select **Foundation**.

➤ Select **Alerting**.

➤ In the **Alerting - Triggered alerts** table, locate the **Default Exe path** and **Default URL** settings and update the parameters according to the following table:

BAC 8.07 Parameters	BSM 9.10 Parameters
Profile Name	Entity Name
SubAlerts	Alert XML
Id	Alert ID
Page Name	Transaction Name
User Message	Alert User Description
Group Name	N/A in BSM 9.10

General Information

Alerts samples were changed. For details about the upgrade of the Custom Query Builder, see "Custom Query Builder Upgrade" on page 193.

CI-Based Alerts

CI-based alerts that were defined on End User Management Administration CIs in the old model (in BAC 8.x) are upgraded to be defined on the new corresponding CIs (in BSM 9.10). For example, an alert defined for a specific Business Process Group is upgraded to be defined on the corresponding business transaction flow.

Notification Template Upgrade

The names of some of the parameters that can be included in a notification template have been changed in BSM 9.10.

Topics	BAC 8.x	BSM 9.10
Profile Name (changed - automatically upgraded)	Profile Name	Entity Name
User Message (changed - automatically upgraded)	User Message	Alert User Description
HP BAC URL (changed - automatically upgraded)	HP BAC URL	HP BSM URL
Entity Type attribute was added		
Group Name removed from the Transaction's parameters list		

Alert Permissions Upgrade

The permissions mechanism used for alert users was changed in BSM 9.10.

- **Alerts - Create dependencies** permissions resource was moved from the **Monitors** context to the **End User Management** context.
- **Alert - Event template** permission was added to the **End User Management** context.
- **Send SNMP trap** permissions were moved from the **Monitors** context to the **Platform** context.
- **Run executable file** permissions were moved from the **Monitors** context to the **Platform** context.
- **Log to event Viewer** permissions resource was moved from the Monitors context to the **Platform** context.

Event-Based Alerts

The table describes the changes that occurred between the BAC 8.x and BSM 9.x versions, and describes how the upgrader handles these changes.

Topics	BAC 8.x	BSM 9.x
Event-Based alerts (name was changed)	Event-Based alerts	EUM alerts
Location of the event-based alerts applications	In the Alerts application	In the End User Management application

Topics	BAC 8.x	BSM 9.x
Action parameters (names have changed - automatically upgraded)	Profile Name	Entity Name
	SubAlerts	Alert XML
	Id	Alert ID
	Page Name	Transaction Name
	User Message	Alert User Description
	Group Name	N/A in BSM 9.10 - The Group Name parameter used by actions defined for BAC alerts in BAC 8.x, is discarded by the upgrade.
Group-by option field names (names have changed - automatically upgraded)		
SNMP trap structure		The SNMP trap structure has changed. For details, see SNMP Trap Structure Changes below.
Alert dependencies (automatically upgraded)	RUM alerts assigned to RUM profiles with dependencies	The dependencies are transferred to the alerts assigned to RUM Application CIs for each of the applications that were running on the RUM engine.

SNMP Trap Structure Changes

The following table describes the changes to the SNMP trap structure between BAC 8.x and BSM 9.x.

OID (starts with 1.3.6.1.4.1.5233.)	Variable description (BAC 8.x)	Variable description (BSM 9.x)	Example
4.9	Start of the Subalerts table. Subalerts trigger alerts (listed in Events table)	The ID of the CI related to the alert	Allow the ID of the alert related CI (Application ID in the EUM alert)
4.10	Start of the subalert instance table	The parameters specified in the Grouped By definition of the alert.	Allows Event correlation on the group by parameters between different alert triggers. Example: transaction: tx5
4.11.1.1.2 - 4.11.1.1.8	Various event parameters (organization, host location, script etc.)	Replaced by 4.11.1.4.1.2.[n].[m]: the actual description of the event	

BPM Alerts

The table describes the changes that occurred between the BAC 8.x and BSM 9.x versions, and describes how the upgrader handles these changes.

Topics	BAC 8.x	BSM 9.x
BPM alerts assigned to a BPM profile (automatically upgraded)	BPM alerts assigned to a BMP profile	BPM alerts are changed to BPM Transaction alerts and assigned to the Application CI that corresponds to the application that was defined for the profile.
BPM alerts grouped by groups (not supported)	BPM alerts grouped by groups	Group by group is not supported. The pre-upgrader provides the list of these alert groups. You cannot filter using **Limit to <group_name>** in the Filters tab of the EUM alerts.
	Limit to <group_name> options in the Filters tab of the event-based alerts	**Limit to <group_name>** options are not supported. The **Groupby Business Transaction Flow** option was added.
Sub-alert parameters (names changed, XML file structure changed - automatically upgraded)	Sub Alerts parameters	The name of the parameter was changed to 'Alert XML',.
		The structure of the XML file was changed and now contains: ➤ General data about the alert (name, ID, severity). ➤ For each trigger, data about the events that triggered the alert (if such events exist). For an example of such an XML file, see "Example of an Alert XML Structure" on page 97.

Topics	BAC 8.x	BSM 9.x
SNMP structure of event-based alerts (changed - automatically performed)	SNMP structure of the event-based alerts	The SNMP trap structure of the EUM alerts was changed. ➤ There is only one trap type: **eventAlert** ➤ Some of the OIDs and the names have changed ➤ Sub alerts/triggers table structure and events table structure changed For details, see "Alerts MIB Varbinds" in *Using End User Management*.
<<Trigger ID>> parameter value was changed (automatically performed)	Value is a number	Value is text

Topics	BAC 8.x	BSM 9.x
Action parameters with extensions (num or tx_resp)	**Event-based triggers (BPM only).** If more than one event triggers an alert, sequential numbers are adjusted to each trigger and event parameter. If more than one triggers' requirements are met, trigger types are adjusted. Trigger types were **tx_resp** for "Transactions response time" and empty for "Transactions response time relevant to EUM threshold. For example: <<parameter>>1, <<parameter>>1 tx_resp, <<parameter>>2, <<parameter>>2 tx_resp The **TriggerTypeMessage** parameter is added with the relevant trigger ID.	If more than one trigger and/or event are configured; it is recommended to use the out-of-the-box <<Alert XML>> that contains all the triggered alert information (to access it click the **Action** tab and select **Generate Event** and then the **BPM Trans Alert** default) and insert it as an action parameter. For details about its structure see the Example on the next page. **TO DO:** To use these parameters you must enable the setting and manually upgrade the parameters. For details, see "Action Parameters Manual Upgrade" on page 98
When BPM adapter was configured to transaction\location mode in the previous version, after the upgrade these views are upgraded into Local Impact Views. The CI Status alerts that were defined for CIs in these views are not copied to the corresponding Local Impact Views and will not be accessible through these views.		

Example of an Alert XML Structure

```
<Alert>
    <Name>Michal</Name>
    <Id>xxx</Id>
    <Severity>Major</Severity>
    <Purpose>Regular Alert</Purpose>
    <UserMessage>N/A</UserMessage>
    <EntityName>Default Client_Snt_Ap1_1</EntityName>
    <EntityId>3fb61099e47ed1b527b48ab2cff636a2</EntityId>
     <Triggers>
       <Trigger>
        <TriggerCause>Response time for 1 out of 1 transactions greater than 0.00
seconds.</TriggerCause>
        <ActualDetails>Response time for 1 out of 1 transactions was greater than 0.00
seconds.</ActualDetails>
        <Events>
        <Event>
        <ActualDetails>Response time was 9.99 seconds.</ActualDetails>
        <Transaction>
        <BTFName />
        <BTFId>701db88f4335742ff454da2216ab4c94</BTFId>
        <Name>tx_10</Name>
        <Time>Tue Dec 14 11:24:34 AM 2010 (GMT +0200)</Time>
        <LocationName>VMAMRND12</LocationName>
        <ScriptName>tx_5_10_15</ScriptName>
        <szBpmAgentName>VMAMRND12</szBpmAgentName>
        <Description />
        <Error>N/A</Error>
        <BPMTriageReportUrl>http://machine
name:80/topaz/rfw/popupAction.do?popUp=true&filter.filters.TIME_PERIOD.timeBarBean.view=pastHo
ur&filter.filters.DATA_COLLECTOR.dataCollector=BPM&autoGenerate=true&reportID=triage_report&filt
er.filters.APPLICATION.selectedIdsInTree=0x3fb61099e47ed1b527b48ab2cff636a2&filter.filters.APPLI
CATION.fromDashboard=true</BPMTriageReportUrl>
        <BPMPerfAnalysisReportUrl>http://machine
name:80/topaz/rfw/popupAction.do?popUp=true&filter.filters.TIME_PERIOD.timeBarBean.view=pastHo
ur&filter.filters.DATA_COLLECTOR.dataCollector=BPM&autoGenerate=true&reportID=performance_su
mmary_report&filter.filters.APPLICATION.selectedIdsInTree=0x3fb61099e47ed1b527b48ab2cff636a2&
filter.filters.APPLICATION.fromDashboard=true</BPMPerfAnalysisReportUrl>
        </Transaction>
        </Event>
        </Events>
        </Trigger>
      </Triggers>
 </Alert>
```

Action Parameters Manual Upgrade

To use the action parameters extensions:

1 Change the value of the **settings.enable.legacy.action.parameters** setting in **<HPBAC Gateway server>\conf\settings\alertengine.xml** to true.

Once the setting is enabled, the parameters are generated with extensions in new format.

2 The parameters are not automatically upgraded. Perform the upgrade manually using the tables below.

➤ **BPM event-based triggers - once:**

Old parameter	New parameter
[param] tx_resp	[param]_TransactionRespTimeOnce
[param]	[param]_TransactionRespTimeRelativeOnce
[param] tx_fail	[param]_TransactionFailOnce

➤ **BPM event-based triggers - X out of Y:**

Old parameter	New parameter
[param]1 tx_resp	[param]_1_TransactionRespTimeXy
[param]1	[param]_1_TransactionRespTimeRelativeXy
[param] tx_fail	[param]_TransactionFailXy

➤ **Over-time BPM and RUM triggers:**

Old parameter	New parameter	Description
[param]1	[param]_[trigger id]	For over-time triggers, parameter number extensions

3 The **TriggerTypeMessage** parameter is added with the relevant trigger ID. The parameter remains the same. Map its values according to the table Trigger IDs' mapping table.

➤ **Trigger IDs' mapping table:**

Alert	Trigger	Old ID	New ID
BPM Once	Transaction fail	6	TransactionFailOnce
	Transaction response time	4	TransactionRespTimeOnce
	Transaction response time relative to EUM	2	TransactionRespTimeRelativeOnce
BPM X out of Y	Transaction fail	16	TransactionFailXy
	Transactions response time	14	TransactionRespTimeXy
	Transactions response time relative to EUM	12	TransactionRespTimeRelativeXy
BPM Time-based	Availability	27	TransactionAvailability
	Transactions response time	23	TransactionRespTimeOverTime
	Transactions response time relative to EUM	21	TransactionRespTimeRelativeOver Time
	Average transaction response time	25	TransactionAvgRespTime

Alert	Trigger	Old ID	New ID
RUM Transaction	Transaction availability	111	TransAvailability
	Transaction performance (gross)	113	GrossTransPerformance
	Transaction performance (net)	115	NetTransPerformance
	Transaction performance (server)	117	ServerTransPerformance
	Transaction volume - all	119	TransVolume
	Transaction volume - completed	121	CompletedTransVolume
RUM Server	Server application requests availability	109	RumAppRequestOverTime
	Server network connections availability	110	RumAppNetworkOverTime

RUM Page Alerts

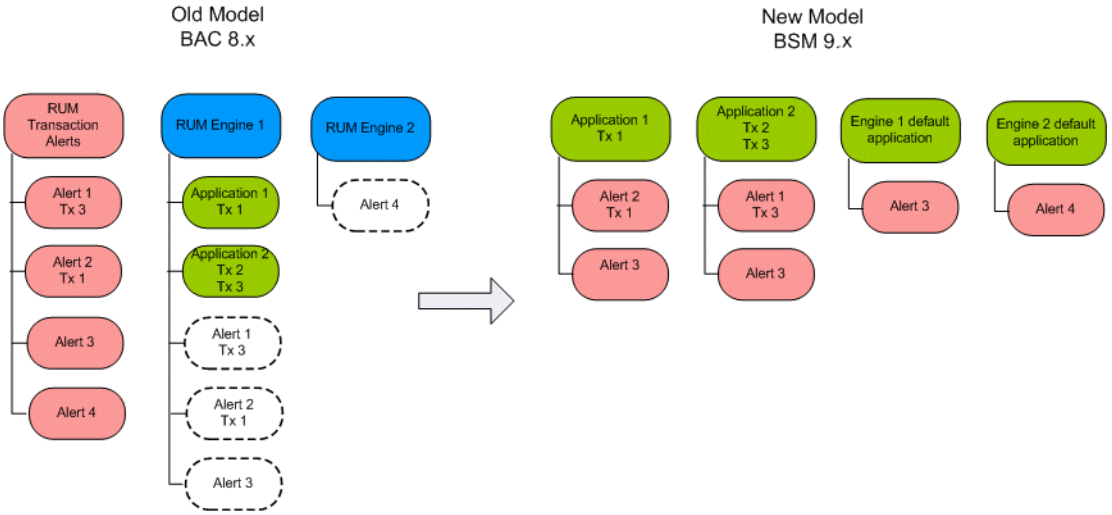
The table describes what changed between the BAC 8.x and BSM 9.x versions, and describes how the upgrader handles the changes.

Topics	BAC 8.x	BSM 9.x
RUM Page alerts (type changed - automatically upgraded)	RUM Page alerts	RUM Application Transaction alerts. The transaction on which the alert is set is the transaction that was created (or mapped to) by the upgrade process for the specific page. For details on the page upgrade process, see "RUM Pages Upgrade" on page 331. **Note:** A RUM alert configuration at the application level that does not filter a certain transaction will receive more data (samples) that fits its filter (both the pages and transactions). This will cause a difference in the calculation result between the previous version and the new version.
	The RUM Page alerts are defined for a Real User Monitor engine.	The upgrade process assigns the corresponding RUM Application Transaction alerts to all the RUM applications that are configured in the new model for the specific engine.

Topics	BAC 8.x	BSM 9.x
RUM page alerts (continued)	If an alert was filtered for specific pages.	The upgrade process duplicates the corresponding RUM Application Transaction alert only to the applications that include these pages. (This is similar to RUM Transaction Alerts. For details, refer to the graphic in "RUM Transaction Alerts" on page 103.)
Trigger criteria (names changed d- automatically upgraded)	Page Availability	Transaction Availability
	Page Response Time	Transaction Gross Response Time
	Page Server Response Time	Transaction Server Response Time
	Transaction Volume	All
	Page Name	Transaction ID
	Group by page	Group by transaction
	User Message	User Message
	Page names for RUM Page alerts	Transaction IDs
	Group-by page for RUM Page alerts	Group-by Transaction

RUM Transaction Alerts

The following graphic shows the upgrade flow for RUM Transaction alerts defined for a Real User Monitor engine and also for alerts filtered for specific transactions:



The table describes what changed between the BAC 8.x and BSM 9.x versions, and describes how the upgrader handles the changes.

Topics	BAC 8.x	BSM 9.x
RUM Transaction alerts (changes - automatically upgraded)	RUM Transaction alerts assigned to RUM profiles	Automatically upgraded to RUM Application Transaction alerts assigned to RUM Application CIs for each of the applications that were running on the RUM engine
	RUM Transaction alert configured with filtering by transaction	Automatically upgraded to alerts assigned to RUM Application CIs for each of the applications that were running on the RUM engine only for the applications that includes that transaction

RUM Server Alerts

The table describes what changed between the BAC 8.x and BSM 9.x versions, and describes how the upgrader handles the changes.

	BAC 8.x	BSM 9.x
RUM Server alerts name was changed	RUM Server alerts	RUM Application alerts
RUM Server alerts (changes - automatically upgraded)	RUM Server alerts assigned to RUM profiles	Automatically upgraded to alerts assigned to RUM Application CIs for each of the applications that were running on the RUM engine
	RUM Server alert configured with filtering by transaction	Automatically upgraded to alerts assigned to RUM Application CIs for each of the applications that were running on the RUM engine only for the applications that run on that server

EUM (Formerly Event-based) Alert Reports and Favorite Filter Upgrade

The table describes what changed between the BAC 8.x and BSM 9.x versions, and describes how the upgrader handles the changes.

Topics	BAC 8.x	BSM 9.x
Alert's model (changed - automatically upgraded)		

Topics	BAC 8.x	BSM 9.x
Filtering in reports (changed due to model change - automatically upgraded)		
	BPM Profile ID	Application ID
	RUM Session ID: ➤ Filter that was defined on the **Default RUM profile**.	➤ Filter display a list of the applications that were monitored by the specific RUM engine and that had alerts configured for them. **Note:** A default RUM profile option (hidden by default) can be displayed. It shows the **Default RUM profile** that was available by default in 8.0 and does no longer exist in 9.0 (unless you select **Admin** > **Platform** > **Infrastructure Settings** > **Applications** > **End User/System Availability Management**, and in the **End User/System Availability Management - Data** table, set the **Show legacy data in alert reports** option to **true**). The Filter might contain a legacy RUM configuration (RUM default profile). In order to be able to view it, set the **Show legacy data in alert reports** option to **true** as explained above.

Topics	BAC 8.x	BSM 9.x
Reports	Alert Log report	Alert Log report (report and filter automatically upgraded)
	Alert Count Over Time report	Alert Count Over Time report (report and filter automatically upgraded)
	Alert Count Summar report	Alert Count Summary report (report and filter automatically upgraded)
	Baseline Suggested Alerts Log report	Removed in 9.10
	Actual vs. Baseline Suggested Alerts report	Removed in 9.10
	Actual vs. Baseline Suggested Alerts - Detailed report	Removed in 9.10
Parameters in report's filters (automatically upgraded)	Profile	Configuration Item
	N/A	Recipients **Default:** All

Troubleshooting and Limitations

This section includes troubleshooting and limitations for the End User Management Administration upgrade of EUM Alerts.

➤ **Server name field is empty in Server events directly after the upgrade**

A Server event is upgraded to an Application event. If the event was filtered by server (Host CI), the upgrade adds the filter to the new event. If you display the event immediately after the upgrade and before Real User Monitor has sent any samples for this server, the server name filter field is empty. This is because BSM is trying to mach the server ID to all the servers that are linked to the application.

In BAC 8.x, the server CI was not linked to an application and the upgrade process does not create this link. In BSM 9.x, the Real User Monitor engine creates this link when it reports data for the server. Until such data is reported after the upgrade, the server name filter field is empty.

➤ **CI based alerts on RUM events are not upgraded**

Details of such alerts are logged by the upgrade process so that you can manually reconfigure them in the upgraded system.

CI Status and SLA Alerts Upgrade

The table describes what changed between the BAC 8.x and BSM 9.x versions, and describes how the upgrader handles the changes.

Topics	BAC 8.x	BSM 9.x
CI Status alerts that were defined on Monitor CIs are upgraded and moved to the parent CI (for example, the alert is moved from the BPM Monitor CI to the Business Transaction CI.		
CI Status alerts based on RUM events (not supported - removed during the upgrade)		
KPI identification was changed (automatically upgraded)	KPI Name	KPI Type

Topics	BAC 8.x	BSM 9.x
Action parameters (used for executable actions and for URLs) (automatically upgraded)	Trigger Time	Alert Trigger Time
	Previous Severity Description	Previous Status Name
	Next Severity Description	Current Status Name
	KPI Display Name	➤ KPI Name (for CI Status alerts) ➤ Tracking Period (for SLA alerts)
	Entity Name	➤ CI Name (for CI Status alerts) ➤ SLA Name (for SLA alerts)
	Entity Name	➤ CI Name (for CI Status alerts) ➤ SLA Name (for SLA alerts)
The **KPI Value** parameter of CI Status Alerts is automatically upgraded to the **Calculation Value** parameter.		
When a BPM adapter was configured to transaction\location mode in the previous version, after the upgrade Custom views are upgraded to Local Impact Views. The CI Status alerts that were defined for CIs in these views are not copied to the corresponding Local Impact Views and will not be accessible through these views.		

CI Status Alert Reports and Favorite Filter Upgrade

The table describes what changed between the BAC 8.x and BSM 9.x versions, and describes how the upgrader handles the changes.

Topics	BAC 8.x	BSM 9.x
KPI Names (changed - automatically upgraded)	KPI Names Favorite filters of CI Status Alert and SLA Alerts reports include lists of KPI names.	KPI Types. Favorite filters of CI Status Alert and SLA Alerts reports include lists of KPI types.
End User Monitor View (name was changed - automatically upgraded)	End User Monitor View listed in the report filter's list of views	End User Monitors is listed in the report filter's list of views