HP Business Availability Center

for the Windows and Solaris operating systems

Software Version: 8.01

Alerts

Document Release Date: March 2009
Software Release Date: March 2009

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.

Third-Party Web Sites

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

Copyright Notices

Trademark Notices

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

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

Java™ is a US trademark of Sun Microsystems, Inc.

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

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.

Unix® is a registered trademark of The Open Group.

Documentation Updates

This guide's title page 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

You can 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 Support Online 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 HP Software 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 find more information about access levels, go to:

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

To register for an HP Passport ID, go to:

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

Table of Contents

PART II: CI STATUS ALERTS

PART III: SLA STATUS ALERTS

PART IV: EVENT-BASED ALERTS

PART V: SEND ALERTS TO THIRD-PARTY APPLICATIONS

Welcome to This Guide

This guide describes how to manage CI Status alerts, SLA alerts, and event-based alerts, and how to send HP Business Availability Center alerts to the EMS console.

This chapter includes:

How This Guide Is Organized

The guide contains the following parts:

Part I Alerts and Recipients

Provides general information about the alerts, describes how to manage recipients, and how to automatically open events in Operations Manager, when a CI Status alert, SLA alert, or event-based alert is triggered in HP Business Availability Center.

Part II CI Status Alerts

Provides general information about the process of creating and maintaining CI Status alerts, and how HP Service Manager automatically opens incidents when a CI Status alert is triggered in HP Business Availability Center.

Part III SLA Status Alerts

Provides general information about the process of creating and maintaining SLA alerts.

Part IV Event-Based Alerts

Provides general information about the process of creating and maintaining event-based alerts, notification templates, and alert dependencies.

Part V Send Alerts to Third-Party Applications

Describes how to integrate HP Business Availability Center with different EMS applications, and how to send HP Business Availability Center alerts to the EMS console.

Who Should Read This Guide

This guide is intended for the following users of HP Business Availability Center:

- HP Business Availability Center administrators
- HP Business Availability Center application administrators
- HP Business Availability Center end users

Readers of this guide should be knowledgeable about navigating and using enterprise applications, and be familiar with HP Business Availability Center and enterprise monitoring and management concepts.

Getting More Information

For a complete list of all online documentation included with HP Business Availability Center, additional online resources, information on acquiring documentation updates, and typographical conventions used in this guide, see the the *HP Business Availability Center Deployment Guide* PDF.

Part I

Alerts and Recipients

1

Introducing Alerts

This chapter provides information on alerts.

This chapter includes:

Concepts

Tasks

Reference

Alerts Overview

HP Business Availability Center alerts proactively inform you when predefined performance limits are breached by sending alerts to predefined users. You can configure alerts for:

- **CIs in a view.** CI Status alerts are triggered by a pre-defined status change for the selected configuration item (CI) detected by the Business Logic Engine. For details, see "CI Status Alerts" on page 63.
- **SLAs.** SLA status alerts send notifications about changes to an SLA's Key Performance Indicator (KPI) status. For details, see "SLA Alerts" on page 217.
- **Event-based alerts.** Event-based alerts are triggered when pre-defined conditions, such as transaction response time, availability, success or failure, or completion time, are reached. For details, see "Event-Based Alerts" on page 251.

In each alert scheme, you define a unique set of alert properties. After you create an alert scheme, you view and edit it in the appropriate Alerts table. For detailed tips and guidelines, see "Tips for Creating Effective Alert Schemes" on page 17.

For a step-by-step process flow describing how to set up a system for delivering alerts to defined recipients, see "Set Up an Alert Delivery System – Workflow" on page 18.

Guaranteed Delivery of Alerts

If the HP Business Availability Center online components are experiencing downtime, HP Business Availability Center guarantees that the data is stored in the bus for one hour by default. After the components are back online, the Alerts engine generates alerts from data in the bus.

Alerts Administration and Application

You can use the Alerts Administration pages to configure the different types of alerts. You can use the Alerts application to view the alerts that were triggered during a specified time period.

This section includes the following topics:

Alerts Administration

To access the Alerts Administration pages select **Admin** > **Alerts**.

The Alert Administration includes the following tabs:

- **CI Status Alerts tab.** Enables you to specify the status change that triggers a CI Status alert. For details, see "CI Status Alerts" on page 63.

  You can automatically open events in HP Operations Manager (OM), when a CI Status alert is triggered in Business Availability Center. For details, see "Open Events in HP Operations Manager For Triggered Alerts" on page 47.

  HP Service Manager automatically opens incidents when a CI Status alert is triggered in Business Availability Center. For details, see "Open Incidents Using the CI Alert Retrieval Service" on page 129 or "Open an Incident in HP Service Manager Using the Legacy URL" on page 211.

- **SLA Alerts tab.** Enables you to specify the SLA's KPI status change that triggers an SLA alerts. For details, see "SLA Alerts" on page 217.

  You can automatically open events in OM, when an SLA alert is triggered in Business Availability Center. For details, see "Open Events in HP Operations Manager For Triggered Alerts" on page 47.

- **Event Based Alerts tab.** Enables you to specify the conditions, such as transaction response time, availability, success or failure, or completion time, that trigger an event-based alert when they are reached. For details, see "Event-Based Alerts" on page 251.

You can automatically open events in OM, when an event-based alert is triggered in Business Availability Center. For details, see "Open Events in HP Operations Manager For Triggered Alerts" on page 47.

- **Recipients tab.** Enables you to specify alert recipients. For each recipient, you can specify the notification method (any combination of email, pager, and/or SMS) and the template to use for alert notices. You can also create a notification schedule for the alerts. For details, see "Recipients Overview" on page 33.

Alerts Application

To access the Alerts application select **Application > Alerts.**

The Alerts application includes the following tabs:

- **CI Status Alerts Report tab.** Enables you to list all of the CI Status alert triggers that occurred during the specified time range. For details, see "Configuration Item Status Alerts Report" on page 109.
- **SLA Alerts Report tab.** Enables you to list all of the Service Level Management alert triggers that occurred during the specified time range. For details, see "SLA Status Alerts Report" on page 245.
- **Event-Based Alerts Report tab.** Enables you to access the following reports:
  - **Alert Log report.** Enables you to track all alert details for event-based alerts sent by HP Business Availability Center during the specified time range. For details, see "Alerts Log Report" on page 279.
  - **Baseline Suggested Alert Log report.** Enables you to track all alert details for event-based alerts that would be sent by HP Business Availability Center during the specified time range if you were using Baselining. For details, see "Baseline Suggested Alerts Log Report" on page 333.
  - **Alert Count Over Time report.** Enables you to display an overview of the frequency of alerts. For details, see "Alerts Count Over Time Report" on page 274.

- **Actual vs. Baseline Suggested Alert Comparison report.** Enables you to compare the actual alerts that were triggered by user-defined thresholds and the baselined suggested alerts that would be triggered during the specified time range. For details, see "Actual vs. Baseline Suggested Alerts Report" on page 272.
- **Actual vs. Baseline Suggested Alert Detailed Comparison report.** Enables you to view the details of the actual alerts that were triggered by user-defined thresholds and of the baselined alerts that would be triggered during the specified time range. For details, see "Actual vs. Baseline Suggested Alerts – Detailed Report" on page 269.

Tips for Creating Effective Alert Schemes

Before creating alert schemes, you should consider how to most effectively alert users to performance issues. The information described below can assist you with effective alert planning.

Note: HP Professional Services offers best practice consulting on this subject. For information on how to obtain this service, contact your HP representative.

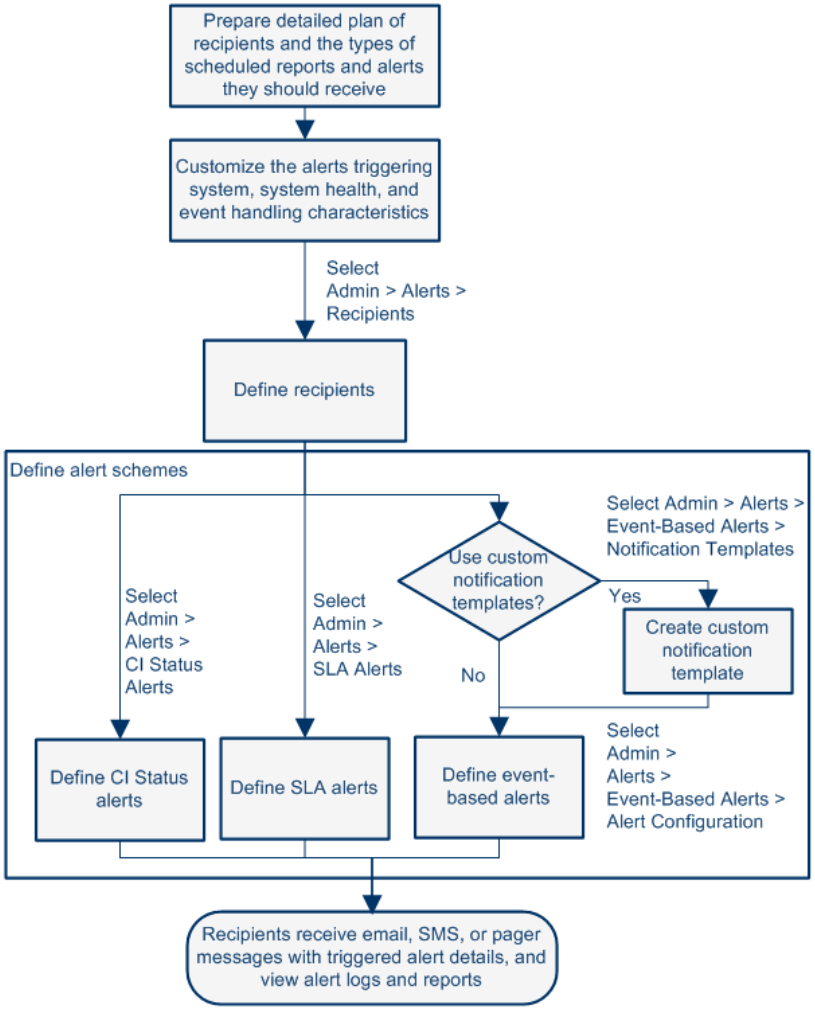
- When creating alert schemes, categorize alerts by severity. Create critical alerts for events that require immediate corrective action (for example, transaction failure, or excessive response times for critical transactions). Create non-critical alerts for events that require early notification (for example, slow response times).
- Determine the users that receive the different types of alerts, and consider the alert delivery method that best suits the alert type. For example, pager delivery as opposed to email delivery might be more effective for critical alerts. When determining the delivery method, take the time of day into account as well. For example, email alerts might not be effective during non-business hours.

- Set HP Business Availability Center to alert you to a recurring problem, not one-time events. Recurring alerts are the most accurate indicator of problems with your application. For example, as a rule, you should compare the number of recurring events to the number of Business Process Monitor locations from which you are monitoring. For example, if you had three failures, but you were monitoring from 100 locations, it would not be as critical as if you had five failures in all five locations.

Set Up an Alert Delivery System – Workflow

This task and the associated flowchart describe how to set up a system for delivering CI Status alerts, SLA alerts, or event-based alerts to recipients.

This task includes the following steps:


Prepare detailed plan of recipients and the types of scheduled reports and alerts they should receive
Customize the alerts triggering system, system health, and event handling characteristics
Select Admin > Alerts > Recipients
Define recipients
Define alert schemes
Select Admin > Alerts > Event-Based Alerts > Notification Templates
Use custom notification templates?
Yes
Create custom notification template
No
Select Admin > Alerts > CI Status Alerts
Select Admin > Alerts > SLA Alerts
Define CI Status alerts
Define SLA alerts
Define event-based alerts
Select Admin > Alerts > Event-Based Alerts > Alert Configuration
Recipients receive email, SMS, or pager messages with triggered alert details, and view alert logs and reports

1 Plan the Alert Recipient Requirements

It is recommended to:

- List the required recipients of alerts, including contact information and required delivery method to the recipient (email, SMS, pager). For suggestions on how to proceed, see "Tips for Creating Effective Alert Schemes" on page 17.
- Map out the types of alerts you plan to deliver. Alerts include CI Status alerts, SLA alerts, and/or Event-based alerts. For details on the types of alerts, see "Define the Alerts Schemes" on page 21.

For additional information about planning the alerts and recipients, see "Tips for Creating Effective Alert Schemes" on page 17.

2 Customize the Alerts Triggering System, System Health, and Event Handling Characteristics

Customize the alerts triggering system, system health, and event handling characteristics. For more information, see "Customize Alerts" on page 22.

3 Define Recipients

On the Recipients page, you define system recipients for alerts (except SiteScope alerts). You can specify email, SMS, or pager delivery methods. If required, enter specific alert delivery schedules (for example, recipients who receive alerts during business hours as opposed to evenings and weekends). For more information, see "Configure and Manage Recipients" on page 34.

4 Create Custom Notification Templates – Optional

If required, when defining event-based alerts, you have the option to create custom notification templates that customize the format and information included in alert emails. For more information, see "Configure Alerts Notification Templates" on page 387.

5 Define the Alerts Schemes

You can define the alert schemes you require:

➤ **CI Status Alerts**

Define CI Status alerts as required to alert recipients to KPI status changes for specific CIs and KPIs being monitored in Dashboard. For more information, see "Create a CI Status Alert Scheme and Attach it to a CI" on page 65.

➤ **SLA Alerts**

Define SLA alerts as required to alert recipients to changes in the current and forecasted status for service agreements. For more information, see "Define an SLA Alert Scheme" on page 218.

➤ **Event-Based Alerts**

Define event-based alerts as required to alert recipients to performance variance of Real User Monitor entities or Business Process Monitor transactions. For more information, see "Create Event-Based Alert Schemes – Workflow" on page 257.

6 Set Up to Open an Event in OM When an Alert is Triggered in Business Availability Center

You can set up to open events in OM when an alert is triggered in Business Availability Center. For details, see "Open an Event in Operations Manager When an Alert is Triggered" on page 49.

7 Set Up to Open Incidents in HP Service Manager Corresponding to CI Status Alerts Triggered in Business Availability Center

You can set up to open incidents in HP Service Manager that correspond to CI Status alerts triggered in Business Availability Center. For details, see "Open Incidents in HP Service Manager using the CI Alert Retrieval Service" on page 113.

8 Result

When an alert is triggered, the recipients receive the email, SMS, and Pager messages configured for the triggered alert. In addition, the triggered alerts are logged in the appropriate alert logs and reports. For details, see "Alerts Application" on page 16.

Customize Alerts

This section describes the customization you can perform for CI Status, SLM, and event-based alerts.

Note: All the steps in the task are optional and can be performed in any order.

This task includes the following steps:

- "Modify the Way Events are Handled" on page 23
- "Modify the Alerting System Health" on page 24
- "Modify the Alerts Triggering Defaults" on page 25

1 Modify the Way Events are Handled

To modify the way events are handled, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, select **Foundations**, scroll to the **Alerting - Event handling** area, and modify any of the following parameters:

Purpose	Parameter	Description
Specify the default delay for alerts	**Acceptable event delay (minutes)**	Modify the default delay (60 minutes) after which alerts are discarded.
Enable/disable calculation persistency	**Calculation persistency**	When calculation persistency is enabled, the calculated data, which existed before the system goes down, is taken into consideration in data calculations after the system goes up. Select **false** to disable calculation persistency and **true** to enable calculation persistency.

2 Modify the Alerting System Health

To modify the way events are handled, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, select **Foundations**, scroll to the **Alerting - System Health** area, and modify any of the following parameters:

Purpose	Parameter	Description
Specify when notification queue status changes to error	**Error threshold for the notification queue monitor**	Enter the maximum number of messages waiting in the alert queue of the notification queue monitor after which the notification queue monitor status changes to **error**.
Specify when notification queue status changes to warning	**Warning threshold for the notification queue monitor**	Enter the maximum number of messages waiting in the alert queue of the notification queue monitor after which the notification queue monitor status changes to **warning**.
Specify when alert queue status changes to error	**Error threshold for the alert queue monitor**	Enter the maximum number of messages waiting in the alert queue of the alert queue monitor after which the alert queue monitor status changes to **error**.
Specify when alert queue status changes to warning	**Warning threshold for the alert queue monitor**	Enter the maximum number of messages waiting in the alert queue of the alert queue monitor after which the alert queue monitor status changes to **warning**.

3 Modify the Alerts Triggering Defaults

To modify the way events are handled, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, select **Foundations**, scroll to the **Alerting - Triggered alerts** area, and modify any of the following parameters:

Purpose	Parameter	Description
Add year to notification messages	**Add year to notification message**	Select: ➤ **true** to add the year to the date in Email notifications. ➤ **false** to add the year to the date in Email notifications.
Modify the default sender used in emails	**Email sender**	Modify the default sender used in emails.
Modify the default sender email address used in emails	**Alerts email sender address**	Use the parameter to modify the default value (**HP_BAC_Alert_Manager**) that appears in the **From** field when HP Business Availability Center sends alerts is set when you install the Data Processing Server.

Purpose	Parameter	Description
Modify the primary and alternate SMTP server	**SMTP server** **SMTP server port** **Alternate SMTP server**	Both the primary and alternate SMTP server can be defined as either: ➤ **A designated server with a defined port number.** Enter a server name for sending SMTP emails as the value in the **SMTP server** or **Alternate SMTP server** field and enter a port number for the server in the **SMTP server port** or **Alternate SMTP server** field. ➤ **Microsoft's SMTP services.** Enter <SMTPSVC> as the value in the **SMTP server** or **Alternate SMTP server** field.
Modify the default timeout for an action	**Command line execution timeout (seconds)**	Use the parameter to modify the default timeout (30 seconds) after which a command line alert action is not executed.
Modify the default SNMP Trap host address	**Default SNMP Target Address** / **Default SNMP Port**	Modify the default SNMP trap host address, by entering the IP address or server name in the **Default SNMP Target Address** parameter, and the port number in the **Default SNMP Port** parameter. **Note to HP Software-as-a-Service customers:** You can set the default host address per customer by selecting a customer when you log in. The updated host address is defined only for the specific customer. You can also define a global host address.

Purpose	Parameter	Description
Reset the notification frequency timer	**Enable alert timer reset**	Select: ➤ **false.** (Default) An alert is triggered by a specific condition, then the condition that triggered the alert does not exist any more. If the condition that triggered the alert occurs again before the end of time period specified in the **Acceptable events delay** parameter ends, the alert is not sent. ➤ **true.** An alert is triggered by a specific condition, then the condition that triggered the alert does not exist any more. If the condition that triggered the alert occurs again before the end of time period specified in the **Acceptable events delay** parameter ends, the alert is sent because the trigger condition has reset the notification frequency timer.
Enable alert dependencies between profiles	**Enable cross profile alert dependencies**	Select: ➤ **false.** (Default) Alert dependencies are not allowed between profiles. ➤ **true.** Alert dependencies are allowed between profiles.

Purpose	Parameter	Description
Enable logging alerts and notifications in the Profile database	**Enable logging to DB**	**Note:** This customization is available only for event-based alerts. Select: ➤ **true.** (Default) Alerts and notifications are logged in the Profile database. ➤ **false.** Alerts and notifications are not logged in the Profile database.
Enable the alert engine to perform actions and send notifications	**Enable notifications and actions**	**Note:** This customization is available only for event-based alerts. Select: ➤ **true**. (Default) Actions are performed and notifications are sent by the alert engine. ➤ **false.** Actions are not performed and notifications are not sent to the user.
Specify the number of retries of a notification	**Notification execution retries**	**Note:** This customization is available only for event-based alerts. By default, a notification is sent once. Change the default using the **Notification execution retries** parameter. The number of retries that is performed equals the number you specify plus one.

Purpose	Parameter	Description
Modify the message's character set	**Email alerts charset** / **SMS alert charset** / **Pager alert charset**	When an alert is triggered, recipients for the generated alert can be notified by email, SMS, or pager messages. You can select one of the following character sets for emails, SMS, or pager messages separately: ➤ **UTF-8.** The default character set. ➤ **ISO-2022-JP**. **Note to HP Software-as-a-Service customers:** The settings described in this section are per customer.
Modify the timeout of an SMTP Server socket connection	**SMTP server socket connection timeout (seconds) (Windows)**	Use the parameter to modify the default timeout (60 seconds) after which an SMTP server socket is disconnected. This is for Windows operating systems only.
Modify the maximum length of an SNMP trap	**SMTP trap max length (bytes)**	Use the parameter to modify the default maximum length of an SNMP trap (in bytes).
Modify the waiting interval between retries	**Wait interval between retries (seconds)**	Use the parameter to modify the default waiting interval between notification retries.

Change the Default _FOLLOWUP String

This section describes the customization you can perform for CI Status alerts, SLA alerts, and event-based alerts.

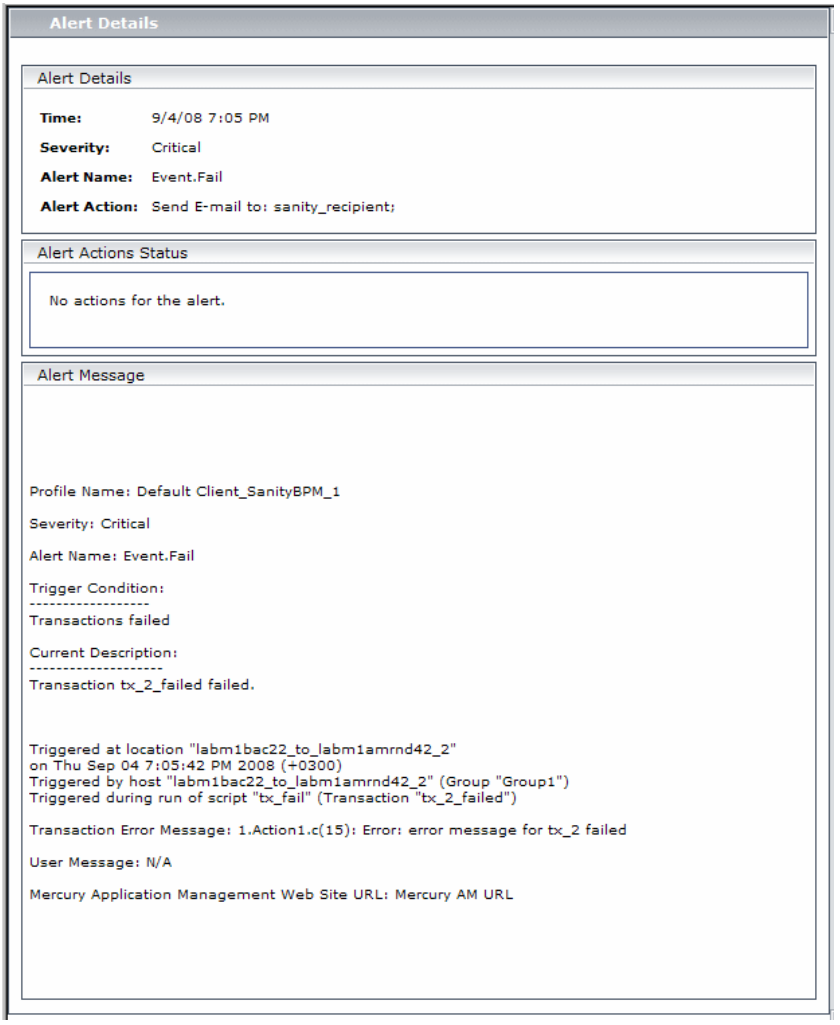
You can change the default string by selecting **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings** > **Foundation: Alerting**. Edit the **Followup notifications suffix** value and make sure to use the same string when creating a follow up template. For details on follow up templates, see "Configure a Template for Follow-up Notifications" on page 388.

Introducing Alerts User Interface

This section describes:

Alert Details Report

The following is an example of the Alert Details report.



Alert Details

Alert Details

Time: 9/4/08 7:05 PM

Severity: Critical

Alert Name: Event.Fail

Alert Action: Send E-mail to: sanity_recipient;

Alert Actions Status

No actions for the alert.

Alert Message

Profile Name: Default Client_SanityBPM_1

Severity: Critical

Alert Name: Event.Fail

Trigger Condition:

Transactions failed

Current Description:

Transaction tx_2_failed failed.

Triggered at location "labm1bac22_to_labm1amrnd42_2"
on Thu Sep 04 7:05:42 PM 2008 (+0300)
Triggered by host "labm1bac22_to_labm1amrnd42_2" (Group "Group1")
Triggered during run of script "tx_fail" (Transaction "tx_2_failed")

Transaction Error Message: 1.Action1.c(15): Error: error message for tx_2 failed

User Message: N/A

Mercury Application Management Web Site URL: Mercury AM URL

Description	Displays the triggering information that is available for the alert, including the actual conditions at the time of the alert. **To access:** Click  in the Configuration Item Status Alerts page, SLA Status Alerts page, Alerts Log or in the Baseline Suggested Alerts Log.
Important Information	For CI Status Alerts, see details about the Alert Details page in "Configuration Item Status Alert Notifications Report" on page 100. For SLA Status Alerts, see details about the Alert Details page in "SLM Alert Notifications Page" on page 243. For event-based alerts, see details about the Alert Details page in "Alert Wizard" on page 287.

Troubleshooting and Limitations

Forbidden Characters

The following characters are forbidden:

Where	Forbidden Characters
Alert name and alert description	' ~ ! @ # $ % ^ & * - + = [ ] { } \ | / ? . , " ' : ; < >
Recipient name	' ~ ! @ # $ % ^ & * - + = [ ] { } \ | / ? . , " ' : ; < >
Message sender name in alerts	' ~ ! # $ % ^ * _ - + = { } \ | / ? . ' <space>
SMTP server name in alerts	_ . -

2

Recipients

This chapter provides information on recipients.

This chapter includes:

Concepts

Tasks

Reference

Recipients Overview

Recipients receive information about the alerts that are triggered so they can take care of the problems that triggered the alerts.

For each recipient, you define one or more notification method, the template to use for alert notices, and a notification schedule.

You can define the following types of notification methods: email, pager, and SMS.

For details on where to configure and manage recipients, see "Recipients Page" on page 37.

Note: Only those recipients who have been configured to receive email can be selected to receive scheduled reports. These recipients are listed in Available Recipients when configuring scheduled reports.

Configure and Manage Recipients

You create recipients by defining one or more notification method, the template to use for alert notices, and a notification schedule. For details, see "Recipient Properties Wizard" on page 38.

You manage existing recipients in the Recipients page. For details, see "Recipients Page" on page 37.

Add a Custom Pager or SMS Service Provider

If your pager or SMS service provider does not appear on the default provider list, and the provider uses an email gateway, you can manually add your provider to HP Business Availability Center. After doing so, your provider appears on the list.

To add a provider that uses an email gateway, manually add the gateway information to the management database. If necessary, ask your database administrator for assistance.

To add a provider that uses an email gateway:

1. Open the **NOTIFICATION_PROVIDERS** table in the management database.
2. In the **NP_NOTIFICATION_PROVIDER_NAME** column, add the name of the provider to the bottom of the list.

   Add the name exactly as you want it to appear in the provider list that opens in the SMS tab of the Recipient Properties wizard. For details, see "SMS Tab" on page 45.

   Note the ID number that is automatically assigned to the provider.
3. Close the **NOTIFICATION_PROVIDERS** table, and open the **NOTIFPROVIDER_NOTIFTYPE** table.
4. In the **NN_NOTIF_PROVIDER_ID** column, add the ID number that was assigned to the new provider in step 2 on page 35.
5. In the **NN_NOTIF_TYPE_ID** column, assign the provider one of the following notification types:
   - **102** – for pager service provider
   - **101** – for SMS service provider
6. Close the **NOTIFPROVIDER_NOTIFTYPE** table, and open the **NOTIFICATION_PROVIDER_PROP** table.
7. In the **NPP_NOTIFICATION_PROVIDER_ID** column, add the ID number that was assigned to the new provider in step 2 on page 35.

   Note that you add the ID number to two consecutive rows.

8 In the **NPP_NPROVIDER_PROP_NAME** and **NPP_NPROVIDER_PROP_VALUE** columns, add the following new property names and values for the provider, one beneath the other (for examples, see existing entries):

Property Name	Property Value	Description
EMAIL_SUFFIX	<email_suffix>	The gateway's email suffix. For example, if the gateway email address is 12345@xyz.com, enter xyz.com as the property value for EMAIL_SUFFIX.
EMAIL_MAX_LEN	<max_length>	The maximum message length, in characters, of the body of the email message. For example, 500. When determining this value, take into consideration the maximum length limit imposed by your service provider, as well as limitations to your pager or mobile phone.

9 In the **NPP_NPROVIDER_PROP_DATATYPE_ID** column, specify an ID value as follows:

- for EMAIL_SUFFIX, specify: 1
- for EMAIL_MAX_LEN, specify: 2

10 Restart HP Business Availability Center.

Recipients User Interface

This section describes:

Recipients Page

Description	Enables you to create new recipients or edit the properties of existing recipients. **To access:** Select **Admin** > **Alerts** > **Recipients**
Included in Tasks	"Configure and Manage Recipients" on page 34

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Click the button beside the recipient whose properties you want to modify. The Recipient Properties wizard opens. For details, see "Recipient Properties Wizard" on page 38.
<check box>	Select when you want to perform the same action on several recipients simultaneously.
Email	The email address of the recipient. **Note:** The text displayed in email messages can only be in English except for the contents of fields inserted by the user that can be in any supported and relevant language. Those fields can be for example: Alert Name, Alert description, KPI name, and so on.
New Recipient	Click the **New Recipient** button to define a new recipient. For details, see "Recipient Properties Wizard" on page 38.
Pager	The pager of the recipient. **Note:** The text displayed in pager messages can only be in English except for the contents of fields inserted by the user that can be in any supported and relevant language. Those fields can be for example: Alert Name, Alert description, KPI name, and so on.

GUI Element (A-Z)	Description
Recipient Name	The provider and number of the recipient.
SMS	The SMS provider and telephone number of the recipient.

Recipient Properties Wizard

Description	Enables you to define recipients and how notices are sent to those recipients in the Recipients page of Platform Administration. **To access:** Select **Admin > Alerts > Recipients**
Included in Tasks	"Configure and Manage Recipients" on page 34
Wizard Map	**Recipient Properties Wizard**: General Tab > Email Tab > Pager Tab > SMS Tab

General Tab

Description	Enables you to define a recipient general properties.
Wizard Map	Recipient Properties Wizard: **General Tab** > Email Tab > Pager Tab > SMS Tab

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Alert Notification Template	**Note:** This field is relevant only for event-based alerts. Select an alert notification template: ➤ **Per notification method** if you want the recipient's alert notification template to differ for each notification method; for example, if you want to use the LONG template for email alerts and the SHORT template for pager alerts. ➤ **Same for all** if you want the recipient's alert notification template to be identical for all notification methods. Choose **LONG**, **SHORT**, or any custom template already created. For details on alert notification templates and creating custom templates, see "Notification Templates Page" on page 394. **Note:** You must select the alert notification template and specify an alert notices schedule for alert recipients. You do not have to perform this procedure for recipients who are to receive only scheduled reports.

GUI Element (A-Z)	Description
Offset from GMT	Select the time zone according to which HP Business Availability Center sends alert notices and HP Software-as-a-Service notifications to the selected recipient. The GMT offset selected for the recipient is the time zone specified in the alert notifications that the recipient receives. For example, if an alert is triggered anywhere in the world and a notification is sent, the date and time of the alert is converted to the time zone in the GMT offset selected for the recipient. If you defined a notification schedule for the recipient, the GMT offset selected for the recipient is also the time zone that HP Business Availability Center uses for calculating when to send the recipient notifications. For example, if you configure a recipient to receive pager alerts from 9:00 AM - 9:00 PM, and choose a GMT offset of -5 hours, the recipient receives alerts through a pager only from 9:00 AM - 9:00 PM Eastern Time. **Note:** Scheduled reports are sent based on the schedule configured in the Scheduled Reports page and not on the schedule configured for the recipient. For details, see "Create a Schedule" in *Reports*. For a reference list of GMT time zones for locations throughout the world, see "GMT Time Zones" in *Reference Information*.
Recipient Name	The name of the recipient.

GUI Element (A-Z)	Description
Schedule for Receiving Alerts	Specify a schedule for receiving notifications. The schedule enables you to control exactly at which hours of the day a recipient receives notices. Select: ➤ **Per notification method.** If you want the recipient's schedule to differ for each notification method. For example, a recipient may want to receive notices through email from 9:00 AM to 5:00 PM, and through a pager from 5:00 PM to 7:00 PM. ➤ **Same for all.** If you want the recipient's schedule to be identical for all notification methods. Select also one of the following: ➤ **All Day.** To send messages any time of the day. ➤ **From... to.** To send messages only during the specified time of day.

Email Tab

Description	Enables you to specify multiple email addresses for the recipient, the type of notification template, the schedule for sending email notifications, and the security certificate if necessary.
Important Information	Only those recipients who have been configured to receive email can be selected to receive scheduled reports and are listed in Available Recipients when configuring scheduled reports. **Note:** The text displayed in email messages can only be in English except for the contents of fields inserted by the user that can be in any supported and relevant language. Those fields can be for example: Alert Name, Alert description, KPI name, and so on.
Wizard Map	Recipient Properties Wizard: General Tab > **Email Tab** > Pager Tab > SMS Tab

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Address(es)	Enter one or more email addresses. Separate multiple entries with a semi-colon (;).
Alert Notification Template	Enabled if you selected the **Per notification method** alert notification template option for the recipient in the **Alert Notification Template** in the General tab. Select the template you want to use: **LONG**, **SHORT**, or any custom template already created. For details on alert notification templates and creating custom templates, see "Configure Alerts Notification Templates" on page 387.
Schedule for Receiving Alerts	Enabled if you selected the **Per notification method** scheduling option for the recipient in the **Schedule for Receiving Alerts** in the General tab. Select: ➤ **All Day.** If you want the recipient to receive email messages all day. ➤ **From... to.** If you want the recipient to receive email messages during the specified time period. The time range is calculated based on the GMT offset selected for the recipient. Scheduled reports are sent based on the schedule configured in the Scheduled Reports page and not on the schedule configured for the recipient. For details, see "Create a Schedule" in *Reports*.

GUI Element (A-Z)	Description
Secure Mail	Select **Enabled** if you want the recipient to receive encrypted mail. You must then copy, into the text box, the contents of the certificate that the recipient used to secure incoming email messages. **Note:** ➤ The encrypted mail option is supported only for alerts. Encrypted mail is not supported for scheduled reports or subscription and package notifications (HP Software-as-a-Service customers only). ➤ The encrypted mail option is supported only when the HP Business Availability Center Data Processing Server is installed on a Windows machine.

Pager Tab

Description	Enables you to specify the pager service provider, the pager numbers, the type of notification template, and the schedule for sending alert notification to the pager.
Important Information	You can use a pager service provider that does not appear on the default list. To do so, you define a custom pager service provider email gateway or create a custom pager service provider script using the Virtual User Generator (VuGen). You then add the new provider to the database. For details, see “Add a Custom Pager or SMS Service Provider” on page 34. **Note:** The text displayed in pager messages can only be in English except for the contents of fields inserted by the user that can be in any supported and relevant language. Those fields can be for example: Alert Name, Alert description, KPI name, and so on.
Wizard Map	Recipient Properties Wizard: General Tab > Email Tab > **Pager Tab** > SMS Tab

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Alert Notification Template	If you selected the **Per notification method** alert notification template option for the recipient, choose the template you want to use. Choose **LONG**, **SHORT**, or any custom template already created. For details on alert notification templates and creating custom templates, see "Configure Alerts Notification Templates" on page 387.
Number(s)	Enter one or more pager access numbers. Separate multiple entries with a semi-colon (;).
Schedule for Receiving Alerts	If you selected the **Per notification method** scheduling option for the recipient, choose whether you want the recipient to receive pager messages all day, or only between the specified time range.
Type	Select a pager service provider. The following providers are supported: ➤ **MetroCall** ➤ **PageNet** ➤ **PageOne** ➤ **PageMci** ➤ **Arch** ➤ **Nextel** ➤ **PageMart** ➤ **AmeriPage** ➤ **btpaging** ➤ **Att** ➤ **SkyTel** ➤ **AirTouch**

SMS Tab

Description	Enables you to specify the SMS (short message service) service provider, the SMS numbers, the type of notification template and the schedule for sending alert notification to the SMS.
Important Information	SMS is a text messaging service provided by most GSM-based cellular phone providers. SMS messages are useful to notify staff who are mobile, or who do not have email or pager access. Note that the maximum message length of SMS text messages is generally 160 characters.
Wizard Map	Recipient Properties Wizard: General Tab > Email Tab > Pager Tab > **SMS Tab**

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Alert Notification Template	If you selected the **Per notification method** alert notification template option for the recipient, choose the template you want to use. Choose **LONG**, **SHORT**, or any custom template already created. For details on alert notification templates and creating custom templates, see “Configure Alerts Notification Templates” on page 387.
Number(s)	Type one or more SMS access numbers in the box. Separate multiple entries with a semi-colon (;).

GUI Element (A-Z)	Description
Provider	Select an SMS service provider from the list. If your provider does not appear on the default provider list, and the provider uses an email gateway, you can manually add your provider to HP Business Availability Center. For details, see "Add a Custom Pager or SMS Service Provider" on page 34.
Schedule for Receiving Alerts	If you selected the **Per notification method** scheduling option for the recipient, choose whether you want the recipient to receive SMS messages all day, or only between the specified time range.

3

Open Events in HP Operations Manager For Triggered Alerts

This chapter provides information on opening events in HP Operations Manager (OM) when alerts are triggered in HP Business Availability Center.

This chapter includes:

Concepts

Tasks

Reference

Events Opened in Operations Manager by An Alert – Overview

You can automatically open an event in Operations Manager when a CI Status alert, SLA Status alert, or an event-based alert is triggered and the appropriate settings in the Integrations with other applications - HP Operations Manager (OM) table in the Infrastructure Settings.

Data about the alert is passed to Operations Manager and used to open events. Each type of alert is identified with a different set of parameters:

- CI/SLA alerts: <alert name> <CI Id/SLA Id> <event severity>.
- Event based alerts:
  - Business Process Monitor - <alert name> <event severity> <profile name> <transaction name> (if it exists).
  - RUM Transaction Alerts - <alert name> <severity> <transaction name>.
  - RUM Page Alerts - <alert name> <severity> <page name>.
  - RUM server alerts - <alert name> <severity> <server name>.

A event previously opened is updated with new alert data when an alert is triggered with the same identifying information. Two alerts are considered duplicated when their identifiers have the same values. Depending on the configuration in Operations Manager, two separate events are opened or the counter of the corresponding open event increases by one.

The event is opened in Operations Manager using a web service provided by Operations Manager, after Business Availability Center sends data to Operations Manager using the Operations Manager web service. The web service listens to the data coming from Business Availability Center and creates the events on Operations Manager and then returns the event ID to Business Availability Center.

In Operations Manager, you can keep track of the system status and handling. You can also validate and monitor the alert by looking at the events related to the alert.

For details on how to automatically create an event in Operations Manager, see “Open an Event in Operations Manager When an Alert is Triggered” on page 49.

An event previously opened is updated with new alert data when an alert is triggered with the same identifying information, if Operations Manager is configured to update it events, otherwise a new event is opened and the previous event is not modified.

How Events are Opened in Operations Manager

Infrastructure settings specify how events are opened in Operations Manager when alerts are triggered in Business Availability Center. When communication is enabled between Operations Manager and Business Availability Center (**Enable OM** is set to **true**), and an alert is triggered, the type of alert is checked against the value of the **Enable Events From CI Status Alerts**, **Enable Events From Event-Based Alerts**, **Enable Events From SLM Alerts** parameters. If the corresponding parameter is set to **true,** the creation of Operations Manager events is enabled, a mapping between the alert properties and the Operations Manager event properties takes place. The mapping includes the translation of alert's severity scale into the Operations Manager event's severity scale. An Operations Manager event with the relevant alert data such as CI name for CI Status alerts and SLA Status alerts or transaction name and CI ID for event-based alerts, is sent to the Operations Manager web service. An event is created by the Operations Manager application. The event ID is sent back to the Business Availability Center application.

For details on how to perform this task, see "Set Up the Parameters Related to Opening Events in Operations Manager" on page 50.

Open an Event in Operations Manager When an Alert is Triggered

To automatically open an event in Operations Manager when an alert is triggered, follow the steps described in this section.

The event is opened in Operations Manager using a web service provided by Operations Manager, after Business Availability Center sends data to Operations Manager using the Operations Manager web service.

For details on the mechanism used to open an event in Operations Manager when an alert is triggered, see "Events Opened in Operations Manager by An Alert – Overview" on page 48.

This task includes the following steps:

- "Set Up the Parameters Related to Opening Events in Operations Manager" on page 50
- "Define the Alerts That Open Events in Operations Manager" on page 53
- "Modify the Severity Mapping – Optional" on page 53
- "View the Triggered Alerts in the Reports" on page 53

1 Set Up the Parameters Related to Opening Events in Operations Manager

Infrastructure settings specify how events are opened in Operations Manager when alerts are triggered in Business Availability Center. For details on this topic, see "How Events are Opened in Operations Manager" on page 49.

To set up the parameters used to specify the host where Operations Manager is installed, the type of alert for which you want to send data to Operations Manager, and other parameters needed for opening events in Operations Manager, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, choose **Foundations**, select **Integration with other applications**, and enter the appropriate values for the parameters of the Integrations with other applications - HP Operations Manager (OM) table:

Parameter (A - Z)	Description
Emitting Node	A property of the Operations Manager application that determines the view where events are displayed.
Enable Events From CI Status Alerts	Set to **true** to enable the creation of events when CI Status alerts are triggered. **Note:** The change takes place immediately.

Parameter (A - Z)	Description
Enable Events From Event-Based Alerts	Set to **true** to enable the creation of events when event-based alerts are triggered. **Note:** The change takes place immediately.
Enable Events From SLM Alerts	Set to **true** to enable the creation of events when SLM alerts are triggered. **Note:** The change takes place immediately.
Enable OM	Set to **true** to enable the capability to open events in Operations Manager when alerts are triggered in Business Availability Center. **Note:** The change takes place immediately.
Enable OM In Staging Mode	Set to **true** to enable the capability to open events in Operations Manager when alerts are triggered in Business Availability Center, during staging. **Note:** The change takes place immediately.
Enable passing CI's Reports Links	Specifies whether to pass the links to the Business Availability Center reports associated with the alert.
Enable SSL Mode	Set to **true** to enable a secure connection to the Operations Manager host. **Note:** The change takes place immediately.
Number of Retries	Specify the number of retries to connect from Business Availability Center to the Operations Manager server. **Default:** 4. **Note:** The change takes place immediately.
OM Host Name	Specify the name of the host where the Operations Manager application is located. **Note:** The value of this setting is retrieved from the settings of the integration between Operations Manager and Business Availability Center. A manually specified parameter overrides the value retrieved from the integration settings. **Default:** 16.59.42.86

Parameter (A - Z)	Description
OM Password	Specify the password to use when connecting to the Operations Manager application. **Note:** The value of this setting is retrieved from the settings of the integration between Operations Manager and Business Availability Center. A manually specified parameter overrides the value retrieved from the integration settings.
OM Port	Specify the port of the host of the Operations Manager application. **Note:** The value of this setting is retrieved from the settings of the integration between Operations Manager and Business Availability Center. A manually specified parameter overrides the value retrieved from the integration settings. **Default:** 443
OM User Name	Specify the user name to use when connecting to the Operations Manager application. **Note:** The value of this setting is retrieved from the settings of the integration between Operations Manager and Business Availability Center. A manually specified parameter overrides the value retrieved from the integration settings. **Default:** Administrator
Severity Map	Specify the mapping between the alerts severity and the Operations Manager events severity. When you click the **Edit** button  the Edit Setting dialog box opens where you map Business Availability Center severities to Operations Manager severities. For details, see "Mapping Business Availability Center Severities to Operations Manager Severities" on page 54.

2 Define the Alerts That Open Events in Operations Manager

You can use existing alerts or create new alerts to open events in Operations Manager.

The alerts open events only when **Enable OM** is set to **true**, and the appropriate parameter (**Enable Events From CI Status Alerts**, **Enable Events From Event-Based Alerts**, **Enable Events From SLM Alerts**) corresponding to the type of alert is also set to **true**.

For details about creating alert schemes or managing existing alert schemes, see "Set Up an Alert Delivery System – Workflow" on page 18.

3 Modify the Severity Mapping – Optional

To modify the severity mapping, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **Integration with other applications**, and modify the severity mapping in the XML file corresponding to the **Severity Map** parameter in the Integrations with other applications - HP Operations Manager (OM) table. For details about the contents of the XML file, see "Mapping Business Availability Center Severities to Operations Manager Severities" on page 54.

4 View the Triggered Alerts in the Reports

You can view the alerts that opened an event in Operations Manager:

- In the Configuration Item Status Alerts report for a CI Status alert. For details, see "Configuration Item Status Alerts Report" on page 109.
- In the Alerts Log report and in the Alert Details report for an event-based alert. For details, see "Alerts Log Report" on page 279 and in the "Alert Details Report" on page 31.
- In the SLA Status Alerts report for an SLA status alert. For details, see "SLA Status Alerts Report" on page 245.

Mapping Business Availability Center Severities to Operations Manager Severities

The mapping of Business Availability Center statuses to Operations Manager severities is specified in the XML file corresponding to the **Severity Map** parameter in the Integrations with other applications - HP Operations Manager (OM) table. For details, see "Modify the Severity Mapping – Optional" on page 53.

```
<map>
   <EVENT alert_severity="OK" om_severity="Normal"/>
   <EVENT alert_severity="Warning" om_severity="Warning"/>
   <EVENT alert_severity="Minor" om_severity="Minor"/>
   <EVENT alert_severity="Major" om_severity="Major"/>
   <EVENT alert_severity="Critical" om_severity="Critical"/>

   <DASHBOARD alert_severity="warning" om_severity="Warning"/>
   <DASHBOARD alert_severity="minor" om_severity="Minor"/>
   <DASHBOARD alert_severity="major" om_severity="Major"/>
   <DASHBOARD alert_severity="critical" om_severity="Critical"/>
   <DASHBOARD alert_severity="ok" om_severity="Normal"/>
   <DASHBOARD alert_severity="uninitialized" om_severity="Unknown"/>
   <DASHBOARD alert_severity="info" om_severity="Unknown"/>
   <DASHBOARD alert_severity="stop" om_severity="Unknown"/>
   <DASHBOARD alert_severity="nodata" om_severity="Unknown"/>
   <DASHBOARD alert_severity="downtime" om_severity="Normal"/>

   <SLM alert_severity="exceeded" om_severity="Normal"/>
   <SLM alert_severity="met" om_severity="Warning"/>
   <SLM alert_severity="minor_breached" om_severity="Minor"/>
   <SLM alert_severity="breached" om_severity="Major"/>
   <SLM alert_severity="failed" om_severity="Critical"/>
   <SLM alert_severity="uninitialized" om_severity="Unknown"/>
   <SLM alert_severity="info" om_severity="Unknown"/>
   <SLM alert_severity="stop" om_severity="Unknown"/>
   <SLM alert_severity="nodata" om_severity="Unknown"/>
   <SLM alert_severity="downtime" om_severity="Normal"/>

</map>
```

where:

- **EVENT alert_severity** represents the severity of the event-based alerts.
- **DASHBOARD alert_severity** represents the severity of the CI Status alerts.
- **SLM alert_severity** represents the severity of the SLM alerts.
- **om_severity** represents the severity of the Operations Manager events.

Mapping of Properties

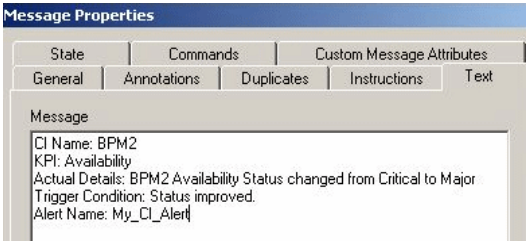
This section provides the event mapping of Operations Manager fields and Business Availability Center fields for CI Status alerts, SLA Status alerts, and event-based alerts.

This section includes the following topics:

Properties Mapping for CI Status Alerts

Operations Manager Event Field (A-Z)	Business Availability Center Alert Field
AffectedCI	Internal to Operations Manager
Alert Type (Custom Attribute)	The type of alert. **Example:** CI status alert
Application	Business Availability Center name **Example:** Business Availability Center
AssignedOperator	Internal to Operations Manager
Category(Message group)	The type of alert. **Example:** CI Status Alert
CollaborationMode	Internal to Operations Manager

Operations Manager Event Field (A-Z)	Business Availability Center Alert Field
Correlation key (Message Key)	<alert name> - <CI Id> - <severity> **Example:** My_alert - 701df092e6fdd106182297d763a2d342- Major
Creation Time	Triggered time
Customer Id (Custom attribute)	The customer Id.
Description	The user's description of the alert. **Example:** Trigger when CI...
EmittingCI	Internal to Operations Manager
IncidentID	Internal to Operations Manager
LifecycleState	Internal to Operations Manager
Message Type	The name of the KPI.
Primary Node Name (EmittingNode)	The URL of the Business Availability Center's Processing Machine. **Example:** scdam012.devlab.ad
PrimaryAssignmentGroup	Internal to Operations Manager
ProblemType	Internal to Operations Manager
ProductType	Internal to Operations Manager
RequesterReference	Internal to Operations Manager
Service Id	UCMDB: <CI ID> **Example:** UCMDB: 701df092e6fdd106182297d763a2d342
Severity	The alert status from Business Availability Center. The Business Availability Center alert status is mapped to an Operations Manager severity. For details, see "Mapping Business Availability Center Severities to Operations Manager Severities" on page 54.

Operations Manager Event Field (A-Z)	Business Availability Center Alert Field
Solution	Internal to Operations Manager
Source Type (Custom Attribute)	Source application. When the source is Business Availability Center, the value is **Business Availability Center**.
SubCategory	Not Mapped
Title	<CI name> <KPI name> <actual details> <triggering condition> <alert name>. **Example:** 

Properties Mapping for SLA Status Alerts

Operations Manager Event Field	Business Availability Center Alert Field
AffectedCI	Internal to Operations Manager
AssignedOperator	Internal to Operations Manager
Category	The type of alert. **Example:** SLA Status Alert
CollaborationMode	Internal to Operations Manager

Operations Manager Event Field	Business Availability Center Alert Field
Description	The user's description of the alert. **Example:** Trigger when an agreement is broken
EmittingCI	Internal to Operations Manager
EmittingNode	The CI Id. **Example:** 701df092e6fdd106182297d763a2d342
IncidentID	Internal to Operations Manager
LifecycleState	Internal to Operations Manager
ProblemType	Internal to Operations Manager
ProductType	Internal to Operations Manager
RequesterReference	Internal to Operations Manager
Severity	The next severity. **Example:** 15 (require translation for Operations Manager severities)
Solution	Internal to Operations Manager
SubCategory	Internal to Operations Manager
Title	<CI name> <KPI name> <actual details> <trigger condition> <alert name>
Type	The name of the KPI.

Properties Mapping for Event-based Status Alerts

Operations Manager Event Field (A-Z)	Business Availability Center Alert Field
AffectedCI	Internal to Operations Manager
Alert Type (Custom Attribute)	The alert type. **Example:** Event Based Alert
Application	The name of Business Availability Center. **Example:** Business Availability Center
AssignedOperator	Internal to Operations Manager
Category	The type of alert. **Example:** Event-based Alert
CollaborationMode	Internal to Operations Manager
Correlation key (Message Key)	Depend on the alert type (RUM/BPM). In general it is: <alert name> <severity> <profile name> <transaction name (if it exists)>.
Creation Time	Triggered time
Customer Id (Custom attribute)	The customer Id.
Description	The user's description of the alert. **Example:** Trigger when performance demands were not met
EmittingCI	Internal to Operations Manager
IncidentID	Internal to Operations Manager
LifecycleState	Internal to Operations Manager
Primary Node Name (EmittingNode)	The URL of the Business Availability Center Processing Machine **Example:** scdam012.devlab.ad
PrimaryAssignmentGroup	Internal to Operations Manager

Operations Manager Event Field (A-Z)	Business Availability Center Alert Field
ProblemType	Internal to Operations Manager
ProductType	Internal to Operations Manager
RequesterReference	Internal to Operations Manager
Severity	The severity of the alert. **Example:** 40 (need translation)
Solution	Internal to Operations Manager
Source Type (Custom Attribute)	The alert subcategory: ➤ HP BPM (for Business Process Monitor alert) ➤ HP RUM (for Real User Monitor alerts) ➤ HP SLM (for Service Level Management alerts)
SubCategory	The alert subcategory. It can be: ➤ BPM ➤ RUM server ➤ RUM transactions ➤ RUM pages
Title	<transaction name> <actual details> <trigger condition> <alert name>
Type	The name of the KPI.

Part II

CI Status Alerts

4

CI Status Alerts

This chapter provides information on CI Status alerts.

This chapter includes:

Concepts

Tasks

Reference

CI Status Alerts Overview

CI Status alerts are triggered by a pre-defined status change for the selected CI, detected by the Business Logic Engine.

To create CI Status alert schemes access the tab, select **Admin** > **Alerts** > **CI Status Alerts**. You can:

- Create a CI Status alert scheme and attach it to a CI in a view. The decision to send an alert is handled by the rules attached to the CI's KPIs. The alert engine sends alert messages (notifications) to the recipients, and executes the actions and executable files defined for the alert.
- Define the CI Status alert to apply to a specific KPI or to all the KPIs attached to the CI, so that any change to the status of one KPI triggers the alert. For details, see "Related Configuration Items Page" on page 80.
- Attach more than one CI Status alert to a CI.
- Send the same CI Status alert notification to different recipients according to the CI status. For details, see "Recipients" on page 33.
- Share the same CI Status alert scheme definition between several CIs. For details, see "Related Configuration Items Page" on page 80.

To view the CI Status alerts that have been triggered by the pre-defined status change for the selected CI, select **Application** > **Alerts** > **CI Status Alerts**.

Any changes you make to the alert schemes for a CI—adding new alert schemes, deleting alert schemes, or editing alert scheme properties— is propagated to any view that includes the CI.

When an alert is triggered, it sends a predefined notification (with email, SMS, or Pager) to a predefined recipient, or triggers a predefined action (exe file, URL, or SMNP trap). Whenever a notification is sent, information related to the notification is logged into the profile database. You can view the log in the Alert report. For details, see "Configuration Item Status Alerts Report" on page 109.

You can also open incidents in HP Service Manager when a specified CI Status Alert is triggered. For details, see "Opening Incidents in HP Service Manager – Overview" on page 114.

You can automatically open events in HP Operations Manager (OM), when a CI Status alert is triggered in Business Availability Center. For details, see "Open Events in HP Operations Manager For Triggered Alerts" on page 47.

One CI alert can be defined for several CIs. If one of those CIs is deleted then the CI is not part of the alert any more. If a CI alert is based on one CI only, then if the CI is deleted, the CI alert is also deleted.

Create a CI Status Alert Scheme and Attach it to a CI

You can create new alert schemes and attach them to any CI. You can attach more than one alert scheme to a CI. You can also attach the same alert scheme to more than one CI.

An alert attached to a CI in a view is attached to the CI in any view where the CI is included.

This task includes the following steps:

- "Create an Alert Scheme" on page 66
- "Add a CIT's Additional Parameters to a CI Status Alert – Optional" on page 66
- "Customize the Alert System – Optional" on page 67
- "Set Up CI Status Alerts Triggered by Downtime Status" on page 67
- "Administer the Alert Schemes" on page 68
- "Schedule the Configuration Item Status Alerts Report – Optional" on page 68
- "Open Incidents in HP Service Manager or in HP ServiceCenter Corresponding to CI Status Alerts Triggered in Business Availability Center" on page 68
- "Open Events in HP Operations Manager When an Alert is Triggered in Business Availability Center" on page 69
- "Results" on page 69

1 Create an Alert Scheme

Attach an alert scheme to a CI using the Create New Alerts wizard where you specify:

- The alert general information including the triggering conditions.
- The CIs and KPIs to which you want to attach to the alert scheme.
- The alert recipients and templates.
- The user-defined alert handlers (actions) that are triggered by the alert.

To access the wizard, select **Admin** > **Alerts** > **CI Status Alerts**, and click **New Alert**. For details on the Alerts wizard, see "Create New Alert Wizard" on page 76.

You can create a notification URL to attach to an alert. This notification URL is used to pass alert information to external systems, such as a customer Web application. For details, see "Specify a Notification URL" on page 71.

You can create an executable file to write information in special logs or to insert information into external databases. For details, see "Create an Executable Notification File" on page 73.

2 Add a CIT's Additional Parameters to a CI Status Alert – Optional

---

Note to HP Software-as-a-Service customers: This capability is not available for HP Software-as-a-Service customers.

If you create a new CIT, you can add the CIT's Additional Parameters to a CI Status Alert. For details, see "Configuration Item Status Alert Notifications Report" on page 100.

To add additional parameters to a CIT:

a Recommended. Save the original package under a different name before modifying the original package.

b Open the <**CIT_package**>**.zip** file at the following location: <**uCMDB Data Processing Server root directory**>**\mamlib\packages** or at the location where the CIT package is located.

c Open the <**CIT**>**.xml** file, locate the parameter you want to display, and add the following line between the <**Attribute-Qualifiers**> tags: <**Attribute-Qualifier name**="**ALERT_NOTIFICATION_ATTRIBUTE**"/>

d Save and re-deploy the package.

Example

For example, add the line as follows:

```
<Attribute name="database_dbversion" display-name="Version" description="The
database version" type="string" size="25">
 <Attribute>
      <Attribute-Qualifiers>
           <Attribute-Qualifier name="ALERT_NOTIFICATION_ATTRIBUTE"/>
      </Attribute-Qualifiers>
 </Attribute>
```

3 Customize the Alert System – Optional

You can customize some features of the Alerts application. For details, see "Introducing Alerts" on page 13 in the **Customization** section. After you complete defining an alert scheme, it is listed in the CI Status Alerts tab.

4 Set Up CI Status Alerts Triggered by Downtime Status

Downtime events are configured only on profiles (Business Process Monitor and SiteScope). When you configure a CI Status alert scheme for CIs that match a Business Process Monitor or SiteScope profile, you get the downtime functionality for CI Status alerts.

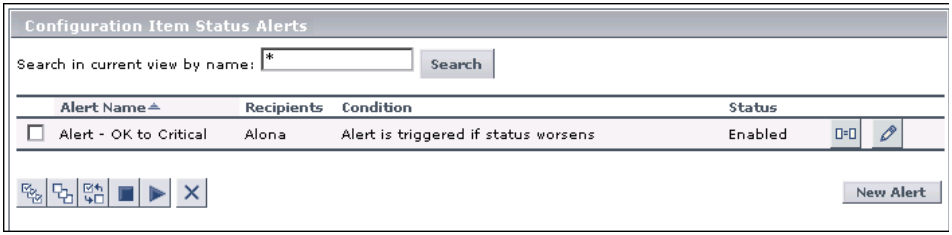
5 Administer the Alert Schemes

In the CI Status Alerts tab, you administer existing alert schemes by cloning a scheme and customizing it, or deleting a scheme that is no longer needed. You can also enable alert schemes so that they send notifications to the recipients when the appropriate KPIs status changes, or you can disable these alert schemes. By default, alert schemes are enabled.

You can search for specific alert schemes assigned to a CI in the current view using the search feature. The search feature works only on alert scheme names.

For details, see "Configuration Item Status Alerts Page (Administration)" on page 107.

Example



6 Schedule the Configuration Item Status Alerts Report – Optional

You can schedule the Configuration Item Status Alerts report. For details, see "Create a Schedule" in *Reports*.

7 Open Incidents in HP Service Manager or in HP ServiceCenter Corresponding to CI Status Alerts Triggered in Business Availability Center

You can open incidents in HP Service Manager or in HP ServiceCenter that correspond to CI Status alerts triggered in Business Availability Center. For details, see "Open Incidents Using the CI Alert Retrieval Service" on page 129 or in "Open an Incident in HP Service Manager Using the Legacy URL" on page 211.

8 Open Events in HP Operations Manager When an Alert is Triggered in Business Availability Center

You can open events in HP Operations Manager (OM) when an alert is triggered in Business Availability Center. For details, see "Open an Event in Operations Manager When an Alert is Triggered" on page 49.

9 Results

You can view the alert schemes you have created in the Configuration Item Alerts page. For details, see "Configuration Item Status Alerts Page (Administration)" on page 107.

You can manage the alert schemes. For details, see "Manage the CI Status Alert Schemes" on page 69.

You can view a log of the alerts that were triggered in the Configuration Item Status Alerts report and in the Configuration Item Status Alert Notifications report. For details, see "View the Triggered CI Status Alerts and Notifications" on page 70.

Manage the CI Status Alert Schemes

After you complete defining an alert scheme, it is listed in the Configuration Item Status Alerts tab. For details, see "Configuration Item Status Alerts Page (Administration)" on page 107.

You can perform the following actions:

- Clone and edit an existing alert scheme. The cloned alert inherits all the properties of the existing alert, including CIs and recipients. The creator of the new alert is the user who cloned it.
- Delete an existing alert scheme.
- Enable alert schemes, so they send notifications to the recipients when the relevant conditions occur. You can also disable alert schemes.
- Search for an alert scheme using the search feature. The search feature works only on alert scheme names. For details, see "Configuration Item Status Alerts Page (Administration)" on page 107.

View the Triggered CI Status Alerts and Notifications

You can view information about the CI Status alerts that were triggered in the CI Status Alerts report and in the CI Status Alert Notifications report. Recipients can view the alert details in the emails, SMSs, or Pager messages that are sent to them when the alert is triggered.

This task includes the following steps:

- "View the CI Status Alerts Report" on page 70
- "View the CI Status Alert Notifications Report" on page 70
- "View the CI Status Alert Details in Emails, SMSs, or Pager Messages" on page 71

1 View the CI Status Alerts Report

To display alert information, select **Applications** > **Alerts** > **CI Status Alerts report**.

The report is a log of CI Status alerts that occurred in the specified period of time. For details, see "Configuration Item Status Alerts Report" on page 109.

An alert is also attached to the CI in any view where the CI is included.

2 View the CI Status Alert Notifications Report

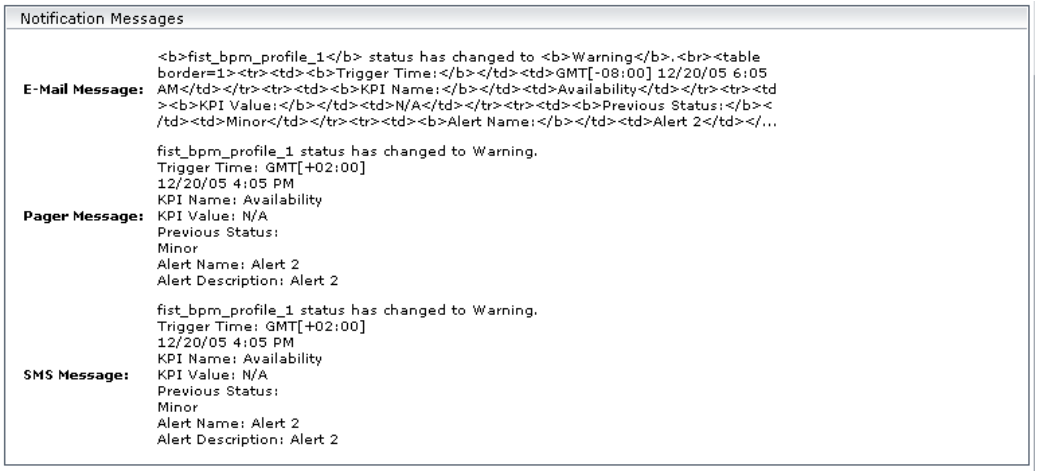
To display detailed alert information, access the Configuration Item Status Alerts page, and click the **Details** button for the relevant alert to open the Configuration Item Status Alert Notifications report. For details, see "Configuration Item Status Alert Notifications Report" on page 100.

The Configuration Item Status Alert Notifications report includes details on the alert, the notification, the notification message, and the type of message followed by the text of the message.

HTML is encoded in the report. The text of the email received by the recipient is decoded and is similar to the Pager message text. For more information on the different formats available to send emails or pager messages, see "Examples of HTML and Text Messages" on page 88.

You can also see whether the event corresponding to the alert in the Operation Manager (OM) was created (when the integration with HP Operation Manager is enabled).

Example


Notification Messages

E-Mail Message:

fist_bpm_profile_1 status has changed to Warning.
<table border=1><tr><td>Trigger Time:</td><td>GMT[-08:00] 12/20/05 6:05 AM</td></tr><tr><td>KPI Name:</td><td>Availability</td></tr><tr><td>KPI Value:</td><td>N/A</td></tr><tr><td>Previous Status:</td><td>Minor</td></tr><tr><td>Alert Name:</td><td>Alert 2</td></tr></...

Pager Message:

fist_bpm_profile_1 status has changed to Warning.
Trigger Time: GMT[+02:00]
12/20/05 4:05 PM
KPI Name: Availability
KPI Value: N/A
Previous Status:
Minor
Alert Name: Alert 2
Alert Description: Alert 2

SMS Message:

fist_bpm_profile_1 status has changed to Warning.
Trigger Time: GMT[+02:00]
12/20/05 4:05 PM
KPI Name: Availability
KPI Value: N/A
Previous Status:
Minor
Alert Name: Alert 2
Alert Description: Alert 2

3 View the CI Status Alert Details in Emails, SMSs, or Pager Messages

Recipients can view the CI Status alert details in the emails, SMSs, or Pager messages that are sent to them when the alert is triggered.

For details, see “Examples of HTML and Text Messages” on page 88.

Specify a Notification URL

You can create a notification URL to attach to an alert. This notification URL is used to pass alert information to external systems, such as a customer Web application.

You can embed predefined alert parameters in the notification URL. The parameters are used as placeholders when the message is formatted.

For details, see “Create New/Edit URL Dialog Box” on page 97.

Example – Create a Notification URL

To include the name of the CI and the current status of the CI in the URL, perform the following steps:

1. Enter the following string in the **Enter URL** box:

```
http://dogbert.com/myjsp?entityname=
```

2. Select **CI Name** in the **Field** box, and press **Insert Field** to insert the <<**CI Name**>> variable.

   The string in the **Enter URL** box is now:

```
http://dogbert.com/myjsp?entityname=<<CI Name>>
```

3. At the end of the string in the **Enter URL** box, enter:
   severity=
4. Select **Current Status** in the **Field** box, and press **Insert Field** to insert the <<**Current Status**>> variable.

   The string in the **Enter URL** box is now:

```
http://dogbert.com/myjsp?entityname=<<CI Name>> severity=
<<Current Status>>
```

Create an Executable Notification File

You can create an executable file to write information in special logs or to insert information into external databases.

Note to HP Software-as-a-Service customers: To create an executable file, contact HP Software-as-a-Service Support.

This task includes the following steps:

- "Set Up the Appropriate Administrative Privileges" on page 73
- "Create/Edit an Executable File" on page 74

1 Set Up the Appropriate Administrative Privileges

Only users with administrative privileges can create an executable file to be run when the alert it is attached to is triggered. You can set the appropriate administrative privileges to create a command that can be attached to an alert scheme.

To set the appropriate administrative privileges:

a Select **Admin** > **Platform** > **Users and Permissions**.

b Select the appropriate user in the left column, and click the **Permissions** tab.

c Select the **Monitors** context, and under Active user, click **Alerts - Run executable file**.

d Click the **Operations** tab, and select the **Change** option.

2 Create/Edit an Executable File

You create an executable file to write information in special logs or to insert information into external databases. For details, see "Create New/Edit Executable File Dialog Box" on page 94.

Example – Creating An Executable File

To include the name of the CI in the command, proceed as follows:

a Enter the following string in the **Enter command** box:

```
\\servername\myfolder\run.exe -name
```

b Select **CI Name** in the **Field** box and press **Insert Field** to insert the <<**CI Name**>> variable.

The string in the **Enter command** box is now:

```
\\servername\myfolder\run.exe -name <<CI Name>>
```

Configure a Notification SNMP Trap

You can create an SNMP trap to attach to an alert. This SNMP trap is sent when the alert criteria is met. The alert notice can be viewed with any SNMP management console in the organization.

For details, see "Create New/Edit SNMP Trap Dialog Box" on page 96.

The default host address of the SNMP trap appears automatically in the **Enter host destination** box in the Create New SNMP Trap or in the Edit SNMP Trap dialog box. If, when you create or edit an SNMP trap, you select the default host address and then modify it afterwards in the Infrastructure Settings, the address in the SNMP trap you created is updated to the new default. Any alert that is sent causes the SNMP trap to be sent to the new default address.

CI Status Alerts User Interface

This section describes:

Create New Alert Wizard

Description	Enables you to create new alert schemes and attach them to any CI. You can attach more than one alert scheme to a CI. You can also attach the same alert scheme to more than one CI. An alert attached to a CI in a view is attached to the CI in any view where the CI is included. **To access:** Select **Admin** > **Alerts** > **CI Status Alerts**.
Important Information	To open an incident in OM when a CI Status Alert is triggered, you must: ➤ Create a CI Status alert. If you do not specify a recipient or an action for the alert, the message: **The alert you just defined opens an event in Operations Manager when the communication with Operations Manager is enabled** is displayed in the Summary page, when you complete the definition of the alert. ➤ Set up specific parameters to enable the communication with OM. For details, see "Open an Event in Operations Manager When an Alert is Triggered" on page 49.
Included in Tasks	"Create a CI Status Alert Scheme and Attach it to a CI" on page 65
Wizard Map	The **Create New Alert Wizard** includes: Welcome Page > General Page > Related Configuration Items Page > Templates and Recipients Page > Actions Page > Summary Page

General Page

Description	Enables you to define the alert scheme general information including the triggering conditions.
Wizard Map	The **Create New Alert Wizard** includes: Welcome Page > **General Page** > Related Configuration Items Page > Templates and Recipients Page > Actions Page > Summary Page

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Alert Type	Select one of the following options: ➤ **All KPIs** if you want the alert to be triggered by the specified status change in any of the KPIs attached to any of the selected CIs ➤ **Selected KPIs** if you want the alert to be triggered by the specified status change in the selected KPIs attached to any of the selected CIs You select CIs and KPIs in the next step of the wizard.
Description	Enter the alert scheme's description.
Name	Enter the name of the alert scheme.
Notification frequency	Select one of the following options: ➤ **Send alert for every trigger occurrence** to send an alert notification every time an alert is triggered. ➤ **Send no more than one alert per <time_period>** and specify the time period and unit to send an alert notification every time period.

GUI Element (A-Z)	Description
Send alert if	Select one of the following options: ➤ **Status is equal to or** <condition> **than** <status> **for** <value><time unit> to trigger the alert when the status of the CI is equal to or better/worse than the selected status (**Critical**, **Major**, **Minor**, **Warning**, or **OK**) for the specified time period (minutes, hours, or days). For detailed examples, see "Examples of Status is equal to or <condition> than <status> for <value><time unit>" on page 79. ➤ **Status worsens (not including "No Data" and "Downtime")** to trigger the alert when the current status of the KPIs is worse than the previous status. The **No Data** and **Downtime** statuses are not taken into consideration. For example, the alert is triggered when the status changes from Warning to Minor. ➤ **Status improves (not including "No Data" and "Downtime")** to trigger the alert when the current status of the KPIs is better than the previous status. The **No Data** and **Downtime** statuses are not taken into consideration. For example, the alert is triggered when the status changes from Warning to OK. ➤ **Status value was changed from** <status> **to** <status> to set the appropriate conditions for sending an alert. Select the appropriate status in the **from** box, and in the **to** box. The available statuses are: **Any Status** (only available in the **from** box), **Critical, Major, Minor, Warning, OK, No Data, Downtime, Stop, Info**, and **Uninitialized**. If you select **Any Status**, the alert is triggered when the CI status changes from any status to the target status.

Examples of Status is equal to or <condition> than <status> for <value><time unit>

➤ You specify the following condition: "Send alert if status is equal to or worse than Major for 15 minutes" and the following scenarios occur:

CI's KPI	Status changes to	What happens
Availability	Major for 15 minutes	Alert is sent
Availability	Critical for 20 minutes	Alert is not sent (status is still worse than Major for over 15 minutes). **Note:** Before the alert is triggered again, the alert must be reset. To reset the alert, the status must return to a value within the status threshold (better than Major). After the alert is reset, it can be triggered as before (when the status changes to worse or equal to Major for 15 minutes).
Performance	Critical for 20 minutes	Alert is sent (another KPI status becomes worse than Major for over 15 minutes).
Availability	Minor	Alert is not sent (status is better than Major and counter is reset)
Availability	Critical for 20 minutes	Another alert is sent after 15 minutes

➤ You specify the following condition: "Send alert if status is equal to or better than Minor for 30 minutes" and "Send no more than one alert per 60 minutes", and the following scenarios occur:

CI's KPI	Status changes to	What happens
Availability	OK for 45 minutes	Alert is sent
Performance	OK for 30 minutes	Alert is not sent (it was already sent 15 minutes ago)

CI's KPI	Status changes to	What happens
Availability	Minor for 15 minutes	Alert is not sent (it was already sent for the Availability KPI 15 minutes ago)
Availability	OK for 20 minutes	Alert is not sent
Availability	No Data for 15 minutes	The status of the alert is reset.
Availability	OK for 10 minutes	The status of the alert is not sent as the time interval condition is not met (30 minutes)

Related Configuration Items Page

Description	Enables you to specify the CIs and KPIs to which you want to attach the alert scheme. If you selected **All KPIs** in the **General** page, then in the Related Configuration Items page, select the CIs to which you want to attach the alert scheme. The alert is triggered by the specified status change in any of the KPIs attached to any of the selected CIs. If you selected **Selected KPIs** in the **General** page, then in the Related Configuration Items page, select the CIs to which you want to attach the alert scheme. You must also select one or more of the KPIs that are listed in the KPIs area. The KPIs area lists all the types of KPIs that are attached to the selected CIs. The alert is triggered by the specified status change in the selected KPIs attached to any of the selected CIs. You can share the same CI Status alert scheme definition between several CIs when you select more than one CI in the Related Configuration Items page.
Wizard Map	The **Create New Alert Wizard** includes: Welcome Page > General Page > **Related Configuration Items Page** > Templates and Recipients Page > Actions Page > Summary Page

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Click the right arrow button to move your selections to the **Selected Configuration Items** list. You can select multiple CIs using the CTRL key. To remove a CI from the **Selected Configuration Items** list, select it in the **Selected Configuration Items** list and click the left arrow button.
	Click to display the CI General Properties page. For details, see "CI Properties" in *Model Management*.
<Tree>	In View Explorer, select the CIs to which you want to attach the alert scheme (you can expand the tree if needed), and click the right arrow button  to move your selections to the Selected Configuration Items list. You can select multiple CIs using the Ctrl key. To remove a CI from the Selected Configuration Items list, select it and click the left arrow button  . The alert is triggered by any change in any of the KPIs attached to the CI to which the alert scheme is assigned.
KPIs	If you selected **Selected KPIs** in the **General** page, select the KPIs whose change of status triggers the alert. 

Templates and Recipients Page

Description	Enables you to define the alert recipients and templates. When an alert is triggered, an email, SMS message, or Pager message is sent to a predefined recipient. The email, SMS message, or Pager messages have predefined templates.
Important Information	The notification method that is used to notify a recipient depends of the recipient definition. You cannot use customized templates for emails, SMS messages, or Pager messages with the CI Status alerts.
Wizard Map	The **Create New Alert Wizard** includes: Welcome Page > General Page > Related Configuration Items Page > **Templates and Recipients Page** > Actions Page > Summary Page

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Click the right arrow button to move your selections to the **Selected Recipients** list. You can select multiple recipients using the CTRL key. To remove a recipient from the **Selected Recipients** list, select it and click the left arrow button.
Available recipients	Select the recipients to whom you want notifications sent, and click the right arrow button  to move your selections to the Selected recipient list. You can select multiple recipients using the Ctrl key. To remove a recipient from the Selected recipient list, select it and use the left arrow button  .
Email Message Template	Select one of the following options: ➤ **Short HTML email message, short text email message.** These messages include the change in status only. ➤ **Long HTML email message, long text email message.** These messages include a subject line and body. For examples of HTML or text messages, see "Examples of HTML and Text Messages" on page 88. The structure of the messages is described in "Message Syntax" on page 85. For details on modifying the message character set, see **Email alerts charset / SMS alert charset / Pager alert charset** in "Modify the Alerts Triggering Defaults" on page 25. For details on the structure of the email, SMS, and Page message templates, see "Add a CIT's Additional Parameters to a CI Status Alert – Optional" on page 66. **Note:** The text displayed in email messages can only be in English except for the contents of fields inserted by the user that can be in any supported and relevant language. Those fields can be for example: Alert Name, Alert description, KPI name, and so on.

GUI Element (A-Z)	Description
New Recipient	Click the **New Recipient** button to define a new recipient. For details, see "Recipient Properties Wizard" on page 38.
Pager template	Pager messages are sent through email to the service provider. The pager messages use the same templates as the SMS messages. The email address is: **<Pager provider access number>@<Pager provider email address>**. Select one of the following options: ➤ **Long SMS/Pager message.** The message includes the change in status and information about the SLA. ➤ **Short SMS/Pager message.** The message includes the change in status only. For examples of HTML or text messages, see "Examples of HTML and Text Messages" on page 88. The structure of the messages is described in "Message Syntax" on page 85. For details on modifying the message character set, see **Email alerts charset / SMS alert charset / Pager alert charset** in "Modify the Alerts Triggering Defaults" on page 25. For details on the structure of the email, SMS, and Page message templates, see "Add a CIT's Additional Parameters to a CI Status Alert – Optional" on page 66. **Note:** The text displayed in pager messages can only be in English except for the contents of fields inserted by the user that can be in any supported and relevant language. Those fields can be for example: Alert Name, Alert description, KPI name, and so on.
Selected recipient	Lists the recipients that you have selected.

GUI Element (A-Z)	Description
SMS template	SMS messages are sent through email to the service provider. The pager messages use the same templates as the SMS messages. The email address is: **<SMS provider access number>@<SMS provider email address>** Select one of the following options: ➤ **Long SMS/Pager message.** The message includes the change in status and information about the SLA. ➤ **Short SMS/Pager message.** The message includes the change in status only. For examples of HTML or text messages, see "Examples of HTML and Text Messages" on page 88. The structure of the messages is described in "Message Syntax" on page 85. For details on modifying the message character set, see **Email alerts charset / SMS alert charset / Pager alert charset** in "Modify the Alerts Triggering Defaults" on page 25. For details on the structure of the email, SMS, and Page message templates, see "Add a CIT's Additional Parameters to a CI Status Alert – Optional" on page 66.

Message Syntax

The syntax used in the message is a subset of a long or short HTML template or long or short text template.

➤ Syntax for a long or short HTML template:

ci_name status has changed to/remained *current_status* for *time-period*.

Status Change Time:	*trigger_time*
KPI Name:	*alert_name*
KPI value:	*alert_value*
Previous status:	*previous_status*
Alert name:	*alert_name*
Alert Description:	*alert_description*
Time Since Condition Threshold Met	*time-period + time since end of time-period*

The alert was triggered for the following CI:

CI Type	*ci_type*
data_name	*ci_name*
<additional_parms>	*additional_parms*

The CI impacts the following Business Services/Business Processes/Applications:

Business Service/Business Process/Application	*business_services/business_processes/applications*

The following CIs are associated with the triggered CI and may be affected by its status:

Service name	*service_name*
Application name	*application_name*

Over Time Report

Business Impact Report

Go to Problem Isolation

For more details log into *url*

➤ Syntax for a long or short text template:

ci-name status has changed to/remained *current-status* for *time-period*.

Trigger Time: *trigger-time*

KPI Name: *KPI-name*

KPI value: *KPI-value*

Previous status: *previous-status*

Alert name: *alert-name* (Long text)

Alert Description: *alert-description*

Time Since Condition Threshold Met: *time-period* + *time since end of time-period*

The alert was triggered for the following CI:

CI Type: *ci_type*

data_name: *ci_name* <additional_parms>: *additional_parms*

The CI impacts the following Business Services/Business Processes/Applications:

Business Service/Business Process/Application: *business_services/business_processes/applications*

The following CIs are associated with the triggered CI and may be affected by its status:

Service name: *service_name*

Application name: *application_name*

link to Over Time Report

link to Business Impact Report

Go to Problem Isolation

For more details log into *url*

Note: When the CI to which the alert is attached, is connected directly or indirectly to CI with the type Service or Application, the notification includes the section "The following CIs are associated with the triggered CI and may be affected by its status."

For details on the parameters, see “Configuration Item Status Alert Notifications Report” on page 100.

Examples of HTML and Text Messages

The email messages that the user receives depend on the format you select in the **Email Message Template**, **SMS Template**, or **Pager Template** list. The structure of the messages is described in “Message Syntax” on page 85.

➤ **Example of a long HTML email, SMS, or Pager message**

10per50ava status has changed to **Warning**.

Status Change Time:	GMT[+03:00] 4/12/07 11:59 AM
KPI Name:	Performance
KPI value:	N/A
Previous status:	Minor
Alert name:	Alert 1
Alert Description:	

The alert was triggered for the following CI:

CI Type	Business Process Step
Data Name	10per50ava

The following CIs are associated with the triggered CI and may be affected by its status:

Service name	Hosting Service
Service name	Online Desk
Application name	My Book Store

Over Time Report

Business Impact Report

Go to Problem Isolation

For more details log into HP Business Availability Center

➤ **Example of a long text email, SMS, or Pager message**

10per50ava status has changed to Warning.
Status Change Time: GMT[+03:00] 4/12/07 11:59 AM
KPI Name: Performance
KPI value: N/A
Previous Status: Minor
Alert name: Alert 1 (Long text)
Alert Description:
The alert was triggered for the following CI:
CI Type: Business Process Step
Data Name: 10per50ava
Over Time Report
Business Impact Report
Go to Problem Isolation

➤ **Example of a short HTML email, SMS, or Pager message**

10per50ava status has changed to **Warning**.
For more details log into HP Business Availability Center

➤ **Example of a short text email, SMS, or Pager message**

10per50ava status has changed to Warning.
For more details log into HP Business Availability Center

Actions Page

Description	Enables you to define the user-defined alert handlers (actions) that is triggered by the alert.
Wizard Map	The **Create New Alert Wizard** includes: Welcome Page > General Page > Related Configuration Items Page > Templates and Recipients Page > **Actions Page** > Summary Page

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Select the appropriate URL and click to open the Edit URL dialog box. For details, see “Create New/Edit URL Dialog Box” on page 97. Select the appropriate Executable File and click to open the Edit Executable File dialog box. For details, see “Create New/Edit Executable File Dialog Box” on page 94. Select the appropriate SNMP Trap and click to open the Edit SNMP Trap dialog box. For details, see “Create New/Edit SNMP Trap Dialog Box” on page 96.
	Select the appropriate URL and click to delete it. Select the appropriate Executable File and click to delete it. Select the appropriate SNMP Trap and click to delete it.
Executable Files	Lists the executable files that are to execute when the alert is issued.
New Executable File	Click the **New Executable File** button to define a new executable file. The **Create Executable File** page opens. For details, see “Create New/Edit Executable File Dialog Box” on page 94.

GUI Element (A-Z)	Description
New SNMP Trap	Click the **New SNMP** button to configure a new SNMP trap. The Create New SNMP Trap page opens. For details, see "Configuration Item Status Alerts Page (Administration)" on page 107.
New URL	Click the **New URL** button to create a new URL. The **Create New URL** page opens. For details, see "Create New/Edit URL Dialog Box" on page 97.
Open Ticket in Service Center	Select the option to automatically open an incident for the alert in HP ServiceCenter when the alert is triggered. Clear the option to disable the feature. For information about the feature prerequisite steps, see "Open Incidents Using the CI Alert Retrieval Service" on page 129.
SNMP Traps	Lists the SNMP traps that are to be sent when the alert is issued.
URLs	Lists the URLs that are to open when the alert is issued.

Summary Page

Description	Displays a summary of the alert scheme definition.
Wizard Map	The **Create New Alert Wizard** includes: Welcome Page > General Page > Related Configuration Items Page > Templates and Recipients Page > Actions Page > **Summary Page**

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Cancel	Click the **Cancel** button to close the wizard and return to the Configuration Item Status Alerts page. The alert scheme is not saved.
Finish	Click the **Finish** button to close the wizard and return to the Configuration Item Status Alerts page. The alert scheme is saved.

Create New/Edit Executable File Dialog Box

Description	Enables you to create or edit an executable file and embed predefined alert parameters in the file. The parameters are used as placeholders when the message is formatted. **Note to HP Software-as-a-Service customers:** To create an executable file, contact HP Software-as-a-Service Support. **To access:** Click **New Executable File** or the appropriate  button in the Executable File area in the Actions page of the Alerts wizard.
Important Information	Only users with administrative privileges can create an executable file to be run when the alert it is attached to is triggered. The executable file writes information in special logs or inserts information into external databases. To set the appropriate administrative privileges, select **Admin** > **Platform** > **Users and Permissions** > **Permissions Management**, select the **Monitors** context, click **Alerts - Run executable file**, select the **Operations** tab, set the permissions to **Change**.
Included in Tasks	"Create an Executable Notification File" on page 73

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Enter command	Displays the command and the selected fields. The selected field appears between double angle brackets.
Field	In the list, select the name of the field and click **Insert Field**. The field values represent: ➤ **CI Name.** The name of the CI. ➤ **Alert Name.** The name of the alert. ➤ **Trigger Time.** The time and date when the alert was triggered. The format is: dd/mm/yy hh:mm GMT[<offset>] ➤ **Previous Status.** The previous status of the KPIs. ➤ **Current Status.** The current status of the KPIs. The change from previous status to current status triggers the alert. ➤ **KPI Name.** The name of the KPI. ➤ **KPI Value.** The value of the KPI.
Insert Field	Select the name of a field in the Field box and click the **Insert Field** button to copy the field to the Enter command box.

Create New/Edit SNMP Trap Dialog Box

Description	Enables you to create or edit an SNMP trap to attach to an alert. This SNMP trap is sent when the alert criteria is met. The alert notice can be viewed with any SNMP management console in the organization. **To access:** Click **New SNMP Trap** or the appropriate  button in the SNMP Trap area in the Actions page of the Alerts wizard.
Important Information	**Note:** HP Business Availability Center uses the CI alerts MIB by default and supports SNMP V2. To enable alerts through SNMP trap, it is recommended that you configure your SNMP management console to read the Alerts MIB. For details, see "Configure the Alerts MIB" on page 261. This enables you to see names, rather than Object IDs (OIDs), when working in the management console. The MIB file is located at <Business Availability Center processing server home directory>\HPBAC\SNMP_MIBS\CIAlerts.mib.
Included in Tasks	"Configure a Notification SNMP Trap" on page 74

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Enter destination host	Enter the host address. You can use different formats: ➤ If you work with Alerts for profiles, use the following format: ➤ <target_host_IP_address> ➤ <target_host_IP_address>[:<port_number>] ➤ If you work with CMDB, use the following format: ➤ <target_host_name|target_host_IP_address> ➤ <target_host_name|target_host_IP_address> [:<port_number>] For details on the default host address, see **Default SNMP Target Address** / **Default SNMP Port** in "Modify the Alerts Triggering Defaults" on page 25.

Create New/Edit URL Dialog Box

Description	Enables you to create or edit a notification URL to attach to an alert. The notification URL is used to pass alert information to external systems, such as a customer Web application. You can embed predefined alert parameters in the notification URL. The parameters are used as placeholders when the message is formatted. **To access:** Click **New URL** or the appropriate  button in the URL area in the Actions page of the Alerts wizard.
Important Information	You can modify the default URL that appears in the notifications. This URL represents the URL of the Data Processing Server. For details, see "Specify a Notification URL" on page 71.
Included in Tasks	"Specify a Notification URL" on page 71

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Enter URL	Displays the URL and the selected fields. The selected field appears between double angle-brackets. For examples of URLs, see "Specify a Notification URL" on page 71. You can also enter the URL of a Business Impact report for the relevant CI. For details, see "Business Impact Report" in *Using Dashboard*.
Field	Select the name of a field and click **Insert Field**. The field values represent: ➤ **CI Name.** The name of the CI. ➤ **Alert Name.** The name of the alert scheme. ➤ **Trigger Time**. The time and date when the alert was triggered. The format is: dd/mm/yy hh:mm GMT[<offset>]. ➤ **Previous Status**. The previous status of the KPIs. ➤ **Current Status**. The current status of the KPIs. The change from previous status to current status triggers the alert. ➤ **KPI Name.** The name of the KPI. ➤ **KPI Value.** The result of the calculation performed by the rule attached to the KPI. This is the result that triggered the alert.
Insert Field	Select the name of a field in the Field box and click the **Insert Field** button to copy the field to the Enter URL box.

Configuration Items Dialog Box

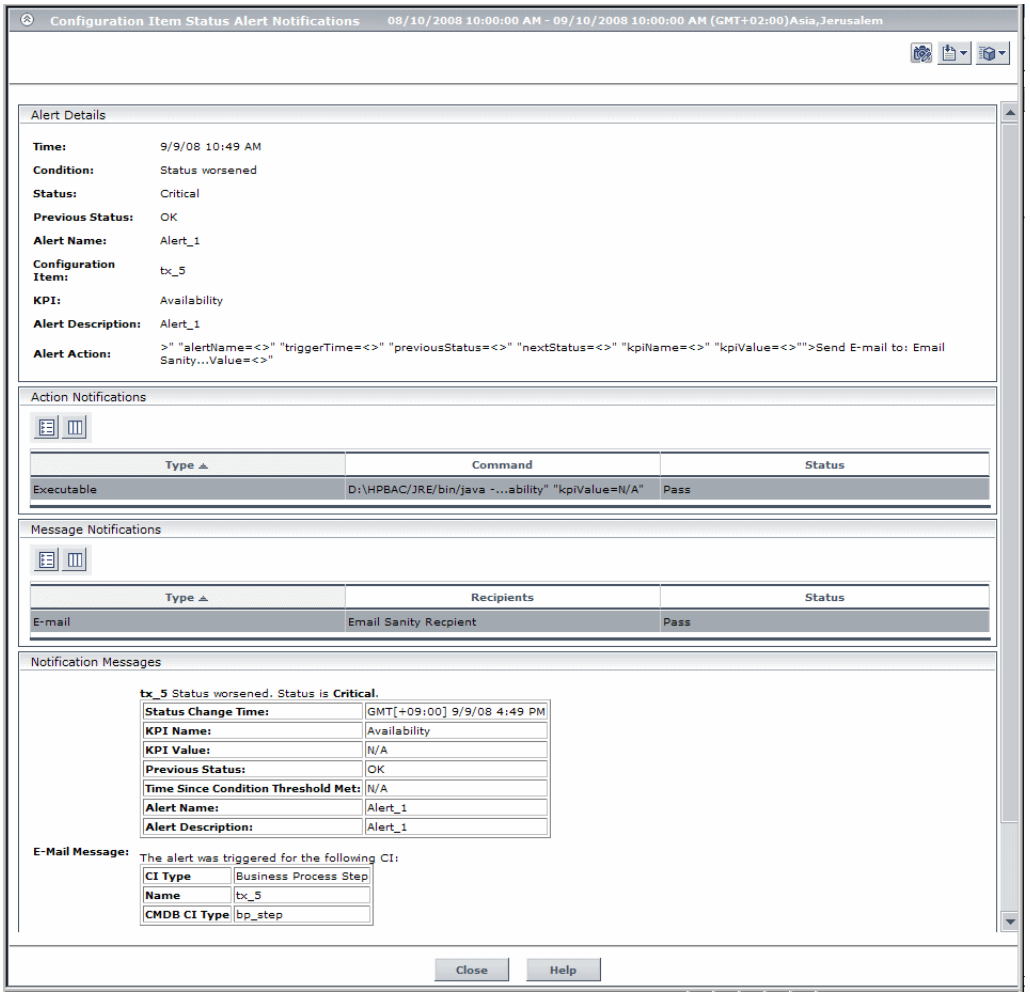
Description	Enables you to select the CIs to be included in the CI Status Alerts report, for the duration of a Web session. The report provides information based on the selected CIs. **To access:** In the CI Status Alerts report, click **Configuration Items** in the reports settings area.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<View tree>	Displays the CIs that belong to the selected view. Select the required CIs.
Browse	The default mode for the Configuration Items dialog box, enabling you to select a view and CIs.
Search	Click **Search** to move to Search mode, where you can search for CIs. For details, see "Working with View Explorer" in *Model Management*.
View	Select the relevant view from the dropdown list (start typing in the view name to filter the list), or click the ellipse button to open the Select View dialog box, where you can select a view from the view folders tree. **Note:** Only the CIs selected in the currently displayed view are saved for the report filter when you click **OK**. If you select another view before clicking **OK**, all previous CI selections are discarded.

Configuration Item Status Alert Notifications Report

The following is an example of the Configuration Item Status Alert Notifications report.



Description	Enables you to display detailed alert information. **To access:** Access the Configuration Item Status Alerts page, and click the **Details** button.
Included in Tasks	"View the Triggered CI Status Alerts and Notifications" on page 70

Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<Common report elements>	See "Common Report Elements" in *Reports*.

Alert Details Area

Description	Includes details on the alert.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Alert Action	The action that has been assigned to the alert.
Alert Description	The description of the alert.
Alert Name	The name of the alert.
Condition	The condition that caused the alert to be triggered.
Configuration Item	The name of the CI to which the alert is attached.
KPI	The name of the KPI whose change of status triggered the alert.
Previous Status	The previous status of the KPI.

GUI Element (A-Z)	Description
Status	The current status of the alert.
Time	The time when the alert was triggered.

Action Notifications Area

Description	Includes details on the notification.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Select the alert and click the button to display the alert notification details in the Alert Details page. For details, see "Configuration Item Status Alert Notifications Report" on page 100.
	Click the **Select Columns** button to open the Select Columns dialog box and select the columns you want to display in the table. For details on the Select Columns dialog box, see "Select Columns Dialog Box" in *Reference Information*.
Command	The action that was executed: ➤ for executables: the command line ➤ for URLs: the URLs ➤ for SNMP traps: **Send SNMP trap to <address>** ➤ for Open ticket in HP ServiceCenter: **Open incident** ➤ for Open event in HP Operations Manager (OM)
Status	The status of the action: ➤ **Pass** when the action has been performed. ➤ **Fail** when the action failed.
Type	The type of action notification: **Executable**, **URL**, **SNMP trap**, **OM**, or **Service Center.**

Message Notifications Area

Description	Includes details on the notification message.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Click to reset the table's column width to its default setting. You can adjust the width of the table's columns by dragging the borders of the column to the right or the left. If the button does not appear in the report, click the **Reset the table's column width button**  and make the Details column visible.
	Click the **Select Columns** button to open the Select Columns dialog box and select the columns you want to display in the table. For details on the Select Columns dialog box, see "Select Columns Dialog Box" in *Reference Information*.
Recipients	The names of the recipients who receive the notification that the alert has been triggered and that the alert scheme has been executed.
Status	The status of the message: ➤ **Pass.** When the message has been sent. ➤ **Fail.** When the message was not sent.
Type	The type of message notification: email, SMS message, or Pager message.

Notification Messages Area

Description	Displays details about the notification message and the email message sent to the recipients when the alert was triggered.
Important	Depending on the definition of the CI Status alert, the report may display only a subset of the fields described in the following table.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<ci-name> <condition>. Status is <current-status>	**<ci-name>.** The name of the CI whose change of status triggered the alert. **<condition>.** The condition that triggered the alert. For example: Status improved. **<current-status>.** The new status of the CI.
Additional Parameters	Depending on the type of the CI, additional parameters are automatically added to the notification. For details, see "Additional Parameters" on page 106. To add additional parameters to the CIT, see "Add a CIT's Additional Parameters to a CI Status Alert – Optional" on page 66.
Alert Description	The description of the alert.
Alert Name	The name of the alert.
Business Impact Report	Click to open the Business Impact report for selected CI. For details, see "Business Impact Report" in *Using Dashboard*.
CI Type	The type of the CI that triggered the alert.

GUI Element (A-Z)	Description
Due to a large number of alerts at current time, impact calculations were not performed	This message is displayed when a large number of alerts was issued, and in this case the **CI impacts the following Applications**, the **CI impacts the following Business Processes**, and the **CI impacts the following Business Service** sections are not displayed in the report.
For more details log into HP Business Availability Center	Click the link to Business Availability Center to open the application where the CI Status Alert was triggered.
Go to Problem Isolation	Click to start Problem Isolation for the CI that triggered the alert. **Note:** ➤ The link is not included in HP Software-as-a-Service. ➤ The link is included but does not open Problem Isolation, if you do not have a licence for Problem Isolation. ➤ The link is included only for the CI types representing business CIs for which you can create a problem. To check or add a CI to the list, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Allowed CI types for problem creation** entry in the Problem Isolation - General Settings table. Enter the CI internal names. To display a CI internal name, select **Admin** > **Universal CMDB** > **CI Type Manager**, click the CI Type in the left tree and click the **Details** tab, the CI internal name is displayed in the **Name** box.
KPI Name	The name of the KPI.
KPI Value	The value of the KPI.
Name	The name of the CI whose change of status triggered the alert.
Over Time Report	Click to open the KPIs Over Time report for all the KPIs of the selected CI. For details, see "KPIs Over Time Report" in *Using Dashboard*.

GUI Element (A-Z)	Description
Previous Status	The status of the CI before it changed to the status that triggered the alert.
Status Change Time	The time and date when the alert was triggered. The format is: dd/mm/yy hh:mm GMT[<offset>].
The alert was triggered for the following CIs	Provides the details of the CI that triggered the alert: ➤ **CI Type.** The display name of the CI type. ➤ **Name.** The code name of the CI. ➤ **CMDB CI Type.** The CMDB name of the CI type.
The CI impacts the following Applications	Lists the Applications impacted by the CI.
The CI impacts the following Business Processes	Lists the Business Processes impacted by the CI.
The CI impacts the following Business Services	Lists the Business Services impacted by the CI.
Time Since Condition Threshold Met	The time that has passed since the condition that triggered the alert occurred, in minutes.
URL	The URL of the HP Business Availability Center Data Processing Server.

Additional Parameters

The additional parameters are:

CI Type	Parameter
Business Unit	**Contact information.** The business unit contact information.
Host	➤ **IP.** The IP number of the host. ➤ **Vendor.** The name of the vendor. ➤ **Operating system.** The type of operating system.

CI Type	Parameter
Siebel Application Server	➤ **Version.** The Siebel version that is in use. ➤ **Language.** The language that is in use.
SAP Application Server	➤ **Version.** The SAP version that is in use. ➤ **IP.** The IP number that is in use. ➤ **Port.** The number of the port that is in use.
Database	➤ **Type.** The type of database. ➤ **Version.** The version that is in use. ➤ **Port.** The number of the port that is in use.
Service	➤ **Service Operating Status.** The status of the operating system· ➤ **Service Description.** A description of the service.

Configuration Item Status Alerts Page (Administration)

Description	Enables you to manage existing CI Status alerts. **To access: Admin > Alerts > CI Status Alert tab**
Included in Tasks	"Create a CI Status Alert Scheme and Attach it to a CI" on page 65

The following elements are included (unlabeled GUI elements are shown in angle brackets):

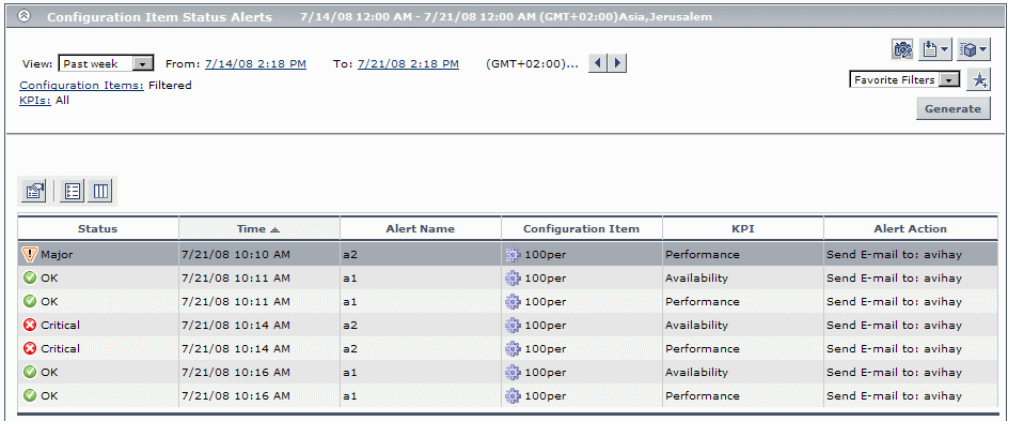
GUI Element (A-Z)	Description
	Click the button beside the alert whose properties you want to modify. The Alert Wizard opens. For details, see "CI Status Alerts Overview" on page 64.
	Click the button next to the alert scheme you want to clone. HP Business Availability Center adds a copy of the alert scheme to the profile tree, with a new name. Rename and edit the alert scheme as required.

GUI Element (A-Z)	Description
	Click the button beside the alert to delete the alert. **Note:** To delete multiple alerts simultaneously, select their check boxes in the left column, and click the button located at the bottom of the Alerts table.
	If an alert is enabled, click the **Disable Alert** button beside the alert to disable it. When an alert is disabled, HP Business Availability Center does not send an alert notice when the trigger conditions defined in the alert occur. **Note:** To enable or disable multiple alerts simultaneously, select their check boxes in the left column and click the button located at the bottom of the Alerts table.
	If the alert is disabled, click the **Enabled Alert** button beside the alert to enable it. When an alert is disabled, HP Business Availability Center does not send an alert notice when the trigger conditions defined in the alert occur. **Note:** To enable or disable multiple alerts simultaneously, select their check boxes in the left column and click the button located at the bottom of the Alerts table.
Alert Name	The name of the alert scheme.
Condition	A description of the condition.
New Alert	Click the **New Alert** button to define a new alert. The Alerts wizard opens. For details on the Alert wizard, see “CI Status Alerts Overview” on page 64.
Recipients	The names of the recipients.
Search	Click **Search** to perform the search.

GUI Element (A-Z)	Description
Search in current view by name	Enables you to search for specific alert schemes assigned to a CI in the current view using the search feature. The search feature works only on alert scheme names. For example, search for all the alert schemes whose names include the string OK so that you can change their conditions. You can also use: ➤ an asterisk wildcard (*) to represent a string of characters ➤ a question mark wild card (?) to represent one character only Click **Search** to perform the search. The relevant alerts are listed. **Note:** To restore the complete list of alerts after a search, enter an asterisk and click **Search**.
Status	Indicates if the alert scheme is enabled or disabled.

Configuration Item Status Alerts Report

The following is an example of the Configuration Item Status Alerts report.



Description	Enables you to list all of the alerts that occurred in the specified period of time. **To access:** Select: ➤ **Applications** > **Alerts** > **CI Status Alerts Report** ➤ **Applications** > **Dashboard** > **Console tab**, click the appropriate context menu, and select **Configuration Item Status Alerts** or click the **Alerts Over Time report** option in the Alerts tab.
Included in Tasks	"View the Triggered CI Status Alerts and Notifications" on page 70

Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<Common report elements>	See "Common Report Elements" in *Reports*.
Configuration Items	Lists the CIs that are included in the report. To select CIs, click the **Configuration Items** link. For details, see "Configuration Items Dialog Box" in *Using Dashboard*.
KPIs	Lists the KPIs that are included in the report. To select KPIs, click the **KPIs** link. For details, see "KPIs Dialog Box" on page 272.

Table Area

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Click the button relevant to the appropriate alert to see the alert notification details. For details, see "Configuration Item Status Alert Notifications Report" on page 100.
Alert Action	The action that is triggered by the alert. **Note: Open an incident in Operations Manager** indicates that the alert should have opened an incident in Operations Manager when the alert was triggered and communication with OM was established. For details about establishing communication with OM, see "Open an Event in Operations Manager When an Alert is Triggered" on page 49. To see whether the incident was opened in Operations Manager, click the **Detail** button to go to the alert notification report.
Alert Name	The name of the alert.
Configuration Item	The name of the CI the alert is attached to.
KPI	The name of the KPI.
Status	The current status of the KPIs represented by a status icon. The change from previous status to current status triggers the alerts. For details about the icons, see "KPI Status" in *Using Dashboard*.
Time	The time and date when the alert was triggered. The format is: dd/mm/yy hh:mm GMT[<offset>].

KPIs Dialog Box

Description	Enables you to select the KPIs to be included in a CI Status Alerts report, for the duration of a Web session. The report provides information based on the selected KPIs. **To access:** In the CI Status Alerts report, click **KPIs** in the reports settings area.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
KPIs	Lists the KPIs that are attached to the selected CIs. Availability and Performance are listed first, then all other KPIs in alphabetical order. Select the check boxes for the required KPIs.

5

Open Incidents in HP Service Manager using the CI Alert Retrieval Service

This chapter provides information on opening incidents in HP Service Manager, using the CI Alert Retrieval Service, when CI Status alerts are triggered in HP Business Availability Center 8.0.

Note: HP Business Availability Center integrates with both HP ServiceCenter and HP Service Manager though only HP Service Manager is mentioned in this chapter. For details about the supported versions, see "Opening Incidents in HP Service Manager – Overview" on page 114.

This chapter includes:

Concepts

Tasks

Reference

Troubleshooting and Limitations on page 154

Opening Incidents in HP Service Manager – Overview

You can automatically manage (open, update, or close) an incident in HP Service Manager when a CI Status alert is triggered in Business Availability Center.

Depending on the version of HP ServiceCenter or HP Service Manager, the method used to manage the incident is different.

HP ServiceCenter and HP Service Manager Versions	Procedure used to Open Incidents in HP Service Manager when a CI Status Alert is Triggered
HP ServiceCenter 6.26 HP Service Manager 7.01	**Legacy URL** For details, see "Open an Incident in HP Service Manager Using the Legacy URL" on page 211
HP Service Manager 7.02 + HPSM_00028 patch HP Service Manager 7.10	**CI Alert Retrieval Service** For details, see "Open Incidents Using the CI Alert Retrieval Service" on page 129 **Note:** To retrieve the patch access http://support.openview.hp.com/selfsolve/patches

Incidents Opened in HP Service Manager by CI Status Alerts Using the CI Alert Retrieval Service

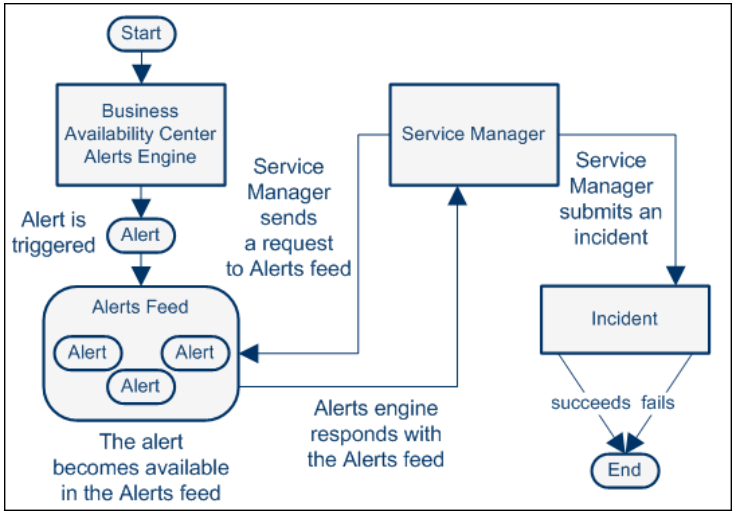
You can automatically open an incident in HP Service Manager when a CI Status alert is triggered using the CI Alert Retrieval Service.

This section includes the following topics:

How HP Service Manager Retrieves Alert Information

The Business Availability Center engine triggers a CI Status alert when the specified conditions occur. The alert is sent to the Alerts feed.

By default, every 5 minutes, HP Service Manager retrieves information about the CI Status alerts triggered in Business Availability Center, from the Alerts feed, using the CI Alert Retrieval Service. For details, see "CI Alert Retrieval Service API Overview" on page 164. HP Service Manager uses the information to submit an incident.



You can modify the default retrieval time period in HP Service Manager. For details, see HP Service Manager documentation.

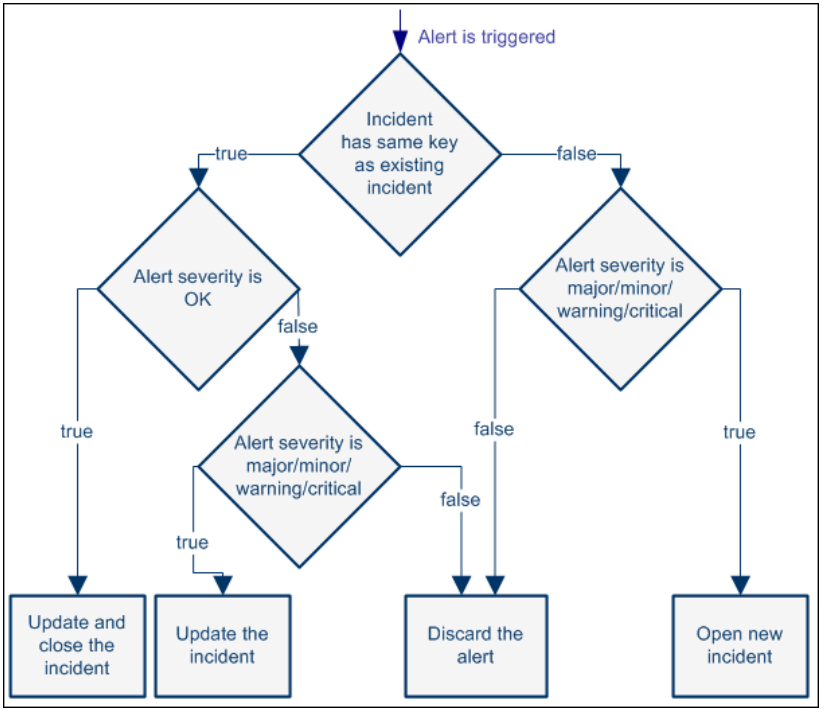
For each alert retrieved from the Alerts feed, and depending upon the configuration of the HP Service Manager, the content of a retrieved alert and the state of existing incidents are handled differently. For details see "How HP Service Manager Handles Alerts" on page 116.

How HP Service Manager Handles Alerts

An incident is identified by its key, which is composed of the CI ID and the KPI name of the CI whose change of status triggered the alert.

An incident previously opened is updated with new alert data when a CI Status with the same identifying information is triggered.

HP Service Manager handles alerts as shown in the following diagram:



All correlations (checking the identity of the incident) are done using the combination of the CI ID and the KPI name.

The default mapping between Business Availability Center to HP Service Manager is as follows:

Business Availability Center	**HP Service Manager**
Critical	Critical
Major	High
Minor	Average
Warning	Low
OK	Update and close the incident
No Data /Uninitialized/Stop/ Downtime/No Data	**Default:** Discard You can customize the default to any other value. You can also create an unknown HP Service Manager severity and map it to **Discard**. For details, see HP Service Manager User's Guide

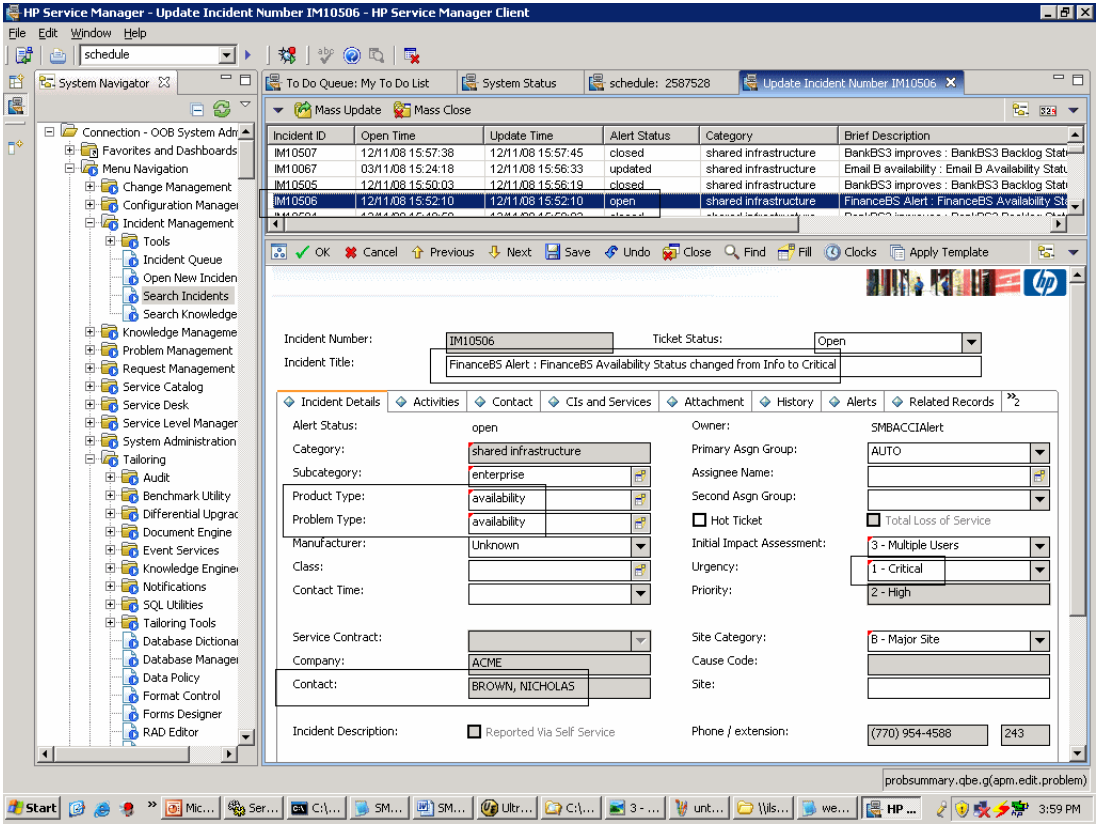
The default mapping can be modified in HP Service Manager.

For details about how HP Service Manager handles alerts, see "Life-Cycle of an Incident Triggered by a CI Status Alert in HP Service Manager – Scenario" on page 118.

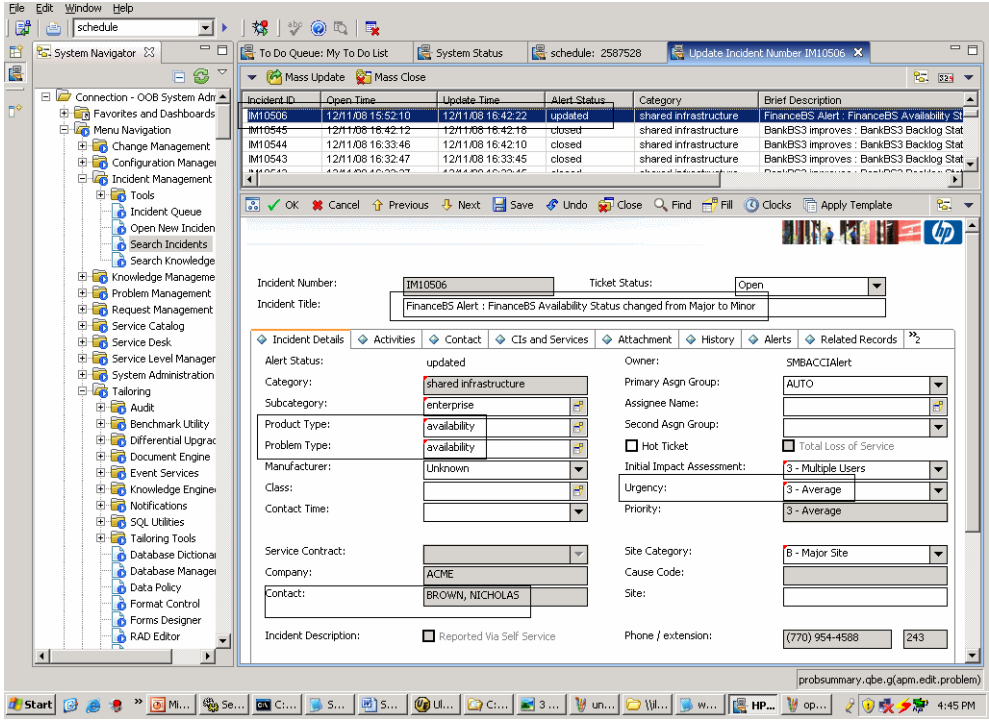
Life-Cycle of an Incident Triggered by a CI Status Alert in HP Service Manager – Scenario

The scenario is as follows: a CI Status alert is triggered in Business Availability Center, and at the scheduled time HP Service Manager retrieves the alert information from Business Availability Center and creates an incident. The alert is then updated and closed in Business Availability Center. You can view what happens in HP Service Manager as follows:

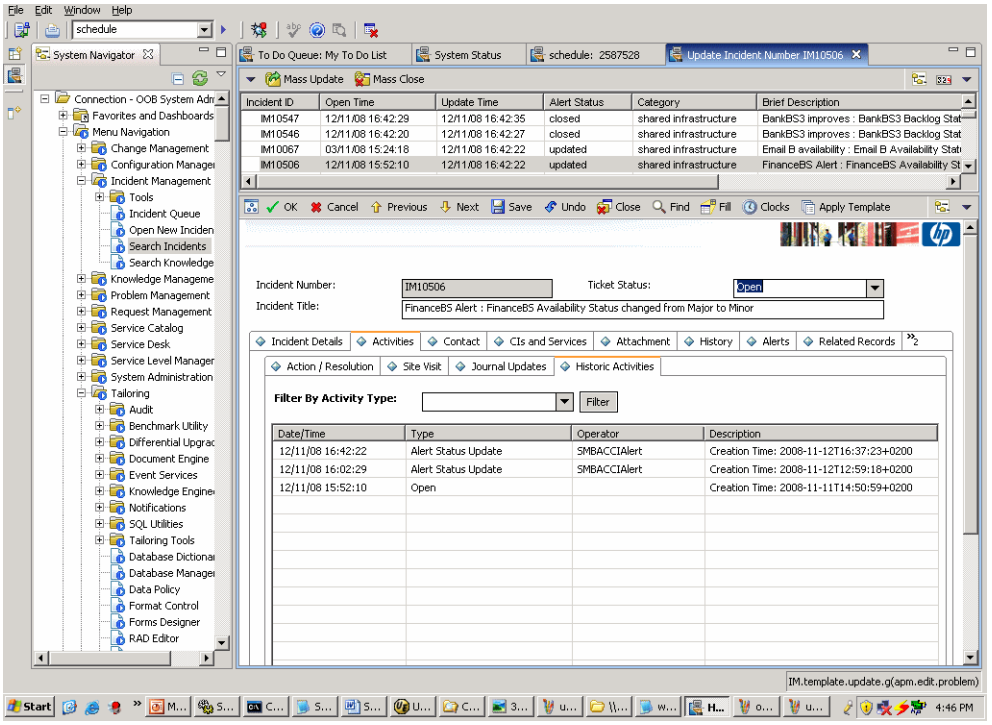
➤ **An incident is created.** The Incident Details tab displays the fact that an alert triggered because the FinanceBS CI status changed to Critical was retrieved by HP Service Manager and as a result a new incident was opened in HP Service Manager where the Urgency is Critical, the Product Type and Problem Type as availability, and the contact person is Nicholas Brown. The log indicates that the incident was opened.



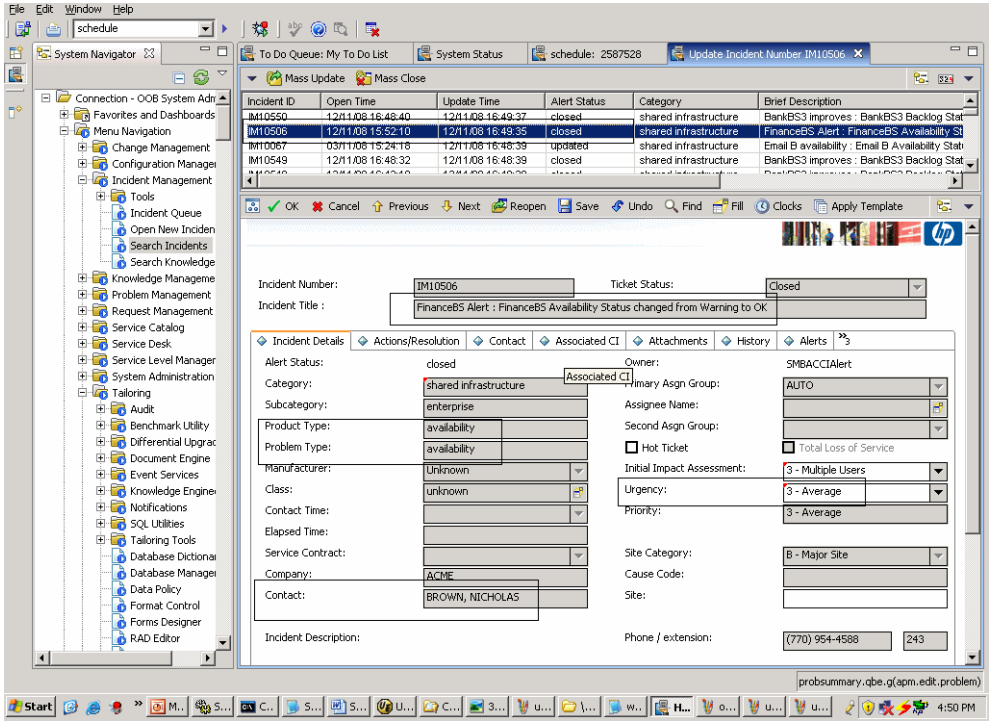
➤ **An incident is updated**. The Incident Details tab displays the fact that an alert triggered because the FinanceBS CI status changed from Major to Minor, was retrieved by HP Service Manager and as a result the previous incident was updated in HP Service Manager. The Urgency changed to Average. The other parameters stayed the same. The log indicates that the incident was updated.



You can view the incident history by clicking on each entry in the log.



➤ **An incident is closed.** The Incident Details tab displays the fact that an alert triggered because the FinanceBS CI status changed from Warning to OK was retrieved by HP Service Manager and as a result the incident was closed in HP Service Manager. The Urgency is Average. The other parameters stayed the same. The log indicates that the incident was closed.



Rule and Field Mapping in HP Service Manager

This section describes the rule and the field mapping used in the integration of HP Service Manager with Business Availability Center.

Note: This section is for advanced users.

This section includes the following topics:

Business Availability Center Alert/HP Service Manager Incident Correlation Rules

In the Business Availability Center Alert Feed process workflow, rules are used to search, create, update and close incidents.

The rules are configured in the Business Availability Center Alert Integration Configuration page. (To access the page, in the HP Service Manager client, select **Menu Navigation** > **System Administration** > **BAC Alert Integration** > **BAC Alert Integration Configuration**.)

For details about the correlation rules, see "Business Availability Center Alert/HP Service Manager Incident Correlation Rules" on page 178.

How the Rules Work

When an Business Availability Center CI Status alert is retrieved, the HP Service Manager database searches for a keyword (CI ID and the KPI name of the CI whose change of status triggered the alert) that is part of the data retrieved with the alert. The keyword is used to determine if the corresponding incident already exists in the database and thus should be updated or closed or if the incident does not exist and should be created. The search is done as follows:

- The search process uses information from the alert. The Correlation Rule is appended to the search clause. If there is no compatible information, the process searches again using the legacy Correlation Rule.
- If a target incident is not found, the process creates a new incident using the fields in the alert.
- If a target incident is found, the process checks if one of the three rules matches the alert retrieved from Business Availability Center (target incident is **true**).
  - If no rule matches, the rule **failed** and the target incident cannot be updated. The process then checks if the target incident is **true** to the Close Rule. If it is **true**, the process closes the action for target incident; if it is not **true**, the target incident is **Dropped.**
  - If a rule matches, its action is performed. For example, if the incident matches the Update Rule the process updates the existing incident in HP Service Manager with the alert information.

For additional details, see Opening Incidents in HP Service Manager – Overview on page 114.

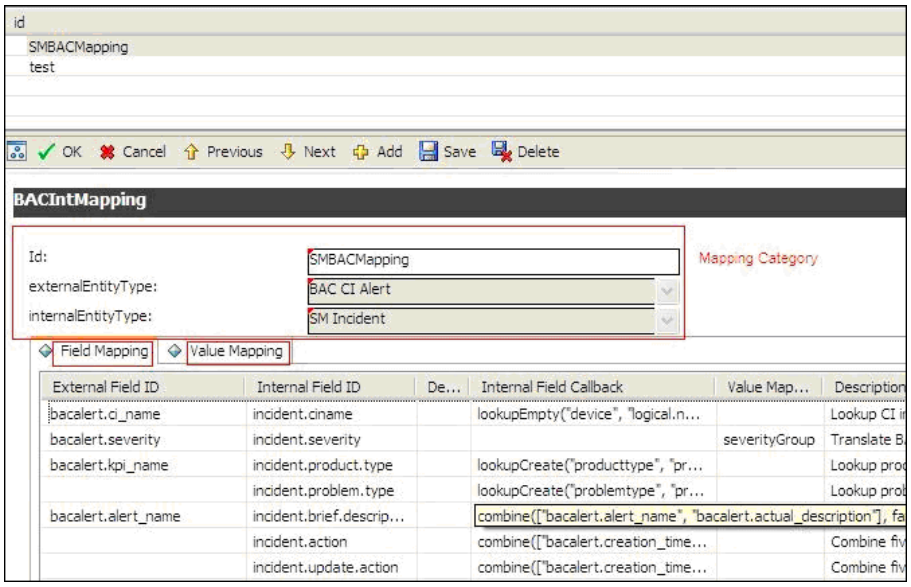
Note: The three rules use the severity value as the condition value, so when the three rules are changed, the severity value should be taken into consideration. The severity values are set in the **Value Mapping.**

Field Mapping Relationship

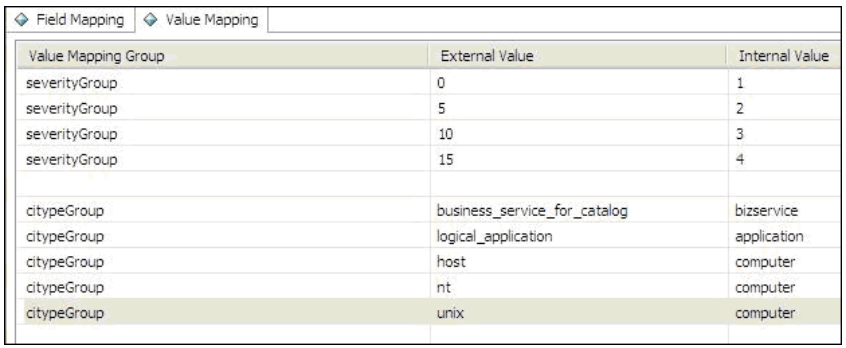
A field mapping relationship includes the following components:

Components	Description
Entity	Defines the side to be mapped as an Entity, where HP Business Availability Center CI Status alert is one entity and the HP Service Manager incident is another entity. For details, see "Entity" on page 192.
Field	Each entity has many fields used to define it. This component defines the fields of each entity (defined above). Each field has several properties detailed in the Mapping component description. For details, see "Field" on page 188.
Mapping	Both the Entity and Field components represent the basic data of the Mapping Component. The Mapping Component uses Entity and Field to show the relationship between the special entities. For details, see "Field Mapping" on page 193. The Mapping Component includes the following: **Mapping Category** ➤ It defines the main properties of this Mapping. ➤ It specifies the external entity and the internal entity. **Field Mapping** ➤ It defines the fields mapping relationship between the internal system and external entity. ➤ It also defines the default value used if the external field does not exist or if it does not have a value. ➤ It provides the Callback function for the assignment of default value. Five callback functions are defined in this process. These functions are invoked to assign a value to the field of HP Service Manager. For details about the callback function, see "Callback Functions" on page 203. These functions can be used for field mapping instead of values. **Value Mapping** ➤ It defines the fields that have the Enumerate values in both systems and how they are mapped between the internal system and external system.

Example of Mapping category and field mapping:



Example of value mapping:



How to Build a Field Mapping Relationship

Field Mapping represents the relationship between the Business Availability Center Alert Field and HP Service Manager Incident.

If you want to add additional mapping or you want to modify existing mapping, you must create or modify the Field Mapping relationship between a Business Availability Center Alert field and the corresponding HP Service Manager Incident field. After the two fields have been mapped, proceed as explained in "Configure HP Service Manager for Integration with Business Availability Center Alerts" on page 132.

For details on adding a new mapping or modifying an existing mapping, see "Maintain the BAC Alert Integration Field" on page 158.

Rules for Building Field Mapping Relationship

When you build the new Field Mapping, the following rules should be followed.

➤ **Rule of the Callback Function in the Internal Field Callback column**:

Condition	Description
No callback is used	This means that the **Internal Field Callback** column is empty. ➤ If the external (Business Availability Center Alert) field has value, set this value. ➤ If the value is empty, use the default value in the **Default Internal Field Value** column. **Example:** The example is based on the out-of-the-box data. Select **System Administration** -> **Base System Configuration** -> **BAC Alert Integration Field Mapping** and check the record line that includes **bacalert.ci_id**. In this scenario, the value in **bacalert.ci_id** is used as the value for **incident.bac.ci.id**. For example, check as above, the record line that includes **incident.category**. In this scenario, the default value in **Default Internal Field Value** is used as the value for **incident.category**.
The **lookup** Callback is used	➤ The **lookup** Callback sets the value. ➤ If the lookup fails, the Callback uses the value passed from the external field (Business Availability Center Alert). ➤ If the value is empty, the Callback uses the default value in the **Default Internal Field Value** column. **Example:** The example is based on the out-of-the-box data. Select **System Administration** -> **Base System Configuration** -> **BAC Alert Integration Field Mapping** and check the record line that includes **incident.category**. In this scenario, the value in **bacalert.ci_id** is used as the value for **incident.category**. For example, check as above, the record line that includes **incident.site.category**. In this scenario, if the lookup is successful, the lookup value is used as the value for **incident.site.category**; if lookup fails, the default value is used.

Condition	Description
The **setValue** Callback is used	➤ If this function only has one parameter, the Callback sets the value from Business Availability Center only when the current action corresponds to the action specified by the parameter; if this value is empty, set the default value. ➤ If this function has two parameters, the current action uses the second parameter to set the value of the current field, and the value from Business Availability Center or the default value is ignored. **Example:** The example is based on the out-of-the-box data. Select **System Administration -> Base System Configuration -> BAC Alert Integration Field Mapping** and check the record line that includes **incident.resolution.code** In this scenario, the value **User Closure** is used as the value for **incident.resolution.code**.
Other callback functions are used	These functions include: ➤ **lookupCreate** ➤ **lookupEmpty** ➤ **setValue** ➤ **combine** They handle the value assignment. The **External Field ID** and **Default Internal Field Value** are ignored. **Example:** The example is based on the out-of-the-box data. Select **System Administration -> Base System Configuration -> BAC Alert Integration Field Mapping** and check the record line that includes **incident.brief.description**. In this scenario, the **combine** Callback sets the value for **incident.brief.description**, independently of the value passed from Business Availability Center. For details about the callback functions, see "Callback Functions" on page 203.

➤ **Rule of the Severity.** If you modify the severity (in the Value Mapping tab), the mapping between HP Service Manager severity and Business Availability Center status might affect the processes, so the corresponding rule (Create, Update, and Close rules) might have to be modified. Please refer the content of chapter **BAC Alert/SM Incident Correlation Rules** in HP Service Manager documentation.

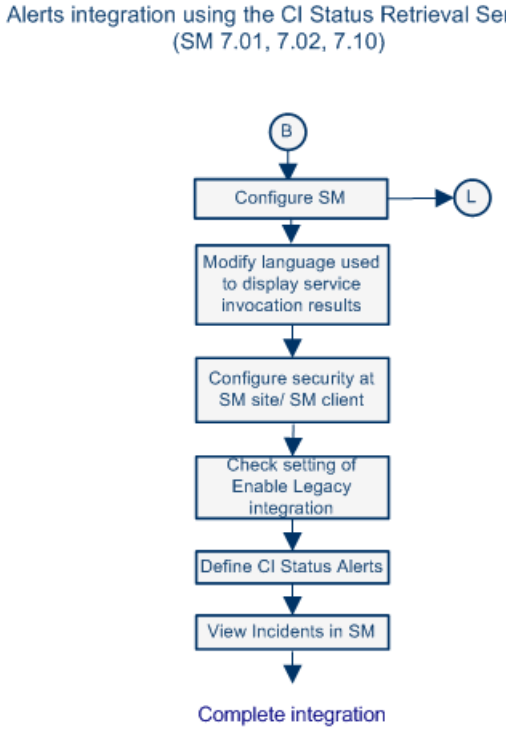
Open Incidents Using the CI Alert Retrieval Service

You can automatically manage (open, update, or close) an incident in HP Service Manager when a CI Status alert is triggered in Business Availability Center.

HP Service Manager retrieves the information about the alert from Business Availability Center using the CI Alert Retrieval Service. For details, see "CI Alert Retrieval Service API Overview" on page 164.

For details on the mechanism used to open an incident in HP Service Manager when a CI Status alert is triggered, see "Opening Incidents in HP Service Manager – Overview" on page 114.

The flowchart is as follows:



For details about L, see "Configure HP Service Manager for Integration with Business Availability Center Alerts" on page 132.

For details about Complete integration, see "Set Up the Integration of HP Service Manager Data with HP Business Availability Center Components - Workflow" in *Solutions and Integrations*.

This task includes the following steps:

- "Configure HP Service Manager" on page 131
- "Check the Setting of the Enable Legacy Integration with Service Manager Parameter" on page 131
- "Define CI Status Alerts" on page 131

➤ "Results - View Incidents in HP Service Manager" on page 131

1 Configure HP Service Manager

You must configure HP Service Manager before performing its integration with Business Availability Center. For details, see "Configure HP Service Manager for Integration with Business Availability Center Alerts" on page 132.

2 Check the Setting of the Enable Legacy Integration with Service Manager Parameter

When you perform the integration of the Alerts application with HP Service Manager using the CI Alert Retrieval Service you must make sure that the **Enable legacy integration with Service Manager** is set to **false**.

To check if the parameter is set to **false**, in Business Availability Center, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **Integration with other applications**, and locate the **Enable legacy integration with Service Manager** entry in the Integrations with other applications - Alerts-Service Manager Integration table.

3 Define CI Status Alerts

Define CI status alerts. For details, see "Create a CI Status Alert Scheme and Attach it to a CI" on page 65.

Select the Open incident in Service Manager option in the Actions page in the CI Status Alerts wizard. For details, see "Actions Page" on page 91.

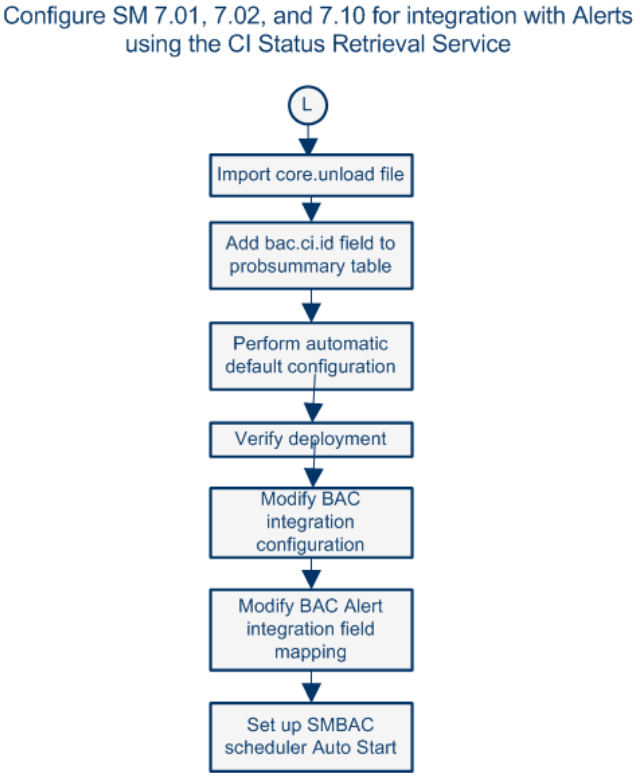
4 Results - View Incidents in HP Service Manager

View, in HP Service Manager, the incidents related to the CI Status alerts in Business Availability Center. For details, see HP Service Manager documentation.

Configure HP Service Manager for Integration with Business Availability Center Alerts

This section describes how to deploy and administer HP Service Manager for integration with Business Availability Center before the integration with Business Availability Center. The steps are performed in HP Service Manager.

The flowchart is as follows:



After you complete this task, proceed to “Open Incidents Using the CI Alert Retrieval Service” on page 129.

This task includes the following steps:

1 Import the Core Unload File

The core Unload file includes the basic logic of the integration with Business Availability Center integration.

Import the core Unload file as follows:

a In HP Service Manager, click **Menu Navigation** > **Tailoring** > **Database Manager**.

b Right-click the detail button and select **Import/Load**.

c In the HP Service Manager File Load/Import, click **Specify File** to locate the appropriate file:

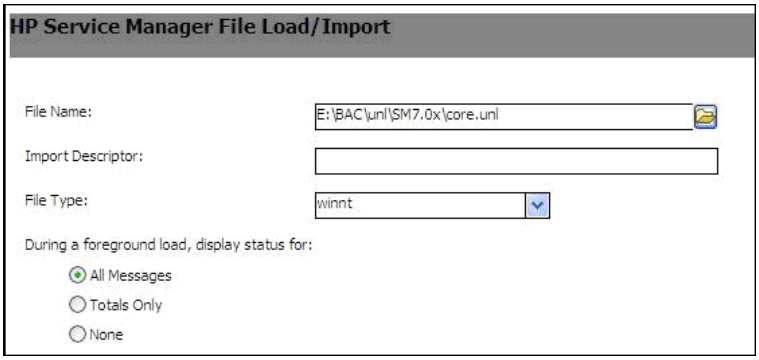
Integration with	File:
HP Service Manager 7.02	**<zip file>\unloads\SM7.0\smbac_core_sm7.02.unl**
HP Service Manager 7.10	**<zip file>\unloads\SM7.1\smbac_core_sm7.10.unl**

d Enter the description in the **Import Description** box.

e Select **winnt** in the **File Type** list.

f Select a display option.

g Click **Load FG** to start loading.



2 Add the bac.ci.id Field to the probsummary Table

Add one field to the **probsummary** table:

a In HP Service Manager, click **System Definition** > **Tables** > **probsummary** > **Fields.**

b Click the **New Field** button to add a new field.

c Enter **bac.ci.id** in the **Field Name** box.

d In the General Properties area, select **Character** in the **Data Type** list.

e Click the **Save** button to save the new field.

3 Perform the Automatic Default Configuration

This step describes how to import the **smbac_out-of-boxXXX.unl** file (where XXX represents different versions) to create the default configuration.

Note: You can also perform the equivalent procedure manually. For details, see "Mapping of Business Availability Center CI Types to HP Service Manager CI Types" in *Model Management*.

---

a In HP Service Manager, click **Menu Navigation** > **Tailoring** > **Database Manager**.

b Right-click the detail button and select **Import/Load**.

c In the HP Service Manager File Load/Import page, click **Specify File** to locate the appropriate file. The file is loaded via the file browser. It is located at:

Integration with	File:
HP Service Manager 7.02	**<zip file>\unloads\SM7.0\smbac_out-of-box_sm7.02.unl**
HP Service Manager 7.10	**<zip file>\unloads\SM7.1\smbac_out-of-box_sm7.10.unl**

d Enter the description in the **Import Description** box.

e Select **winnt** in the **File Type** list.

f Select a display option.

g Click **Load FG** to start loading.

After the deployment, the following components are affected as follows:

Contents	Description
Data about creating menu	The corresponding manual tasks are described in "Add a Main Menu" on page 156 and in "Add a Details Menu" on page 157.
Business Availability Center alert integration entity data	The corresponding manual task is described in "Maintain a BAC Alert Integration Entity" on page 158.
Business Availability Center alert integration field data	The corresponding manual task is described in "Maintain the BAC Alert Integration Field" on page 158.
Business Availability Center alert integration field mapping data	The corresponding manual task is described in "Maintain the Business Availability Center Alert Integration Field Mapping" on page 159.
Schedule data	The corresponding manual task is described in "Create Schedule" on page 161.
Link Customization	For details, see "Link Customization" on page 161.

4 Verify the Deployment

To verify that the deployment completed correctly, in HP Service Manager, use the following methods:

Verify Item	Method
Schedule	1 Go to the **Schedule** form (for details, see "Create Schedule" on page 161). 2 Enter **SMBAC CI Alert Integration** in the **Name box**. 3 Click **Search**. 4 Check the data against the "Create Schedule" on page 161.
Menu	1 Go to the **Menu** form (for details, see "Add a Main Menu" on page 156). 2 Enter **SYSTEM ADMINISTRATION** in the **Menu Name box** to check the Main menu data against "Main Menu Folder" on page 183. 3 Go to the **Menu** form (for details, see "Add a Main Menu" on page 156). 4 Enter **SMBAC Alert Integration** in the **Menu Name** box to check the Details menu data against "Detail Menu Items" on page 183.
BAC Alert Integration Entity	1 Go to **BAC Alert Integration Entity** form (for details, see "Maintain a BAC Alert Integration Entity" on page 158). 2 Click **Search** to check the data. (Refer to the "Field" on page 188 for details).
BAC Alert Integration Field	1 Go to **BAC Alert Integration Field** form (for details, see "Maintain the BAC Alert Integration Field" on page 158). 2 Click **Search** to check the data. (Refer to the "Entity" on page 192 for details).
BAC Alert Integration Field Mapping	1 Go to **BAC Alert Integration Field Mapping** form (for details, see "Maintain the Business Availability Center Alert Integration Field Mapping" on page 159). 2 Click **Search** to check the data. (Refer to the "Entity" on page 192 and "Field Mapping" on page 193 for details).
Link Customization	For details, see "Link Customization" on page 161.

5 Modify Business Availability Center Alert Integration Configuration

After the deployment is complete, you can configure the system to fit the customer's system environment.

HP Service Manager retrieves information about the CI Status alerts from Business Availability Center using the CI Alert Retrieval Service. For details, see "CI Alert Retrieval Service API Overview" on page 164.

a In HP Service Manager, click **Menu Navigation** > **System Administration** > **Base System Configuration** > **BAC Alert Integration** > **BAC Alert Integration Configuration**.

b Set up the CI Alert Retrieval Service API

The URL is used to access Business Availability Center. The original value of the URL is **http://<host name>/topaz/services/technical/customers/1/alerts/ci**. For details about the URL, see "CI Alert Retrieval Service API Overview" on page 164.

- Enter **bac.cialert.rest.url** in the **Name** box.
- Click **Search** to display the target configuration.
- Change the <**hostname**> to the Business Availability Center Gateway server URL.
- If you use SSL, change **http** to **https**.

c Set up the username

This username used to access the CI Alert Retrieval Service.

- Enter **username** in the **Name** field.
- Click **Search** to display the target configuration.
- Modify the value of this configuration. Change <**username**> to the available user name.

d Set up the password

The password used to access the CI Alert Retrieval Service.

- Enter **password** in the **Name** field.
- Click **Search** to display the target configuration.

- Modify the value of this configuration.
- Change the <**password**> to match the username above.

e Set up the BAC CI Alert Update Time

- Enter **update.time** in the **Name** field.
- Click **Search** to display the target configuration.
- Modify the value of this configuration; this time represents the time when HP Service Manager receives the Business Availability Center alert. Make sure you use the same format as in the original value.

6 Modify BAC Alert Integration Field Mapping

Display the currently-used Mapping ID (default: **SMBACMapping**) on the Configuration page and type the Description as **BAC-SM Mapping ID**.

a In HP Service Manager, click **Menu Navigation** > **System Administration** > **Base System Configuration** > **BAC Alert Integration** > **BAC Alert Integration Field Mapping**.

b Enter **SMBACMapping** in the **Id** box on the Field Mapping page, and click **Search**.

c Locate the cells under the Default Internal Field Value column. They should look like the table below (The default values must be populated, but the values may be different for different version of HP Service Manager. For example, 'shared infrastructure' does not exist in version 7.10, but exists in 7.02).

d Follow the Comments in the table to Insert/Modify the value. (When the field of a HP Service Manager incident is not matched, the callback function does not return a value, the default listed in the Default Internal Field Value column is used.)

Note: The Default Internal Field Value is case-sensitive.

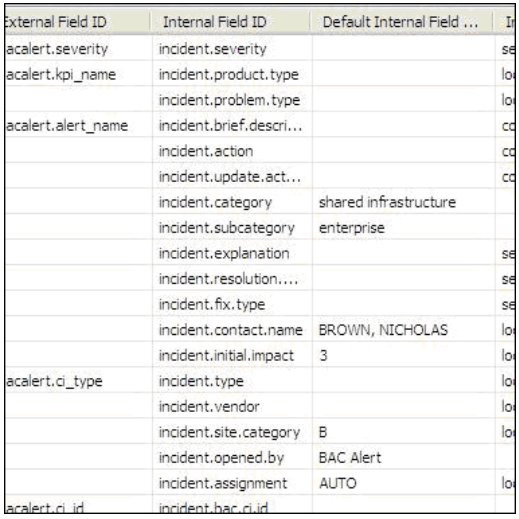
Internal Field ID (A-Z)	Default Internal Field Value (Recommend)	Comments
incident.assignment	AUTO	**Note: For HP Service Manager 7.02:** You can replace the default value with another assignment that exists in HP Service Manager. **Note: For HP Service Manager 7.10:** No recommended value. You can replace the default value with another assignment that exists in HP Service Manager. To see the existing values, select **Incident Management** > **Search Incidents** and select a value in the **Assignment Group** list.
incident.area		**Note: For HP Service Manager 7.10:** No recommended value. You can replace the default value with another area that exists in HP Service Manager. To see the existing values, select **Incident Management** > **Search Incidents**, set the cursor in the **Area** box and click the **Fill Information** button.

Internal Field ID (A-Z)	Default Internal Field Value (Recommend)	Comments
incident.category	shared infrastructure	**Note: For HP Service Manager 7.02:** Can be changed to another value that exists in HP Service Manager. **Note: For HP Service Manager 7.10:** No recommended value. You can replace the default value with another category that exists in HP Service Manager. You can change the default value **shared infrastructure** (in HP Service Manager, click **Menu Navigation** > **System Administration** > **Base System Configuration** > **BAC Alert Integration** > **BAC Alert Integration Field Mapping**). The new default value must exist in HP Service Manager. To check if the value exists, select **Incident Management** >**Tools** > **Categories**.
incident.contact.name		**Note: For HP Service Manager 7.02 only:** No recommended value. Enter an existing contact name. This field is not used when working with HP Service Manager 7.1.
incident.initial.impact	3	**Note: For HP Service Manager 7.02 and HP Service Manager 7.10:** 1-Enterprise 2-Site/Dept 3-Multiple Users 4-User
incident.opened.by	BAC Alert	**Note: For HP Service Manager 7.02 and HP Service Manager 7.10:** You can replace the default value with another word.

Internal Field ID (A-Z)	Default Internal Field Value (Recommend)	Comments
incident.service	applications	**Note: For HP Service Manager 7.1 only:** You can change the default value to any value that exists in HP Service Manager. To check if the value exists, select I**ncident Management >Incident Management** > **Search Incidents**, set the cursor on the **Service** box and click the **Fill Information** button.
incident.site.category	B	**Note: For HP Service Manager 7.02 only:** This field is not used when working with HP Service Manager 7.1. A-Critical Site B-Major Site C-Satellite Site D-Home Site remote-Remote
incident.subcategory	enterprise	**Note: For HP Service Manager 7.02 only:** Can be changed to another value that exists in HP Service Manager. You can change the default value **shared enterprise** (in HP Service Manager, click **Menu Navigation** > **System Administration** > **Base System Configuration** > **BAC Alert Integration** > **BAC Alert Integration Field Mapping**). The new default value must exist in HP Service Manager. To check if the value exists, select Incident Management >Tools > Subcategories.

Example

This is an example for HP Service Manager 7.02.



External Field ID	Internal Field ID	Default Internal Field ...	I
acalert.severity	incident.severity		se
acalert.kpi_name	incident.product.type		lo
	incident.problem.type		lo
acalert.alert_name	incident.brief.descri...		co
	incident.action		co
	incident.update.act...		co
	incident.category	shared infrastructure	
	incident.subcategory	enterprise	
	incident.explanation		se
	incident.resolution....		se
	incident.fix.type		se
	incident.contact.name	BROWN, NICHOLAS	lo
	incident.initial.impact	3	lo
acalert.ci_type	incident.type		lo
	incident.vendor		lo
	incident.site.category	B	lo
	incident.opened.by	BAC Alert	
	incident.assignment	AUTO	lo
acalert.ci_id	incident.bac.ci.id		

7 Set Up the SMBAC Scheduler Auto Start

To make sure the SMBAC scheduler auto-starts/restarts after HP Service Manager stars/restarts, check that scheduler starts at the right time, as follows:

a In HP Service Manager, type the **info** command in the Service Manager command line, and enter **startup** in the **Type** box.

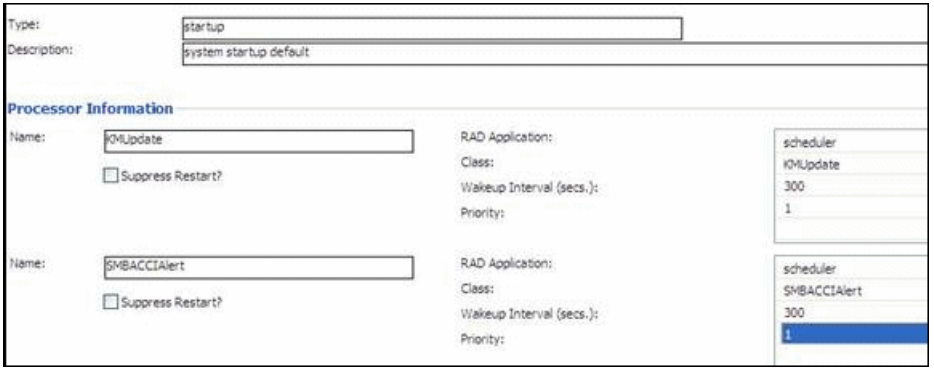
b Click **Search**, in the Processor Information area, scroll down to SMBACCIAlert, and check that the data is like in the following table. If needed.

c Click **Add** to save the changes.

Field	Value	Description
RAD application	scheduler	
Class	SMBACCIAlert	The same class as the one in the above table.

Field	Value	Description
Wakeup Interval (Seconds)	300	The time that is converted into seconds by the Repeat Interval field in the table above.
Priority	1	

The Processor Information user interface is as follows:



8 Modify the Language Used to Display the Service Invocation Results

The language you selected for the browser is used to display the Service Invocation results. It causes the CI Alert Retrieval service to retrieve the description and condition description of the alert for this language, from Business Availability Center. If you are not using a browser to display the Service Invocation results, you must specify the requested language in the header of the HTTP request.

You set the supported language in BAC Alert Integration Configuration form: in HP Service Manager, select **System Administration> Base System Configuration > BAC Alert Integration Configuration**, and modify the value of the **Accept-Language** configuration. The default value is **en**.

For details about the languages are supported by Business Availability Center, see “Working in Non-English Locales” in *Reference Information*.

9 Configure the Security at the HP Service Manager Site – Optional

To ensure the communication security between the CI Alert Retrieval Service (HP Service Manager site) and Business Availability Center CI Alert Retrieval Service web server (Business Availability Center site), the system supports using HTTP over SSL or HTTPS.

The CI Alert Retrieval Service web server URL is contained in the Configuration component.

For additional details, see "Examples of Security Configuration" on page 150.

To support HTTPS communication at the HP Service Manager site:

a In HP Service Manager, generate a public/private key pair with the following keytool, using the following command:
keytool -genkey -keystore sm_keystore.jks -alias sm

You are prompted to type in the password and private key for the keystore, and your last name and first name. You must type in the FQDN (full qualified domain name) of your server when you are prompted for your last name and first name.

b Generate the certificate signing request, using the following command:
keytool -certreq -keystore sm_keystore.jks -alias sm -file sm.csr

c Sign using the Certificate Authority (CA).

- **Sign the certificate by trusted CA.** You must use a trusted CA private key to sign the certificate. You send your own CSR (**smclientcert_req.crs**) to the trusted CA. It returns a certification as **smclientcert.cer**.
- **Sign the Certificate by the Self-signed CA.** See the "Sign the Certificate by the Self-signed CA (optional)" on page 151 section to get more information.

d Import the CA root certificate to the keystore, using the following command:
keytool -import -file ca.cer -trustcacerts -keystore sm_keystore.jks -alias ca

e Import the **certificate reply** back to key store, using the following command:
keytool -import -file sm.cer -trustcacerts -keystore sm_keystore.jks -alias sm

The alias name used in this command must be the same as the alias name used in the first step so that the signed certificate reply can be paired with the original private key correctly.

f Create a directory to hold your key store (for example, **%SM_SERVER%/RUN/security**), and save the **sm_keystore.jks** file in this directory.

g Enable SM SSL Setting by opening **sm.ini** in the directory where you install the HP Service Manager server, and set the setting as indicated below. For details, see "Parameters Setting in the sm.ini File" on page 181.

```
# SSL configuration
ssl:1
ssl_reqClientAuth:1
sslConnector:1
httpsPort:13443

# Certificates
truststoreFile:security/sm_keystore.jks
truststorePass:password
keystoreFile:security/sm_keystore.jks
keystorePass:password
```

h Restart the HP Service Manager server service. In the HP Service Manager server machine, select **Start** > **Settings** > **Control Panel** > **Administrative tools** > **Services**, and restart HP Service Manager 7.XX Server.

10 Configure the Security at the HP Service Manager Client – Optional

Perform this step to ensure that the client can connect to the HP Service Manager site when the HP Service Manager site opens the SSL.

To support HTTPS communication at the HP Service Manager client:

a Generate a public/private key pair with the following keytool, using the following command: **keytool -genkey -alias smclient -keystore smclient_keystore.jks**

b Generate the certificate signing request, using the following command: **keytool -certreq -alias smclient -keystore smclient_keystore.jks -file smclientcert_req.crs**

c Sign using the Certificate Authority (CA).

- **Sign the certificate by trusted CA.** You must use a trusted CA private key to sign the certificate. You send your own CSR (**sm.csr**) to the trusted CA. It returns a certification as **sm.cer**.
- **Sign the Certificate by the Self-signed CA.** See the "Sign the Certificate by the Self-signed CA (optional)" on page 151 section to get more information.

d Import the CA root certificate to the keystore, using the following command: **keytool -import -trustcacerts -alias smca -keystore smclient_keystore.jks -file ca.cer**

e Import the certificate reply back to key store, using the following command: **keytool -import -trustcacerts -alias smclient -keystore smclient_keystore.jks -file smclientcert.cer**

f Import the CA root certificate to trust key store, using the following (key store cacerts is in **<windows path >\HP\Service Manager 7.02\Client\plugins\com.hp.ov.sm.client.common_7.02**, it is better direct to this folder to run the following command) command: **keytool -import -keystore cacerts -trustcacerts -alias smca -file ca.cer**

You must also configure the SSL in the HP Service Manager client:

a Open the Service Manager Client.

b From the menu select **Window** > **Preferences...** to open the Preferences dialog box.

c Expand the HP Service Manager node in the left menu tree. Select **Security** to open the client security dialog.

d Click **Browse...**

e Specify the CA certificates file (**cacerts**) and Client keystore file (**smclient_keystore.jks**).

f Input the password of the client keystore in the Client keystore password field. Click **OK**.

g Restart Service Manager Client to enable the newly configured Security information.

h In the **Connections** dialog box, the value of the **Server host name** field must be the fully qualified name of the Service Manager server.

i In the **Advanced** tab, make sure that the **Use SSL Encryption** option is selected.

Important:

- If you have already set up HP Service Manager SSL with a certificate signed using the CA trusted by Business Availability Center, you do not need to make changes.
- If you have already set up HP Service Manager SSL with a certificate signed by a CA not trusted by Business Availability Center, you have two choices: to import the CA root certificate to Business Availability Center or to perform the steps above to create a new key pair and sign it with the CA root certificate which Business Availability Center trusts.
- HP Service Manager supports only the JKS format (PKCS12 format is not supported).
- The keystore password and the private key password must be the same.
- The Certificate has an expiry date; make sure you update your certificate periodically.
- Your key store and trust certificate store can be one JKS format store.
- You must specify the FQDN instead of IP address anytime you use HTTPS/SSL.

Examples of Security Configuration

➤ **Generate public/private key pair with keytool:**

```
D:\Program Files\HP\Service Manager 7.02\Server\RUN>keytool -genkey -keystore sm
_keystore.jks -alias sm

Enter keystore password: vinson
Re-enter new password: vinson
What is your first and last name?
  [Unknown]:  vinson
What is the name of your organizational unit?
  [Unknown]:  hp
What is the name of your organization?
  [Unknown]:  hp
What is the name of your City or Locality?
  [Unknown]:  shanghai
What is the name of your State or Province?
  [Unknown]:  shanghai
What is the two-letter country code for this unit?
  [Unknown]:  cn
Is CN=vinson, OU=hp, O=hp, L=shanghai, ST=shanghai, C=cn?
  [no]:  y
Enter key password for <sm>
(RETURN if same as keystore password):vinson
```

➤ **Generate the certificate signing request**

```
D:\Program Files\HP\Service Manager 7.02\Server\RUN>keytool -certreq -keystore s
m_keystore.jks -alias sm -file sm.csr
Enter keystore password: vinson
```

➤ **Sign it with the CA**

```
D:\Program Files\HP\Service Manager 7.02\Server\RUN>openssl x509 -req -days 365
-in sm.csr -out sm.cer -CA ca.cer -CAkey cakey.pem –Cacreateserial

Loading 'screen' into random state - done
Signature ok
subject=/C=cn/ST=shanghai/L=shanghai/O=hp/OU=hp/CN=vinson
Getting CA Private Key
Enter pass phrase for cakey.pem:
```

➤ **Import the CA root certificate to keystore**

```
D:\Program Files\HP\Service Manager 7.02\Server\RUN>keytool -import -file ca.cer
  -trustcacerts  -keystore sm_keystore.jks -alias ca

Enter keystore password: vinson
Owner: EMAILADDRESS=mail@mail.com, CN=vinson, OU=hp, O=hp, L=hp,
ST=shanghai, C=cn
Issuer: EMAILADDRESS=mail@mail.com, CN=vinson, OU=hp, O=hp, L=hp,
ST=shanghai,C=cn
Serial number: e611ad0fd5bc9e10
Valid from: Fri Oct 10 11:12:39 CST 2008 until Fri Jul 08 11:12:39 CST 2011
Certificate fingerprint:
      MD5: B5:D8:9F:A4:8B:24:70:79:DD:4D:0D:5A:44:12:F1:37
      SHA1: 7B:55:63:95:C7:14:F9:3B:C8:57:B6:81:24:A0:4F:00:78:CD:D1:94
Trust this certificate [no]:  y
Certificate was added to keystore
```

➤ **Import the "certificate reply" back to key store**

```
D:\Program Files\HP\Service Manager 7.02\Server\RUN>keytool -import -file sm.cer  -
trustcacerts  -keystore sm_keystore.jks -alias sm
Enter keystore password: Vinson
Certificate reply was installed in keystore
```

➤ **Sign the Certificate by the Self-signed CA (optional)**

This step generates the signed certification sm.cer.

➤ Generate the key pairs (private/public key):

```
D:\Program Files\HP\Service Manager 7.02\Server\RUN>openssl genrsa -des3 -out
cakey.pem 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus .............+++.............+++e is
65537 (0x10001)
Enter pass phrase for cakey.pem: Vinson
Verifying - Enter pass phrase for cakey.pem: vinson
```

➤ Generate the self-signed CA:

```
D:\Program Files\HP\Service Manager 7.02\Server\RUN>openssl req -config
openssl.conf -new -x509 -days 1001 -key cakey.pem -out ca.cer

Enter pass phrase for cakey.pem:
You are about to be asked to enter information that will be incorporated into your
certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:cn
State or Province Name (full name) [Some-State]: shanghai
Locality Name (e.g. city) []: shanghai
Organization Name (e.g. company) [Internet Widgits Pty Ltd]: hp
Organizational Unit Name (e.g. section) []: hp
Common Name (e.g. YOUR name) []: vinson
Email Address []:mail@mail.com
```

➤ Sign the certificate by the self-signed CA:

```
D:\Program Files\HP\Service Manager 7.02\Server\RUN>openssl x509 -req -days 365 -
in sm.csr -out sm.cer -CA ca.cer -CAkey cakey.pem –Cacreateserial

Loading 'screen' into random state – done
Signature ok
subject=/C=cn/ST=shanghai/L=shanghai/O=hp/OU=hp/CN=Vinson
Getting CA Private Key
Enter pass phrase for cakey.pem: vinson
```

Upgrade from the Previous Version of HP Service Manager Integration with Alerts

If you have installed the previous version of the integration of HP Service Manager with Alerts you must perform the following step to upgrade to the new version.

This task includes the following steps:

- "Uninstall the legacy HP ServiceCenter/HP Service Manager Integration" on page 153
- "Modify the Enable Legacy Integration in Business Availability Center Infrastructure Setting" on page 153

1 Uninstall the legacy HP ServiceCenter/HP Service Manager Integration

To uninstall the legacy HP ServiceCenter/HP Service Manager integration, proceed as follows:

a Stop the connected service.

b Undeploy the **smbac-1.00.war** from the web server.

c Maybe need manually deleted all of the scripts and tables created by the two unload files.

2 Modify the Enable Legacy Integration in Business Availability Center Infrastructure Setting

Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **Integrations with other applications**, and locate the **Enable Legacy Integration in Service Manager** entry in the Integrations with other applications - Alerts - Service Manager Integration table. Make sure the value is **false**.

Troubleshooting and Limitations

This section describes how to troubleshoot HP Service Manager deployment.

This section includes the following topics:

Business Availability Center Integration

Problem	Error Message	Root Cause	Solution
Error when performing an HTTP request	Error when doHTTPRequest. Please check the bac.cialert.rest.url in the configuration.	Error when Sending HTTP request to the REST server.	Check the configuration of the server URL. Modify URL to the correct URL. The name of this configuration is **bac.cialert.rest.url**
HP Business Availability Center alert feed not found	BAC alert feed not found, please check the Json format of BAC server response.	There is no **feed** attribute in the response file (json) from REST server.	Check the json data format. If needed, check the Business Availability Center Server.
BACRestClient parse error	BACRestClient parse error; Please check the json data format.	Json data cannot be parsed correctly.	Check the json data format. If needed, check the Business Availability Center Server.

Problem	Error Message	Root Cause	Solution
HP Business Availability Center fields validation fail	BAC fields validation fail! Please check the mapping settings with data from BAC Server.	The data from Business Availability Center Server is not consistent with mapping settings.	Check the Field Mapping and the Value Mapping.
Cannot find Mapping	Cannot find Mapping in SMBACMapping table with ID.	Mapping ID configured not found in SMBACMapping table.	Check the configuration of the Mapping ID. Modify the Mapping ID with the correct Mapping ID. The configuration name is **BAC-SM Mapping ID**.

Security (SSL)

Problem	Error Message	Root Cause	Solution
java.io.IOException: Cannot recover key	java.io.IOException: Cannot recover key at org.apache.tomcat.util.net.jsse.JSSE14SocketFactory.init(JSSE14SocketFactory.java:125).	The key entry password is different from the keystore password.	Make the two passwords consistent.
java.io.IOException: Cannot recover key	java.security.cert.CertificateNotYetValidException: NotBefore.	The server time is not correct. It is not included in the certificate valid time.	Modify the server time to match the certificate valid time.

Manually Install Out-of-Box Unload

All the configurations described in this section are provided by the out-of-box Unload (see "Perform the Automatic Default Configuration" on page 135) and typically require no modifications.

This section's steps serve as a reference and are only required if the Out-of-box Unload is not used or requires modification.

This task includes the following steps:

- "Add a Main Menu" on page 156
- "Add a Details Menu" on page 157
- "Maintain a BAC Alert Integration Entity" on page 158
- "Maintain the BAC Alert Integration Field" on page 158
- "Maintain the Business Availability Center Alert Integration Field Mapping" on page 159
- "Create Schedule" on page 161
- "Link Customization" on page 161
- "Modify the condition of the im.first Processes" on page 162

1 Add a Main Menu

This step describes how to add the Main Menu.

a Enter **menu** in the HP Service Manager command line.

b Go to the **Menu** page.

c Enter **SYSTEM ADMINISTRATION** in the **Menu Name** box to search the menu list.

d Add the data in "Main Menu Folder" on page 183 as one record to the **SYSTEM ADMINISTRATION** menu.

e Click **Save**.

The main menu records are as follows:

27	Ongoing Mainten...	Communication Utilities		menu.manager	name	COMM UTILITIES	index("SysAdmin", $lo.ucapex)>0
28	Ongoing Mainten...	System		menu.manager	name	SYSTEM	index("SysAdmin", $lo.ucapex)>0
29	Ongoing Mainten...	Environment Records		menu.manager	name	ENV RECORDS	index("SysAdmin", $lo.ucapex)>0
	Base System Co...	BAC Alert Integration		menu.manager	name	SMBAC Alert Integ...	index("SysAdmin", $lo.ucapex)>0

2 Add a Details Menu

This step describes how to add the Details Menu.

a Type **menu** in the HP Service Manager command line.

b Go to the **Menu** page.

c Type **SMBAC Alert Integration** in the **Menu Name** box, and type **menu.gui.base.bacalert** in the **Format** box.

d Click **Add** button to add this as a new menu.

e Add the data in “Detail Menu Items” on page 183 as the records to the new menu.

f Click **Save**.

The details menu records is as follows:

O..	G	Description	C.	Application	Pa...	Parameter Value	T	Condition
1		BAC Alert Integration Conf...		database	name	SMBACConfiguration		index("SysAdmin", $lo.ucapex)>0
2		BAC Alert Integration Entity		database	name	SMBACEntityType		index("SysAdmin", $lo.ucapex)>0
3		BAC Alert Integration Field		database	name	SMBACField		index("SysAdmin", $lo.ucapex)>0
4		BAC Alert Integration Field...		database	name	SMBACMapping		index("SysAdmin", $lo.ucapex)>0

3 Maintain a BAC Alert Integration Entity

This step describes how to maintain the Entity. For information about the possible values, see "Entity" on page 192.

a Click **Menu Navigation** > **System Administration** > **Base System Configuration** > **BAC Alert Integration** > **BAC Alert Integration Entity**.

b Proceed as follows:

- To add one entity, fill the **ID** and **Description** boxes, select the **BAC Entity** checkbox if necessary, and click **Add**.
- To update/remove one Entity, type the keyword of one or more fields, click **Search** to display the Entities to be updated/removed, modify the fields, and click **Save/Delete**.

4 Maintain the BAC Alert Integration Field

This step describes how to maintain the Field. For information about the possible values, see "Field" on page 188.

Click **Menu Navigation** > **System Administration** > **Base System Configuration** > **BAC Alert Integration** > **BAC Alert Integration Field**:

- To add one field, fill out the fields in the **BACIntField** area and click **Add**.
- To update/remove one field, type the keyword of one or more attributes, click **Search** to display the Fields to be updated/removed, modify the attributes, and click **Save/Delete**.

When you select the field type, take into consideration the real data type in file (table). Take the Field with the **incident.citype** id for example, you should check the real data type of the **type** field name in the **probsummary** file (select **System Definition** >**Tables** > **probsummary**) and match the real data type in the table (string, number, date, or Boolean).

The Max string length and multivalue attributes are for future use.

Note: If you add a new field to the table and configure it to the Field Mapping, you must restart the scheduler (as shown in step "Create Schedule" on page 161) to populate the new field.

---

5 Maintain the Business Availability Center Alert Integration Field Mapping

This step describes how to maintain the Field Mapping. For information about the possible values, see "Field Mapping" on page 193 and "Value Mapping" on page 202.

a Click **Menu Navigation** > **System Administration** > **Base System Configuration** > **BAC Alert Integration** > **BAC Alert Integration Field Mapping**.

b Proceed as follows:

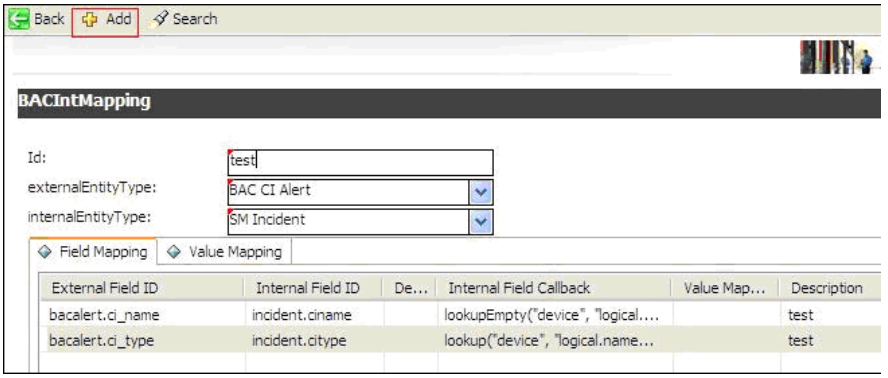
➤ To add one Field Mapping, fill the **Id** box, select one value from the drop list of **externalEntityType** and **internalEntityType**, for the cells in the picture below: select one value in **External Field ID** drop list, select one value in Internal **Field ID**, fill the **Internal Field Callback** and fill the other cells if needed, and click **Add** button to add the new Field mapping.

Note: When you add a new Field Mapping, you must only select the values available in the **externalEntityType** list (BAC CI Alert) and **internalEntityType** list (SM Incident). You cannot modify those values.

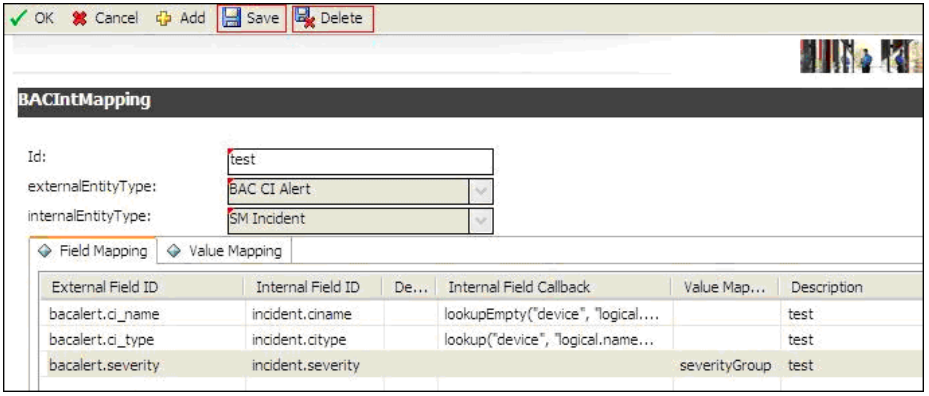
➤ To update one Field Mapping, get the target Field Mapping record via search system, modify the any fields value or table cells value, Or add records to the table **Field Mapping** and **Value Mapping**, and click **Save** to save the modification.

➤ To remove one Field Mapping, get the target **Field Mapping** record via search system, and click **Delete** to remove the modification.

Example of adding one field mapping:



Example of field mapping:



6 Create Schedule

This step describes how to maintain the Schedule. The schedule is used to start up the process.

Click **Menu Navigation** > **Tailoring** > **Database Manager**, type **schedule.looksee** in the **Form** field, go to the schedule editor, and use the data shown in the following table to setup the schedule:

Field	Default Value	Comments
Name	SMBAC CI Alert Integration	
Class	SMBACCIAlert	
Expiration		Choose a time
Action Time		Choose a time
Description	SMBAC CI Alert Integration	The field is in the Description tab.
Repeat Interval	00:05:00	The field is in the Description tab. It means the schedule runs every 5 minutes.
	var bacClient = new system.library.SMBACAlert Client.SMBACAlertClient(); bacClient.startup();	Enter the value in the Javascript tab.

7 Link Customization

Note: Perform this step if you are working with HP Service Manager 7.02. Skip this step if you are working with other versions.

To update the expression of the **contact.name** field and the two **logical.name** fields as **Source Field Name**:

a Click **Tailoring** > **Tailor Tools** > **Links**.

b Type **probsummary** as the Name and click **Search**.

c Find the line with **contact.name** as the **Source Field Name**.

d Right-click this line and select **SelectLine**.

e Modify the **contact.name** expression.

f Add one clause expression:
;if (nullsub($G.BACAlert, false)=true) then ($fill.recurse=false) else ($fill.recurse=true)

g Use the steps above to modify the expressions of the two **logical.name** fields.

8 Modify the condition of the im.first Processes

This step describes how to modify the condition of the im.first Processes.

Note: Perform this step if you are working with HP Service Manager 7.1. Skip this step if you are working with other versions.

---

a Click **System Administration** > **Tailoring** > **Document Engine** > **Processes**.

b Enter **im.first** in the Process Name field and click **Search**.

c Check the expression in the **Initial Expressions** tab. Change the condition from: **if ((operator()="problem" or operator()="EXTERNAL") and $G.bg) then ($L.add=true) else ($L.add=nullsub(evaluate(scm.add.condition in $L.object), false))**
to:
$L.add=nullsub(evaluate(scm.add.condition in $L.object), false)

6

CI Alert Retrieval Service

This chapter provides information on the CI Alert Retrieval service.

This chapter includes:

Concepts

Reference

CI Alert Retrieval Service API Overview

The CI Alert Retrieval Service can be used to retrieve information from the Alerts feed where CI Status alerts are stored after they are triggered. You access the service using URLs. The alert information is displayed in HTML, XML, or JSON format.

For details on how to open an incident in HP Service Manager, see "Open Incidents Using the CI Alert Retrieval Service" on page 129.

CI Alert Retrieval Service - Invocation

The URL used to invoke the CI Alert Retrieval Service, which retrieves alerts from Business Availability Center, has the following structure:

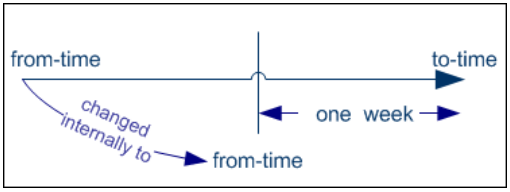
```
http://<host>/topaz/services/<security>/customers/1/alerts/ci?
alt=<alt>&mode=<mode>&ci-id=<ci-id>&extended-info=<extended-info>
&target-type=<target-type>&from-time=<from-time>
&to-time=<to-time>&severity=<severity>
```

Note: In the invocation URL, 1 is the customer ID (Business Availability Center supports more than one customer; the customer with ID=1 is the default client in a regular installation).

Parameters Passed to the Invocation URL

The following parameters are passed to the URL when invoking the CI Alert Retrieval Service:

Parameter Name (A - Z)	Remarks	Mandatory?
alt	Use one of the following media types: ➤ **application/atom%2Bxml** to return the alert information in XML format. ➤ **application/json** to return the alert information in JSON format. ➤ **text/html** to return the alert information in HTML format. For details, see "CI Alert Retrieval Service - Invocation" on page 164. For details on the alert information, see "Content Description" on page 174.	Mandatory
ci-id	Enter the list of CI IDs, separated with commas, that you want to use to filter the service invocation results. **Example:** A6912224862B7F15FC2081, C6612224862B7F15FC20813 To access the ID of a CI, select **Admin** > **Universal CMDB** > **Modeling** > **IT Universe Manager**, right-click the CI and select **Properties**, the CI ID is displayed.	Optional
extended-info	Use one of the following: ➤ **true** to return the CI Type and CI Name in the Service Invocation results during additional processing time. ➤ **false** not to return the CI Type and CI Name in the Service Invocation results.	Optional **Default:** false

Parameter Name (A - Z)	Remarks	Mandatory?
from-time	Enter the time from when the alerts are returned using the following format: **yyyy-mm-ddThh:mmZGMT_time_zone**. **Example:** 2007-11-15T21:19Z +03:00 **Note:** If the period of time between **from-time** and **to-time** is more than one week, **from-time** is moved to exactly one week before **to-time**. 	Optional **Note:** If you do not specify a value, the default is 24 hours before the current time when the URL is launched and no more than 500 alerts are displayed on a page.
mode	Use: ➤ **serial.** Use this mode when you want the recipient to receive the alerts triggered from the time indicated by the **Updated** field in the last Service Invocation results. The recipient receives the alerts one by one and does not receive alerts from overlapping time periods, after invoking the service. When you use **serial**, you do not have to enter a value for the **to-time** parameter. ➤ **regular.** Default. Use this mode when you want the recipient to receive all the alerts triggered between the **from-time** and **to-time** period.	Mandatory.
security	Use: ➤ **technical** when only the super user is allowed to retrieve the alerts. ➤ **business** when user authentication is required and security is handled by LWSSO.	Mandatory
severity	Enter a list of severities, separated with commas, to filter the information returned in the Service Invocation results. For details about the correspondence between the severities and the Business Availability Center statuses, see “Severity and Business Availability Center Status” on page 167.	Optional **Default:** All severities

Parameter Name (A - Z)	Remarks	Mandatory?
target_type	Use: ➤ **Incident.** To return only the alerts marked with the **Open incident in Service Manager** option in the CI Status Alert wizard. ➤ **All.** To return all the alerts.	Optional **Note:** If you do not specify a value, the default is **all**.
to-time	This represents the time after which the alerts are not returned in the Service Invocation results. **Example:** 2007-11-15T21:19Z +03:00	Optional **Note:** If you do not specify a value, the default is the current time when the URL is launched.

Severity and Business Availability Center Status

The correspondence between the HP Service Manager severity and the Business Availability Center status is as follows:

HP Business Availability Center Status	Severity
downtime	-4
stop	-3
no data	-2
uninitialized	-1
critical	0
major	5
minor	10

HP Business Availability Center Status	Severity
warning	15
OK	20

CI Alert Retrieval Service User Interface

This section describes:

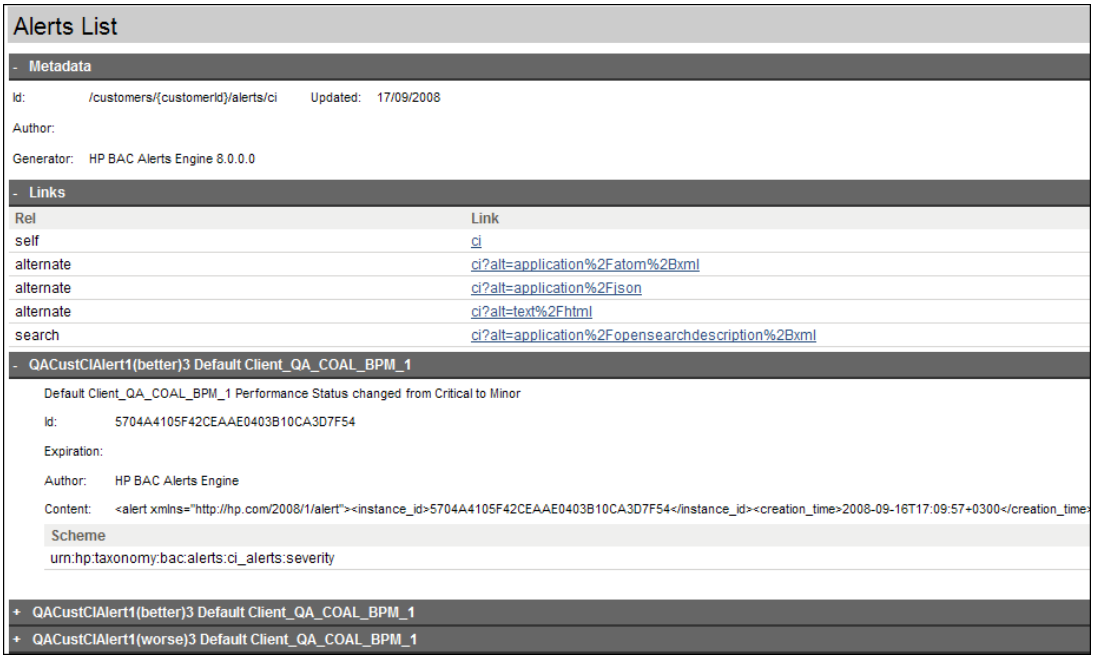
➤ CI Alert Retrieval Service Invocation Report on page 168

CI Alert Retrieval Service Invocation Report

Description	Displays the results of the CI Alert Retrieval Service Invocation in HTML, XML, or JSON format depending on your selection in the **alt** parameter: **To access:** Invoke the CI Alert Retrieval Service.
Important Information	Example of URLs used to invoke the service: ➤ To display the report in HTML format, use: http://<server>/topaz/services/technical/customers/1/alerts/ci?alt=text%2Fhtml ➤ To display the report in XML format, use: http://<server>/topaz/services/technical/customers/1/alerts/ci?alt=application%2Fatom%2Bxml ➤ To display the report in JSON format, use: http://<server>/topaz/services/technical/customers/1/alerts/ci?alt=application%2Fjson
Included in Tasks	➤ "CI Alert Retrieval Service API Overview" on page 164 ➤ "Open Incidents Using the CI Alert Retrieval Service" on page 129
Useful Links	➤ "Opening Incidents in HP Service Manager – Overview" on page 114 ➤ "CI Alert Retrieval Service API Overview" on page 164

Report Content

The following is an example of the CI Alert Retrieval Service Invocation in HTML format.



Alerts List

- Metadata

Id: /customers/{customerId}/alerts/ci Updated: 17/09/2008

Author:

Generator: HP BAC Alerts Engine 8.0.0.0

- Links

Rel	Link
self	ci
alternate	ci?alt=application%2Fatom%2Bxml
alternate	ci?alt=application%2Fjson
alternate	ci?alt=text%2Fhtml
search	ci?alt=application%2Fopensearchdescription%2Bxml

- QACustCIAlert1(better)3 Default Client_QA_COAL_BPM_1

Default Client_QA_COAL_BPM_1 Performance Status changed from Critical to Minor

Id: 5704A4105F42CEAAE0403B10CA3D7F54

Expiration:

Author: HP BAC Alerts Engine

Content: <alert xmlns="http://hp.com/2008/1/alert"><instance_id>5704A4105F42CEAAE0403B10CA3D7F54</instance_id><creation_time>2008-09-16T17:09:57+0300</creation_time>

Scheme
urn:hp:taxonomy:bac:alerts:ci_alerts:severity

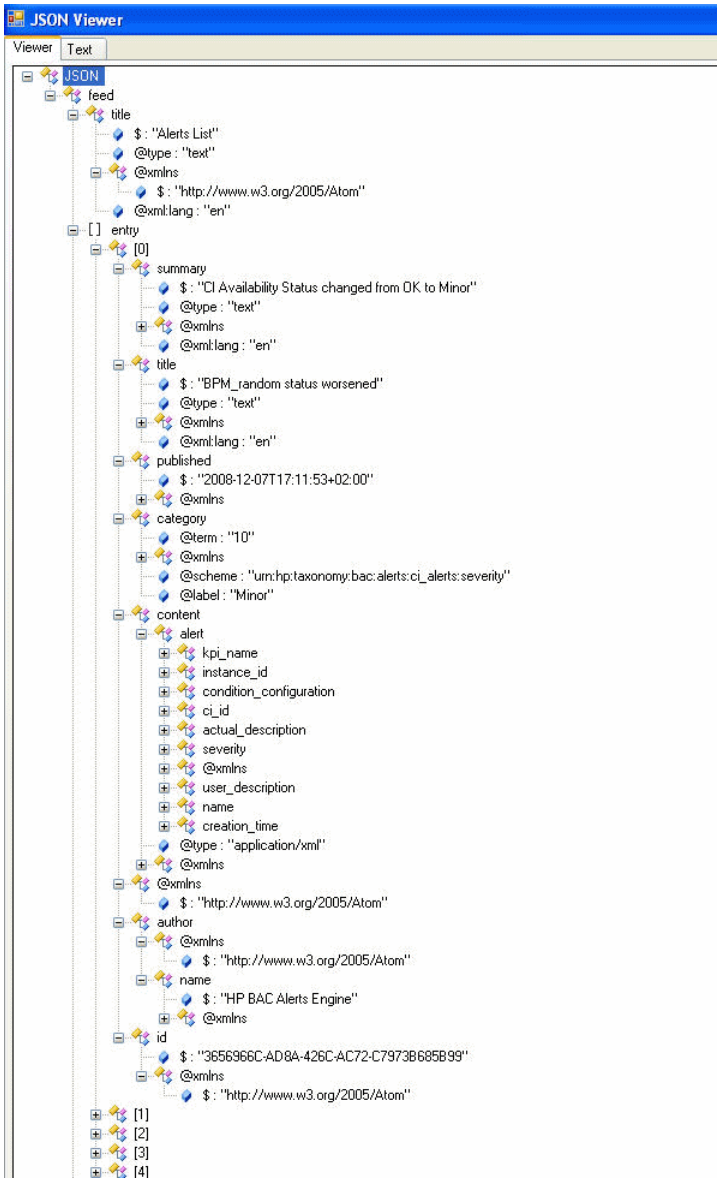
+ QACustCIAlert1(better)3 Default Client_QA_COAL_BPM_1

+ QACustCIAlert1(worse)3 Default Client_QA_COAL_BPM_1

The following is an example of the CI Alert Retrieval Service Invocation in XML format.

```
- <feed xmlns="http://www.w3.org/2005/Atom">
    <id>/customers/{customerId}/alerts/ci</id>
    <updated>2008-09-17T07:46:50+03:00</updated>
    <title type="text" xml:lang="en">Alerts List</title>
    <link href="ci" rel="self" />
    <link href="ci?alt=application%2Fatom%2Bxml" type="application/atom+xml" rel="alternate" />
    <link href="ci?alt=application%2Fjson" type="application/json" rel="alternate" />
    <link href="ci?alt=text%2Fhtml" type="text/html" rel="alternate" />
    <link href="ci?alt=application%2Fopensearchdescription%2Bxml"
      type="application/opensearchdescription+xml" rel="search" />
    <generator uri="/customers/{customerId}/alerts/ci" version="8.0.0.0">HP BAC Alerts
      Engine</generator>
  - <entry>
      <id>5704A4105F42CEAAE0403B10CA3D7F54</id>
      <title type="text" xml:lang="en">QACustCIAlert1(better)3 Default
        Client_QA_COAL_BPM_1</title>
      <category label="Minor" scheme="urn:hp:taxonomy:bac:alerts:ci_alerts:severity" term="10" />
    - <author>
        <name>HP BAC Alerts Engine</name>
      </author>
      <published>2008-09-16T17:09:57+03:00</published>
    - <content type="application/xml">
      - <alert xmlns="http://hp.com/2008/1/alert">
          <instance_id>5704A4105F42CEAAE0403B10CA3D7F54</instance_id>
          <creation_time>2008-09-16T17:09:57+0300</creation_time>
          <kpi_name>Performance</kpi_name>
          <ci_id>a6912224862b7f15fc208132cf1aa6d6</ci_id>
          <severity>10</severity>
          <name>QACustCIAlert1(better)3 Default Client_QA_COAL_BPM_1</name>
          <user_description>FIST Massive CI Alert Creation</user_description>
          <actual_description>CI Performance Status changed from Critical to
            Minor</actual_description>
          <condition_configuration>Status improved</condition_configuration>
        </alert>
      </content>
      <summary type="text" xml:lang="en">CI Performance Status changed from Critical to
        Minor</summary>
    </entry>
  - <entry>
```

The following is an example of the CI Alert Retrieval Service Invocation in XML format.



The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<CI_name> (HTML format) or **<entry> (XML or JSON format)**	The report includes a <CI_name> or <entry> section for each CI selected in the CI Alert Retrieval Service invocation. **Note:** The <CI_name> or <entry> sections are ordered by the alert time of occurrence. This section includes the following information: ➤ **author** displays the name of the Alerts Engine (always HP BAC Alerts Engine). ➤ **category** (only in XML or JSON format) lists the severity of the alert. For details, see "Severity and Business Availability Center Status" on page 167. ➤ **content** displays information about the alert. For details about the displayed information, see "Content Description" on page 174. ➤ **expiration** (only in HTML format) is empty. ➤ **id** displays the ID of the alert instance. ➤ **scheme** (only in HTML or XML format) displays the list of severities that the alert instance may have. ➤ **summary** provides a summary of the condition that occurred and caused the CI Status alert to be triggered. ➤ **title** (only in XML or JSON format) displays the alerts's name. ➤ **published** (only in XML or JSON format) displays the time when the alert was triggered in Business Availability Center.

GUI Element (A-Z)	Description
Links	This section includes the following links: ➤ **alternate** provides a link to the current report in XML, HTML, or JSON format. ➤ **next** (only in JSON format) provides a link to the next page. ➤ **search** provides a link to the OpenSearch description document. ➤ **self** provides a link to the OpenSearch description document.
Metadata (HTML format) or **<first section> (XML format and JSON format)**	This section includes general information about the invocation: ➤ **generator.** The version of the Alerts Engine in HTML or JSON format and the URI and the version and name of the Alerts Engine in XML format. ➤ **id.** The permanent URI where the feed can be read. ➤ **links.** (in XML or JSON format) See the row describing the links in this table. ➤ **Next link** or **next.** This field is returned if during the query time period, more alerts exist than the maximum alerts allowed in the response (500). The field is used as a link for paging to the next 500 alerts. ➤ **title.** (only in XML and JSON format) Always Alerts List. ➤ **updated.** The field returns the index of the last alert included in the feed (the time when the most recent alert was retrieved from Business Availability Center by HP Service Manager). The next invocation starts retrieving alert information from the time specified in the **Updated** field. If the alert's REST invocation is empty, the **updated** field returns the value of the **from-time** field.

Content Description

The alert details section or tag includes the following information:

Element Name (A - Z)	Description
actual_ description	Displays the condition that caused the alert to be triggered. **Example:** Application X status has changed to **Critical** from **Minor**
ci_id	The ID of the CI whose status change triggered the alert. **Example:** a6912224862b7f15fc208132cf1aa6d6
ci_name	The name of the CI whose status change triggered the alert. **Note:** This is displayed if you selected **extended_info=true**. **Example:** Login application
ci_type	The name of the Business Availability Center CI type. HP Service Manager should map it to the appropriate HP Service Manager CI types. For details, see "Mapping of Business Availability Center CI Types to HP Service Manager CI Types" in *Model Management*. **Note:** This is displayed if you selected **extended-info=true**. **Example:** Host, tx_from_location
condition_ configuration	The alert triggering condition that was configured by the user. **Example:** Send alert if CI status worsens
creation_time	The time when the alert was triggered. Depending on the mode you selected, the time when the alert was triggered might be outside of the time range specified in the invocation. **Example:** 2008-09-14T1709:57+03:00
instance_id	The internal ID number of the alert.
kpi_name	The name of the KPI that caused the status change for the CI for which the alert was created. **Example:** Performance

Element Name (A - Z)	Description
name	The name of the alert as configured by the user.
severity	The severity of the alert. For details about the severities, see "Severity and Business Availability Center Status" on page 167.
user_ description	The description of the alert as it was configured by the Business Availability Center user. **Example:** My alert - restart server when alert occurs.

7

Open Incidents Reference

This chapter provides reference information about the opening of incidents in HP Service Manager, using the CI Alert Retrieval Service, when CI Status alerts are triggered in HP Business Availability Center 8.0.

For details about how to open incidents in HP Service Manager, see "Opening Incidents in HP Service Manager – Overview" on page 114.

This chapter includes:

Reference

Business Availability Center Alert/HP Service Manager Incident Correlation Rules

In the Business Availability Center Alert Feed process work flow, rules are used to search, create, update and close incidents.

The rules are configured in the Business Availability Center Alert Integration Configuration page. To access the page, make sure you have installed the out-of-box unload file in the HP Service Manager navigator, and select **System Administration** > **Base System Configuration** > **BAC Alert Integration Configuration**. In the table below, the columns describe the rules:

Configuration Name	Category	Description
incident.correlation.rule	Rules	The value of this rule is a SQL clause Expression. This configuration is the condition for searching for the incident in HP Service Manager database. **Configurationvalue:** bac.ci.id = "$external.ci_id$" and product.type = "$external.kpi_name$" and problem.status <> "Closed" and problem.status <> "Resolved"
v1.incident.correlation.rule	Rules	The value of this rule is a SQL clause Expression. This configuration is the condition for searching for the incident in HP Service Manager database. **Configurationvalue:** logical.name = "$external.ci_name$" and problem.type = "$external.kpi_name$" and problem.status <> "Closed" and problem.status <> "Resolved"

Configuration Name	Category	Description
incident.create.rules	Rules	The value of this rule is a javascript Expression. The numbers (such as 10,20) are the severity value in Business Availability Center Alert, which is mapped in value mapping. $external.severity$ is the reference variable for the severity value. This rule means that if the value of the severity equals 0 or 5 or 10 or 15, the rule passes. **Configurationvalue:** $external.severity$ ==0 || $external.severity$ ==5 || $external.severity$ ==10 || $external.severity$ ==15
incident.create.action	Action	HP Service Manager action. Add a new incident which is translated from Business Availability Center Alert. **Configurationvalue:** addsave
incident.update.rules	Rules	The value of this rule is a javascript Expression. This rule means that if the value of the severity does **not** equal 20, the rule passes. **Configurationvalue:** $external.severity$ ==0 || $external.severity$ ==5 || $external.severity$ ==10 || $external.severity$ ==15
incident.update.action	Action	HP Service Manager action. Update the existed incident in HP Service Manager via the new related data in Business Availability Center Alert. **Configurationvalue:** save

Configuration Name	Category	Description
incident.close.rules	Rules	The value of this rule is a javascript Expression. This rule means that if the value of the severity equals 20, the rule passes. **Configurationvalue:** $external.severity$ ==20
incident.close.action	Action	HP Service Manager action. Close the existed incident in HP Service Manager via the new related data in Business Availability Center Alert. **Configurationvalue:** close

Where:

- **Configuration Name** provides the internal name of the rule.
- **Category** has two values: Rules and Action. The value of the configuration with the Rules category is the real constraint. The value of the configuration with the Action category is the action (the operation that is performed when the retrieved Alert matches the corresponding rule).
- **Description** describes the rule. Each create, update, or close rule has a corresponding Action configuration. When a rule is considered passed, the corresponding action is performed.
- **Configurationvalue** describes the rule condition. If the condition is fulfilled the rule is considered to have **passed**. The rule is considered to have **failed**, if the condition is not fulfilled.

Note: All the variables between dollar ($) signs represent fields in Business Availability Center CI Status alerts. The other variables represent fields in HP Service Manager incidents.

Parameters Setting in the sm.ini File

The table lists the parameters that can be used for SSL. For details, see "Configure the Security at the HP Service Manager Site – Optional" on page 145.

Parameters	Comments
-ssl: 1	0 = Does not require SSL for SOAP connections. 1=Require SSL for SOAP connections (optional).
-sslConnector: 1	0 = Does not load SSL connector. Default is 0 (optional). 1 = Load SSL connector.
-ssl_reqClientAuth: n	0 = Does not require client authentication. 1=Do client authentication. 2=Do client authentication and the client has to be a trusted client (optional).
-keystoreFile	Server keystore (optional).
-keystorePass	Pass phrase for server keystore. Default value is **changeit** (optional).
-truststoreFile	The TrustStore file to use to validate client certificates. Default to the cacerts in the **RUN\jre\security** directory (optional).
-truststorePass	The pass phrase for the TrustStore file. Default value is **changeit** (optional).
-ssl_trustedClientsJKS	A keystore file. This file contains a list of certificates that server trusts (optional).
-ssl_trustedClientsPwd	Pass phrase for the trusted client keystore file. (optional).

Business Availability Center Setting Parameters

The default settings used in the integration are as follows:

Settings and Details	Default value
Max time to retrieve data from the history The maximum period of time used to retrieve data from the history. **Note:** The maximum period of time is used only when you use a **serial** mode. There is no limit for **regular** mode. The default value can be modified by the HP Software Support.	1 week
Max number of rows returned in response The maximum number of rows returned in the Service Invocation results. **Note:** If more than 500 alerts are returned, the following line is added at the end of the report: <link href="ci?alt=application%2Fatom%2Bxml&mode=serial&from-time=2008-08-14T14%3A27%3A52%2B0300&extended-info=false" rel="next/> You can use the link to access the rest of the alert details.	500
Enable legacy ServiceCenter integration	false

Mapping Details

This section describes the data included in the out-of-box unload file used for the customization.

This section includes the following topics:

- "Entity" on page 192
- "Field Mapping" on page 193
- "Value Mapping" on page 202

Main Menu Folder

Option	Description
# Note: Enter a different number than the existing one. When you manually add this record to HP Service Manager, several records are already present.	Business Availability Center Alert Integration (can be customized). **Group:** Base System Configuration (can be customized). **Note:** Can be customized in other super menus. **Parameter name:** name **Application:** menu.manager **Parameter value:** SMBAC Alert Integration **Condition:** index("SysAdmin", $lo.ucapex)>0

Detail Menu Items

Option	Application	Description
1	database	Business Availability Center Alert Integration Configuration (can be customized). **Default value:** name **Additional information:** SMBACConfiguration **Condition:** index("SysAdmin", $lo.ucapex)>0
2	database	Business Availability Center Alert Integration Entity (can be customized). **Default value:** name **Additional information:** SMBACEntityType **Condition:** index("SysAdmin", $lo.ucapex)>0

Option	Application	Description
3	database	Business Availability Center Alert Integration Field (can be customized). **Default value:** name **Additional information:** SMBACField **Condition:** index("SysAdmin", $lo.ucapex)>0
4	database	Business Availability Center Alert Integration Field Mapping (can be customized). **Default value:** name **Additional information:** SMBACMapping **Condition:** index("SysAdmin", $lo.ucapex)>0

Configuration

Field Name (A-Z)	Application	Description
Accept-Language	Header	Business Availability Center Request Language Setting (can be customized). **Default value: en**
Bac.cialert.rest.url	Basic	REST WebService URL (CI Alert Retrieval Service API) (can be customized). **Default value:** http://<hostname>/topaz/services/technical/customers/1/alerts/ci **Additional information:** Hostname should be changed to Business Availability Center Rest web service URL.
http.conn.timeout	General	Http Connection Timeout Setting (can be customized). **Default value:** 30 (can be customized).
http.rec.timeout	General	Http Receive Timeout Setting (can be customized). **Default value:** 30 (can be customized).
http.send.timeout	General	Http Send Timeout Setting (can be customized). **Default value:** 30 (can be customized).

Field Name (A-Z)	Application	Description
Incident.close.action	Action	Business Availability Center Incident Close Action (can be customized). **Default value:** close
incident.close.rules	Rules	Business Availability Center In.cident Close Rule Condition (can be customized). **Default value:** $external.severity$ ==20 **Additional information:** $external.severity$ is the value of the **severity** field in Business Availability Center Alert. This expression follows the **JavaScript** grammar.
incident.corelation.rule	Rules	Incident correlation rule (can be customized). **Default value:** bac.ci.id = "$external.ci_id$" and product.type = "$external.kpi_name$" and problem.status <> "Closed" and problem.status <> "Resolved" **Additional information:** This expression follows the **SQL clause** grammar. This configuration is the condition used for searching the incident in the database.
Incident.create.action	Action	Business Availability Center Incident Creation Action (can be customized). **Default value:** addsave
incident.create.rules	Rules	Business Availability Center Incident Creation Rule Condition (can be customized). **Default value:** $external.severity$ ==0 || $external.severity$ ==5 || $external.severity$ ==10 || $external.severity$ ==15 **Additional information:** This expression follows the **JavaScript** grammar.
Incident.update.action	Action	Business Availability Center Incident Update Action (can be customized). **Default value:** save

Field Name (A-Z)	Application	Description
incident.update.rules	Rules	Business Availability Center Incident Update Rule Condition (can be customized). **Default value:** $external.severity$ ==0||&external.severity$==5\|\|$external.severity$ ==15 **Additional information:** This expression follows the **JavaScript** grammar.
json.feed.path	General	Business Availability Center Response Json Feed Path (can be customized). **Default value:** content.alert
logging.level	General	HP Service Manager Business Availability Center Logging Level (can be customized). **Default value:** INFO (can be customized). **Additional information:** The candidate values are DEBUG,INFO,WARN,ERROR,OFF
mappingId	General	Business Availability Center-HP Service Manager Mapping ID (can be customized). **Default value:** SMBACMapping (can be customized). **Additional information:** It can be changed according to the mapping ID in FieldMapping table.
password	Header	Password (can be customized). **Default value:** <Password> (Must be customized).
retry.times	General	Queue Retry Times (can be customized). **Default value:** 2 (can be customized).
updated.time	General	Business Availability Center CI Alert Update Time. **Note:** Can be customized. **Default value:** 2001-11-11T13:09:16+0800 (can be customized). **Additional information:** It usually should not be updated by customer.

Field Name (A-Z)	Application	Description
user	Header	User Name (can be customized). **Default value:** <user> (Must be customized). **Additional information:** The account of the REST Web Service. Set the checkbox **Is Password** to **true** for the Password configuration.
v1.incident. corelation.rule	Rules	Incident correlation rule when using the legacy URL (can be customized). **Default value:** ➤ **For HP Service Manager 7.02:** logical.name = "$external.ci_name$" and problem.type = "$external.kpi_name$" and problem.status <> "Closed" and problem.status <> "Resolved" ➤ **For HP Service Manager 7.1:** logical.name = "$external.ci_name$" and product.type = "$external.kpi_name$" and problem.status <> "Closed" and problem.status <> "Resolved" **Additional information:** This expression follows the **SQL clause** grammar. This configuration is the condition for searching the incident in the database (For the legacy URL data only).
version	General	Business Availability Center CI Alert and HP Service Manager Incident Submission Integration Version (can be customized). **Default value:** 01.00.001 **Additional information:** The version of the current build.

Field

The customization data listed in the table is for HP Service Manager 7.1 and 7.02 unless indicated otherwise.

Primary key in the Description column, indicates that the customization data is part of the keywords needed to identify the alert. This setting is used for fields of the BAC CI Alert type.

Required in the Description column, means that the field must have a value when the current alert is retrieved. If a required field is empty, the current alert is not retrieved. This setting is used for fields of the BAC CI Alert type.

ID (A-Z)	Entity Type	Description
bacalert. actual_description	BAC CI Alert	Actual Description (can be customized). **Field Name:** actual_description **Field Type:** string
bacalert.alert_name	BAC CI Alert	Alert name (can be customized). **Field Name:** name **Field Type:** string
bacalert.ci_id	BAC CI Alert	CI Alert ID (can be customized). **Note:** Primary Key **Field Name:** ci_id **Field Type:** string
bacalert.ci_name	BAC CI Alert	CI Alert Name (can be customized). **Field Name:** ci_name **Field Type:** string
bacalert.ci_type	BAC CI Alert	CI Alert Type (can be customized). **Field Name:** ci_type **Field Type:** string
bacalert.condition_ configuration	BAC CI Alert	Condition Configuration (can be customized). **Field Name:** condition_configuration **Field Type:** string

ID (A-Z)	Entity Type	Description
bacalert.creation_time	BAC CI Alert	Creation Time (can be customized). **Field Name:** creation_time **Field Type:** string
bacalert.kpi_name	BAC CI Alert	KPI Name (can be customized). **Note:** Primary Key **Field Name:** kpi_name **Field Type:** string
bacalert.severity	BAC CI Alert	Severity (can be customized). **Field Name:** severity **Field Type:** string
bacalert.user_description	BAC CI Alert	User Description (can be customized). **Field Name:** user_description **Field Type:** string
incident.action	SM Incident	Action (can be customized). **Field Name:** action **Field Type:** string
incident.area	SM Incident	**Note:** For HP Service Manager 7.1 Area (can be customized). **Field Name:** subcategory **Field Type:** string
incident.assignment	SM Incident	Assignment (can be customized). **Field Name:** assignment **Field Type:** string
incident.bac.ci.id	SM Incident	Business Availability Center CI Alert ID (can be customized). **Note:** Primary Key **Field Name:** bac.ci.id **Field Type:** string

ID (A-Z)	Entity Type	Description
incident.brief.description	SM Incident	Brief Description (can be customized). **Field Name:** brief.description **Field Type:** string
incident.category	SM Incident	Category (can be customized). **Field Name:** category **Field Type:** string
incident.ciname	SM Incident	CI Name (can be customized). **Field Name:** logical.name **Field Type:** string
incident.citype	SM Incident	CI Alert Type (can be customized). **Field Name:** type **Field Type:** string
incident.contact.name	SM Incident	Contact Name (can be customized). **Field Name:** contact.name **Field Type:** string
incident.explanation	SM Incident	Explanation (can be customized). **Note:** Multivalue **Field Name:** explanation **Field Type:** string
incident.fix.type	SM Incident	Fix Type (can be customized). **Field Name:** fix.type **Field Type:** string
incident.initial.impact	SM Incident	Initial Impact (can be customized). **Field Name:** initial.impact **Field Type:** string
incident.opened.by	SM Incident	Opened by (can be customized). **Field Name:** opened.by **Field Type:** string

ID (A-Z)	Entity Type	Description
incident.problem.type	SM Incident	Problem type (can be customized). **Field Name:** problem.type **Field Type:** string
incident.product.type	SM Incident	**Note:** For HP Service Manager 7.02 only. HP Service Manager Incident Product Type (can be customized). **Note:** ➤ Primary Key ➤ Required **Field Name:** Product.type **Field Type:** string
incident.resolution	SM Incident	Resolution (can be customized). **Note:** Multivalue **Field Name:** resolution **Field Type:** string
incident.resolution.code	SM Incident	Resolution Code (can be customized). **Field Name:** resolution.code **Field Type:** string
incident.service	SM Incident	**Note:** For HP Service Manager 7.1 only. Service (can be customized). **Field Name:** Affected.item **Field Type:** string
incident.severity	SM Incident	Severity (can be customized). **Field Name:** severity **Field Type:** string
incident.site.category	SM Incident	Site Category (can be customized). **Field Name:** site.category **Field Type:** string

ID (A-Z)	Entity Type	Description
incident. subarea	SM Incident	**Note:** For HP Service Manager 7.1 only. Sub area (can be customized). **Field Name:** Product.type **Field Type:** string **Note:** ➤ Primary Key ➤ Required
incident. subcategory	SM Incident	**Note:** For HP Service Manager 7.02 only. Sub Category (can be customized). **Field Name:** subcategory **Field Type:** string
incident.type	SM incident	Type (can be customized). **Field Name:** type **Field Type:** string
incident.update. action	SM Incident	Update Action (can be customized). **Field Name:** update.action **Field Type:** string
incident.vendor	SM Incident	Vendor (can be customized). **Field Name:** vendor **Field Type:** string

Entity

ID	Description
SM Incident	Incident Entity in HP Service Manager. **Note:** Can be customized.
BAC CI Alert	CI Alert Entity in Business Availability Center. **Note:** Can be customized.

Field Mapping

The customization data listed in the table is for HP Service Manager 7.1 and 7.02 unless indicated otherwise.

The contents of the **Internal Field Callback** in the Description column in the table below, provide information about the search that is performed and the results that are created. The contents of the **Internal Field Callback** have the following format:
<callback function>(<conditions that need to be matched>, <resulting actions>).

For details about the Callback functions, see “Callback Functions” on page 203.

For example:

- If the contents of the **Internal Field Callback** are l**ookupCreate("producttype", "product.type=\"$bacalert.kpi_name$\" and category=\"$incident.category$\" and subcategory =\"$incident.area$\"", "product.type", ["product.type", "category", "subcategory"], ["$bacalert.kpi_name$","$incident.category$","$incident.area$"])**, the lookupCreate callback is used to perform the search and attempts to find a CI for which the value of **product.type** field is $bacalert.kpi_name$, the value of the **category** field is **$incident.category$** and the value of the **subcategory** field is $incident.area$.
- If no correlation is found, then a new items is created with the following characteristics: the value of the **product.type** field is $bacalert.kpi_name$, the value of the **category** field is **$incident.category$** and the value of the **subcategory** field is $incident.area$. The search uses key-value pairs: the value of the **product.type** field is the value of the $bacalert.kpi_name$ variable.

External Field ID	Internal Field ID	Description
-	incident.subarea	**Note:** For HP Service Manager 7.1 only. Uses the callback function described below to find a correlation or to create a new record if no correlation is found. **Note:** Do not modify. **Internal Field Callback:** lookupCreate("producttype", "product.type=\"$bacalert.kpi_name$\" and category=\"$incident.category$\" and subcategory =\"$incident.area$\"", "product.type", ["product.type", "category", "subcategory"], ["$bacalert.kpi_name$","$incident.category$","$incident.area$"]) For details, see “LookupCreate Function” on page 204.

External Field ID	Internal Field ID	Description
-	incident.problem .type	**Note:** For HP Service Manager 7.02 . Uses the callback function described below to find a correlation or to create a new record if no correlation is found. **Note:** Do not modify. **Internal Field Callback:** lookupCreate("problemtype", "product.type=\"$bacalert.kpi_name$\" and problem.type=\"$bacalert.kpi_name$\" and limited.given.level2 =\"$incident.subcategory$\"", "problem.type", ["product.type", "problem.type", "limited.given.level2"], ["$bacalert.kpi_name$","$bacalert.kpi_name$","$incident.subcategory$"]) For details, see “LookupCreate Function” on page 204. **Note:** For HP Service Manager 7.1 Uses the callback function described below to find a correlation or to create a new record if no correlation is found. **Note:** Can be customized. **Internal Field Callback:** lookupCreate("problemtype", "product.type=\"$bacalert.kpi_name$\" and problem.type=\"$bacalert.kpi_name$\" and limited.given.level2 =\"$incident.area$\"", "problem.type", ["product.type", "problem.type", "limited.given.level2"], ["$bacalert.kpi_name$","$bacalert.kpi_name$","$incident.area$"]) For details, see “LookupCreate Function” on page 204.

External Field ID	Internal Field ID	Description
-	incident.action Note: Do not modify	Uses the callback function described below to combine the **name** and **actual_description** fields from the Business Availability Center alerts. **Note:** Do not modify. **Internal Field Callback:** combine(["bacalert.creation_time", "bacalert.alert_name", "bacalert.actual_description", "bacalert.user_description", "bacalert.condition_configuration"], true, "\n") For details, see "combine Function" on page 206. **Note:** Do not modify.
-	incident.category	Customized by user.
-	incident.area	**Note:** For HP Service Manager 7.1 only.
-	incident.resolution	**Note:** For HP Service Manager 7.1 only.
-	incident. subcategory	**Note:** For HP Service Manager 7.02 only. Customized by user.
-	incident. resolution	**Note:** For HP Service Manager 7.02 only. Uses the callback function described below to set the value with the BAC Alert **actual_description** field when a close action is performed. If you do not specify a value, the default value is used. **Note:** Can be modified. **Internal Field Callback:** setValue("close", "$bacalert.actual_description$") For details, see "setValue Function" on page 206. **Note:** Do not modify.

External Field ID	Internal Field ID	Description
-	incident. resolution.code	Uses the callback function described below to set the value with the BAC Alert **User Closure** field when a close action is performed. If you do not specify a value, the default value is used. **Note:** Can be modified. **Internal Field Callback:** setValue("close", "User Closure") For details, see “setValue Function” on page 206.
-	incident.fix.type	**Note:** For HP Service Manager 7.02 only. Uses the callback function described below to set the value with the BAC Alert **permanent** field when a close action is performed. If you do not specify a value, the default value is used. **Note:** Can be modified. **Internal Field Callback:** setValue("close","permanent") For details, see “setValue Function” on page 206.
-	incident.contact. name	**Note:** For HP Service Manager 7.02 only. Uses the callback function described below to find a correlation or to set the default value if no correlation is found. **Note:** Can be modified. **Internal Field Callback:** lookup("device", "logical.name=\"$bacalert.ci_name$\" and type=\"$incident.type$\"", "contact.name") For details, see “Lookup Function” on page 203.

External Field ID	Internal Field ID	Description
-	incident.initial. impact	Uses the callback function described below to find a correlation or to set the default value if no correlation is found. **Note:** Can be modified. **Internal Field Callback:** lookup("producttype", "product.type=\"$bacalert.kpi_name$\" and category=\"$incident.category$\" and subcategory =\"$incident.subcategory$\"", "severity") For details, see “Lookup Function” on page 203.
-	incident. assignment	**Note:** For HP Service Manager 7.1
-	incident.vendor	**Note:** For HP Service Manager 7.02 only. Uses the callback function described below to find a correlation or to set the default value if no correlation is found. **Note:** Can be modified. **Internal Field Callback:** lookup("device", "logical.name=\"$bacalert.ci_name$\" and type=\"$incident.type$\"", "vendor") For details, see “Lookup Function” on page 203.
-	incident.site. category	**Note:** For HP Service Manager 7.02 only. Uses the callback function described below to find a correlation or to set the default value if no correlation is found. **Note:** Can be modified. **Internal Field Callback:** lookup("device", "logical.name=\"$bacalert.ci_name$\" and type=\"$incident.type$\"", "site.category") For details, see “Lookup Function” on page 203.
-	incident.opened. by	Customized by user.

External Field ID	Internal Field ID	Description
-	incident. assignment	**Note:** For HP Service Manager 7.02 only. Uses the callback function described below to find a correlation or to set the default value if no correlation is found. **Note:** Can be modified. **Internal Field Callback:** lookup("producttype", "product.type=\"$bacalert.kpi_name$\" and category=\"$incident.category$\" and subcategory =\"$incident.subcategory$\"", "assignment") For details, see “Lookup Function” on page 203.
-	incident.closing. comments Note: Do not modify	Uses the callback function described below to find a correlation or to set the default value if no correlation is found. **Internal Field Callback:** setValue("close", "Creation time: $bacalert.creation_time$\nAlert Name: $bacalert.alert_name$\nActual Description: $bacalert.actual_description$\nUser Description: $bacalert.user_description$\nCondition Configuration: $bacalert.condition_configuration$") For details, see “setValue Function” on page 206. **Note:** Do not modify.
bacalert.alert_ name	incident.brief. description	Combine **name** and **actual_description** fields from Business Availability Center Alert. **Note:** Can be modified. **Internal Field Callback:** combine(["bacalert.alert_name", "bacalert.actual_description"], false, " : ") For details, see “combine Function” on page 206.
bacalert.ci_id Note: Do not modify	incident.bac.ci.id Note: Do not modify	Internal.

External Field ID	Internal Field ID	Description
bacalert.ci_name	incident.ciname	**Note:** For HP Service Manager 7.02. Lookup CI in device table. When HP Service Manager opens an incident it tries to find a corresponding HP Service Manager CI. It there is a correlation (CI type and CI name matching), it adds the HP Service Manager CI name in the logical.name field. If there is no correlation, it leaves the logical.name field empty. **Note:** Can be modified. **Internal Field Callback:** lookupEmpty("device", "logical.name=\"$bacalert.ci_name$\" and type=\"$incident.type$\"", "logical.name") For details, see "LookupEmpty Function" on page 205. **Note:** For HP Service Manager 7.10. When HP Service Manager opens an incident it tries to find a corresponding HP Service Manager CI. It there is a correlation (CI type and CI name matching), it adds the HP Service Manager CI name in the logical.name field. If there is no correlation, it leaves the logical.name field empty. **Note:** Can be modified. **Internal Field Callback:** lookupEmpty("device", "ucmdb.id=\"$bacalert.ci_id$\" || (logical.name=\"$bacalert.ci_name$\" and type=\"$incident.type$\") ", "logical.name") For details, see "LookupEmpty Function" on page 205.

External Field ID	Internal Field ID	Description
bacalert.ci_type Note: Do not modify	incident.type Note: Do not modify	**Note:** For HP Service Manager 7.02 Lookup HP Service Manager CI info. When HP Service Manager opens an incident it tries to find a corresponding HP Service Manager CI. It there is a correlation (CI type and CI name matching), it adds the HP Service Manager CI Type in the logical.name field. If there is no correlation, it leaves the logical.name field empty. **Note:** Can be modified. **Internal Field Callback:** lookup("device", "logical.name=\"$bacalert.ci_name$\" and type=\"$incident.type$\"", "type") For details, see "Lookup Function" on page 203. **Value Mapping Group:** citypeGroup **Note:** Do not modify. **Note:** For HP Service Manager 7.1 Lookup SM CI info. When HP Service Manager opens an incident it tries to find a corresponding HP Service Manager CI. It there is a correlation (CI type and CI name matching), it adds the HP Service Manager CI Type in the logical.name field. If there is no correlation, it leaves the logical.name field empty. **Note:** Do not modify. **Internal Field Callback:** lookup("device", "ucmdb.id=\"$bacalert.ci_id$\" || (logical.name=\"$bacalert.ci_name$\" and type=\"$incident.type$\")", "type" For details, see "Lookup Function" on page 203. **Value Mapping Group:** citypeGroup **Note:** Do not modify.

External Field ID	Internal Field ID	Description
bacalert.kpi_name	incident.product.type	**Note:** For HP Service Manager 7.02 only. Creates a new product type record if correlation is not found. **Note:** Can be modified. **Internal Field Callback:** lookupCreate("producttype", "product.type=\"$bacalert.kpi_name$\" and category=\"$incident.category$\" and subcategory =\"$incident.subcategory$\"", "product.type", ["product.type", "category", "subcategory"], ["$bacalert.kpi_name$","$incident.category$", "$incident.subcategory$"]) For details, see “LookupCreate Function” on page 204.
bacalert.severity	incident.severity	Translates Business Availability Center alert severity into HP Service Manager Incident severity value. **Note:** Can be modified. **Value Mapping Group:** severityGroup **Internal Field Callback:** setValue("insert|update") For details, see “setValue Function” on page 206.

Value Mapping

Value Mapping Group	External Value	Internal Value
severityGroup	0	1
	5	2
	10	3
	15	4

Value Mapping Group	External Value	Internal Value
citypeGroup	business_service_for_catalog	bizservice
	logical_application	application
	host	computer
	nt	computer
	unix	computer

Callback Functions

This section describes the functions that are invoked to assign values to the fields in HP Service Manager.

This section includes the following topics:

Lookup Function

Method Name:	Lookup		
Description:	Searches the table specified by the first parameter of the function using the search condition. If a matching condition is found, is uses the value of the field. If the search sails, it uses the predefined default values.		
Input Parameters:	**Type**	**Name**	**Description**
	String	filename	File name to query, for example "device".
	String	query	Search condition.
	String	fieldname	The field to retrieve value.

Return:	None
Example:	lookup ("device", "ucmdb.id = \"$ bacalert.ci_id \"$ || logical.name=\"$bacalert.ci_name$\"", "contact.name")
	If **bacalert.ci_id** is 1111111, and **bacalert.ci_name** is bpm3, the lookup function uses the following query **[ucmdb.id** = "**1111111**" || **logical.name** = "**bpm3**"**]** to search the device table. The query **[ucmdb.id** = "**1111111**"**]** is run first. If the table includes this value, the condition **[logical.name** = "**bpm3**"**]** is ignored. If the table does not include this value, the function uses the following query **[logical.name** = "**bpm3**"**]**. If the table includes this value, **contact.name** field is given the value of the current field in incident. If the table does not include this value, **contact.name** is assigned the default value.

LookupCreate Function

Method Name:	LookupCreate		
Description:	Searches the database table using the search condition behaving like the Lookup function. If it does not find a matching record, a new item is created.		
Input Parameters:	**Type**	**Name**	**Description**
	String	filename	File name to query, for example "device".
	String	query	Search condition.
	String	fieldname	The field to retrieve value.
	Array	fieldArray	If lookup fails, this parameter is used to create a new item. This array contains the fields to be set value when creating new instance.
	Array	valueArray	If lookup fails, this parameter is used to create a new item. This array contains value when creating new instance.
Return:	None		

Example:	lookupCreate ("producttype", "product.type=\"$bacalert.kpi_name$\" and category=\"shared infrastructure\" and subcategory =\"enterprise\"", "product.type", ["product.type", "category", "subcategory"], ["$bacalert.kpi_name$","shared infrastructure","enterprise"])
	If **bacalert.kpi_name** is Performance, this function uses the **[product.type**="**Performance**" **category**="**shared infrastructure**" **subcategory** ="**enterprise**"] query to search in the **producttype** table. If a corresponding record is found, it sets the value of the **product.type** field to the current field in the incident. If the search fails, it creates a new product type following the rule below. The value for the field **product.type** in the incident is Performance; the value for this **category** in the incident is shared infrastructure; the value for field **subcategory** in the incident is enterprise.

LookupEmpty Function

Method Name:	LookupEmpty		
Description:	Searches the device table using the search condition behaving like the Lookup function. If it finds a matching record in the device table, the field is to set to an empty value whether the “default value” has been defined or not.		
Input Parameters:	**Type**	**Name**	**Description**
	String	filename	File name to query, for example "device".
	String	query	Search condition.
	String	fieldname	The field to retrieve value.
Return:	None		
Example:	lookupEmpty ("device", "logical.name=\"$bacalert.ci_name$\"", "logical.name")		
	If **bacalert.ci_name** is bpm3, this function uses the **[logical.name** = "**bpm3**"**]** query to search the device table. If a matching record is found, the value of **logical.name** is changed to the current field in the incident. If the search fails, the value of **logical.name** is set to an empty value independently of the default value or of the value passed from Business Availability Center.		

setValue Function

Method Name:	setValue		
Description:	The function inserts, updates, or close using the specified value. If you do not specify a value, the default value is used.		
Input Parameters:	**Type**	**Name**	**Description**
	String	action	Action type (**insert**/**update**/**close**), it may be a combination of the types. For example: insert|update.
	String	Value	Value to be used. If this parameter is missing, the value from Business Availability Center or default value is used.
Return:	None		
Example:	Example 1: setValue ("close", "$bacalert.actual_description$") Example 2: setValue("close|update", "description");		
	1. If **bacalert.actual_description** is brief description; the function is **setValue ("close", "brief description")**. 2. Only when the action is insert or update, the value from external field (Business Availability Center) or the default value is used.		

combine Function

Method Name:	combine		
Description:	This function combines the fields in the input parameters into the HP Service Manager field.		
Input Parameters:	**Type**	**Name**	**Description**
	Array	fieldArray	Fields to combine.
	boolean	hasTitle	Whether contain title for each field. The title is the description for each field.
	String	splitStr	The space mark.
Return:	String, the combined string with the parameters.		

Example:	Combine (["bacalert.alert_name", "bacalert.actual_description"], false, "| ")
	If **bacalert.alert_name** is alert name, and **bacalert.actual_description** is Alert Name (where description is one of the properties of the **Alert Name** field and the value of the **bacalert.actual_description** property is brief description), the result of this function is: alert name| brief description. If the parameter **hasTitle** is TRUE, the result is: Alert Name: alert name| Actual Description: brief description

8

Open Incidents in HP Service Manager Using the Legacy URL

This chapter provides information on opening incidents in HP Service Manager using the legacy URL when CI Status alerts are triggered in HP Business Availability Center 8.0.

Note: HP Business Availability Center integrates with both HP ServiceCenter and HP Service Manager though only HP Service Manager is mentioned in this chapter. For details about the supported versions, see "Opening Incidents in HP Service Manager – Overview" on page 114.

This chapter includes:

Concepts

Tasks

Opening Incidents in HP Service Manager Using the Legacy URL

You can automatically open an incident in HP Service Manager when a CI Status alert is triggered.

Data about the alert is passed to HP Service Manager and used to open incidents identified by the CI Name. Those parameters are among the parameters passed to HP Service Manager by the alert. An incident previously opened is updated with new alert data when a CI Status is triggered with the same identifying information.

The incident is opened in HP Service Manager using a URL that is sent to HP Service Manager from Business Availability Center.

The URL has the following format:
<protocol_type>://<ServiceCenter_host_name>:<port>/<directory_path>?ciname=<<CI_name>>&alertname=<<alert_name>>&triggertime=<<trigger_time>>&currstatus=<<current_status>>&prevstatus=<<Previous Severity Description>>&kpiname=<<KPI_name>>&kpivalue=<<KPI_value>>

You must specify some of the parameters and optionally modify the defaults of other parameters. The alert-related parameters (**CI_name**, **alert_name**, **trigger_time**, **current_status**, **previous_status, KPI_name**, and **KPI_value)** are provided by the alert.

In HP Service Manager, you can keep track of the system status and handling. You can also validate and monitor the alert.

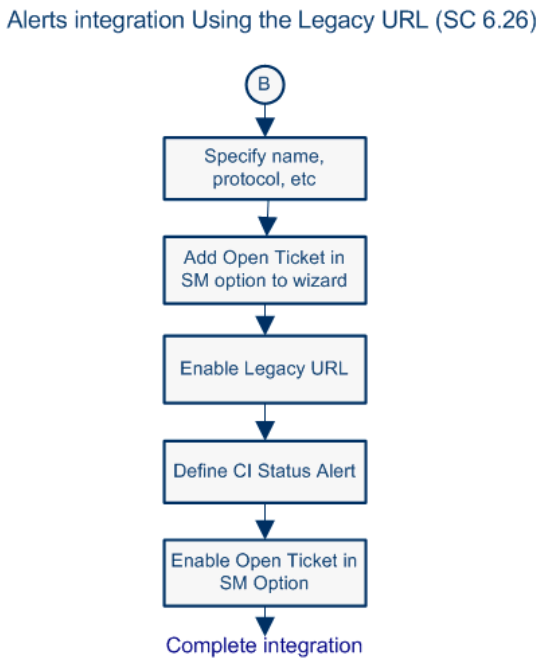
For details on how to automatically create an incident in HP Service Manager, see “Open an Incident in HP Service Manager Using the Legacy URL” on page 211.

Open an Incident in HP Service Manager Using the Legacy URL

To automatically open an incident in HP Service Manager using the legacy URL, when a CI Status is triggered in Business Availability Center, follow the steps described in this section.

For details about the mechanism used to open an incident in HP Service Manager when a CI Status alert is triggered, see "Opening Incidents in HP Service Manager Using the Legacy URL" on page 210.

The flowchart is as follows:



For details about Complete integration, see "Set Up the Integration of HP Service Manager Data with HP Business Availability Center Components - Workflow" in *Solutions and Integrations*.

This task includes the following steps:

1 Specify the Name of the HP Service Manager Host

To specify the name of the host where HP Service Manager is located (**ServiceCenter host name** parameter), select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **Integration with other applications**, and enter the name of the host in the **ServiceCenter host name** entry in the Integration with other applications - ServiceCenter Integrations table.

2 Specify the Protocol to be Used For the Interface

To specify the protocol to be used for the interface between the Alerts application and the HP Service Manager application, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **Integration with other applications**, and enter the protocol (either **http** or **https**) in the **Protocol type** entry in the Integration with other applications - ServiceCenter Integrations table.

3 Specify the Hidden Parameters – Optional

You can change the hidden parameters to match the new information, if, for example, HP Service Manager changes the path to their directories or the port dedicated to listening to Business Availability Center alerts.

Optionally, you can also add parameters to the URL.

To change the hidden parameters or to add parameters to the URL, contact HP Software Support.

4 Add the Open ticket in ServiceCenter Option in the CI Status Alert Wizard

To add the **Open ticket in ServiceCenter** option to the CI Status Alert wizard, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **Integration with other applications**, and locate the **Enable alerts to ServiceCenter** entry in the Integration with other applications - ServiceCenter - Alert Integration table. Specify **true** to add the **Open ticket in ServiceCenter** option to the CI Status Alert wizard or **false** to remove the option.

5 Enable the Legacy URL to Open Incidents in HP Service Manager

To enable the legacy URL to open incidents in HP Service Manager, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **Integration with other applications**, and in the Integrations with other applications - Alerts-Service Manager Integration table, locate:

- the **Enable legacy integration with Service Manager** entry, and change the value to **true**.
- the **Enable url action for opening incident in Service Manager** entry, and change the value to **true**.

6 Define CI Status Alerts

Define CI status alerts. For details, see “Create a CI Status Alert Scheme and Attach it to a CI” on page 65.

7 Enable the Open ticket in ServiceCenter Option in the CI Status Alert Wizard

While defining the CI Status alerts, select the **Open ticket in ServiceCenter** option in the CI Status Alert wizard to automatically sent CI Status to ServiceCenter when the CI Status alert is triggered.

For details about the option for the CI Status alert, see "Actions Page" on page 91.

8 Result

When a CI Status alert is triggered in Business Availability Center, a corresponding incident is opened in HP Service Manager. For details, see "Opening Incidents in HP Service Manager Using the Legacy URL" on page 210.

Part III

SLA Status Alerts

9

SLA Alerts

This chapter provides information on SLA alerts.

This chapter includes:

Concepts

Tasks

Reference

SLA Alerts Overview

SLA alerts notify you or another user of changes to the status of an SLA's KPI.

Note: When defining SLA alert schemes, the term **SLA** includes OLAs and UCs.

For details on configuring and managing SLA Alerts, see "SLA Alerts Page - Administration" on page 241. For details on the SLA Alerts that were triggered, see "SLA Status Alerts Report" on page 245.

You can automatically open events in HP Operations Manager (OM), when an SLA Status alert is triggered in HP Business Availability Center. For details, see "Open Events in HP Operations Manager For Triggered Alerts" on page 47.

Define an SLA Alert Scheme

You set up an alert scheme to monitor current status or forecast status for one or more SLAs, and to define the notifications that are sent when the alert is triggered. An alert scheme is defined in the Create New Alert wizard, accessed by clicking **New Alert** in the **Admin** > **Alerts** > **SLA Alerts** tab.

This task includes the following steps:

1 Prerequisite

Before setting up an alert scheme, you must have defined one or more SLAs To define an SLA, select **Admin** > **Service Level Management** > **Agreements Manager**.

2 Define SLA Alert Schemes

In the Create New Alert wizard, you select one or more SLAs that are monitored by the alert scheme. (You can later add additional SLAs by editing the alert scheme.)

In the wizard, you also choose the recipients and templates for the generated alerts. You can select from the available recipients, or define new recipients while working in the wizard.

The Create New Alert wizard is described in "Create New Alert/Edit Alert Wizard" on page 224.

3 Customize the Alert System – Optional

You can customize some features of the Alerts application. For details, see "Customize Alerts" on page 22.

4 Open an Event in HP Operations Manager When an Alert is Triggered in Business Availability Center

You can open events in HP Operations Manager (OM) when an alert is triggered in Business Availability Center. For details, see "Open an Event in Operations Manager When an Alert is Triggered" on page 49.

5 Results

You can view the alert schemes you have created in the SLA Alerts page. For details, see "SLA Alerts Page - Administration" on page 241.

You can manage the alert schemes. For details, see "Manage the SLA Alert Schemes" on page 220.

You can view a log of the alerts that were triggered in the SLA Status Alerts report and the details of each alert in the SLA Status Alert Notifications report. For details, see "View SLA Alert and SLA Alert Notification Reports" on page 220.

Manage the SLA Alert Schemes

After you complete defining an alert scheme, it is listed in the SLA Alerts tab. For details, see "SLA Alerts Page - Administration" on page 241.

You can perform the following actions:

- Clone and edit an existing alert scheme. The cloned alert inherits all the properties of the existing alert, including SLAs and recipients. The creator of the new alert is the user who cloned it.
- Delete an existing alert scheme.
- Enable alert schemes, so they send notifications to the recipients when the relevant conditions occur. You can also disable alert schemes.
- Search for an alert scheme using the search feature. The search feature works only on alert scheme names. For details, see "SLA Alerts Page - Administration" on page 241.

View SLA Alert and SLA Alert Notification Reports

The SLA Alerts report is a log of the alerts that are triggered during a specified time period, based on the defined SLA alert schemes. For details, see "SLA Status Alerts Report" on page 245.

You can view more details on a specific alert in the SLA Status Alert Notification page. For details, see "SLM Alert Notifications Page" on page 243.

SLA Alerts User Interface

This section describes:

- Create Executable File Dialog Box/Edit Executable File Dialog Box on page 221
- Create New Alert/Edit Alert Wizard on page 224

- Create SNMP Trap/Edit SNMP Trap Dialog Box on page 238
- Create URL/Edit URL Dialog Box on page 239
- SLA Alerts Page - Administration on page 241
- SLM Alert Notifications Page on page 243
- SLAs Filter Dialog Box on page 245
- SLA Status Alerts Report on page 245
- Tracking Periods Dialog Box on page 247

Create Executable File Dialog Box/Edit Executable File Dialog Box

Description	Enables you to define a command line for running an executable file. HP Business Availability Center runs the executable file (for example, an **.exe** or **.bat** file) when the alert is triggered. You can embed alert parameters in the executable file. The parameters are substituted with the relevant values when the message is formatted. **To access:** In the **Actions** page of the Create New Alert wizard, click **New Executable File** or the **Edit** button for a listed executable file.
Important Information	➤ The executable file is run from the Business Availability Center Data Processing Server, so the path to the executable file must be available from the server machine. ➤ The executable file must not be interactive (no user response required) and should not have a user interface.

The Create Executable File or Edit Executable File dialog box includes the following elements:

GUI Element (A-Z)	Description
Enter Command	Enter the command line using the following format: <full path to program from Business Availability Center Data Processing Server machine> <program command line switches> You embed the alert parameters in the switch section of the command line. The parameters are substituted with the actual values before the command line is executed. For example: C:\Bin\MyAlertReporter.exe –title "<Alert Name> for <SLA Name>" –Text "<Current Status>"

GUI Element (A-Z)	Description
Field	Select alert parameters to insert into the command line. Use the same parameters for forecast alerts. The alert parameters are: ➤ **SLA Name.** If the alert scheme monitors more than one SLA, the name of the SLA that triggered the alert is used for this parameter. ➤ **Alert Name.** The name you defined for the alert scheme. ➤ **Trigger Time.** The start date and time of the event that triggered the alert. **Note:** Trigger time is not necessarily the time of the alert. For example, if the alert engine is down when the alert is triggered, the alert may be sent several minutes later. ➤ **Previous Status.** The status of the SLA before the alert was triggered. Service Level Management includes the following statuses: Exceeded, Met, Minor Breached, Breached, and Failed. ➤ **Current Status.** The current status of the SLA. (The change from previous status to current status is the trigger for the alert.) ➤ **Tracking Period.** The monitored SLA tracking period in which the alert occurred.
Insert Field	Click the **Insert Field** button to insert the alert parameter displayed in the **Field** box into the **Enter Command** box. The alert parameter is added at the cursor location, between double angle brackets.

Create New Alert/Edit Alert Wizard

Description	Enables you to create an SLA status alert scheme to notify you or another user of changes to SLA status (occurring in the present or predicted to occur in the future). **To access:** Select **Admin** > **Alerts** > **SLA Alerts**, then click **New Alert**, or the **Edit** button for an existing alert.
Important Information	To open an event in OM when an SLA Status Alert is triggered, you must: ➤ Create an SLA Status alert without specifying a recipient or an action for the alert. When you complete the definition of such an alert, the message: **The alert you just defined opens an event in Operations Manager i when the communication with Operations Manager i is enabled** is displayed in the Summary page. ➤ Set up specific parameters to enable the communication with OM. For details, see "Open an Event in Operations Manager When an Alert is Triggered" on page 49.
Wizard Map	The Create New Alert wizard contains: Welcome > General Page > Related SLAs Page > Templates and Recipients Page > Actions Page > Summary Page
Useful Links	"Define an SLA Alert Scheme" on page 218

General Page

Description	Enables you to define alert scheme parameters and alert conditions.
Important Information	➤ The forecast calculations are based on averages, so if an SLA contains a KPI that is based on an accumulative result (the Outage Duration KPI or the Number of Outages KPI), the calculations yield inaccurate forecast results. Do not create a status alert scheme for SLAs that contain either of these KPIs. ➤ After saving an SLA alert scheme, you cannot change the alert type from status to forecast, or vice versa.
Wizard Map	The Create New Alert/Edit Alert Wizard contains: Welcome > **General Page** > Related SLAs Page > Templates and Recipients Page > Actions Page > Summary Page

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Alert Definition	Select the required definition: ➤ **All Tracking Periods.** The alert scheme monitors all tracking periods. ➤ **Selected Tracking Periods.** You select the tracking periods in the next stage of the procedure. **Note:** For a forecast alert scheme, the **Alert Definition** parameter is disabled and the forecast calculation is automatically applied to all tracking periods.
Alert Type	Select the required type: ➤ **Forecast Alert.** The alert scheme monitors changes in the forecast SLA status. ➤ **Status Alert.** The alert scheme monitors changes in the current SLA status. **Note:** You cannot modify the Alert Type when editing an alert scheme.

GUI Element (A-Z)	Description
Condition	Select the required condition: ➤ **Send alert if status worsens.** Triggers the alert when the current or forecast status of an SLA is worse than the previous status. For example, if the status changes from Met to Minor Breached, the alert is triggered. Statuses **No Data** and **Downtime** are ignored. ➤ **Send alert if status improves.** Triggers the alert when the current or forecast status of the SLA is better than the previous status. For example, if the status changes from Breached to Minor Breached, the alert is triggered. Statuses **No Data** and **Downtime** are ignored. ➤ **Send alert if status value was changed from.** Sets the appropriate conditions for sending an alert. Select the appropriate status in the **from** and **to** boxes. ➤ **Send alert if status value was changed from** <status> **to** <status> to set the appropriate conditions for sending an alert. Select the appropriate status in the **from** box, and in the **to** box. The available statuses are: **Any Status** (only available in the **from** box), **Exceeded, Met, Minor Breached, Failed**, and **No Data**. If you select **Any Status**, the alert is triggered when the SLA's KPI status changes from any status to the target status.
Description	Enter a description to appear in Service Level Management reports.
Name	The name of the alert scheme must be unique and no longer than 100 characters.
Notification Frequency	Select the required notification frequency: ➤ **Send alert for every trigger occurrence.** Send an alert each time the condition is triggered. ➤ **Send no more than one alert per.** Send an alert once only during the time period you select, even if the condition is triggered more than once during that time period.

Related SLAs Page

Description	Enables you to select the SLAs. Where relevant, it enables you to select the tracking periods or the alert forecasting periods that the alert scheme should monitor.
Wizard Map	The Create New Alert/Edit Alert Wizard contains: Welcome > General Page > **Related SLAs Page** > Templates and Recipients Page > Actions Page > Summary Page

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Base Forecasting On	This parameter is displayed for alert schemes of the **Forecast Alert** type (selected in the previous page of the wizard). Select the analysis period to use for the forecast calculation. The results from the analysis period serve as the basis for the forecast calculation, on the assumption that the SLA performs in the future as it did during this analysis period. The options for this parameter are based on the SLA tracking period, up to the current date. The available options include only the tracking periods that are common to all SLAs added to the **Selected SLAs** list, and that are also included in the following list: ➤ Week to date ➤ Month to date ➤ Quarter to date ➤ Year to date
Give Forecasting For	This parameter is displayed for alert schemes of **Forecast Alert** type (selected in the previous page of the wizard). Select the period that you want the forecast to cover. For example, select **End of month** for a forecast of the SLA status at the end of the current month. The options for this parameter are based on the SLA tracking periods; however, only the tracking periods that are common to all SLAs added to the **Selected SLAs** list, and that are also included in the following list, are available: ➤ End of week ➤ End of month ➤ End of quarter ➤ End of year

GUI Element (A-Z)	Description
Selected SLAs	Lists the SLAs (including OLAs and UCs) that are monitored by the alert scheme.
SLAs	Lists the existing SLAs (including OLAs and UCs even if they are not currently running, or have been terminated). The list displays those SLAs for which you have change or delete permission. Add SLAs from the **SLAs** list to the **Selected SLAs** list: ➤ To add an SLA to the Selected SLAs list, select the SLA in the left pane and use the upper arrow. ➤ To remove an SLA from the Selected SLAs list, select the SLA in the right pane and use the lower arrow. ➤ Select multiple SLAs by holding down the CTRL key while making your selections.
Tracking Periods	Enables you to select the tracking periods that you want the alert scheme to monitor. The **Tracking Periods** table is displayed only if you selected the following in the previous page of the wizard: ➤ Alert Type: **Status Alert** ➤ Alert Definition: **Selected Tracking Periods** After you select SLAs, the available tracking periods are listed in the table. The available options include each tracking period that is defined for at least one of the selected SLAs. **Note:** ➤ An alert scheme cannot be defined for the **Hour** tracking period. For this reason, this tracking period does not appear in the table. ➤ For each included SLA, the alert scheme monitors only the selected tracking periods that are relevant for that SLA. **Tip:** To make your selections, you can also use the buttons at the bottom of the list for **Select All**, **Clear All**, and **Invert Selection**.

Templates and Recipients Page

Description	Enables you to define to whom a triggered alert should be sent, and to define the template to be used for each alert type.
Important Information	The default character set for email, SMS, and pager messages sent by Business Availability Center is **UTF-8**. You can change the default to ISO-2022-JP. **Customizable:** For details on changing the character set to ISO-2022-JP, see "View SLA Alert and SLA Alert Notification Reports" on page 220. **Note:** You cannot edit the email, SMS, and Pager message templates.
Wizard Map	The Create New Alert/Edit Alert Wizard contains: Welcome > General Page > Related SLAs Page > **Templates and Recipients Page** > Actions Page > Summary Page

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Email message template	Select the email template format to be used when HP Business Availability Center sends the alert to recipients: ➤ **Short HTML email message/short text email message.** These messages include the change in status only. ➤ **Long HTML email message/long text email message.** These messages include a subject line and body. HP Business Availability Center supports secure mail. For details, see "Email Tab" on page 41. **Note:** The text displayed in email messages can only be in English except for the contents of fields inserted by the user that can be in any supported and relevant language. Those fields can be for example: Alert Name, Alert description, KPI name, and so on.
New recipient	Click the **New Recipient** button to open the Recipient Properties dialog box, where you can define a new recipient. For details, see "Recipient Properties Wizard" on page 38.

GUI Element (A-Z)	Description
Pager template	Select the pager template format to be used when HP Business Availability Center sends the alert to recipients: Choose between: ➤ **Long SMS/Pager message.** The message includes the change in status and information about the SLA. ➤ **Short SMS/Pager message.** The message includes the change in status only. Pager messages are sent through email to the service provider. The email address is: **<Pager provider access number>@<Pager provider email address>**. **Note:** The text displayed in pager messages can only be in English except for the contents of fields inserted by the user that can be in any supported and relevant language. Those fields can be for example: Alert Name, Alert description, KPI name, and so on.
SMS template	Select the SMS template format to be used when HP Business Availability Center sends the alert to recipients: Choose between: ➤ **Long SMS/Pager message.** The message includes the change in status and information about the SLA. ➤ **Short SMS/Pager message.** The message includes the change in status only. SMS messages are sent through email to the service provider. The email address is: **<SMS provider access number>@<SMS provider email address>**

Message Syntax

The syntax used in the message is a subset of one of the following:

➤ Syntax for a long or short HTML template:

sla_name status *condition-change*/remained *current_status* for *time-period.* Status is *current_status*.

Status Change Time:	*trigger_time*
Tracking Period:	*hour/day/week/month/quarter/year/ sla_period*
Previous Status:	*previous_status*
Time Since Condition Threshold Met:	*time-period + time since end of time-period*
Alert Name:	*alert_name*
Alert Description:	*alert_description*

➤ Syntax for a long or short text template:

sla-name status changed to/remained *current-status* for *time-period*.

Status Change Time: *trigger-time*

Previous Status: *previous-status*

Alert name: *alert-name* (Long text)

Alert Description: *alert-description*

Data Name: *sla-name*

Time Since Condition Threshold Met: *time-period + time since end of time-period*

For more details log into HP Business Availability Center

Examples of HTML and Text Messages

The email messages that the user receives depend on the format you select in the **Email message template**, **SMS template**, or **Pager template** list. The structure of the messages is described in "Message Syntax" on page 234.

➤ **Example of a long HTML email, SMS, or Pager message**

sla2 Status worsened. Status is **Failed**.

Status Change Time:	GMT[+03:00] 4/12/07 11:59 AM
Tracking Period:	Month
Previous Status:	Exceeded
Time Since Condition Threshold Met:	0 minutes
Alert Name:	change to crit
Alert Description:	

For more details log into HP Business Availability Center

➤ **Example of a long text email, SMS, or Pager message**

```
sla2 status changed to Failed.
Status Change Time: GMT[+03:00] 4/12/07 11:59 AM
Previous Status: Minor
Alert name: change to crit
Alert Description:
Data Name: sla2
For more details log into HP Business Availability Center
```

➤ **Example of a short HTML email, SMS, or Pager message**

sla2 status changed to **Failed**.
For more details log into HP Business Availability Center

➤ **Example of a short text email, SMS, or Pager message**

```
sla2 status changed to Failed.
For more details log into HP Business Availability Center
```

Actions Page

Description	Enables you to define actions that you want to Business Availability Center to perform when an alert is triggered.
Wizard Map	The Create New Alert/Edit Alert Wizard contains: Welcome > General Page > Related SLAs Page > Templates and Recipients Page > **Actions Page** > Summary Page

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Executable Files	Lists the executable files that run when the alert is triggered. You can edit or delete an executable file.
New Executable File	Click the **New Executable File** button to open the Create New Executable File dialog box. For details, see "Create Executable File Dialog Box/Edit Executable File Dialog Box" on page 221.
New SNMP Trap	Click the **New SNMP Trap** button to open the Create New SNMP Trap dialog box. For details, see "Create SNMP Trap/Edit SNMP Trap Dialog Box" on page 238.
New URL	Click the **New URL** button to open the Create New URL dialog box. For details, see "Create URL/Edit URL Dialog Box" on page 239.

GUI Element (A-Z)	Description
Open Ticket in Service Center	Select to automatically open an incident for the alert in HP ServiceCenter when the alert is triggered. Clear to disable the feature. For information about the feature prerequisite steps, see "Open Incidents Using the CI Alert Retrieval Service" on page 129.
SNMP Traps	Lists the SNMP traps that run when the alert is triggered.
URLs	Lists the URLs, with embedded alert parameters, that are accessed by Business Availability Center when the alert is triggered. You can edit or delete a URL.

Summary Page

Description	Lists the settings you defined for the alert scheme. To make changes to the alert scheme, click **Back** or click the alert scheme page in the left menu to go directly to the page you want to change. Click **OK** to save the alert scheme.
Wizard Map	The Create New Alert/Edit Alert Wizard contains: Welcome > General Page > Related SLAs Page > Templates and Recipients Page > Actions Page > **Summary Page**

Create SNMP Trap/Edit SNMP Trap Dialog Box

Description	Enables you to specify that HP Business Availability Center should send an SNMP trap when alert trigger criteria are met. The alert notice can be seen with any SNMP management console in the organization. **To access:** In the **Actions** page of the Create New Alert wizard, click **New SNMP Trap** or the **Edit** button for a listed SNMP trap.
Important Information	HP Business Availability Center supports only SNMP V1 traps. For details on configuring the alerts MIB in your SNMP management console, see "Configure the Alerts MIB" on page 261. (For traps created through the SLA Alerts page, use the file **CIAlerts.mib**.)

The dialog box includes the following elements:

GUI Element (A-Z)	Description
Enter destination host	Enter the IP address or name of the destination host to which the SNMP traps are sent. Example of an IP address: 1.1.1.1. Example of a destination host: \\HostName If Service Level Management displays a default host destination, you can accept the default, or replace it with another IP address or name. If you do not enter a port number, Service Level Management uses a default port number. The default values for the SNMP trap destination host and port are set in Infrastructure Settings Manager. To modify the default values, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **Alerting**, and locate the **Default SNMP port** and the **Default SNMP target address** entries in the **Triggered Alerts** table. Modify the values as required.

Create URL/Edit URL Dialog Box

Description	Enables you to define a URL with embedded predefined alert parameters. The parameters are substituted with the relevant values when the URL is accessed, so that the alert information can be inserted into special logs or external databases. The URL is accessed when an alert is triggered, so that the alert can be sent through a Web site, for example, using Active Server Pages, CGI, or Perl. The URL can activate an executable program on a Web server, report to a custom database, activate a Web-based fax service, and so on. **To access:** In the **Actions** page of the Create New Alert wizard, click **New URL** or the **Edit** button for a listed URL.
Important Information	When accessing a URL, HP Business Availability Center supports the GET method only. This enables the URL to be copied from HP Business Availability Center, pasted into an email, and sent to the user. (If the POST method was used, the HTML file would first have to be saved on the client computer, and then sent by the administrator to the specific user.) For information on the differences between the methods, see one of the following: http://www.cs.tut.fi/~jkorpela/forms/methods.html http://en.wikipedia.org/wiki/HTTP

The dialog box includes the following elements:

GUI Element (A-Z)	Description
Enter URL	Enter the URL in the box, and inset alert parameters where required. When embedding alert parameters in a URL, use the following format: http://<servername>.<domainname>?<alert parameters> For example: http://financesystem.com?name=<AlertName>&sla= <SLA Name>&TriggerTime= <Trigger Time>&CurrentStatus=<Current Status>
Field	Select alert parameters to insert into the URL. Use the same parameters for forecast alerts. The alert parameters are: ➤ **SLA Name.** If the alert scheme monitors more than one SLA, the name of the SLA that triggered the alert is used for this parameter. ➤ **Trigger Time.** The start date and time of the event that triggered the alert. **Note:** Trigger time is not necessarily the time of the alert. For example, if the alert engine is down when the alert is triggered, the alert may be sent several minutes later. ➤ **Previous Status.** The status of the SLA before the alert was triggered. Service Level Management includes the following statuses: Exceeded, Met, Minor Breached, Breached, and Failed. ➤ **Current Status.** The current status of the SLA. (The change from previous status to current status is the trigger for the alert.) ➤ **Tracking Period.** The monitored SLA tracking period in which the alert occurred.

GUI Element (A-Z)	Description
Insert Field	Click the **Insert Field** button to insert the alert parameter displayed in the **Field** box into the **Enter URL** box. The alert parameter is added at the cursor location, between double angle brackets.

SLA Alerts Page - Administration

Description	You use this page to create SLA status alert schemes (based on current status or forecast status), or to perform actions on existing alert schemes. The page lists the existing alert schemes. **To access:** Click **Admin** > **Alerts** > **SLA Alerts**
Useful Links	"Define an SLA Alert Scheme" on page 218

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Click to run the alert scheme, or to run all selected alert schemes. If this button is disabled, the alert scheme is running.
	Click to stop the alert scheme, or to stop all selected alert schemes.
	Click to clone the alert scheme. A copy of the alert scheme is added to the list, named **Copy of <name>**. The copy has the same properties as the original.
	Click to edit the alert scheme. Opens the Edit Alert wizard at the General page. For details, see "General Page" on page 225.
	Click to delete the alert scheme, or to delete all selected alert schemes.

GUI Element (A-Z)	Description
<**check box**>	Select for each alert scheme, as required, to perform an action on multiple alert schemes simultaneously.
Alert Name	The name of the alert scheme. For a long name, hold the cursor over the name to view it in full in a tooltip. Click the column header to sort the list by this column, in either ascending or descending order.
Alert Type	Shows whether the alert scheme is monitoring current status (**SLM Alert**) or forecast status (**Forecast Alert**).
Condition	The condition that trigger an alert. For example, if the SLA status worsens.
New Alert	Click the **New Alert** button to define a new alert scheme. For details, see "Create New Alert/Edit Alert Wizard" on page 224.
Recipients	The names of the users who are to be informed when an alert is triggered. Click the column header to sort the list by this column, in either ascending or descending order.
Search	Enter the name of an alert scheme in the **Search in current view by name** box and click **Search**. You can also enter part of an alert scheme name, using an asterisk (*****) to replace missing characters or words. For example, enter *B* to display all alert schemes that contain the letter **B** in their name. Service Level Management filters the list of alert schemes to display the alerts that fit the search criteria. To clear the filtering, type an asterisk only in the box and click **Search**. **Note:** The search is case-sensitive.

SLM Alert Notifications Page

Description	Displays detailed information about the relevant alert. **To access:** In the SLA Alerts report, click the button.
Important Information	Click the Details button relevant to the appropriate alert to see the alert notification details. If the button does not appear in the report, click the **Reset the table columns' width button** and make the Details column visible. For details, see "Configuration Item Status Alert Notifications Report" on page 100.

Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<Common report elements>	See "Common Report Elements" in *Reports*.

Alert Details Area

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Alert Action	The action that has been assigned to the alert.
Alert Name	The name of the alert.
SLA	The name of the SLA whose change of status triggered the alert.
Status	The previous status of the SLA.

GUI Element (A-Z)	Description
Time	The time of the SLA's change of status.
Tracking Period	The time period that defines which granularities are to be displayed in the alert.

Message Notifications Area

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Recipients	The names of the recipients who receive the notification that the alert has been triggered and that the alert scheme has been executed.
Status	The status of the message: ➤ **Pass** when the message has been sent. ➤ **Fail** when the message has not been sent.
Type	The type of message notification: email, SMS message, or pager message.

Notification Messages Area

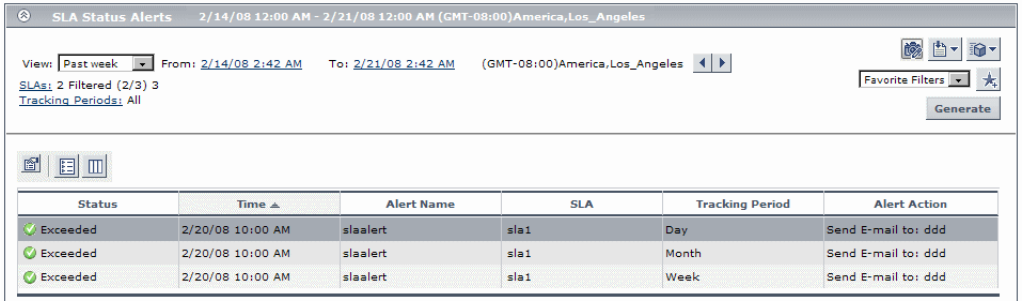
Description	The Notification Messages area displays the type of message followed by the text of the message. The text of the email messages has different formats, depending on the email format selected by the sender. HTML is encoded in the report. The text of the email received by the recipient is decoded and is similar to the Pager message text. For details on the available formats, see "Actions Page" on page 236.

SLAs Filter Dialog Box

Description	Enables you to select the SLAs to be included in a Dashboard report, for the duration of a Web session. The report provides information based on the selected SLAs. **To access:** In the SLA Status Alerts, click **SLAs** in the reports settings area.

SLA Status Alerts Report

The following is an example of the SLA Status Alerts report.



Description	Lists the alerts that were triggered during a specified time period. Service Level Management alerts proactively inform you of SLA status changes by sending alerts to predefined users. **To access:** Select **Applications** > **Alerts** > **SLA Alerts Report**
Useful Links	“Manage the SLA Alert Schemes” on page 220

Filter Area

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<filter area>	"Choose the Time Range and Granularity" in *Reports*
Generate	Click the **Generate** button to generate the report.
SLAs	Click the **SLAs** link to open the SLAs Filter dialog box where you select the relevant SLAs. For details, see "SLAs Filter Dialog Box" on page 245.
Tracking Period	Click the **Tracking Period** link to open the Tracking Periods dialog box where you select the tracking period. For details, see "Tracking Periods Dialog Box" on page 247.

Table Area

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Select the alert and click the button to display the alert notification details in the Alert Details page. For details, see "SLM Alert Notifications Page" on page 243.
Alert Action	The action that is triggered by the alert. For a long name, hold the pointer over the name to view it in full in a tooltip. **Note: Open an incident in OM** indicates that the alert opened an incident in OM when the alert was triggered and communication with OM was established. For details about establishing communication with OM, see "Open an Event in Operations Manager When an Alert is Triggered" on page 49.
Alert Name	The name of the alert.
SLA	The name of the SLA that the alert is attached to.

GUI Element (A-Z)	Description
Status	The current status of the SLA. The status change (from previous status to current status) triggers the alert.
Time	The time and date when the status changed. The format is: dd/mm/yy hh:mm GMT[<offset>].
Tracking Period	The time periods selected during SLA creation. The tracking periods that you select here define which granularities are to be displayed in the alert.

Tracking Periods Dialog Box

Description	Enables you to select the tracking period for which you can view data in the SLA Alerts report. **To access:** Click **Tracking Period** in the SLA Alerts Report.
Important Information	Select one or more of the tracking periods: **Hour**, **Day**, **Week**, **Month**, **Quarter**, **Year**, or **SLA Period**. (The tracking periods that are listed are defined during SLA creation. For more information on SLA tracking periods, see "Tracking Periods Dialog Box" in *Using Service Level Management*.)

Part IV

Event-Based Alerts

10

Event-Based Alerts

This chapter provides information on event-based alerts.

This chapter includes:

Concepts

Tasks

Reference

Event-Based Alerts Overview

Event-based alerts are triggered when pre-defined conditions are breached. The conditions can be transaction response time, availability, success or failure, or completion time.

You can automatically open events in HP Operations Manager (OM), when a CI Status alert is triggered in HP Business Availability Center. For details, see "Open Events in HP Operations Manager For Triggered Alerts" on page 47.

Administration

In the Admin Alerts application, the Event Based Alerts tab provides access to the elements you need to configure an event-based alert scheme. To access the tab, select **Admin** > **Alerts** > **Event Based Alerts**. The tab includes the following elements:

- **Event-Based Alert Configuration.** Use this option to view the existing alert schemes. For details, see "Alert Schemes" on page 253.
- **Notification Templates.** Use this option to view the existing notification templates. For details, see "Notification Templates Page" on page 394.
- **View Dependencies.** Use this option to view the existing alert dependencies. For details, see "Alerts Dependency Overview Page" on page 404.

Application

In the Alerts application, the Event-Based Alerts tab provides access to the event-based alerts that have been triggered. To access the tab, select **Application** > **Alerts** > **Event Based Alert Reports**. The tab includes the following elements:

- **Alerts Log.** To track all alert details for alerts sent by HP Business Availability Center, during the specified time range, for the selected Business Process Monitor profile. For details, see "Alerts Log Report" on page 279.
- **Baselined Suggested Alerts Log.** To track all alert details for event-based alerts that would be sent by HP Business Availability Center if you were using Suggested Baselining, during the specified time range, for the selected Business Process Monitor profiles. For details, see "Baseline Suggested Alerts Log Report" on page 333.

- **Alerts Count Over Time.** To view, for the selected profile, the number of alerts that occurred over the specified time range, organized by time and severity. For details, see "Alerts Count Over Time Report" on page 274.
- **Alerts Count Summary.** To view, for the selected profile, the total number of alerts that occurred over the specified time range, organized by severity. For details, see "Alerts Count Summary Report" on page 276.
- **Actual vs. Baseline Suggested Alerts.** To compare the actual alerts that were triggered by the thresholds that you have specified and the baseline suggested alerts that would be triggered during the specified time range if you were using Baselining, for the selected Business Process Monitor profiles. For details, see "Actual vs. Baseline Suggested Alerts Report" on page 272.
- **Actual vs. Baseline Suggested Alerts - Detailed.** To compare the actual alerts and the baselined alerts that would be triggered if you were using Baselining, during the specified time range. For details, see "Actual vs. Baseline Suggested Alerts – Detailed Report" on page 269.

Alert Schemes

After you create a Business Process profile, you can create one or more alert schemes for the profile, using the Alert Wizard. In each alert scheme, you define a unique set of alert properties. You can add as many alert schemes to your Business Process profile as required.

You can create one or more alert schemes per Real User Monitor engine, using the Alert Wizard. In each alert scheme, you define a unique set of alert properties.

For details on creating an alert scheme, see "Alert Wizard" on page 287.

Triggering Conditions

An event-based alert is triggered, every time a sample arrives on the bus, when the triggering condition on the transaction response time, availability, success or failure, or completion time status is met and when the received sample also meets the condition.

Example 1

The alert scheme definition is: trigger an alert if the transaction response time is greater than 10 seconds in at least 2 out of 4 occurrences.

The alert scheme definition includes a follow up alert.

The received samples include the following data:

Response time in sample	Condition met	Condition met in sample	Alert is triggered?
12 seconds	No 1 alert out of 1	Yes	No
11 seconds	Yes 2 alerts out of 2	Yes	Yes
5 seconds	Yes 2 alerts out of 3	No Response time in sample is 5 and does not meet the alert scheme condition.	No
20 seconds	Yes 3 alerts out of 4	Yes	Yes
4 seconds	Yes 2 alerts out of 4	No Response time in sample is 4 and does not meet the alert scheme condition.	No

Response time in sample	Condition met	Condition met in sample	Alert is triggered?
7 seconds	No 1 alert out of 4 Condition was met until the new sample arrived.	No The new sample does not meet the condition.	No The follow-up alert is triggered.

Example 2

The alert scheme definition is: RUM Page availability is less than 80% in the past 10 minutes.

You also create a follow up alert.

The received samples include the following data:

Total hits	Availability	Condition met?	Condition met in sample?	Alert is triggered?
10	1 (10% availability)	Yes	Yes	Yes
10	9 (90% availability)	Yes Average availability over the two samples is (90% + 10%)/2= 50%).	No Sample availability is 90%	No
100	100 (100% availability)	No Average availability over the three samples is 92%	No Sample availability is 100%	No The follow-up alert is triggered although the previous sample did not trigger an alert. The reason is that the condition was met until the new sample arrived.

Working with Baseline Modes

To understand the normal performance of your application, it is essential to use baselining. Baselining helps you understand how your site typically performs by helping you determine whether a performance problem is an isolated incident or a sign of a significant downward performance trend.

You can set alerts to use the regular mode, where you set the thresholds of the alerts. Alternatively, you can use the baseline modes, where the baselining mechanism itself sets the thresholds according to previous results. For details on the baseline modes, see "Baselines" in *Using End User Management*.

This section includes the following topics:

Impact of Using Baselining on Event-Based Alerts

You can use baselining or regular thresholds to trigger the event-based alerts with the following modes:

➤ **Baseline Calculation Disabled**. The event-based alerts are triggered using the user-defined thresholds. The baseline engine is not active.

This option corresponds to clearing all options in the Threshold Baselining area of the Business Process Monitor profile Properties.

➤ **Baseline Calculation Enabled.** The event-based alerts are triggered using the user-defined thresholds, and the baseline thresholds are calculated in the background.

You can display the **Actual vs. Baseline Suggested Alerts Comparison**, **Actual vs. Baseline Suggested Alerts Detailed Comparison**, and **Baseline Suggested Alerts Log** reports to compare the alerts triggered during the specified period using the user-defined thresholds and the alerts that would be triggered using the baseline thresholds. For details on those reports, see "Event-Based Alerts" on page 251.

This option corresponds to selecting the **Activate threshold baseline calculation** and **Suggest mode** options in the Threshold Baselining area of the Business Process Monitor profile Properties.

- **Automatic/Full-Automatic Baseline Calculations.** The event-based alerts are triggered using the baseline thresholds.

  This option corresponds to selecting the **Activate threshold baseline calculation** and one of the **Auto modes** options in the Threshold Baselining area of the Business Process Monitor profile Properties.

  For details on the Business Process Monitor profile properties, see "Edit Business Process Profiles Page" in *Using End User Management*.

Changing Baseline Modes

When working with the **Enabled/Automatic/Full-Automatic** baseline modes, the baseline engine gathers data from the alerts history to calculate the baseline thresholds.

For a short period of time after switching to **Enabled/Automatic/Full-Automatic** baseline modes, the system still uses the user-specified threshold.

When you change baseline modes from **Enabled/Disabled** to **Automatic/Full-Automatic**, the alert trigger criteria that used user-defined thresholds are modified to use the baseline thresholds.

When you change baseline modes from **Automatic/Full-Automatic** back to **Enabled/Disabled**, the trigger criteria that you had specified previously are fully restored.

Create Event-Based Alert Schemes – Workflow

To create an alert scheme using the Alert Wizard, perform the following steps:

This task includes the following steps:

- "Prerequisite" on page 258
- "Select a Profile and Create a New Alert" on page 258

1 Prerequisite

You can use baselining to automatically set alert thresholds. For details on setting up baselining, see "Baselines" in *Using End User Management*.

For details on the impact of baselining on event-based alerts, see "Working with Baseline Modes" on page 256.

2 Select a Profile and Create a New Alert

Click **Admin** > **Alerts** > **Event Based Alerts** > **Event Based Alert Configuration**. In the Alerts page, select the profile for which you want to create the alert, and click **New Alert**.

3 Configure the Alert Scheme

Use the Alert Wizard to:

➤ **Define the Alert Trigger Criteria.** You define the criteria that trigger the alert.

➤ **Set the Alert Filters.** You set alert filters that enable you to customize the alert scheme for more accurate alerting.

- **Configure the Alert Action Setting.** You specify the actions you want HP Business Availability Center to perform when alert trigger criteria are met. The actions can be:
  - **To access a URL when the alert is triggered.** You can embed predefined alert parameters into a URL that is accessed when an alert is triggered. For details, see "Access URL Dialog Box" on page 267.
    For example:
    http://myticketingsystem.com?name=<<Alert Name>>
    &ticketID=<<Id>>&description=<<Alert Description>>
    The URL accesses the myticketingsystem.com site. It uses the name of the alert, the alert Id number and the description of the alert as parameters.
  - **To execute a command or executable file when the alert is triggered.** You can embed predefined alert parameters into a custom command line that runs an executable file when an alert is triggered. For details, see "Run Executable File Dialog Box" on page 363.
    For example:
    C:\Bin\MyAlertReporter.exe –title "Alert <<Alert Name>> for
    <<Profile Name>>" –Text "<<User Message>>"
    The command uses the MyAlertReporter exe file located in C:\Bin. It uses the name of the alert, the name of the profile, and the message to the user as parameters.
  - **To send email alerts and scheduled reports through a configured SMTP server or through the Microsoft SMTP Service.** For details, see "Configure SMTP Mails" on page 262.
- **Configure Additional Alert Settings.** You specify various settings, including alert name, label, and status. You can also specify a custom pager information or an SMS service provider. For details, see "Add a Custom Pager or SMS Service Provider" on page 34.

After you have finished creating the alert scheme, it is added to the Alerts table.

For more information about alert schemes, see "Alert Schemes" on page 253.

For details on creating an alert scheme, see "Alert Wizard" on page 287.

Example of an Alert

```
Profile Name: Default_Client_RUM_Profile

Severity: Major

Alert Name: Page response time relative to threshold is greater than 60 percent


Trigger Condition:
------------------
60.00% hits with page time greater than defined threshold.
 Limitation of minimum 0 hits reaching threshold; Calculate alert over five minute
interval.

Current Description:
--------------------
7 hits which are 70.00% of the hits were with page time greater than defined threshold.

User Message:

HP Web Site URL: http://h20230.www2.hp.com/svi_partner_list.jsp


Results of Requested Actions:
-----------------------------
N/A
```

4 Set an SNMP Trap

You must set an SNMP trap if you enabled alerts through SNMP traps in your alert schemes. For details, see "Configure the Alerts MIB" on page 261.

5 Compare the Baselining Alerts and the Actual Alerts – Optional

If you have enabled baseline calculation, select **Applications** > **Alerts** > **Event-Based Alerts Report** > **Actual vs. Baseline Suggested Alerts** to open the report. In the report, you can view the number of alerts that would be triggered if you were using Baselining, compared to the number of alerts that would be triggered if you were using regular alerts. For details, see the "Actual vs. Baseline Suggested Alerts Report" on page 272.

6 Open an Event in HP Operations Manager When an Alert is Triggered in Business Availability Center

You can open events in HP Operations Manager (OM) when an alert is triggered in Business Availability Center. For details, see "Open an Event in Operations Manager When an Alert is Triggered" on page 49.

7 Results

When an alert is triggered, the recipient may receive an email, a pager message, or an SMS message depending on the recipient's settings.

The alerts triggered by the trigger criteria specified in the Alert Wizard are logged in the Alerts Log. For details, see "Alerts Log Report" on page 279.

If you are not using Baselining, the alerts triggered by Baselining are logged in the Baseline Suggested Alerts Log. To compare the number of alerts received using the trigger criteria and the number of alerts received using Baselining, consult the Actual vs. Baseline Suggested Alerts report. For details, see "Actual vs. Baseline Suggested Alerts Report" on page 272.

Configure the Alerts MIB

If you enabled alerts through SNMP traps in your alert schemes, it is recommended that you configure your SNMP management console to read the Alerts MIB. This configuration enables you to see a name, rather than an OID (Discovery and Dependency Mapping), when working in the management console.

Note: HP Business Availability Center uses the AM alerts MIB 5.0 by default.

To configure the alerts MIB in your SNMP management console:

1 Copy the Alerts MIB file **BACEventBasedAlerts8.0.mib** from the HP Business Availability Center Documentation and Utilities DVD in **Tools_and_Utilities\SNMP_MIBS** to your SNMP management console.

2 To view the Alerts varbinds, use your SNMP management console's MIB browser. For a list of varbinds and their descriptions, see "Alerts MIB Varbinds" on page 369.

3 Using your SNMP management console's event configuration utility, configure the notification content and method for the various alert types. For a list of alert types and their corresponding SNMP-specific codes, see "SNMP-Specific Codes" on page 368.

Configure SMTP Mails

You can send email alerts and scheduled reports using a configured SMTP server or the Microsoft SMTP Service.

Note: UNIX uses the **sendmail** application to send SMTP emails. As a result, SMTP settings are not needed for Unix systems. Contact your system administrator to configure sending emails correctly for UNIX systems.

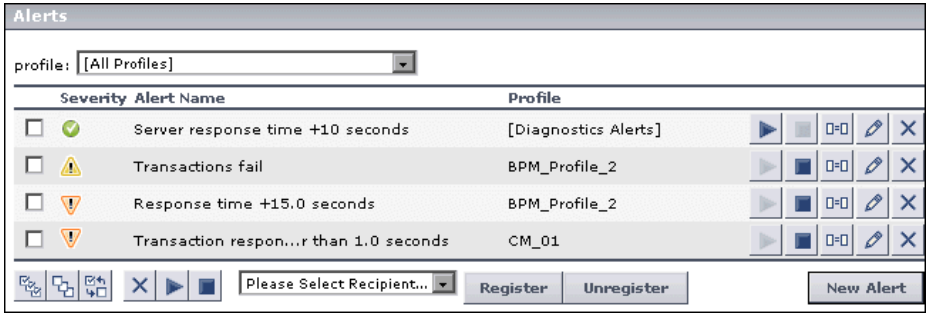
You can configure a primary SMTP server and an alternate SMTP server. HP Business Availability Center usually uses the primary server. It uses the alternate server only if the primary server fails to send the message.

You configure the primary and alternate SMTP servers in Infrastructure Settings. For details, see "Modify the Alerts Triggering Defaults" on page 25 and use the **Modify the primary and alternate SMTP server** setting.

Note: If you use the Microsoft SMTP service to send email alerts, HP Business Availability Center cannot send the email-based Performance Update report (which you configure in Scheduled Reports) in HTML format. The report must be sent as an HTML, MHT, CSV, or PDF attachment.

View and Manage an Alert Scheme

After you create an alert scheme, HP Business Availability Center displays it in the Alerts table. The Alerts table lists alerts by name, severity label, and associated profile.



The Alerts page provides information about the alert severity and the status of the alert (whether it is enabled or disabled).

Over time, you may find it necessary to make changes to alert schemes that you create, due to organizational changes, changes to service level monitoring contracts, and so on. For example, if an alert recipient leaves the company, you need to modify the alert scheme. Alternatively, if, due to a change in a service level monitoring agreement, the availability rate of a specific transaction is now expected to be at 97 percent rather than 90 percent, you may want to modify alert trigger criteria for that transaction accordingly.

For details, see “Alert Schemes” on page 253.

View Event-Based Alert Reports

HP Business Availability Center sends alerts according to the alert trigger criteria you specify when creating alert schemes. Every alert that HP Business Availability Center sends is logged to the database. You view information about the alerts that have been sent in Alert reports. For details on the alert reports, see "Application" on page 252.

For details on working with reports (choosing the time range, selecting the profile, saving and sharing reports, and so on), see "Working in Reports" in *Reports*.

For details on creating HP Business Availability Center alerts, see "Event-Based Alerts" on page 251.

Event-Based Alerts User Interface

This section describes:

Access URL Dialog Box

Description	Enter the URL that you want Business Availability Center to access when alert trigger criteria are met. **To access:** Click **Add URL** in the Access URLs dialog box.
Important Information	You can customize and control the URL by adding parameters to the URL string. **Note:** Business Availability Center supports the GET method only when accessing a URL. This enables the URL to be copied from HP Business Availability Center, pasted into an email, and sent to the user. If your Web server supports only the POST method, or if you want more information on developing custom Web pages for your server, contact your HP Software Support representative. For information on the differences between the methods, see one of the following: http://www.cs.tut.fi/~jkorpela/forms/methods.html http://en.wikipedia.org/wiki/HTTP

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Enter URL	Enter the URL with the following format: **URL?request_parameter_name=<<request_parameter_value>>&request_parameter_name=<<request_parameter_value>>** where **request_parameter_value** must be enclosed in double-angled brackets. For a description and listing of the different alert parameters, see “Alert Parameters” on page 285.

Access URLs Dialog Box

Description	Specify that you want Business Availability Center to access a URL when alert trigger criteria are met. This enables Business Availability Center to send alerts through a Web site, for example, using Active Server Pages, CGI, or Perl. The URL can activate an executable program on a Web server, report to a custom database, activate a Web-based fax service, and so on. You can develop custom pages or use existing ones. **To access:** Click the link in **Access the URLs** as specified in the Alert definitions area in the Actions tab in the Alert wizard.
Important Information	You can customize and control the URL by adding parameters to the URL string. For details, see "Access URL Dialog Box" on page 267. **Note:** Business Availability Center supports the GET method only when accessing a URL. If your Web server only supports the POST method, or if you want more information on developing custom Web pages for your server, contact your HP Software Support representative. For information on the differences between the methods, see one of the following: http://www.cs.tut.fi/~jkorpela/forms/methods.html http://en.wikipedia.org/wiki/HTTP

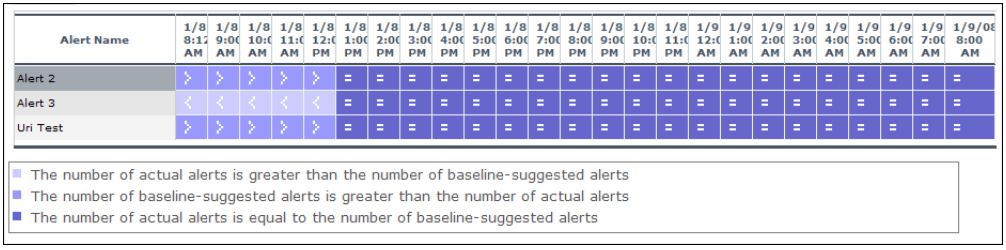
The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Click to open the Access URL dialog box where you can edit the current URL. For details, see "Access URL Dialog Box" on page 267.
	Click to delete the current URL.

GUI Element (A-Z)	Description
<URL>	The URL accessed by HP Business Availability Center when the alert is triggered.
Add URL	Click the **Add URL** button to Access URL dialog box where you can add the URL. For details on embedding predefined alert parameters in the URL, see "Access URL Dialog Box" on page 267.

Actual vs. Baseline Suggested Alerts – Detailed Report

The following is an example of the Actual vs. Baseline Suggested Alerts Detailed report.



Description	Enables you to view, for each time period, whether the number of actual alerts that were triggered by user-defined thresholds is greater than, equal to, or smaller than the baselined alerts that would be triggered during the specified time range, for the selected Business Process Monitor profiles if you were using Baselining. If you drilled down from the **Actual vs. Baseline Suggested Alerts Comparison** report, the time period correspond to the bar you clicked. **To access:** ➤ Select **Applications** > **Alerts** > **Event-Based Alerts Reports** > **Actual vs. Baseline Suggested Alerts - Detailed**. ➤ Drill down by clicking the appropriate bar in the **Actual vs. Baseline Suggested Alerts** report.
Included in Tasks	"View Event-Based Alert Reports" on page 264
Useful Links	"Working with Baseline Modes" on page 256

Report Settings

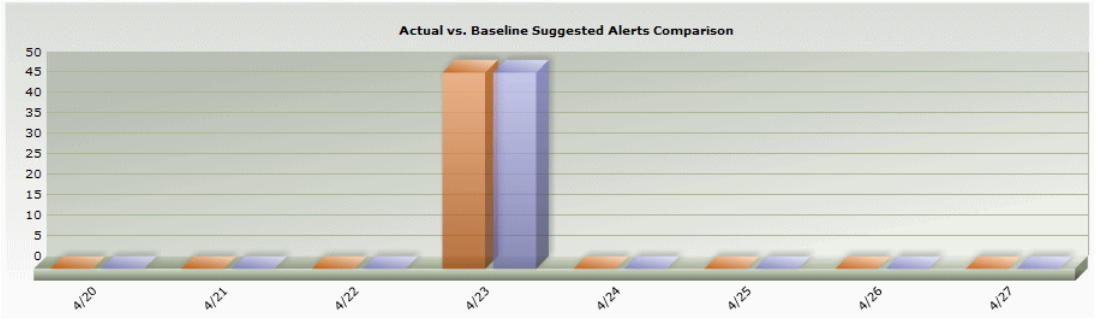
GUI Element (A-Z)	Description
<Common report elements>	See "Common Report Elements" in *Reports*.
Alert	Click the **Alert** link to open the Alerts dialog box where you can select the alert whose log you want to display.
Profile	Click the **Profile** link to open the Profile dialog box where you can select the profile used to filter the alerts displayed in the report.
Severity	Click the **Severity** link to open the Severity dialog box where you can select the severities you want to use to filter the alerts displayed in the report.

Graph Area

Description	Displays per time period granularity, a color that represents the comparison between the number of regular alerts and the number of baselined alerts. The different colors and symbols represent different results: ➤  The number of actual alerts triggered during the selected time period was greater than the number of baseline-suggested alerts triggered during that time period. ➤  The number of baseline-suggested alerts triggered during the selected time period was higher than the number of actual alerts triggered during that time period. ➤  The same number of actual alerts and of baseline-suggested alerts were triggered during the selected time period. A tooltip displays the number of real and baseline-suggested alerts for each cell in the table. Click a cell to open the Detailed Comparison report. For details, see “Detailed Comparison Report” on page 337.

Actual vs. Baseline Suggested Alerts Report

The following is an example of the Actual vs. Baseline Suggested Alerts report.



Description	Enables you to compare the actual alerts that were triggered by user-defined thresholds and the baselined suggested alerts that would be triggered during the specified time range, for the selected Business Process Monitor profiles if you were using Baselining. **To access:** Select **Applications** > **Alerts** > **Event-Based Alerts Reports** > **Actual vs. Baseline Suggested Alerts**
Included in Tasks	"View Event-Based Alert Reports" on page 264
Useful Links	"Working with Baseline Modes" on page 256

Report Settings

GUI Element (A-Z)	Description
<Common report elements>	See "Common Report Elements" in *Reports*.
Alert	Click the **Alert** link to open the Alerts dialog box where you can select the alert whose log you want to display.

GUI Element (A-Z)	Description
Profile	Click the **Profile** link to open the Profile dialog box where you can select the profile used to filter the alerts displayed in the report.
Severity	Click the **Severity** link to open the Severity dialog box where you can select the severities you want to use to filter the alerts displayed in the report.

Graph Area

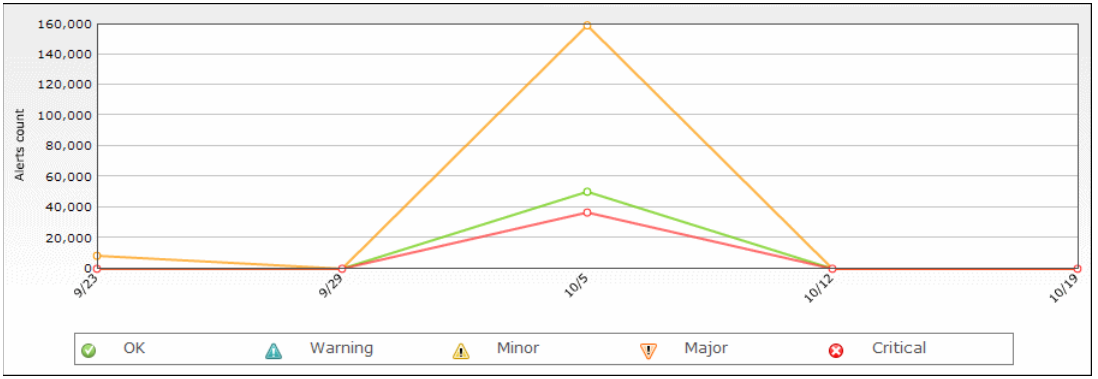
Description	Displays per time period granularity, the number of actual alerts and the number of baseline suggested alerts. A tooltip displays the number of alerts for each bar in the graph.
Important Information	Click on a bar to display the Detailed Comparison report that provides the detailed comparison of the actual and baseline alerts for the selected period of time.

Add User Message Dialog Box

Description	Enables you to type the message you want to include in the alert notice. **To access:** Click the link in **Include the user message** <as_specified> in the Alert definitions area in the Actions tab in the Alert wizard.

Alerts Count Over Time Report

The following is an example of the Alerts Count Over Time report.



Description	Enables you to display, for the selected profile, the number of alerts that occurred over the specified time range, organized by time and severity. In addition, by using the view filter, you can group the data by source, severity label, or alert type, for a specific profile. For example, you can determine how often critical alerts are being sent. **To access:** Select **Applications** > **Alerts** > **Event-Based Alerts Reports** > **Alert Count Over Time.**
Included in Tasks	"View Event-Based Alert Reports" on page 264

Report Settings

GUI Element (A-Z)	Description
<Common report elements>	See "Common Report Elements" in *Reports*.
Active Filters	Click the **Active Filters** link to open the Active Filters dialog box where you can select the severities used to filter the alerts displayed in the report.

GUI Element (A-Z)	Description
Profile(s)	Click the **Profile(s)** link to open the Profiles dialog box where you can select the profile used to filter the alerts displayed in the report.
View By	Select the **View By** link to view the report by Source, Severity, or Type. The legend displayed on the right of the graph, when you generate the report, displays the drillable list of sources, severities, or alert types and their colors.

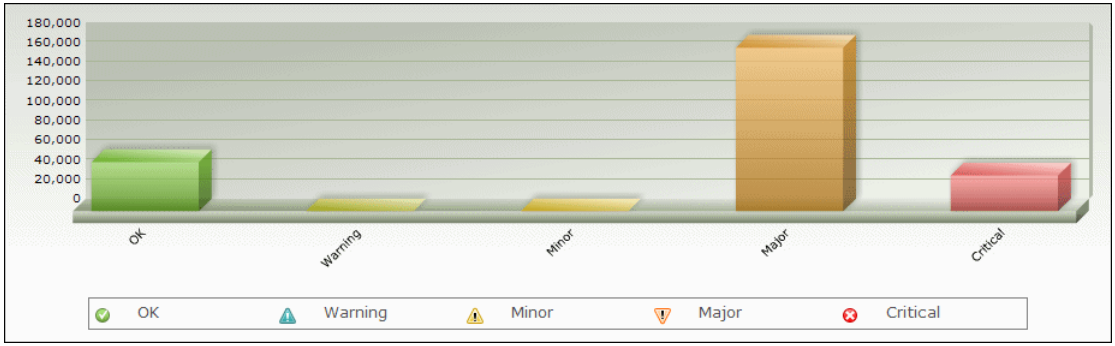
Graph Area

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<any point in graph>	Click any point in the graph to increase the time resolution for the selected source, severity label, or alert type.
<drill down>	Click a point in the report to drill down to the time period for that point. You can continue drilling down until the **Every** field indicates 1 minute.
<tooltip>	Move the mouse over any point in the report to view a tooltip containing details on the number of alerts corresponding to that point in time.

Alerts Count Summary Report

The following is an example of the Alerts Count Summary report.



Description	Enables you to display, for the selected profile, the total number of alerts that occurred over the specified time range, organized by severity. For example, you can determine how often critical alerts are being sent. **To access:** Select **Applications** > **Alerts** > **Event-Based Alerts Reports** > **Alert Count Summary.**
Included in Tasks	"View Event-Based Alert Reports" on page 264

Report Settings

GUI Element (A-Z)	Description
<Common report elements>	See "Common Report Elements" in *Reports*.
Alerts	Click the **Alert** link to open the Alerts dialog box where you can select the alerts whose log you want to display.

GUI Element (A-Z)	Description
Profile(s)	Click the **Profile(s)** link to open the Profiles dialog box where you can select the profile used to filter the alerts displayed in the report.
Severity	Click the **Severity** link to open the Severity dialog box where you can select the severities you want to use to filter the alerts displayed in the report.

Graph Area

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<bar in graph>	Displays for the selected profile and the selected time period, and for the severity represented by the bar, the total number of alerts that were triggered.
<drill down>	Click a bar to drill down to the Alert Count Over Time report for the selected profile, time period, and severity.
<tooltip>	Move the mouse over a bar to view a tooltip containing details on the number of alerts with the severity corresponding to the bar.

Alert Frequency Criteria Dialog Box

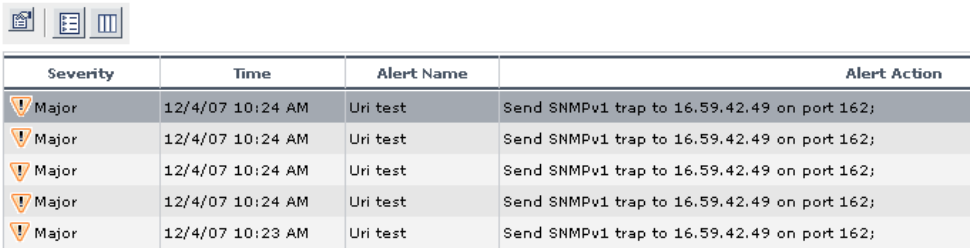
Description	Enables you to define how often HP Business Availability Center sends an alert notice when the event-based alert trigger conditions occur. If you selected any of the event-based alert triggers, you can define the alert frequency criteria. **To access:** Click the link of **Send alert if trigger conditions occur <alert_frequency_criteria>** in the Alert Description area of the Trigger Criteria tab in the Alert wizard.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
At least <X> times out of <Y>	Select to have HP Business Availability Center send an alert only when the defined alert trigger conditions occur X times out of Y, where X represents the number of times the alert conditions occur, and Y represents the total number of transaction instances HP Business Availability Center considers. For example: ➤ For the alert trigger **Transactions fail**, if you specify **at least 3 times out of 5**, an alert is sent only if 3 out of every 5 transactions fail. ➤ For the alert trigger **Transaction response time is greater than 10 seconds**, if you specify **At least 2 times out of 4**, an alert is sent only if transaction response time is greater than 10 seconds in at least 2 out of 4 transaction instances.
Even once	Select to have HP Business Availability Center send an alert every time the defined alert trigger conditions occur.

Alerts Log Report

The following is an example of the Alerts Log report.



Severity	Time	Alert Name	Alert Action
Major	12/4/07 10:24 AM	Uri test	Send SNMPv1 trap to 16.59.42.49 on port 162;
Major	12/4/07 10:24 AM	Uri test	Send SNMPv1 trap to 16.59.42.49 on port 162;
Major	12/4/07 10:24 AM	Uri test	Send SNMPv1 trap to 16.59.42.49 on port 162;
Major	12/4/07 10:24 AM	Uri test	Send SNMPv1 trap to 16.59.42.49 on port 162;
Major	12/4/07 10:23 AM	Uri test	Send SNMPv1 trap to 16.59.42.49 on port 162;

Description	Enables you to track all alert details for event-based alerts sent by HP Business Availability Center during the specified time range, for the selected Business Process Monitor profiles, or Real User Monitor, regardless of the action specified for the alert in the alert scheme. In addition, you can view alerts sent through your organization's enterprise management systems (if configured in EMS profiles). For example, the Alerts Log lists alerts that are not sent to specified recipients and alerts that trigger an executable file. **To access:** Select **Applications** > **Alerts** > **Event-Based Alerts Reports** > **Alerts Log**.
Important Information	The Alerts Log displays up to 20 entries per page. If there are more than 20 entries, use the navigation links at the top or bottom of the screen to move through the Alerts Log.
Included in Tasks	"View Event-Based Alert Reports" on page 264

Report Settings

GUI Element (A-Z)	Description
<Common report elements>	See "Common Report Elements" in *Reports*.
Alert	Click the **Alert** link to open the Alerts dialog box where you can select the alerts whose log you want to display.
Profile	Click the **Profile** link to open the Profile dialog box where you can select the profile used to filter the alerts displayed in the report.
Severity	Click the **Severity** link to open the Severity dialog box where you can select the severities you want to use to filter the alerts displayed in the report.

Report Table Area

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Select an alert in the report and click the button to drill down to the Alert Details dialog box.
Alert Action	Displays alert notification information, for example, the recipients who received the alert. You specify alert recipients in your alert schemes. **Note: Open an incident in OM** indicates that the alert opened an incident in OM when the alert was triggered and communication with OM was established. For details about establishing communication with OM, see "Open an Event in Operations Manager When an Alert is Triggered" on page 49.
Alert Name	Displays the alert name that you specified in your alert scheme.

GUI Element (A-Z)	Description
Severity	Displays an icon that represents the alert severity label you selected for the alert in the alert scheme. The severity is selected in “Settings Tab” on page 327.
Time	Displays the date and time that HP Business Availability Center logged the alert.

Alerts Page

Description	After you create an alert scheme, HP Business Availability Center displays it in the Alerts table. The Alerts table lists alerts by name, severity label, and their associated profile. Over time, you may find it necessary to make changes to alert schemes that you create, due to organizational changes, changes to service level monitoring contracts, and so on. For example, if an alert recipient leaves the company, you need to modify the alert scheme. Alternatively, if, due to a change in a service level monitoring agreement, the availability rate of a specific transaction is now expected to be at 97 percent rather than 90 percent, you may want to modify alert trigger criteria for that transaction accordingly. **To access:** Select **Admin** > **Alerts**.
Included in Tasks	“Create Event-Based Alert Schemes – Workflow” on page 257

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Click the button beside the alert whose properties you want to modify. The Alert Wizard opens. For details, see "Alert Wizard" on page 287.
	Click the button next to the alert scheme you want to clone. HP Business Availability Center adds a copy of the alert scheme to the profile tree, with a new name. Rename and edit the alert scheme as required.
	Click the button beside the alert to delete the alert. To delete multiple alerts simultaneously, select their check boxes in the left column, and click the button located at the bottom of the Alerts table.
	If an alert is enabled, click the **Disable Alert** button beside the alert to disable it. When an alert is disabled, HP Business Availability Center does not send an alert notice when the trigger conditions defined in the alert occur. To enable or disable multiple alerts simultaneously, select their check boxes in the left column and click the button located at the bottom of the Alerts table. **Note:** You can also disable or enable an alert scheme from the Settings page of the Alert Wizard. For details, see "Settings Tab" on page 327.

GUI Element (A-Z)	Description
	If an alert is disabled, click the **Disable Alert** button beside the alert to enable it. When an alert is enabled, HP Business Availability Center sends an alert notification when the trigger conditions defined in the alert occur. To enable or disable multiple alerts simultaneously, select their check boxes in the left column and click the button located at the bottom of the Alerts table. **Note:** You can also disable or enable an alert scheme from the Settings page of the Alert Wizard. For details, see "Settings Tab" on page 327.
<check box>	Select when you want to perform the same action on several alerts simultaneously.
<Please select recipient>	Select the check box beside the alerts for which you want to add or remove a recipient. Select the recipient to add or remove in the recipient list at the bottom of the Alerts table.
Alert Name	The name of the alert.
New Alert	Click the **New Alert** button to define a new alert. Depending on the profile selected in the Profile box at the top of the page, the New Alert dialog box, or the Alerts wizard opens. For details on the New Alert dialog box, see "New Alert Dialog Box" on page 349. For details on the Alert wizard, see "Alert Wizard" on page 287.

GUI Element (A-Z)	Description
Profile	Select the profile for which you want to create the alert from the list of profiles at the top of the page. If you are creating an alert for a Real User Monitor, select the **[RUM Engines]** item from the profile list. **Note:** ➤ If **[All Profiles]** was selected in the profile list when you clicked **New Alert**, the New Alert dialog box for selecting a profile opens. You must select a profile before continuing. For details, see "New Alert Dialog Box" on page 349. ➤ If **[RUM Engines]** was selected in the profile list when you clicked **New Alert**, the New Alert dialog box opens. You must select a Real User Monitor engine as well as the type of alert (page, transaction, or server) before continuing. For details, see "New Alert Dialog Box" on page 349.
Register	After you have selected the check box beside the alerts for which you want to add a recipient, and selected the recipient in the recipient list at the bottom of the Alerts table, click the **Register** button to add the specified recipient to the selected alerts.
Severity	The severity can be: 
Unregister	After you have selected the check box beside the alerts for which you want to remove a recipient, and selected the recipient in the recipient list at the bottom of the Alerts table, click the **Unregister** button to remove the specified recipient to the selected alerts.

Alert Parameters

Description	Use the alert parameters to return information about the Business Process Monitor alerts that HP Business Availability Center sends.
Important Information	When you do not use the **group by** feature, you can use the regular parameters. When you use the **group by** feature, you can use the regular parameters and the group by parameters. For details about the regular parameters, see "Regular Parameters" on page 285. For details about the group by parameters, see "Group By Parameters" on page 286.

Regular Parameters

The parameters are:

Parameter (A - Z)	Description
Actual Details	A description of actual conditions at the time of the alert, generated by HP Business Availability Center.
Alert Name	The alert name specified in the alert scheme.
AlertPurpose	The type of alert. It can be either one of the following types: ➤ A regular alert, which is sent when alert trigger conditions are true. ➤ A follow-up alert, which is sent when the alert trigger conditions that triggered the earlier alert are no longer true.
Id	The unique Id assigned to the alert scheme.
Location Name	The location of the host machine, specified during Business Process Monitor installation, that ran the transactions that triggered the event. This parameter is available to use as an alert parameter only when the alert has been grouped by location.

Parameter (A - Z)	Description
Profile Name	The name of the profile in which the alert scheme was created.
Severity	The alert severity label specified in the alert scheme.
Trigger Cause	The alert trigger criteria specified in the alert scheme.
User Message	The user message specified in the alert scheme.

Group By Parameters

Depending on the selected profile, you can use the following parameters:

Profile	Parameter	Description
BPM	**Transaction Name**	The name of the transaction. **Note:** Can be used only when performance data has been **grouped by** transaction.
	Group Name	The group name of the host machine that ran the transactions that triggered the alert, the event, or both. **Note:** Can be used only when performance data has been **grouped by group**.
	Location Name	The location of the host machine, specified during Business Process Monitor installation, that ran the transactions that triggered the event. **Note:** Can be used only when performance data has been **grouped by** location.
	Script Name	The name of the script.

Profile	Parameter	Description
RUM Page	**End User Name**	The name of the end user.
	Page Name	The name of the page.
RUM Transaction	**Transaction Name**	The transaction name specified in the script. **Note:** Can be used only when performance data has been **grouped by** transaction.
	End User Name	The name of the end user.
RUM Server	**Server Name**	The name of the server.

Alert Wizard

Description	Enables you to create an alert scheme. **To access:** ➤ Click **New Alert** in the Alerts page. ➤ Click the appropriate Edit button  in the Alerts page.
Important Information	To open an event in OM when an event-based alert is triggered, you must: ➤ Create an event-based alert without specifying a recipient or an action for the alert. When you complete the definition of such an alert, the message: **You did not specify an action for the event-based alert you just defined. When this alert is triggered a ticket opens in Operations Manager when the communication with Operations Manager is enabled.** ➤ Set up specific parameters to enable the communication with OM. For details, see "Open an Event in Operations Manager When an Alert is Triggered" on page 49.

Included in Tasks	"Create Event-Based Alert Schemes – Workflow" on page 257
Wizard Map	The **Alert Wizard** includes: Trigger Criteria Tab > Filters Tab > Actions Tab > Settings Tab

Trigger Criteria Tab

Description	Enables you to specify the conditions or criteria that trigger an alert. Alert trigger criteria enable you to specify the transaction response time and availability conditions that trigger an alert. You can choose to trigger the alert based on either an event related to the transaction's success or failure, or based on the time it takes for the transaction to be completed. Depending on the profile you selected in Alerts you can select the following trigger criteria: ➤ "Event-Based Triggers Area" on page 290 ➤ "Time-Based Triggers Area" on page 295 ➤ "Page Triggers Area" on page 304 ➤ "Transaction Triggers Area" on page 306 ➤ "Alert Triggers Area for Server Alerts" on page 310

Important Information	➤ When you set alert filters, HP Business Availability Center considers trigger criteria within the context of the selected items only. ➤ When you select a trigger criteria in the upper part of the page, the **Profile** and **Alert triggers** elements are added to the Alert Description area in the lower part of the page. Depending on the selection, the Alert triggers element displays different information and includes a link to define or edit the trigger definition. ➤ You can select one or more criteria from one of the two categories: event-based or time-based criteria. You cannot combine critters from both categories. ➤ Consider the following guidelines when specifying alert trigger criteria: ➤ Set your alerts to about 10-20% over your average times. ➤ Use the following values for transaction response time alert triggers: 4 seconds for general transactions, like loading a home page; 10 seconds for more complex transactions, like searching; 12 seconds for the most complex activities, like logging to the database. ➤ If you configure transaction thresholds in profiles to be similar to thresholds established in your organization's service level agreements, you can use threshold-based alerts to alert recipients to performance issues related to deviation from SLA criteria.
Wizard Map	The Alert Wizard includes: **Trigger Criteria Tab** > Filters Tab > Actions Tab > Settings Tab

Event-Based Triggers Area

Description	Enables you to select to trigger the alert based on an event related to the transaction's success or failure. For example, you can send an alert when a transaction fails or exceeds a specified amount of time. **Note:** This list of triggers is displayed when you have selected a Business Process Monitor profile in the New Alert dialog box. If you select multiple, event-based alert trigger criteria, you also specify multiple-trigger condition properties.
Important Information	Depending on the baseline mode you have selected, the area displays different information: ➤ "For the Enabled/Disabled Baseline Modes" on page 291 ➤ "For the Automatic/Full-Automatic Baseline Modes" on page 293

For the Enabled/Disabled Baseline Modes

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Transaction Response Time	Select to send an alert if transaction response time is not equal to the selected number of seconds. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Transaction response time is** <condition> **seconds** **Send alert if trigger conditions occur** <alert_frequency_criteria> Click the <condition> link to open the Response Time dialog box. Click the <alert_frequency_criteria> link to open the Alert Frequency Criteria dialog box. Only completed transactions are considered for this alert trigger. If a transaction fails (that is, is not completed successfully) no alert is sent.

GUI Element (A-Z)	Description
Transaction response time relative to End User Management threshold	Select to send an alert if transaction response time is better or worse than the selected transaction threshold. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Transaction response time relative to threshold is** <response_time_ relative_to_ threshold> **Send alert if trigger conditions occur** <alert_frequency_criteria> Click the <condition> link to open the Response Time Relative to Threshold dialog box. Click the <alert_frequency_criteria> link to open the Alert Frequency Criteria dialog box. Only completed transactions are considered for this alert trigger. **Example:** The alert is sent if the response time for a given transaction is worse than the set threshold, but treats the threshold value as 10 percent better. Thus, if the threshold for the transaction is, for example, 10 seconds, HP Business Availability Center sends an alert if transaction response time is worse than 9 seconds (because 9 seconds is 10 percent better than 10 seconds).
Transactions fail	Select to use transaction failure as a criteria. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Transactions fail** **Send alert if trigger conditions occur** <alert_frequency_criteria> Click the <alert_frequency_criteria> link to open the Alert Frequency Criteria dialog box.

For the Automatic/Full-Automatic Baseline Modes

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Transaction Response Time	Select to send an alert if transaction response time is greater than or less than the selected number of seconds. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Transaction response time is** <condition> **seconds** **Send alert if trigger conditions occur** <alert_frequency_criteria> Click the <condition> link to open the Response Time dialog box. Click the <alert_frequency_criteria> link to open the Alert Frequency Criteria dialog box. Only completed transactions are considered for this alert trigger. If a transaction fails—that is, is not completed successfully—no alert is sent.

GUI Element (A-Z)	Description
Transaction response time relative to baseline threshold	Select to send an alert if transaction response time is better or worse than the transaction baseline threshold. Only completed transactions are considered for this alert trigger. You can also select to treat the threshold value as better or worse than the set threshold, by a specified percentage. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Transaction response time relative to baseline threshold is** <response_time_ relative_to_ baseline> **Send alert if trigger conditions occur** <alert_frequency_criteria> Click the <response_time_ relative_to_ baseline> link to open the Response Time Relative to Threshold dialog box. Click the <alert_frequency_criteria> link to open the Alert Frequency Criteria dialog box. **Example:** The alert is sent if the response time for a given transaction is worse than the set threshold, but treats the threshold value as 10 percent better. Thus, if the threshold for the transaction is, for example, 10 seconds, HP Business Availability Center sends an alert if transaction response time is worse than 9 seconds (because 9 seconds is 10 percent better than 10 seconds).
Transactions fail	Select to use transaction failure as a criteria. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Transactions fail** **Send alert if trigger conditions occur** <alert_frequency_criteria> Click the <alert_frequency_criteria> link to open the Alert Frequency Criteria dialog box.

Time-Based Triggers Area

Description	Enables you to select to trigger the alert when specific conditions exist over a specified period of time. For example, when average transaction response time is greater than 10 seconds for a period of 1 hour. **Note:** This list of triggers is displayed when you have selected a Business Process Monitor profile in the Alerts dialog box before clicking the **New** button. If you select multiple, time-based alert trigger criteria, you also specify multiple trigger condition properties. If you set alert filters, HP Business Availability Center considers trigger criteria within the context of the selected items only.
Important Information	➤ When you select more than one time-based criteria the **Send alert if any of the above trigger conditions are met/Send alert if all of the above trigger conditions are met** editable information is displayed in the Alert Description area. To change this element, click the link to open the Multiple Trigger Condition dialog box. ➤ Depending on the baseline mode you have selected the area displays different information: ➤ "For the Enabled/Disabled Baseline Modes" on page 296. ➤ "For the Automatic/Full-Automatic Baseline Modes" on page 300.

For the Enabled/Disabled Baseline Modes

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Availability	Displayed when using Disabled or Enabled baseline modes. Select to send an alert if transaction availability is greater than or less than the selected percentage, calculated over the selected time period. Availability is the number of times that transactions succeed as a percentage of the total number of transaction instances. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Availability is** <transaction_availability> **Calculate over** <calculated_time_period> Click the <transaction_availability> link to open the Transaction Availability dialog box. Click the <calculated_time_period> link to open the Calculated Time Period dialog box. **Note:** Every minute, the system checks if the criteria is fulfilled for the specified time period. If it is, an alert notification is sent. To receive only one alert notification for the same alert event, select **Send no more than one alert as long as the alert continues to exist** in the Settings tab. **Example:** When the criteria is fulfilled five minutes after the start of the time period (15 minutes), a check performed at 16 minutes after the start of the time period finds the criteria fulfilled and sends an alert. The same test is then performed every minute after that, and finds that the criteria is fulfilled five times, up to the 21st minute after the start of the time period. At the 22nd minute after the start of the time period, the criteria is not fulfilled any more.

GUI Element (A-Z)	Description
Average Transaction Response Time	Displayed when using Disabled or Enabled baseline modes. Select to send an alert if average transaction response time is greater than or less than the selected number of seconds, calculated over the selected time period. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Average transaction response time is** <condition> **seconds** **Calculate over** <calculated_time_period> Click the <condition> link to open the Average Response Time dialog box. Click the <calculated_time_period> link to open the Calculated Time Period dialog box. **Note:** Every minute, the system checks if the criteria is fulfilled for the specified time period. If it is, an alert notification is sent. To receive only one alert notification for the same alert event, select **Send no more than one alert as long as the alert continues to exist** in the Settings tab. **Example:** When the criteria is fulfilled five minutes after the start of the time period (15 minutes), a check performed at 16 minutes after the start of the time period finds the criteria fulfilled and sends an alert. The same test is then performed every minute after that, and finds that the criteria is fulfilled five times, up to the 21st minute after the start of the time period. At the 22nd minute after the start of the time period, the criteria is not fulfilled any more.

GUI Element (A-Z)	Description
Transaction response time for specified percentage of transactions	Displayed when using Disabled or Enabled baseline modes. Select to send an alert if the response time is greater or less than the selected number of seconds, for the specified percentage of transactions, calculated over the selected time period. You can also select to count a minimum number of transactions over the calculated time period. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Transaction response time for specified percentage of transactions is** <response_time_for_%_of_trans> **Calculate over** <calculated_time_period> Click the <response_time_for_%_of_trans> link to open the Response Time for Specified Percentage of Transactions dialog box. Click the <calculated_time_period> link to open the Calculated Time Period dialog box. Only completed transactions are considered for this alert trigger. **Note:** Every minute, the system checks if the criteria is fulfilled for the specified time period. If it is, an alert notification is sent. To receive only one alert notification for the same alert event, select **Send no more than one alert as long as the alert continues to exist** in the Settings tab. **Example:** The criteria is fulfilled five minutes after the start of the time period (15 minutes). This means that a check performed at 16 minutes, after the start of the time period, finds the criteria fulfilled and sends an alert. The same test is then performed every minute after that, and finds that the criteria is fulfilled five times, up to the 21st minute after the start of the time period. At the 22nd minute after the start of the time period, the criteria is not fulfilled any more.

GUI Element (A-Z)	Description
Transaction response time relative to End User Management threshold for specified percentage of transactions	Displayed when using the Disabled or Enabled baseline modes. Select to send an alert if the response time is better or worse than the selected transaction threshold, for the specified percentage of transactions, calculated over the selected time period. You can also select to treat the threshold value as better or worse than the set threshold, by a specified percentage or to count a minimum number of transactions over the calculated time period. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Transaction response time relative to threshold for specified percentage of transactions is** <response_time_threshold_for_%_of_trans> **Calculate over** <calculated_time_period> Click the <<response_time_threshold_for_%_of_trans> link to open the Response Time Relative to Threshold for Specified Percentage of Transactions dialog box. Click the <calculated_time_period> link to open the Calculated Time Period dialog box. Only completed transactions are considered for triggering this alert. **Note:** Every minute, the system checks if the criteria is met for the specified time period. If it is, an alert notification is sent. To receive only one alert notification for the same alert event, select **Send no more than one alert as long as the alert continues to exist** in the Settings tab. **Example:** The criteria is met five minutes after the start of the time period (15 minutes). The check performed 16 minutes after the start of the time period finds that the criteria is met and sends an alert. The test is then performed every minute after that, and finds that the criteria is met five times, up to the 21st minute after the start of the time period. 22nd minutes after the start of the time period, the criteria is not met any more.

For the Automatic/Full-Automatic Baseline Modes

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Availability	Select to send an alert if transaction availability is greater than or less than the selected percentage, calculated over the selected time period. Availability is calculated as the number of times that transactions succeed as a percentage of the total number of transaction instances. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Availability is** <transaction_availability> **Calculate over** <calculated_time_period> Click the <transaction_availability> link to open the Transaction Availability dialog box. Click the <calculated_time_period> link to open the Calculated Time Period dialog box. **Note:** Every minute, the system checks if the criteria is fulfilled for the specified time period. If it is, an alert notification is sent. To receive only one alert notification for the same alert event, select **Send no more than one alert as long as the alert continues to exist** in the Settings tab. **Example:** When the criteria is met five minutes after the start of the time period (15 minutes), a check performed at 16 minutes after the start of the time period finds the criteria met and sends an alert. The same test is then performed every minute after that, and finds that the criteria is met five times, up to the 21st minute after the start of the time period. At the 22nd minute after the start of the time period, the criteria is not met any more.

GUI Element (A-Z)	Description
Average Transaction Response Time	Select to send an alert if average transaction response time is greater than or less than the selected number of seconds, calculated over the selected time period. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Average transaction response time is** <condition> **than baseline threshold** **Calculate over** <calculated_time_period> Click the <condition> link to open the Average Response Time dialog box. Click the <calculated_time_period> link to open the Calculated Time Period dialog box. **Note:** Every minute, the system checks if the criteria is fulfilled for the specified time period. If it is, an alert notification is sent. To receive only one alert notification for the same alert event, select **Send no more than one alert as long as the alert continues to exist** in the Settings tab. **Example:** When the criteria is met five minutes after the start of the time period (15 minutes), a check performed at 16 minutes after the start of the time period finds the criteria met and sends an alert. The same test is then performed every minute after that, and finds that the criteria is met five times, up to the 21st minute after the start of the time period. At the 22nd minute after the start of the time period, the criteria is not met any more.

GUI Element (A-Z)	Description
Transaction response time for specified percentage of transactions	Displayed when using Disabled or Enabled baseline modes. Select to send an alert if the response time is greater or less than the selected number of seconds, for the specified percentage of transactions, calculated over the selected time period. You can also select to count a minimum number of transactions over the calculated time period. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Transaction response time for specified percentage of transactions is** <response_time_for_%_of_trans> **Calculate over** <calculated_time_period> Click the <response_time_for_%_of_trans> link to open the Response Time for Specified Percentage of Transactions dialog box. Click the <calculated_time_period> link to open the Calculated Time Period dialog box. Only completed transactions are considered for this alert trigger. **Note:** Every minute, the system checks if the criteria is fulfilled for the specified time period. If it is, an alert notification is sent. To receive only one alert notification for the same alert event, select **Send no more than one alert as long as the alert continues to exist** in the Settings tab. **Example:** The criteria is met five minutes after the start of the time period (15 minutes). This means that a check performed at 16 minutes, after the start of the time period, finds the criteria met and sends an alert. The same test is then performed every minute after that, and finds that the criteria is met five times, up to the 21st minute after the start of the time period. At the 22nd minute after the start of the time period, the criteria is not met any more.

GUI Element (A-Z)	Description
Transaction Response Time Relative to Baseline Threshold for Specified Percentage of Transactions	Select to send an alert if the response time is better or worse than the selected transaction baseline threshold, for the specified percentage of transactions, calculated over the selected time period. You can also select to treat the threshold value as better or worse than the set baseline threshold, by a specified percentage or to count a minimum number of transactions over the calculated time period. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Transaction response time relative to baseline threshold for specified percentage of transactions is** <response_time_threshold_for_%_of_trans> **Calculate over** <calculated_time_period> Click the <response_time_threshold_for_%_of_trans> link to open the Response Time Relative to Threshold for Specified Percentage of Transactions dialog box. Click the <calculated_time_period> link to open the Calculated Time Period dialog box. Only completed transactions are considered for triggering this alert. **Note:** Every minute, the system checks if the criteria is fulfilled for the specified time period. If it is, an alert notification is sent. To receive only one alert notification for the same alert event, select **Send no more than one alert as long as the alert continues to exist** in the Settings tab. **Example:** The criteria is met five minutes after the start of the time period (15 minutes). This means that a check performed at 16 minutes, after the start of the time period, finds the criteria met and sends an alert. The same test is then performed every minute after that, and finds that the criteria is met five times, up to the 21st minute after the start of the time period. At the 22nd minute after the start of the time period, the criteria is not met any more.

Page Triggers Area

Description	Lists the triggers that enable HP Business Availability Center to send alerts when specific conditions exist over a specified period of time. **Note:** This list of triggers is displayed when you have selected a RUM Engines profile in the Alerts page and the **RUM Pages** type in the New Alert dialog box. **Note:** Upgraded Real User Monitor page alerts must be reconfigured.
Important Information	The performance data by which you can group, and the data by which you can limit a Real User Monitor alert scheme, differ from other alert schemes. The grouping and limitation options also differ, depending on the type of Real User Monitor alert you are configuring. For details, see "Grouping and Limitations For Real User Monitor Profiles" on page 320.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Page Availability	Select to send an alert if page availability is less than or greater than the specified percentage, calculated over the selected time period. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Page availability is** <condition> **Calculate over** <time_period> Click the <condition> link to open the Page Availability dialog box. Click the <time_period> link to open the Calculated Time Period dialog box. Only completed transactions are considered when triggering this alert.

GUI Element (A-Z)	Description
Page Performance - percentage of pages with breached page response time	To send an alert if the page download time for the specified percentage of pages has breached the conditions, per sampling period. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Page response time relative to threshold** <as specified> **Calculate over** <time_period> Click the <condition> link to open the Page Availability dialog box. Click the <time_period> link to open the Calculated Time Period dialog box. Only completed transactions are considered when triggering this alert.
Page volume	To send an alert if the number of page accessed is less than or greater than the specified number, calculated over the selected time period. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Page volume is** <condition> **hits** **Calculate over** <time_period> Click the <condition> link to open the Page Volume dialog box. Click the <time_period> link to open the Calculated Time Period dialog box. Only completed transactions are considered when triggering this alert.

Transaction Triggers Area

Description	Lists the triggers that enable HP Business Availability Center to send alerts when specific conditions exist over a specified period of time. **Note:** ➤ This list of triggers is displayed when you have selected a RUM Engines profile in the Alerts page and the **RUM transactions** type in the New Alert dialog box. ➤ Transaction alerts are sent only for transactions that you configure in End User Management.
Important Information	The **rum_trans_t** sample sent to Business Availability Center includes aggregated samples where each sample represents five minutes of data. For details on the **rum_trans_t** sample, see "Sample: RUM Transactions (rum_trans_t)" in *Reference Information*. The transaction performance and availability are calculated by comparing the response time to the specified threshold. For details on setting up the threshold, see "Edit General Settings Page" in *Using End User Management*.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Transaction availability	To send an alert if transaction availability is less than or greater than the specified percentage, per sampling period. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Transaction availability is** <condition> **Calculate over** <time_period> Click the <condition> link to open the Transaction Availability dialog box. Click the <time_period> link to open the Calculated Time Period dialog box. Only completed transactions are considered when triggering this alert.
Transaction performance - percentage of transactions with breached gross transaction response time	To send an alert if the network and server response time for the specified percentage of transactions has breached the conditions, per sampling period. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Percentage of transactions with breached gross transaction response time is** <as_specified> **Calculate over** <time_period> Click the <as_specified> link to open the Transaction Gross Response Time dialog box. Click the <time_period> link to open the Calculated Time Period dialog box. Only completed transactions are considered when triggering this alert.

GUI Element (A-Z)	Description
Transaction performance - percentage of transactions with breached net transaction response time	To send an alert if the network response time for the specified percentage of transactions corresponds to the conditions, per sampling period. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Percentage of transactions with breached net transaction response time is** <condition> **Calculate over** <time_period> Click the <condition> link to open the Transaction Net Response Time dialog box. Click the <time_period> link to open the Calculated Time Period dialog box. Only completed transactions are considered when triggering this alert.
Transaction performance - percentage of transactions with breached server transaction response time	To send an alert if the server response time for the specified percentage of transactions has breached the conditions, per sampling period. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Percentage of transactions with breached server transaction response time is** <conditions> **Calculate over** <time_period> Click the <conditions> link to open the Transaction Server Response Time dialog box. Click the <time_period> link to open the Calculated Time Period dialog box. Only completed transactions are considered when triggering this alert.

GUI Element (A-Z)	Description
Transaction volume - all	To send an alert if the total transaction volume corresponds to the conditions, per sampling period. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Total volume is** <condition> **transactions** **Calculate over** <time_period> Click the <condition> link to open the Total Transaction Volume dialog box. Click the <time_period> link to open the Calculated Time Period dialog box. Only completed transactions are considered when triggering this alert.
Transaction volume - completed	To send an alert if the volume of completed transactions corresponds to the conditions, calculated over the selected time period. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Completed volume is** <condition> **transactions** **Calculate over** <time_period> Only completed transactions are considered when triggering this alert.

Alert Triggers Area for Server Alerts

Description	Lists the triggers that enable HP Business Availability Center to send alerts when specific conditions exist over a specified period of time. **Note:** This list of triggers is displayed when you have selected a RUM Engines profile in the Alerts page and the **RUM servers** type in the New Alert dialog box.
Important Information	The **rum_tcp_server_t** sample sent to Business Availability Center includes aggregated samples where each sample represents five minutes of data. For details on the **rum_tcp_server_t** sample, see "Sample: RUM TCP Servers (rum_tcp_server_t)" in *Reference Information*.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Server application requests availability	To send an alert if the percentage of successful application requests (for example, HTTP requests), compared to the total number of application requests, is less than or greater than the specified percentage, calculated over the selected time period. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Server application requests availability is** <condition> **Calculate over** <time_period> Click the <condition> link to open the Server Availability dialog box. Click the <time_period> link to open the Calculated Time Period dialog box. Only completed transactions are considered when triggering this alert. **Note:** The trigger is calculated using the values of fields in the **rum_server_t** sample sent to Business Availability Center, which includes aggregated samples where each sample represents five minutes of data. For details on the rum_server_t sample, see "Sample: RUM Transactions (rum_trans_t)" in *Reference Information*.

GUI Element (A-Z)	Description
Server network connections availability	To send an alert if the percentage of successfully created TCP connections compared to the total number of created connections is less than or greater than the specified percentage, calculated over the selected time period. After selection, the following editable information is displayed in the Alert Description area in the Alert triggers section: **Server network connections availability is** <condition> **Calculate over** <time_period> Click the <condition> link to open the Server Network Connections Availability dialog box. Click the <time_period> link to open the Calculated Time Period dialog box. Only completed transactions are considered when triggering this alert. **Note:** The trigger is calculated using the values of the **availability** and **tot_connection** fields in the **rum_tcp_server_t** sample sent to Business Availability Center, which includes aggregated samples where each sample represents five minutes of data. For details on the **rum_tcp_server_t** sample, see "Sample: RUM TCP Servers (rum_tcp_server_t)" in *Reference Information*.

Alert Description Area

Description	Displays a summary of the selections you have made in the current tab and in the previous tabs (if relevant). It can include: ➤ **Profile.** The name of the profile you selected in the New Alert dialog box. ➤ **Alert triggers.** The list of triggers you selected in the Trigger Criteria tab. See each trigger description for a list of the elements that can be listed in this section. ➤ **Alert filters.** The list of filters you selected in the Filters tab. See each filter description for a list of the elements that can be listed in this section. In addition, if you have selected the RUM Engine profile in the Alerts page before clicking the **New** button, the name of the RUM Engine is listed in this section. ➤ **Alert actions.** The list of actions you selected in the Actions tab. See each action description for a list of the elements that can be listed in this section.

Filters Tab

Description	Enables you to track performance issues related to specific monitored servers, monitors, or measurements.
Important Information	When you select a filter, the **Alert filters** element is added to the Alert Description area. Depending on the filter you select, the Alert triggers area displays different information. You can combine one or more filters for each type of filters.
Wizard Map	The Alert Wizard includes: Trigger Criteria Tab > **Filters Tab** > Actions Tab > Settings Tab

<Select Filters> Area

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Group performance data	Select to use the group performance data as a criteria. By default, when assessing whether alert trigger criteria have been met, all the relevant performance data in the profile database is considered. For example, when assessing whether a transaction has failed, all the transaction instances are checked. After selection, the following editable information is displayed in the Alert Description area in the Alert filters section: **Group performance data by** <specified criteria> **(Setting not specified)** HP Business Availability Center sends an alert if the performance data you selected by any combination of page name, transaction name, and server name matches the specified criteria. For details, see "Group Performance Data Dialog Box" on page 342. **Note:** When you are using this option, you can add Group Performance Data parameters to return information as alert parameters or event parameters when HP Business Availability Center has been instructed to consider the performance data by transaction, by script (file containing transactions), by group, by location, or by any combination of those groups. How you group performance data has an impact on the triggering of alerts. If you are setting Real User Monitor alert filters, you can select to consider the performance data per page name, transaction name, or server name. The option you select depend on the type of alert you are configuring. For details, see "Group Performance Data Parameters" on page 344.

GUI Element (A-Z)	Description
Limit to end-user locations	Select to use the limit to end-user locations as a criteria. **Note:** This list of triggers is displayed when you have selected both: ➤ A RUM Engines profile in the Alerts page ➤ The **RUM Pages** or **RUM Transaction** type in the New Alert dialog box After selection, the following editable information is displayed in the Alert Description area in the Alert filters section: **Limit to end-user locations** <as_specified> HP Business Availability Center sends an alert if the alert trigger criteria are met for one or more specific end-user locations. By default, alerts are sent when alert trigger criteria are met for any end-user location. **Note:** For more information on Real User Monitor alert filters, see "Grouping and Limitations For Real User Monitor Profiles" on page 320.
Limit to end-user names	Select to use the limit to end-user names as a criteria. **Note:** This list of triggers is displayed when you have selected both: ➤ A RUM Engines profile in the Alerts page ➤ The **RUM Pages** or **RUM Transaction** type in the New Alert dialog box. After selection, the following editable information is displayed in the Alert Description area in the Alert filters section: **Limit to end-user names** <as_specified> HP Business Availability Center sends an alert if the alert trigger criteria are met for one or more specific end-user names. By default, alerts are sent when alert trigger criteria are met for any end-user name. **Note:** For more information on Real User Monitor alert filters, see "Grouping and Limitations For Real User Monitor Profiles" on page 320.

GUI Element (A-Z)	Description
Limit to groups	Select to use the limit to groups as a criteria. After selection, the following editable information is displayed in the Alert Description area in the Alert filters section: **Limit to groups** <as_specified> HP Business Availability Center sends an alert if the alert trigger criteria are met for one or more specific groups. By default, alerts are sent when alert trigger criteria are met for any group. **Note:** For more information on Real User Monitor alert filters, see "Grouping and Limitations For Real User Monitor Profiles" on page 320.
Limit to locations	Select to use the limit to locations as a criteria. After selection, the following editable information is displayed in the Alert Description area in the Alert filters section: **Limit to locations** <as_specified> HP Business Availability Center sends an alert if the alert trigger criteria are met for one or more specific locations. By default, alerts are sent when alert trigger criteria are met for any location. **Note:** For more information on Real User Monitor alert filters, see "Grouping and Limitations For Real User Monitor Profiles" on page 320.

GUI Element (A-Z)	Description
Limit to pages	Select to use the limit to pages as a criteria. **Note:** This list of triggers is displayed when you have selected both: ➤ A RUM Engines profile in the Alerts page ➤ The **RUM Pages** type in the New Alert dialog box. After selection, the following editable information is displayed in the Alert Description area in the Alert filters section: **Limit to pages** <as_specified> HP Business Availability Center sends an alert if the alert trigger criteria are met for one or more specific pages. By default, alerts are sent when alert trigger criteria are met for any page. **Note:** For more information on Real User Monitor alert filters, see "Grouping and Limitations For Real User Monitor Profiles" on page 320.
Limit to servers	Select to use the limit to servers as a criteria. **Note:** This list of triggers is displayed when you have selected both: ➤ A RUM Engines profile in the Alerts page ➤ The **RUM Servers** type in the New Alert dialog box. After selection, the following editable information is displayed in the Alert Description area in the Alert filters section: **Limit to servers** <as_specified> HP Business Availability Center sends an alert if the alert trigger criteria are met for one or more specific servers. By default, alerts are sent when alert trigger criteria are met for any end-user server. **Note:** For more information on Real User Monitor alert filters, see "Grouping and Limitations For Real User Monitor Profiles" on page 320.

GUI Element (A-Z)	Description
Limit to transactions	Select to use the limit to transactions as a criteria. **Note:** This list of triggers is displayed when you have selected both: ➤ A RUM Engines profile in the Alerts page ➤ The **RUM Transaction** type in the New Alert dialog box. After selection, the following editable information is displayed in the Alert Description area in the Alert filters section: **Limit to transactions** <as_specified> HP Business Availability Center sends an alert if the alert trigger criteria are met for one or more specific transactions. By default, alerts are sent when alert trigger criteria are met for any transaction. **Note:** For more information on Real User Monitor alert filters, see "Grouping and Limitations For Real User Monitor Profiles" on page 320.

Alert Description Area

Description	Displays a summary of the selections you have made in the current tab and in the previous tabs (if relevant). It can include: ➤ **Profile.** The name of the profile you selected in the New Alert dialog box. ➤ **Alert triggers.** The list of triggers you selected in the Trigger Criteria tab. See each trigger description for a list of the elements that can be listed in this section. ➤ **Alert filters.** The list of filters you selected in the Filters tab. See each filter description for a list of the elements that can be listed in this section. In addition, if you have selected the RUM Engine profile in the New Alert dialog box, the name of the RUM Engine is listed in this section. ➤ **Alert actions.** The list of actions you selected in the Actions tab. See each action description for a list of the elements that can be listed in this section.

Grouping and Limitations For Real User Monitor Profiles

Important Information	The performance data by which you can group, and the data by which you can limit a Real User Monitor alert scheme, differ from other alert schemes. The grouping and limitation options also differ, depending on the type of Real User Monitor alert you are configuring.

The following table describes the grouping and limitation options available for each type of Real User Monitor alert:

Alert Type	Group Performance Data Options	Limitation Options
Page	Page name End-user name	Pages End-user names End-user locations
Transaction	Transaction name End-user name	Transactions End-user names End-user locations
Server	Server name	Servers
End-User	End-user name	End-user names End-user locations

Actions Tab

Description	Enables you to specify the actions that HP Business Availability Center takes when alert trigger criteria and filter criteria are met. You can select one or more of the following actions: ➤ Send an alert to specified recipients. ➤ Include user messages in the alert notice. ➤ Access URLs. ➤ Send an SNMP trap. ➤ Run an executable file. ➤ Log an event in the Windows Event Viewer application log. ➤ Make an alert the subordinate to another alert.
Important Information	When you select an action, the **Alert actions** element is added to the Alert Description area. Depending on the action, you select the Alert actions area displays different information. You can combine one or more actions.
Wizard Map	The Alert Wizard includes: Trigger Criteria Tab > Filters Tab > **Actions Tab** > Settings Tab

<Select Actions> Area

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Access URLs	Select to specify that you want to access a URL when alert trigger criteria are met. Accessing the URL provides the capability to send alerts through a Web site (for example, using Active Server Pages, CGI, or Perl). The URL can activate an executable program on a Web server, report to a custom database, activate a Web-based fax service, and so on. You can develop custom pages or use existing ones. After selection, the following editable information is displayed in the Alert Description area in the Alert actions section: **Access the URLs** <as_specified> Click the link to open the Access URLs dialog box where enter the URL or select an existing URL. **Note:** Business Availability Center supports the GET method only when accessing a URL. If your Web server supports only the POST method, or if you want more information on developing custom Web pages for your server, contact your HP Software Support representative. You can access the Business Impact report for a specific CI when an event-based alert occurs if you enter the following URL in the email, SMS, or Pager message: **http://<server_name>/login.jsp?portlet_url=/service-impact/main/page.do?cild=<triggered_ci_id>** For details on the Business Impact report, see "Business Impact Report" in *Using Dashboard*.

GUI Element (A-Z)	Description
Include user message	Select to include a user message in the alert notices that recipients receive. when an alert is triggered. After selection, the following editable information is displayed in the Alert Description area in the Alert actions section: **Include the user message** <as_specified> Click the link to open the Add User Message dialog box where you type the message that you want to include in the alert notice.
Log to Event Viewer application log (Windows only)	Select to log the event that triggered the alert to the Windows Event Viewer application log when an alert is triggered. After selection, the following editable information is displayed in the Alert Description area in the Alert actions section: **Log** <as_specified> Click the link to open the Log Event dialog box where you configure the event type, ID, category, and description (standard Event Viewer categories). **Note:** If the Data Processing Server is not installed on a Windows-based machine, HP Business Availability Center cannot execute this alert action.

GUI Element (A-Z)	Description
Make specified alerts subordinate to this alert	Select to suppress all actions configured for the alert if its dominant alert was previously configured as well, and if the conditions that triggered the dominant alert remain true at the time the subordinate alert is triggered. Further, you can define a time limit for each alert you designate as subordinate. HP Business Availability Center begins running the clock on the time limit from the moment the dominant alert is triggered. When a time limit is defined, the actions of the subordinate alert are suppressed as long as the conditions that triggered the dominant alert remain true—but only until the time limit expires. For details, see "Guidelines and Tips for Configuring Alert Dependencies" on page 399. **Note:** Regardless of the actions you select, each time alert trigger criteria are met, HP Business Availability Center logs an alert in the Alerts Log, which you view on the Web site. For details on viewing the alerts log, see "Alerts Log Report" on page 279. After selection, the following editable information is displayed in the Alert Description area in the Alert actions section: **Make the following alert(s) subordinate to this alert:** <specify alerts> Click the link to open the Define Subordinate Alerts dialog box where you specify alerts dependency. For additional information, see "Alerts Dependency Overview Page" on page 404.

GUI Element (A-Z)	Description
Run executable file	Select to run a predefined or custom executable file (for example, an **.exe** or **.bat** file) when an alert is triggered. The executable file must not be interactive (no user response required) and should not have a user interface. After selection, the following editable information is displayed in the Alert Description area in the Alert actions section: **Run executable file** <as_specified> Click the link to open the Run Executable File dialog box where you can specify the location and type of executable file.
Send alert to specified recipients	Select to send an alert notice to selected recipients when an alert is triggered. After selection, the following editable information is displayed in the Alert Description area in the Alert actions section: **Send alert to** <specified_recipients> Click the link to open the Select Recipients dialog box where you can select the recipients of the alert notices.

GUI Element (A-Z)	Description
Send SNMP trap	Select to specify that you want to send an SNMP trap when an alert is triggered. The alert notice can then be seen through any SNMP management console in the organization. After selection, the following editable information is displayed in the Alert Description area in the Alert actions section: **Send SNMP trap to** <specified_IPs> Click the link to open the SNMP Servers dialog box where you can specify information about the SNMP servers. **Note:** HP Business Availability Center supports only SNMP V1 traps. For details on configuring the Alerts MIB in your SNMP management console, see "Configure the Alerts MIB" on page 261.

Alert Description Area

Description	Displays a summary of the selections you have made in the current tab and in the previous tabs (if relevant). It can include: ➤ **Profile.** The name of the profile you selected in the New Alert dialog box. ➤ **Alert triggers.** The list of triggers you selected in the Trigger Criteria tab. See each trigger description for a list of the elements that can be listed in this section. ➤ **Alert filters.** The list of filters you selected in the Filters tab. See each filter description for a list of the elements that can be listed in this section. In addition, if you have selected the RUM Engine profile in the New Alert dialog box, the name of the RUM Engine is listed in this section. ➤ **Alert actions.** The list of actions you selected in the Actions tab. See each action description for a list of the elements that can be listed in this section.

Settings Tab

Description	Enables you to specify additional alert settings and review your alert scheme before saving it. Additional alert settings enable you to: ➤ Specify the name of the alert. ➤ Specify the alert severity. The alert severity can be used for classification purposes. ➤ Send a follow-up alert and to run an executable file when the follow-up alert is triggered. ➤ Specify the alert notification frequency. ➤ Temporarily disable the alert scheme.
Important Information	If the original alert was configured to be sent based on any alert frequency criteria other than **even once**, the executable file run, based on a follow-up alert, cannot include the following parameters: UserMessage, org_name, script_name, txn_err, host_name, time, actual_desc, target_host_name, mon_name, msr_name, con_name, err_msg. This is because HP Business Availability Center records all the data for each event that satisfies the alert criteria and sends the alert only when the defined frequency criteria was met. The follow-up alert no longer contains these parameters. For details on alert frequency criteria, see "Alert Frequency Criteria Dialog Box" on page 278.
Wizard Map	The Alert Wizard includes: Trigger Criteria Tab > Filters Tab > Actions Tab > **Settings Tab**

<Settings> Area

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Action	Click the **Action** link to open the Run Executable File dialog box. For details, see "Run Executable File Dialog Box" on page 363.
Auto Name	Click the **Auto Name** link to restore the default name assigned by HP Business Availability Center.
Enable alert	➤ Select to enable the alert. ➤ Clear to temporarily disable the alert scheme if you do not want to send or log alerts when the trigger criteria are met. For example, disable an alert scheme when you have not finished creating the profile related to the alert or if you temporarily stop the profile run.
Name	Enter the required alert name. The alert name appears in the alert notices that HP Business Availability Center sends. The default alert name is based on the alert trigger criteria you select. If you do not want HP Business Availability Center to use the default alert name, you can give the alert an alternative name.

GUI Element (A-Z)	Description
Notification Frequency	Select one of the following options to specify the frequency with which you want HP Business Availability Center to perform the alert actions that you select: ➤ **send alert for every trigger occurrence** ➤ **send no more than one alert per <specified time>** ➤ **send no more than one alert as long as the conditions that triggered the alert continue to exist** details on these options are also provided in this table. **Note:** Regardless of the frequency you select, each time alert trigger criteria are met, Business Availability Center logs an alert in the Alerts Log. For details on viewing the alerts log, see "Alerts Log Report" on page 279.
Send alert for every trigger occurrence	Select the option to send an alert every time trigger conditions exist.
Send follow up alert	Select the option to send a follow-up alert when the conditions that trigger the original alert are no longer true. Business Availability Center sends the follow-up alert to the same recipients that received the original alert. Business Availability Center uses the system's default follow-up template or a user-defined follow-up template. For details on creating a user-defined follow-up template, and the conditions under which it is used, see "Configure a Template for Follow-up Notifications" on page 388. You can also instruct Business Availability Center to run an executable file when the follow-up alert is triggered. For details, see **Action** description in this table. **Note:** The follow-up alert is logged in the Alerts log, with the status listed as OK, regardless of the status of the original alert.

GUI Element (A-Z)	Description
Send no more than one alert as long as the conditions that triggered the alert continue to exist	Select the option to send no more than one alert notice as long as the conditions that triggered the alert continue to exist. **Note:** When you select this option, HP Business Availability Center automatically selects the **Send follow-up alert** option. If you do not want a follow-up alert to be sent when the conditions that triggered the alert no longer exist, you must manually clear the **Send follow-up alert** setting. **Example:** If you select this option, from the moment alert trigger conditions exist and HP Business Availability Center sends the alert, an additional alert is not sent as long as the conditions that triggered the alert continue to exist.
Send no more than one alert per specified time period	Select the option to send no more than one alert over each specified time period, even if alert trigger conditions continue to exist during the entire time period. **Example:** If you instruct HP Business Availability Center to send no more than one alert notice per 60 minutes, from the moment alert trigger conditions exist and HP Business Availability Center sends the alert, HP Business Availability Center waits 60 minutes before sending another alert. If, after the 60 minutes, the conditions that triggered the alert continue to exist, another alert is sent.
Severity	To provide meaningful labels to your alerts to identify and classify them when you receive them or when you see them in the Alerts Log. Select: **OK**, **Warning**, **Minor**, **Major**, or **Critical** When choosing the severity label, consider the priority of the alert scheme's alert trigger criteria. **Example:** Label the alert OK if the alert trigger criteria do not reflect a problem that affects end users. Label the alert Critical if the alert trigger criteria reflect a total site crash.

Alert Description Area

Description	Displays a summary of the selections you have made in the current tab and in the previous tabs (if relevant). It can include: ➤ **Profile.** The name of the profile you selected in the New Alert dialog box. ➤ **Alert triggers.** The list of triggers you selected in the Trigger Criteria tab. See each trigger description for a list of the elements that can be listed in this section. ➤ **Alert filters.** The list of filters you selected in the Filters tab. See each filter description for a list of the elements that can be listed in this section. In addition, if you have selected the RUM Engine profile in the New Alert dialog box, the name of the RUM Engine is listed in this section. ➤ **Alert actions.** The list of actions you selected in the Actions tab. See each action description for a list of the elements that can be listed in this section.

Average Response Time Dialog Box

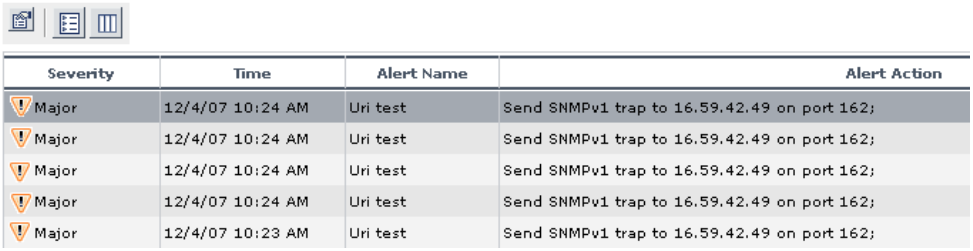
Description	To specify the average response time trigger criteria. HP Business Availability Center sends an alert if the average transaction response time is greater than or less than the selected number of seconds, calculated over the selected time period. Only completed transactions are considered when triggering this alert. **To access:** Click the link in **Average transaction response time is** <average_response_time> **seconds** or in **Average transaction response time is** <condition> **than baseline threshold** in the Alert wizard, in the Trigger Criteria tab in the Alert Description area.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Average response time is <condition> <nn> seconds	Displayed when you select the Enabled/Disabled baseline modes. Select the required criteria. **Example:** Select **greater than** and **10** to instruct HP Business Availability Center to send the alert if average response time is greater than 10 seconds, over the calculated time period.
Average response time is <condition> baseline threshold level	Displayed when you select the Automatic/Full-Automatic baseline modes. Select the required criteria. **Example:** Select **greater than** and **10** to instruct HP Business Availability Center to send the alert if average response time is greater than the baseline threshold, over the calculated time period.

Baseline Suggested Alerts Log Report

The following is an example of the Baseline Suggested Alerts Log report.



Severity	Time	Alert Name	Alert Action
Major	12/4/07 10:24 AM	Uri test	Send SNMPv1 trap to 16.59.42.49 on port 162;
Major	12/4/07 10:24 AM	Uri test	Send SNMPv1 trap to 16.59.42.49 on port 162;
Major	12/4/07 10:24 AM	Uri test	Send SNMPv1 trap to 16.59.42.49 on port 162;
Major	12/4/07 10:24 AM	Uri test	Send SNMPv1 trap to 16.59.42.49 on port 162;
Major	12/4/07 10:23 AM	Uri test	Send SNMPv1 trap to 16.59.42.49 on port 162;

Description	Enables you to track all alert details for event-based alerts that would be sent by HP Business Availability Center during the specified time range, for the selected Business Process Monitor profiles, or Real User Monitor, regardless of the action specified for the alert in the alert scheme, if you were using Baselining. **To access:** Select **Applications** > **Alerts** > **Event-Based Alerts Reports** > **Baseline Suggested Alerts Log**.
Important Information	The Baselined Alerts Log displays up to 20 entries per page. If there are more than 20 entries, use the navigation links at the top or bottom of the screen to move through the Baselined Alerts Log.
Included in Tasks	“View Event-Based Alert Reports” on page 264
Useful Links	“Working with Baseline Modes” on page 256

Report Settings

GUI Element (A-Z)	Description
<Common report elements>	See “Common Report Elements” in *Reports*.
Alert	Click the **Alert** link to open the Alerts dialog box where you can select the alert whose log you want to display.

GUI Element (A-Z)	Description
Profile	Click the **Profile** link to open the Profile dialog box where you can select the profile used to filter the alerts displayed in the report.
Severity	Click the **Severity** link to open the Severity dialog box where you can select the severities you want to use to filter the alerts displayed in the report.

Report Table Area

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Select an alert in the report and click the button to drill down to the Alert Details report.
Alert Action	Displays alert notification information (for example, the recipients who would receive the alert).
Alert Name	Displays the alert name that you specified in your alert scheme.
Severity	Displays an icon that represents the alert severity label you selected for the alert in the alert scheme. The severity is selected in “Settings Tab” on page 327.
Time	Displays the date and time that HP Business Availability Center logged the baselined alert.

Calculated Time Period Dialog Box

Description	Select the calculated time period. **To access:** Click the link of **Calculate over** <calculated_time_period> in the Alert Description area of the Trigger Criteria tab in the Alert wizard.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Calculate over <nn> <time period>	Specify the trigger criteria. You can select up to **525600 minutes**, **721 hours**, or **30 days**. **Example:** ➤ For the **Availability** time-based trigger, select **15** and **minute(s)** to send the alert if transaction availability is less than 95 percent, over a five minute-period. ➤ For the **Transaction Response Time for Specified Percentage of Transactions** time-based trigger, select **2** and **hour(s)** to send the alert if the response time is greater than 7 seconds for 50 percent of all transaction instances that occur over a 2-hour period, but only if there were at least 50 transaction instances during the 2 hours. ➤ For the **Transaction Response Time Relative to Threshold for Specified Percentage of Transactions** time-based trigger, select **2** and **hour(s)** to send the alert if the response time is worse than the set threshold (treated as 10 percent better than the set value) for 90 percent of transaction instances that occur over a 2-hour period, but only if there were at least 100 transaction instances during the 2 hours. ➤ For the **Average Transaction Response Time** time-based trigger, select **2** and **hour(s)** to send the alert if average response time is greater than 10 seconds, over a 2-hour period.

Completed Transaction Volume Dialog Box

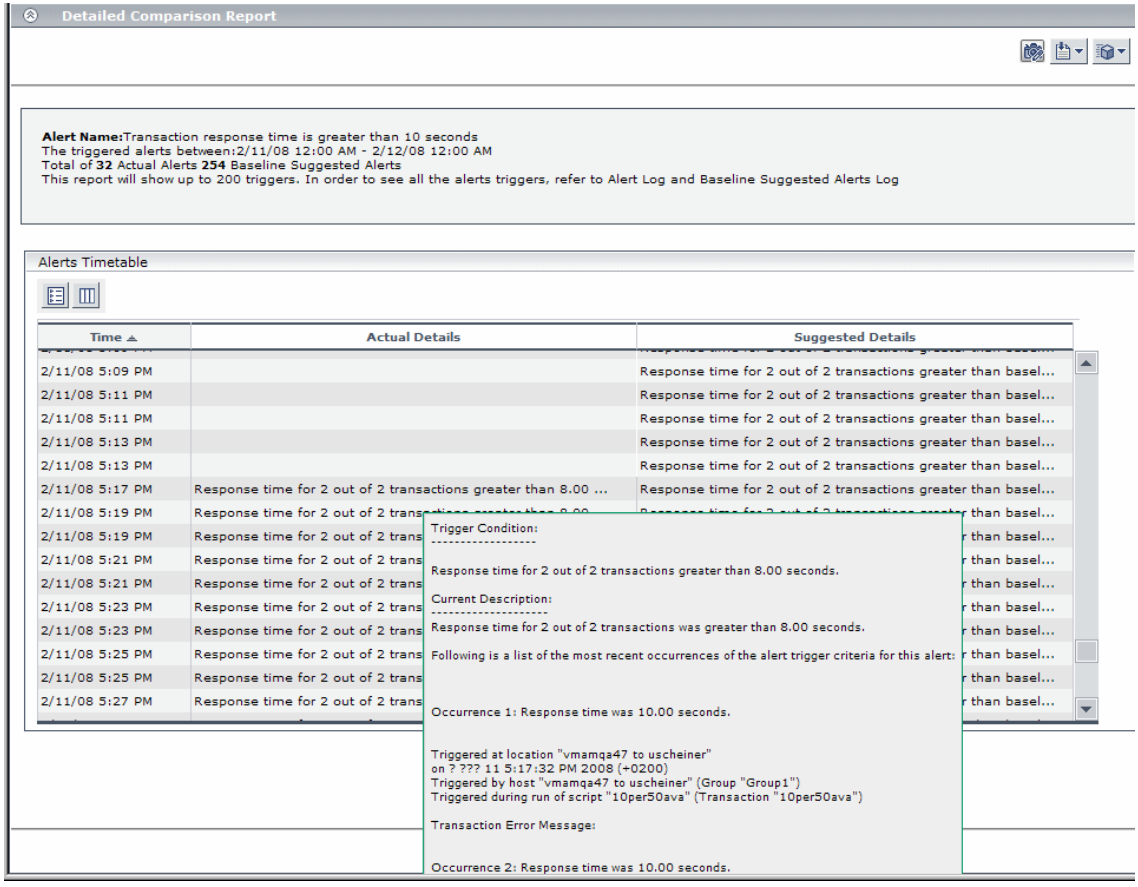
Description	Enables you to specify the conditions on the completed transaction volume. Business Availability Center sends an alert if the number of completed transaction runs is less than or greater than the specified number, calculated over the selected time period. **To access:** Click the link in **Completed volume is <condition> transactions** in the Trigger Criteria page of the Alerts wizard.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Completed volume is <condition> <nn> transactions	Select the required criteria. **Example:** Select **less than** and **80** to send the alert if there were fewer than 80 completed transaction runs, over the calculated time period. For details on how to set the calculated time period, see "Calculated Time Period Dialog Box" on page 335.

Detailed Comparison Report

The following is an example of the Detailed Comparison report.



Description	Enables you to list the details of each actual alert and each baseline-suggested alert for the selected time period, which corresponds to the cell you clicked in the **Actual vs. Baseline Suggested Alerts Comparison** report. **To access:** ➤ Click the appropriate cell in the **Actual vs. Baseline Suggested Alerts Comparison** report.
Included in Tasks	"View Event-Based Alert Reports" on page 264
Useful Links	"Working with Baseline Modes" on page 256

Report Settings

GUI Element (A-Z)	Description
<Common report elements>	See "Common Report Elements" in *Reports*.

Alert Name Area

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Alert Name	The name of the subordinate alert, followed by the alert trigger criteria, the time period of the report, and the total number of actual alerts and of baseline-suggested alerts.

Alerts Timetable Area

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<tooltip>	Move the mouse over a cell in the table to display a tooltip that includes the trigger condition, the actual value of the trigger conditions at the time the alert was triggered, or the value of the trigger conditons at the time the baseline-suggested alert would have been triggered if you were using baselining, and error messages.
Actual Details	The event that triggered the alert.
Suggested Details	The event that would have triggered the alert, if you were using baselining.
Time	The time when the alert occurred or the time when the alert would have occurred, if you were using baselining.

End-User Filters Dialog Box

Description	Enables you to select the end-users that are to be used as criteria for the alert. **To access:** Click the link in **Limit to end-user names** <as_specified> in the Alerts definition area in the Filters tab in the Alert wizard.
Important Information	For details on the options available when setting Real User Monitor alert filters, see “Grouping and Limitations For Real User Monitor Profiles” on page 320.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Available End-Users **Selected End-Users**	Select from the **Available End-Users** list, and use the upper right arrow to move your selections to the **Selected End-Users** list. Use the lower left arrow to remove an entity from the filter. You can select multiple filters using the CTRL key.

End-User Location Filters Dialog Box

Description	Enables you to select the end-user locations that are to be used as criteria for the alert. **To access:** Click the link in **Limit to end-user locations** <as_specified> in the Alerts definition area in the Filters tab in the Alert wizard.
Important Information	For details on the options available when setting Real User Monitor alert filters, see "Grouping and Limitations For Real User Monitor Profiles" on page 320.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Available Locations **Selected Locations**	Select from the **Available Locations** list, and use the upper right arrow to move your selections to the **Selected Locations** list. Use the lower left arrow to remove an entity from the filter. You can select multiple filters using the CTRL key.

Groups Filters Dialog Box

Description	To instruct HP Business Availability Center to limit the alert scheme to one or more specific group. **To access:** Click the link in **Limit to groups** <as_specified> in the Alerts definition area in the Filters tab in the Alert wizard.
Important Information	For the Real User Monitor, you can instruct HP Business Availability Center to limit the alert scheme to one or more specific pages, transactions, or servers depending on the type of alert you are configuring. For more information on Real User Monitor alert filters, see "Grouping and Limitations For Real User Monitor Profiles" on page 320.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Available Groups **Selected Groups**	Select from the **Available** list, and use the upper right arrow to move your selections to the **Selected** list. Use the lower left arrow to remove an entity from the filter. You can select multiple filters using the CTRL key.

Group Performance Data Dialog Box

Description	Enables you to set the alert filters to group the performance data. **To access:** Select **Group performance data** in the Filters tab in the Alert wizard.
Important Information	For details on the options available when setting Real User Monitor alert filters, see "Grouping and Limitations For Real User Monitor Profiles" on page 320. **Note:** When you group data, you can add **Group Performance Data** parameters to return information as alert parameters or event parameters when HP Business Availability Center has been instructed to consider the performance data by transaction, by script (file containing transactions), by group, by location, or by any combination of those groups. For details, see "Group Performance Data Parameters" on page 344. **Note:** When you group alerts, each alert in the group sends emails, SMSs, or pager messages separately.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Transaction **Script** **Location** **Group**	Select whether you want performance data grouped by transactions, scripts, location, or groups. **Example:** A profile contains two transactions, T1 and T2, both running from two locations, L1 and L2. The following combinations of locations and transactions have the following response times: ➤ L1, T1 - 12 seconds ➤ L1, T2 - 11 seconds ➤ L2, T1 - 12 seconds ➤ L2, T2 - 1 second You want an alert to be triggered if the average transaction response time is greater than 10 seconds. Without the filter, the average response time is 9 seconds ((12+11+12+1)/4), and the alert is not sent. When the filter is set to: ➤ **Transaction**. All instances of transaction T1 are considered separately from all instances of transaction T2. Average response time for T1 is calculated as ((12+12)/2)=12 seconds (>10 seconds). An alert is send to T1. Average response time for T2 is calculated as ((11+1)/2)=6 seconds (<10 seconds). Alert for T2 is not sent. ➤ **Location**. An alert is sent for L1 but not for L2. ➤ **Transaction** and **location**. All instances of transaction T1 from location L1 are considered separately from all instances of T1 from L2, all instances of T2 from L1, and all instances of T2 from L2 separately. An alert is sent for T1 from L1, T1 from L2, T1 from L2, but not for T2 from L2.

Group Performance Data Parameters

Description	Embed the parameters so they return information as alert parameters or event parameters only if the alert scheme was defined with **Group performance data** grouped by transaction, by script (file containing transactions), by group, by location, or by any combination of the four. For example, –title "Group by <<transaction>>" - text "<<User Message>>" For details on grouping performance data when creating an alert scheme, see "Group Performance Data Dialog Box" on page 342.

The parameters are:

Parameter	Description
group	The group name of the host machine that ran the transactions that triggered the alert, the event, or both. Can be used only when performance data has been grouped by group.
location	The location of the host machine, specified during Business Process Monitor installation, that ran the transactions that triggered the event. Can be used only when performance data has been grouped by location.
transaction	The transaction name specified in the script. Can be used only when performance data has been grouped by transaction.
transaction file	The name of the script containing the transactions that triggered the alert, the event, or both. Can be used only when performance data has been grouped by script.

Locations Filters Dialog Box

Description	To instruct HP Business Availability Center to limit the alert scheme to one or more specific location. **To access:** Click the link in **Limit to locations** <as_specified> in the Alerts definition area in the Filters tab in the Alert wizard.
Important Information	For the Real User Monitor, you can instruct HP Business Availability Center to limit the alert scheme to one or more specific pages, transactions, or servers, depending on the type of alert you are configuring. For more information on Real User Monitor alert filters, see "Grouping and Limitations For Real User Monitor Profiles" on page 320.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Available Locations **Selected Locations**	Select from the **Available** list, and use the upper right arrow to move your selections to the **Selected** list. Use the lower left arrow to remove an entity from the filter. You can select multiple filters using the CTRL key.

Log Event Dialog Box

Description	You specify that you want HP Business Availability Center to log an event to the Windows Event Viewer application log when an alert is triggered. You configure the event type, ID, category, and description (standard Event Viewer categories). **Note:** If the Data Processing Server is not installed on a Windows-based machine, HP Business Availability Center cannot execute this alert action. **To access:** Click the link in **Log** <as specified> in the Alert definitions area in the Actions tab in the Alert wizard.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Category	If required, specify a numerical category value in the Category box. You can use category values to group alerts by type. Using categories enables you to find events in the Event Viewer. **Default:** 0 **Example:** Assign **1** to availability-related alerts and **2** to response-time related alerts.
Description	If required, type a description of the logged event. **Example:** Type a description that corresponds to the characteristics of the alert scheme (alert filters being used, alert trigger criteria, and so on).

GUI Element (A-Z)	Description
Event ID	If required, specify a numerical event ID in the Event ID box. You can use event IDs to group alerts by trigger criteria, profile, transaction, or any other identifying characteristic. Use event IDs to find events in the Event Viewer. **Default:** 0
Type	Select an event type from the Type list: **Success**, **Error**, **Warning**, **Information**, **Success audit**, or **Failure audit**. Event types are represented by icons to the left of the entries in the Event Viewer.

Multiple Trigger Condition Dialog Box

Description	If you select multiple time-based alert trigger criteria, you specify whether you want Business Availability Center to send the alert: ➤ If any of the trigger conditions are met. ➤ Only if all the time-based trigger conditions are met. **To access:** Click the link of **Send alert if** <any of the above> **trigger conditions are met** in the Alert Description area of the Trigger Criteria tab in the Alert wizard.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
All trigger conditions are met	Select if you want Business Availability Center to send the alert only if all the time-based trigger conditions are met
Any of the trigger conditions are met	Select if you want Business Availability Center to send the alert if at least one of the trigger conditions are met.

Net Transaction Response Time Performance Dialog Box

Description	If you select the **Net transaction response time for specified percentage of transactions is** <as specified> trigger, Business Availability Center sends an alert if net transaction time is greater than or less than the selected number of seconds for no less than the selected percentage of transactions, calculated over the selected time period. You can also set a minimum number of transactions that must run in order for the alert conditions to be calculated. **To access:** Click the link in **Net transaction response time for specified percentage of transactions is** <as specified> in the Trigger Criteria page of the Alerts wizard.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Minimum number of transactions for which condition is calculated:	Select a minimum number of transactions that must run in order for the alert conditions to be calculated.
Net transaction time is <condition> <nn>seconds for <percent> percent of transactions	Select the required criteria. **Example:** Select **greater than**, enter a value of **8** seconds, and select **90** percent to send the alert if net transaction response time exceeds 8 seconds for at least 90 percent of the transactions that were run, over the calculated time period. **Note:** The value of the percentage must be an integer.

New Alert Dialog Box

Description	Enables you to create a new alert. **To access:** Select **[RUM Engines]** in the profile list and click **New Alert** in the Alerts Page.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Engine	If **[RUM Engines]** was selected in the profile list when you clicked **New Alert**, you can select one of the listed engines.
Profile	Select a profile. This field appears if you have selected **[All Profiles]** in the Alerts page. If **[RUM Engines]** was selected in the profile list when you clicked **New Alert**, the New Alert dialog box opens. You must select a Real User Monitor engine as well as the type of alert (page, transaction, or server) before continuing.
Type	If **[RUM Engines]** was selected in the profile list when you clicked **New Alert**, you can select one of the following types: ➤ RUM Pages ➤ RUM Transactions ➤ RUM Servers

Page Availability Dialog Box

Description	If you select the **Page Availability** trigger, HP Business Availability Center sends an alert if page availability is less than or greater than the specified percentage, calculated over the selected time period. **To access:** Click the link in **Page availability is** <condition> in the Trigger Criteria page of the Alerts wizard.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Page availability is <condition> <n> percent	Select the required criteria. **Example:** Select **less than** and **50** to instruct HP Business Availability Center to send the alert if page availability is less than 50 percent, over the calculated time period. For details on how to set the calculated time period, see “Calculated Time Period Dialog Box” on page 335. **Note:** The value of the percentage must be an integer.

Page Filters Dialog Box

Description	To limit the alert scheme to one or more specific page. **To access:** Click the link in **Limit to servers** <as_specified> in the Alerts definition area in the Filters tab in the Alert wizard.
Important Information	For the Real User Monitor, you can instruct HP Business Availability Center to limit the alert scheme to one or more specific pages, transactions, or servers, depending on the type of alert you are configuring. For more information on Real User Monitor alert filters, see "Grouping and Limitations For Real User Monitor Profiles" on page 320.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Available Pages **Selected Pages**	Select from the **Available** list, and use the upper right arrow to move your selections to the **Selected** list. Use the lower left arrow to remove an entity from the filter. You can select multiple filters using the CTRL key.

Page Response Time Performance Dialog Box

Description	If you select the **Page performance - page response time for specified percentage of pages** trigger, HP Business Availability Center sends an alert if the percentage of users that attempt to access the page with a response time that is higher than the threshold has been reached, calculated over the selected time period. For details on setting up the threshold, see "Edit General Settings Page" in *Using End User Management*. **To access:** Click the link in **Page performance - page response time for specified percentage of pages** in the Trigger Criteria page of the Alerts wizard.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Minimum number of pages for which condition is calculated: <pp>	Select the minimum number of pages to count. **Example:** Select **50** to instruct HP Business Availability Center to send the alert only if there are at least 50 accessed pages over the calculated time period.
Page download time is <condition> <nn> seconds for <percent> percent of pages	Select the condition, the required response time, and the percentage criteria. **Example:** Select **greater than**, **7 seconds**, and **50 percent** to send the alert if the response time is greater than 7 seconds for 50 percent of accessed pages, over the calculated time period. For details on how to set the calculated time period, see "Calculated Time Period Dialog Box" on page 335. **Note:** The value of the percentage must be an integer.

Page Server Time Performance Dialog Box

Description	If you select this trigger, Business Availability Center sends an alert if the percentage of users that attempt to access the page located on a server and the server's response time that is higher than the threshold has been reached, calculated over the selected time period. For details on setting up the threshold, see "Edit General Settings Page" in *Using End User Management*. **To access:** Click the link in **Page performance - server response time for specified percentage of pages** in the Trigger Criteria page of the Alerts wizard.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Minimum number of pages for which condition is calculated: <pp>	Select the minimum number of pages to count. **Example:** Select **50** to instruct HP Business Availability Center to send the alert only if there are at least 50 accessed pages over the calculated time period.
Page server time is <condition> <nn> seconds for <percent> percent of pages	Select the condition, the required response time and percentage criteria. **Example:** Select **greater than**, **7 seconds**, and **50 percent** to send the alert if the response time is greater than 7 seconds for 50 percent of accessed pages located on the server, over the calculated time period. For details on how to set the calculated time period, see "Calculated Time Period Dialog Box" on page 335. **Note:** The value of the percentage must be an integer.

Page Volume Dialog Box

Description	If you select the Page Volume trigger, HP Business Availability Center sends an alert if the number of page hits is less than or greater than the specified number, calculated over the selected time period. **To access:** Click the link in **Page volume** in the Trigger Criteria page of the Alerts wizard.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Page volume <condition> <nn> hits	Select the required criteria. **Example:** Select **less than** and **80** to instruct HP Business Availability Center to send the alert if there were fewer than 80 page hits, over the calculated time period. For details on how to set the calculated time period, see “Calculated Time Period Dialog Box” on page 335.

Response Time Dialog Box

Description	To send an alert if transaction response time is greater than or less than the selected number of seconds. Only completed transactions are considered. If a transaction fails (that is, is not completed successfully) no alert is sent. **To access:** Click the link of **Transaction response time is** <condition> in the Alert Description area of the Trigger Criteria tab in the Alert wizard.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Response time is <condition> <X> seconds	Select **greater than** or **less than**, and enter the number of seconds in the appropriate boxes. **Example:** Specify **greater than** and **10** to instruct HP Business Availability Center to send the alert if the response time is greater than 10 seconds.

Response Time for Specified Percentage of Transactions Dialog Box

Description	To specify the transaction availability criteria. An alert is sent if the response time is greater or less than the selected number of seconds, for the specified percentage of transactions, calculated over the selected time period. Only completed transactions are considered for this alert trigger. In addition, you can instruct Business Availability Center to count a minimum number of transactions over the calculated time period. **To access:** Click the link of **Transaction response time for specified percentage of transactions is** <response_time_for_%_of_trans> in the Alert Description area of the Trigger Criteria tab in the Alert wizard.
Important Information	**Example:** An alert is sent if transaction response time is greater than 10 seconds for 90 percent of all transaction instances that occur over the calculated time period (which you set in a separate dialog box). Further, the alert is sent only if at least 100 transactions occur during the calculated time period.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Minimum number of transactions for which condition is calculated <nnn>	Select the minimum number of transactions that must be considered in the calculation. **Example:** Select **50** to instruct HP Business Availability Center to send the alert only if there are at least 50 transaction instances over the calculated time period.
Response time is <condition> <n> seconds for <percentage> percent of transactions	Select the condition, the required response time and percentage criteria. **Example:** Select **greater than**, **7 seconds**, and **50 percent** to instruct HP Business Availability Center to send the alert if the response time is greater than 7 seconds for 50 percent of transaction instances, over the calculated time period. **Note:** The value of the percentage must be an integer.

Response Time Relative to Threshold Dialog Box

Description	If you select this trigger, HP Business Availability Center sends an alert if transaction response time is better or worse than the selected transaction threshold. Only completed transactions are considered for the specified minimum number of transaction. In addition, you can instruct HP Business Availability Center to treat the threshold value as better or worse than the set threshold, by a specified percentage. **To access:** Click the link in **Transaction response time relative to End User Management threshold** or in **Transaction response time relative to baseline threshold** in the Alert Description area of the Trigger Criteria tab in the Alert wizard.
Important Information	**Example:** HP Business Availability Center sends the alert if the response time for a given transaction is worse than the set threshold, but treats the threshold value as 10 percent better. If the threshold for the transaction is 10 seconds, the alert is triggered if the transaction response time is worse than 9 seconds (because 9 seconds is 10 percent better than 10 seconds). You configure transaction thresholds in End User Management. For details, see "Threshold Settings" in *Using End User Management*.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Response time is <condition> <threshold> baseline threshold level for <percentage> percent of transactions	Displayed when you select the Automatic/Full-Automatic baseline modes. You must: ➤ Select the condition criteria: **worse than** or **better than**, and the required threshold criteria: **OK/Minor** or **Minor/Critical** that is compared to the baseline threshold. ➤ Enter the percentage of transactions.

GUI Element (A-Z)	Description
Response time is <condition> <threshold> End User Management threshold level for <percentage> percent of transactions	Displayed when you select the Enabled/Disabled baseline modes. You must: ➤ Select the condition criteria: **worse than** or **better than**, and the required threshold criteria: **OK/Minor** or **Minor/Critical** that is compared to the End User Management threshold. ➤ Enter the percentage of transactions. **Example:** Select **worse than** or **better than**, and **Minor/Critical** to instruct HP Business Availability Center to send the alert if the response time is worse than the set threshold.
Treat threshold value as <value> percent <threshold>	Specify that you want to send an alert when the transaction response time is better or worse than the specified threshold to which is added the specified percentage of the threshold. **Note:** Transaction thresholds for Business Process profiles are set in System Availability Management. For details, see "Transaction Threshold Settings" in *Using End User Management*. **Note:** The value of the percentage must be an integer. **Example:** Select **10** percent and **better** to instruct HP Business Availability Center to treat the threshold value as 10 percent better than the value set in the Business Process profile.

Response Time Relative to Threshold for Specified Percentage of Transactions Dialog Box

Description	If you select this trigger, HP Business Availability Center sends an alert if the response time is better or worse than the selected transaction threshold, for the specified percentage of transactions, calculated over the selected time period. Only completed transactions are considered for triggering this alert. In addition, you can instruct HP Business Availability Center to: ➤ treat the threshold value as better or worse than the set threshold, by a specified percentage ➤ count a minimum number of transactions over the calculated time period **To access:** Click the link in **Transaction response time relative to End User Management threshold** or in **Transaction response time relative to baseline threshold for specified percentage of transactions is** <response_time_threshold_for_%_of_trans> in the Alert Description area of the Trigger Criteria tab in the Alert wizard.

Important Information	**Example:** Business Availability Center sends the alert if the response time is worse than the selected level threshold for 90 percent of all transaction instances that occur over the calculated time period (which you set in a separate dialog box). In addition, Business Availability Center treats the threshold value as 10 percent better, and the alert is sent only if at least 100 transactions occur during the calculated time period. Thus, if the threshold for the transaction is, for example, 10 seconds, and there are, for example, 120 transactions during the calculated time period, HP Business Availability Center sends an alert if transaction response time for at least 108 transactions (120 x 90%) is worse than 9 seconds (because 9 seconds is 10 percent better than 10 seconds). You configure transaction thresholds in End User Management. For details, see "Transaction Threshold Settings" in *Using End User Management*.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Minimum number of transactions for which condition is calculated <nn>	Specify whether HP Business Availability Center should treat the minimum number of transactions to count. **Example:** Select **100** to instruct HP Business Availability Center to send the alert only if there are at least 100 transaction instances over the calculated time period.
Response time is <condition> <threshold> baseline threshold level for <nn> percent of transactions	Displayed when you select the Automatic/Full-Automatic baseline modes. Select the required threshold and percentage criteria. **Example:** Select **worse than**, **Minor/Critical**, and **90 percent** to instruct HP Business Availability Center to send the alert if the response time is worse than the set Minor/Critical threshold for 90 percent of transaction instances, over the calculated time period. **Note:** The value of the percentage must be an integer.

GUI Element (A-Z)	Description
Response time is <condition> <threshold> threshold level for <nn> percent of transactions	Displayed when you select the Enabled/Disabled baseline modes. Select the required threshold and percentage criteria. **Example:** Select **worse than**, **Minor/Critical**, and **90 percent** to instruct HP Business Availability Center to send the alert if the response time is worse than the set Minor/Critical threshold for 90 percent of transaction instances, over the calculated time period. **Note:** The value of the percentage must be an integer.
Treat threshold value as <nn> percent <condition>	Specify that you want to send an alert when the transaction response time is better or worse than the specified threshold to which is added the specified percentage of the threshold. **Example:** Select **10 percent** and **better** to instruct HP Business Availability Center to treat the threshold value as 10 percent better than the value set in the Business Process profile. **Note:** The value of the percentage must be an integer.

Run Executable File Dialog Box

Description	To run an executable file (.**exe** or .**bat** file) when an alert is triggered. The executable file must not be interactive (no user response required) and should not have a user interface. Business Availability Center can run an executable file (.**exe** or .**bat** file) when an alert is triggered—either a predefined or custom executable. **To access:** Click the link in **Run executable file** as specified in the Alert definitions area in the Actions tab in the Alert wizard.

Important Information	**Note to Windows users:** To use the predefined batch files that restart a service (including IIS) or server, you must provide the supervisor service running on the Data Processing Server with permissions to restart a remote service or machine, as follows: 1 Open the **Windows Services** dialog box. 2 Right-click the **HP Business Availability Center** service, select **Properties**, and click the **Log On** tab. 3 In the Log On As section, select **This Account**, and specify the username and password of a user with administrator permissions on the HP Business Availability Center server machine. If the administrative user on the Data Processing Server and on the remote machine are not the same, you must provide the Data Processing Server machine administrator with permissions on the remote machine as follows: 1 On the remote machine, open Windows User Manager, and double-click **Administrators** in the Groups window to open the Local Group Properties dialog box. 2 Click **Add** to open the Add Users and Groups dialog box, and add the name of a user with administrator permissions on the Data Processing Server.
Included in Tasks	"Create Event-Based Alert Schemes – Workflow" on page 257

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<**command line**>	You can customize and control the executable file by adding parameters to the string. If you select: ➤ any template except **User defined,** the appropriate information is automatically displayed. ➤ the **User defined** template, use the following format for the executable file command line: <**path to exe file from Data Processing server**> <<**program command line switches**>> **Parameters:** ➤ <**path to exe file from Data Processing server**> The path to the executable must be available from the Data Processing server for the server to trigger the executable. ➤ <<**program command line switches**>> includes the alert parameters. The program command line switches are expanded before the command line is executed. Use the following format: **–request_parameter_name "string <<request_parameter_value>>" –request_parameter_name "<<request_parameter_value>>"** where **request_parameter_value** must be enclosed in double-angled brackets. For details on the parameters, see “Event Parameters” on page 366. **Example:** \myfile\run.exe -a "123" -b "qwerty asdfg" or d:\myfile\run.exe "123" "qwerty asdfg" **Note:** For additional information, if you select the **Group Performance Data** option, add group performance data parameters to the command line. For details, see “Group Performance Data Parameters” on page 344. **Note:** To send a follow-up alert with an action, use a specific format in the command line. For details, see “Action Format for Follow-Up Alerts” on page 371.

GUI Element (A-Z)	Description
Include output in alert email	To include any output that results from the running of the executable file in email alerts. HP Business Availability Center places this output in the section of the email alert containing the **Actions Result** text parameter. For details, see "Notification Templates Page" on page 394.
Use the following template	Select the type of template to use for running the file: ➤ **User defined** ➤ **ping** ➤ **Restart IIS** (not displayed if the Data Processing Server is on a Solaris platform) ➤ **Restart server** (not displayed if the Data Processing Server is on a Solaris platform) ➤ **Restart service** (not displayed if the Data Processing Server is on a Solaris platform)

Event Parameters

Description	Use event parameters to return information about specific transaction events that meet alert trigger criteria, but for which an alert is not sent. You can define alert trigger criteria in such a way that multiple conditions must be met before an alert is sent. You use the event parameters to return specific information about each of the individual transaction events for which trigger criteria were met.

Important Information	**Format:** The format of event parameters is: **<<parameter_nameevent_number tx_resp|tx_fail>>** **Note: parameter_name** and **event_number** are not separated by a space, but **event_number** and **tx_resp** are separated by a space. **Parameters:** Use double angle-brackets around the parameters. ➤ **parameter_name.** Enter the value of the parameter. ➤ **event_number.** Enter the index of the triggered event. The default value is 1. ➤ **tx_resp.** Enter the value of the parameter. ➤ **tx_fail.** Enter the value of the parameter. **Parameter value:** ➤ **Actual Details.** A description of actual conditions at the time of the event ➤ **Data Collector Name.** The name of the host machine that ran the transactions that triggered the event ➤ **Group Name.** The name of the organization specified during installation ➤ **Location Name.** The location of the host machine, specified during Business Process Monitor installation, that ran the transactions that triggered the event ➤ **Script Name.** The name of the script containing the transactions that triggered the event ➤ **Transaction Error.** A description of the error that the script generated, if an error occurred at the time of the event ➤ **Transaction Name.** The transaction name specified in the script ➤ **Transaction Time.** The time when the event was triggered

Important Information (continued)	If you do not specify the triggered event index, only information on the first event that meets trigger criteria is returned. If you specify the index of an event that does not occur (for example, if you specify 4 and there are only 3 events), an empty string is returned. **Example:** The alert trigger criteria is as follows: Send an alert if transactions fail or if transaction response time is greater than 10 seconds. Send alert if trigger conditions occur at least 3 times out of 5. Each instance of transaction failure or response time greater than 10 seconds is considered to be one transaction event that meets alert trigger criteria. However, the alert is sent only if the criteria are met at least 3 times out of 5.

SNMP-Specific Codes

The following table lists the alert types and their SNMP-specific codes. Use these codes when configuring alert notification events in your SNMP management console. For details, see "Configure the Alerts MIB" on page 261.

SNMP-Specific Code	Alert Type
1	Transaction response time Alert Frequency: **Even once**
2	Transaction failure Alert Frequency: **Even once**
3	Transaction availability
4	Average transaction response time
8	Transaction response time for the specified percentage of transactions
9	Transaction response time Alert Frequency: X out of Y
10	Transaction failure Alert Frequency: X out of Y
100	Complex alert (contains more than one subalert)

Alerts MIB Varbinds

The tables list the varbinds used in the Alerts MIB.

Object Identifier	MIB Label	Description
1.3.6.1.4.1.5233	mercuryInteractive	Company name
1.3.6.1.4.1.5233.4	topazAlerts4	Subject
1.3.6.1.4.1.5233.4.1	profileName	Profile name
1.3.6.1.4.1.5233.4.2	alertName	Alert name (for example, Response time of any transaction < 10.00 sec)
1.3.6.1.4.1.5233.4.3	alertType	Alert type: regular or follow-up
1.3.6.1.4.1.5233.4.4	alarmID	Unique alert ID
1.3.6.1.4.1.5233.4.5	alertSeverity	Alert severity: OK -10, warning - 20, minor - 30, major - 40,critical - 50
1.3.6.1.4.1.5233.4.6	alertTriggerCause	Defined alert trigger conditions (for example, Response time less than 10 seconds)
1.3.6.1.4.1.5233.4.7	alertActualDescription	Actual conditions at time of alert (for example, Current response time is 3.00 seconds)
1.3.6.1.4.1.5233.4.8	alertUserMessage	User message for this alert
1.3.6.1.4.1.5233.4.9	subAlertsTable	Start of the Subalerts table. Subalerts trigger alerts (listed in Events table)
1.3.6.1.4.1.5233.4.9.1	subAlertsEntry	Start of the subalert entry
1.3.6.1.4.1.5233.4.9.1.1	subAlertIndex	Index of the subalert within the subalert list
1.3.6.1.4.1.5233.4.10	subAlertInstances Table	Start of the subalert instance table

Object Identifier	MIB Label	Description
1.3.6.1.4.1.5233.4.9.10.1	subAlertInstances Entry	Start of the subalert instance entry
1.3.6.1.4.1.5233.4.9.10.1.1	subAlertInstances Index	Index of the subalert instance
1.3.6.1.4.1.5233.4.9.10.1.2	subAlertOwner	Index of the subalert owner
1.3.6.1.4.1.5233.4.9.10.1.3	subAlertInstance TriggerCause	Defined alert trigger conditions for the subalert instance
1.3.6.1.4.1.5233.4.9.10.1.4	subAlertInstance ActualDesc	Actual conditions at time of the subalert instance
1.3.6.1.4.1.5233.4.11	alertEvents	Start of the Events table
1.3.6.1.4.1.5233.4.11.1	transactionalEvents Table	Start of the alerts table
1.3.6.1.4.1.5233.4.11.1.1	transEventEntry	Start of the alert entry
1.3.6.1.4.1.5233.4.11.1.1.1	transEventIndex	Index of the event within the event list
1.3.6.1.4.1.5233.4.11.1.1.2	txnSubAlertInstance Owner	Index of the subalert instance owner from the subalert instance table
1.3.6.1.4.1.5233.4.11.1.1.3	transactionName	Transaction name
1.3.6.1.4.1.5233.4.11.1.1.4	organization	Group name
1.3.6.1.4.1.5233.4.11.1.1.5	host	Host name
1.3.6.1.4.1.5233.4.11.1.1.6	location	Location name
1.3.6.1.4.1.5233.4.11.1.1.7	script	Script name
1.3.6.1.4.1.5233.4.11.1.1.8	eventTime	Event time

Object Identifier	MIB Label	Description
1.3.6.1.4.1.5233.4.11.1.1.9	eventActualDescription	Description of event (for example, Response time 3.00 seconds)
1.3.6.1.4.1.5233.4.11.1.1.10	txnErrorMessage	Error message generated during a script run

Action Format for Follow-Up Alerts

Important Information	To send a follow-up alert with an action, you can use a specific format in the command line: **<path to exe file from Data Processing server> <<parameters>>** **Parameters:** ➤ **<path to exe file from Data Processing server>** Because the server triggers the executable, the path to the executable must be available from the Data Processing server. ➤ <<**parameters**>> includes the alert parameters. The parameters are replaced by real information when you grouped the performance data by Transaction, Script, Location, or Group. For details about the parameters, see below. For details about grouping performance data, see “Group Performance Data Dialog Box” on page 342. **Note:** If you do not group the performance data, the parameters are not replaced by real information. **Example:** \myfile\run.exe <<transaction name>> <<location name>> **Note:** Depending on the profile you selected, you can use different parameters. For details about the parameters, see “Alert Parameters” on page 285.

Select Recipients Dialog Box

Description	Specify the recipients that receive alert notices. **To access:** When selecting recipients in: ➤ Alerts: ➤ **Profile alerts.** For details, see "Event-Based Alerts" on page 251. ➤ **SLA status alerts.** For details, see "SLA Alerts". ➤ **CI status alerts.** For details, see "CI Status Alerts". ➤ **Scheduled reports.** For details on defining scheduled reports, see "Create a Schedule" in *Reports*. ➤ **Package information.** This option is needed only when using HP Software-as-a-Service. For details on viewing package information, see "Package Manager Window" in *Model Management*.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Available Recipients **Selected Recipients**	Select the recipients to whom you want alert notifications sent from the **Available Recipients** list, and use the upper arrow to move your selections to the **Selected Recipients** list. You can select multiple recipients using the CTRL key.
New Recipient	Click the **New Recipient** button to define a new recipient. For details on defining recipients, see "Recipient Properties Wizard" on page 38.

Server Filters Dialog Box

Description	To instruct HP Business Availability Center to limit the alert scheme to one or more specific server. **To access:** Click the link in **Limit to servers** <as_specified> in the Alerts definition area in the Filters tab in the Alert wizard.
Important Information	For the Real User Monitor, you can instruct HP Business Availability Center to limit the alert scheme to one or more specific pages, transactions, or servers, depending on the type of alert you are configuring. For more information on Real User Monitor alert filters, see "Grouping and Limitations For Real User Monitor Profiles" on page 320.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Available Servers **Selected Servers**	Select from the **Available** list, and use the upper right arrow to move your selections to the **Selected** list. Use the lower left arrow to remove an entity from the filter. You can select multiple filters using the CTRL key.

Server Network Connections Availability

Description	Specify that you want HP Business Availability Center to send an alert when the server network connection availability meets the alert trigger criteria. **To access:** Click the link in **Server network connections availability is** <condition> in the Alert definitions area in the Trigger Criteria in the Alert wizard.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Server network connections availability is <condition> <nn> percent	Specify the trigger criteria.

SNMP Servers Dialog Box

Description	Specify that you want HP Business Availability Center to send an SNMP trap when alert trigger criteria are met. The alert notice can then be seen from any SNMP management console in the organization. **Note:** HP Business Availability Center supports only SNMP V1 traps. For details on configuring the Alerts MIB in your SNMP management console, see "Configure the Alerts MIB" on page 261. **To access:** Click the link in **Send SNMP trap to <specified_IPs>** in the Alert definitions area in the Actions tab in the Alert wizard.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Click to open the SNMP Target IP dialog box, and modify the current address.
	Click to delete the relevant SNMP target IP.
Add	Click the **Add** button to open the SNMP Target IP dialog box, and specify the required address. Repeat to add multiple addresses.
Use custom SNMP target IPs	Select to define a custom SNMP server IP address.
Use global SNMP target IPs	Select to use the global SNMP server IP address. **Customizable:** For details, see "Access URL Dialog Box" on page 267.

SNMP Target IP Dialog Box

Description	Enables you to specify the IP address of the SNMP server. **To access:** Click the **Add** button in the SNMP Servers dialog box, or click the Edit button  in the SNMP Servers dialog box.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Enter SNMP address	The IP address of the SNMP server.

Total Transaction Response Time Performance Dialog Box

Description	If you select the **Total transaction response time for specified percentage of transactions is <as specified>** trigger, HP Business Availability Center sends an alert if total transaction time is greater than or less than the selected number of seconds for no less than the selected percentage of transactions, calculated over the selected time period. You can also set a minimum number of transactions that must run in order for the alert conditions to be calculated. **To access:** Click the link in **Total transaction response time for specified percentage of transactions is <as specified>** in the Trigger Criteria page of the Alerts wizard.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Minimum number of transactions for which condition is calculated: <nn>	Select a minimum number of transactions that must run in order for the alert conditions to be calculated.
Total transaction time is <condition> <nn> seconds for <percent> percent of transactions	Select the required criteria. **Example:** Select **greater than**, enter a value of **8** seconds, and select **90** percent to instruct HP Business Availability Center to send the alert if total transaction response time exceeds 8 seconds for at least 90 percent of the transactions that were run, over the calculated time period. For details on how to set the calculated time period, see "Calculated Time Period Dialog Box" on page 335. **Note:** The value of the percentage must be an integer.

Total Transaction Volume Dialog Box

Description	If you select the **Total volume is <condition> transactions** trigger, an alert is sent if the number of transaction runs is less than or greater than the specified number, calculated over the selected time period. **To access:** Click the link in **Total volume is <condition> transactions** in the Trigger Criteria page of the Alerts wizard.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Total volume is <condition> <nn> transactions	Select the required criteria. **Example:** Select **less than** and **80** to instruct HP Business Availability Center to send the alert if there were fewer than 80 transactions run, over the calculated time period. For details on how to set the calculated time period, see “Calculated Time Period Dialog Box” on page 335.

Transaction Availability Dialog Box

Description	Enables you to specify the transaction availability criteria. **To access:** Click the link of **Availability is** <transaction_availability> in the Alert Description area of the Trigger Criteria tab in the Alert wizard.
Important Information	HP Business Availability Center sends an alert if transaction availability is greater than or less than the selected percentage, calculated over the selected time period. Transaction availability is defined as the number of times that transactions succeed as a percentage of the total number of transaction instances. You configure transaction thresholds in End User Management. For details, see "New/Edit Transaction Page" in *Using End User Management*.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Transaction availability is <condition> <n> percentage	Select the required criteria. **Example:** Select **less than** and **80** to instruct HP Business Availability Center to send the alert if transaction availability is less than 80 percent, over the calculated time period. **Note:** The value of the percentage must be an integer.

Transaction Filters Dialog Box

Description	To instruct HP Business Availability Center to limit the alert scheme to one or more specific transactions. **Note:** For the Real User Monitor, you can instruct HP Business Availability Center to limit the alert scheme to one or more specific pages, transactions, or servers, depending on the type of alert you are configuring. For more information on Real User Monitor alert filters, see "Trigger Criteria Tab" on page 288. **To access:** Click the link in **Limit to transactions <as_specified>** in the Alerts definition area in the Filters tab in the Alert wizard.
Important Information	For details on the options available when setting Real User Monitor alert filters, see "Grouping and Limitations For Real User Monitor Profiles" on page 320.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Available Transactions **Selected Transactions**	Select from the **Available** list, and use the upper right arrow to move your selections to the **Selected** list. Use the lower left arrow to remove an entity from the filter. You can select multiple filters using the CTRL key.

Transaction Gross Response Time Dialog Box

Description	Enables you to specify the conditions for triggering alerts when more than or less than the specified percentage of transactions have a breached total transaction response time. **To access:** Click the link in **Percentage of transactions with breached gross transaction response time is** <condition> <percentage> in the Trigger Criteria page of the Alerts wizard.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Send alerts if: <condition><percentage> percent of transactions have a breached gross transaction response time	Select the condition and specify the percentage used to trigger the alert.

Transaction Net Response Time Dialog Box

Description	Enables you to specify the conditions for triggering alerts when the response time of more than or less than the specified percentage of transactions was breached while in the network, per sampling period. **To access:** Click the link in **Percentage of transactions with breached net transaction response time is** <condition> <percentage> in the Trigger Criteria page of the Alerts wizard.
Important Information	Select the condition and specify the percentage used to trigger the alert.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Send alerts if: **<condition> <percentage> percent of transactions have a breached network response time**	Select the condition and specify the percentage used to trigger the alert.

Transaction Server Response Time Dialog Box

Description	Enables you to specify the triggering conditions and the percentage of transactions for the **Transaction performance - percentage of transactions with breached server transaction response time** trigger. **To access:** Click the link in **Percentage of transactions with breached server transaction response time** is <condition> in the Trigger Criteria tab of the Alerts wizard.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Percentage of transactions with breached server transaction response time is <condition> <percentage>	Select the condition and specify the percentage used to trigger the alert.

Transaction Server Time Performance Dialog Box

Description	If you select the **Server response time for specified percentage of transactions is <as specified>** trigger, an alert is sent if the transaction server time is greater than or less than the selected number of seconds for no less than the selected percentage of transactions, calculated over the selected time period. You can also set a minimum number of transactions that must run in order for the alert conditions to be calculated. **To access:** Click the link in **Server response time for specified percentage of transactions is** <as specified> in the Trigger Criteria page of the Alerts wizard.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Minimum number of transactions for which condition is calculated: <nn>	Select a minimum number of transactions that must run in order for the alert conditions to be calculated.
Server response time is <condition> <nn> seconds for <percent> percent of transactions	Select the required criteria. **Example:** Select **greater than**, enter a value of **8** seconds, and select **90** percent to instruct HP Business Availability Center to send the alert if server response time exceeds 8 seconds for at least 90 percent of the transactions that were run, over the calculated time period. For details on how to set the calculated time period, see "Calculated Time Period Dialog Box" on page 335. **Note:** The value of the percentage must be an integer.

11

Event-Based Alerts Notification Templates

This chapter provides information on the notification templates for event-based alerts.

This chapter includes:

Concepts

Tasks

Reference

Alerts Notification Templates

To determine the contents and appearance of the alert notices, you can select predefined templates or configure your own template for notifications.

Alerts notification templates specify the information that HP Business Availability Center includes when it sends various types of alert notices. The available default templates are pre-configured with selected parameters for each section of the alert notice. For details on the information included in the default templates, see “Notification Templates Page” on page 394.

You can also create custom templates. For example, you can create different templates for different alert notice delivery methods (email, pager, SMS), or for different recipients. A custom template is defined in the Notification Template Properties page. Each section of the alert notice includes a list of parameters that you can select. For details on the information that can be included in a custom template, see “Notification Templates Page” on page 394.

Note for HP Software-as-a-Service customers: Your list of notification templates includes the default notification templates, the notification templates created for your use by HP Software-as-a-Service representatives and those created by your organization.

Follow-up Notification Templates

When configuring alert schemes, you can set up an alert scheme to automatically send a follow-up notification. For details on selecting this option while creating your alert scheme, see "Alert Schemes" on page 253.

The default template for follow-up notifications is automatically used by HP Business Availability Center. If you do not want HP Business Availability Center to use the default template, you can create your own follow-up template. The follow-up template must be based on an existing notification template. HP Business Availability Center uses the follow-up notification template that you create under the following circumstances:

- An alert has been triggered.
- Notification is sent to a recipient based on an existing template (default or user-defined).
- The alert scheme has been configured to send a follow-up alert.

For details on configuring a follow-up notification template, see "Configure a Template for Follow-up Notifications" on page 388.

Configure Alerts Notification Templates

You can select predefined templates, modify existing templates, or create your own notification templates to determine the contents and appearance of the alert notices. For details on notification templates, see "Alerts Notification Templates" on page 386.

This task includes the following steps:

- "Create Custom Templates" on page 388
- "Manage Existing Templates" on page 388

1 Create Custom Templates

HP Business Availability Center gives you the flexibility to create different notification templates for the different alert schemes and recipients that are defined for your platform.

Every template is divided into sections. You specify the information that you want to appear in each section. For details, see "Notification Template Properties Dialog Box" on page 389.

2 Manage Existing Templates

Over time, you may find it necessary to make changes to notification templates that you create, because of organizational changes, changes in notification policies, changes to service level monitoring contracts, and so on. You use the Notification Templates page to edit, clone, and delete notification templates defined in HP Business Availability Center. For details, see "Notification Templates Page" on page 394.

Configure a Template for Follow-up Notifications

You can select predefined follow-up notification templates, modify existing templates, or create your own follow-up notification templates to determine the contents and appearance of the follow-up alert notices. For details on notification templates, see "Follow-up Notification Templates" on page 387.

Note: The notification template selected for the recipient has a follow-up template based on the notification template's name. For details on naming a follow-up template, see "Notification Template Properties Dialog Box" on page 389. For details on follow-up alerts, see "Settings Tab" on page 327.

To create, modify, or manage follow-up alerts notification templates, see "Notification Templates Page" on page 394.

Event-Based Alerts Notifications User Interface

This section describes:

Notification Template Properties Dialog Box

Description	Enables you to define a new alerts notification template. **To access:** In the Notification Templates page, click the **New Template** button.

Important Information	**Follow-up notifications:** To set up a follow-up notification, select the notification template to use as the basis for your follow-up template and clone it. Make you determination based on the notification templates that was selected for users likely to receive a follow-up alert notification. Change the name of the template by deleting Copy of and adding _FOLLOWUP (all caps, one word). Edit the template details as required. It is recommended that you include in the Subject of a follow-up email, the Header, the Alert Specific Information, or both. **Example:** If you are creating a follow-up template based on the LONG default template, you would call the follow-up template LONG_FOLLOWUP. If the follow-up template is based on a user-defined template called MyTemplate, name the follow-up template MyTemplate_FOLLOWUP. **Default:** The _FOLLOWUP string is the default string recognized by Business Availability Center as the template name for a follow-up alert message. **Customization:** You can customize the _FOLLOWUP string. For details, see "Configure a Template for Follow-up Notifications" on page 388.
Included in Tasks	"Configure a Template for Follow-up Notifications" on page 388

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<insert list for Alert Specific Information>	Select a parameter to add to the section. Repeat to add as many text parameters as you want from the list. ➤ **Trigger Cause.** A description of the alert trigger conditions, as specified in the alert scheme. ➤ **Actual Details.** A description of the actual conditions at the time of the alert.
<insert list for Subject / Header / Footer>	Select a parameter to add to the section. Repeat to add as many text parameters as you want from the list. Add free text before or after the text parameters. ➤ **Alert Name.** The name of the alert, as defined in the alert scheme. ➤ **Severity.** The severity label assigned to the alert in the alert scheme. ➤ **HP AM URL.** The URL of the Business Availability Center Web site. ➤ **Profile Name.** The name of the profile in which the alert scheme was created. ➤ **User Message.** The user message, as specified in the alert scheme. ➤ **Actions Result.** A description of the results of the alert actions specified in the alert scheme. ➤ **Add Hardcoded Strings Flag.** If this field is inserted in the template, then the hardcoded string **Following is a list of the most recent occurrences of the alert trigger criteria for this alert:** is added to the message followed by the occurrence of the alert and information about the triggering of a subordinate alert. For example: "Following is a list of the most recent occurrences of the alert trigger criteria for this alert: Occurrence 5, Subalert triggered (1 of 3))".

GUI Element (A-Z)	Description
<insert list for Transaction>	Select a parameter to add to the section. Repeat to add as many text parameters as you want from the list. ➤ **Transaction Time.** The date and time of the alert. ➤ **Transaction Name.** The name of the transaction related to the alert. ➤ **Script Name.** The name of the script containing the transaction related to the alert. ➤ **Data Collector Name.** The name of the data collector running the transaction related to the alert. ➤ **Location Name.** The location of the data collector running the transaction related to the alert. ➤ **Group Name.** The group defined for the data collector running the transaction related to the alert. ➤ **Transaction Error.** The error message generated by the data collector for the transaction, if a transaction error occurred at the time of the alert. ➤ **Transaction Description.** A description of the transaction, if it has been defined in System Availability Management.
Alert Specific Information	Specify the information that you want HP Business Availability Center to include in alert text itself. Use <insert list for Alert Specific Information> to add parameters and free text to create a customized alert text. Use as many parameters as you want from the list.
Footer	Specify the information that you want to appear at the bottom of the alert notice. Use <insert list for Subject / Header / Footer> to add parameters and free text to create a customized footer. Use as many parameters as you want from the list.
Header	Specify the information that you want to appear at the top of the alert notice. Use the <insert list for Subject/Header/Footer> to add parameters and free text to create a customized header. Use as many parameters as you want from the list.
Message format	Select the format for the message: **Text** or **HTML**.

GUI Element (A-Z)	Description
Name	Enter a name for the template. If possible, use a descriptive name that includes information on the type of alert (email, pager, SMS) for which you plan to use the template, or the recipients who receive alerts using this template.
Subject	Specify the information that you want HP Business Availability Center to include in the subject of the email, pager message, or SMS message. Use the <insert list for Subject/Header/Footer> to add parameters and free text to create a customized subject. Use as many parameters as you want from the list.
Transaction	Specify the information that you want HP Business Availability Center to include in transaction. Use the <insert list for Transaction> to add parameters and free text to create a customized transaction. Use as many parameters as you want from the list.

Notification Templates Page

Description	Enables you to: ➤ Manage default and custom templates and to create new templates. ➤ Edit follow-up notification templates. **To access:** Select **Admin** > **Alerts** > **Event-based Alerts** > **Notification Templates**. HP Business Availability Center opens the Notification Templates page listing the default templates, and any custom templates that have been defined.
Important Information	When configuring alert schemes, you can instruct HP Business Availability Center to automatically follow up the alert by sending a follow-up notification. For details on selecting this option while creating your alert scheme, see "Configure a Template for Follow-up Notifications" on page 388. The default template for follow-up notifications is automatically used by HP Business Availability Center. If you do not want to use that default template, you can create your own follow-up template. It is recommended to clone an existing notifications template and then to modify the cloned template. This follow-up template must be based on an existing notification template. HP Business Availability Center uses the follow-up notification template that you create under the following circumstances: ➤ An alert has been triggered. ➤ Notification is sent to a recipient based on an existing template (default or user-defined). ➤ The alert scheme has been configured to send a follow-up alert. ➤ The notification template (DEFAULT_POSITIVE_FORMAT) selected for the recipient has a follow-up template based on the notification template's name.
Included in Tasks	"Configure Alerts Notification Templates" on page 387

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Click the button beside the notification template you want to modify. The Notification Template Properties dialog box opens. For details, see "View Dominating Alerts Dialog Box" on page 407.
	Click the button beside the notification template you want to clone. The Notification Template Properties dialog box opens. For details, see "Notification Template Properties Dialog Box" on page 389. **Follow up Notification:** To create a Follow-up Notification template, follow the procedure explained in "Notification Template Properties Dialog Box" on page 389.
	To delete multiple templates simultaneously, select their check boxes in the left column, and click the **Delete Selected** button located at the bottom of the templates list.
Delete Selected	To delete multiple templates simultaneously, select their check boxes in the left column, and click the **Delete Selected** button located at the bottom of the templates list.
New Template	Click the **New Template** button to open the Notification Template Properties dialog box. For details, see "Notification Template Properties Dialog Box" on page 389.

GUI Element (A-Z)	Description
Notification Template Name	Lists the default templates and the custom templates. The default templates are: ➤ **LONG.** Includes all the elements needed to create a default long format notification. ➤ **SHORT.** Includes all the elements needed to create a default short format notification. ➤ **DEFAULT_POSITIVE_FORMAT.** Includes all the elements needed to create a default long format notification for positive or follow-up alerts. For details on follow-up alerts, see "Configure a Template for Follow-up Notifications" on page 388. ➤ **DEFAULT_LOG_FORMAT.** Includes all the elements needed to create a default long format notification for reports. **Note:** For details on the parameters displayed in each template, see "Notification Template Properties Dialog Box" on page 389.

12

Event-Based Alert Dependencies

This chapter provides information on the dependencies of event-based alerts.

This chapter includes:

Concepts

Tasks

Reference

Alerts Dependency Overview

You can specify that you want alerts that were previously defined in a specific profile to be subordinate to the alert you are currently defining in the profile, thus making the current alert the dominant alert. If required, you can enable cross-profile dependency, which allows you to define alerts from other profiles as subordinate alerts.

When an alert defined as subordinate is triggered, HP Business Availability Center suppresses all actions configured for the alert if the following conditions are both fulfilled:

- Its dominant alert was previously triggered.
- If the conditions that triggered the dominant alert remain true at the time the subordinate alert is triggered.

You can also define a time limit for each alert you designate as subordinate. When a time limit is defined, the actions of the subordinate alert are suppressed as long as the conditions that triggered the dominant alert remain true—but only until the time limit expires. HP Business Availability Center begins running the clock on the time limit from the moment the dominant alert is triggered.

This section includes the following topics:

Benefits of Alerts Dependency

Defining subordinate alerts allows you to:

➤ **Reduce the amount of alert traffic sent.**

➤ **Define alert dependencies that match transaction dependencies.**

For example, if you have a transaction that checks the login to your application, and a transaction that checks a search in the application after login, you can subordinate the alert that notifies you about poor search performance to the alert that notifies you about failure to log in to your application. In this case, only the dominant alert is necessary to alert staff to a problem.

➤ **Nest alerts according to severity.**

For example, you can make alerts with the Minor severity subordinate to alerts with the Critical severity.

➤ **Define alert dependencies that match alert trigger criteria.**

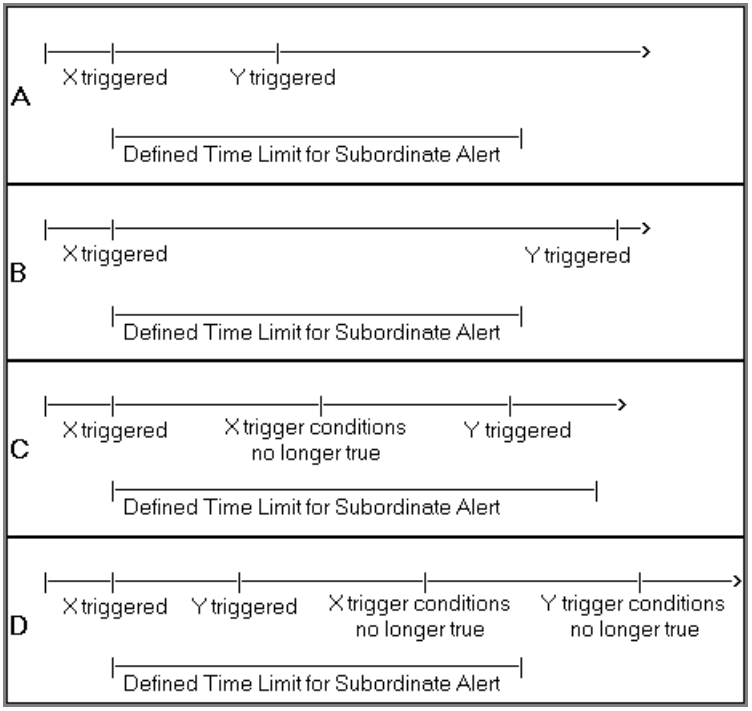
For example, if you define an alert to be triggered if the response time is greater than 15 seconds, and another alert for response time greater than 30 seconds, if the response time was 35 seconds, without dominant or subordinate alert definition, HP Business Availability Center would send two alerts. By making the response time greater than 15 seconds alert subordinate to the response time greater than 30 seconds alert, only the dominant alert is sent if the response time was greater than 30 seconds. The subordinate alert is sent if the response time was between 15 and 30 seconds.

Guidelines and Tips for Configuring Alert Dependencies

- Subordinate alerts are always logged to the Alerts Log.
- Follow-up alerts are sent only if the original alert was sent, regardless of whether the alert is dominant or subordinate. Thus, if a subordinate alert is suppressed, its follow-up alert is not sent. For details on defining follow-up alerts, see "Notification Template Properties Dialog Box" on page 389.
- Subordinate alerts are never triggered in the specified time limit.
- Alert loops are not supported. That is, if you have a series of dependencies, the dependency path cannot loop back on itself. For example, if Alert A is subordinate to Alert B, Alert B is subordinate to Alert C and Alert D, and Alert C is subordinate to Alert E, you cannot define Alerts B, C, D, or E to be subordinate to Alert A.
- Alert dependencies are not transitive. For example, if Alert A is subordinate to Alert B, and Alert B is subordinate to Alert C, Alert A is not subordinate to Alert C.

Example of Alerts Dependency

Consider the following examples, in which alert Y is defined as being subordinate to alert X.



- In example A, HP Business Availability Center suppressed alert Y's defined actions because alert X, the dominant alert, occurred before alert Y. Further, alert Y occurred during its defined time limit, and while the conditions that triggered alert X remained true.
- In example B, HP Business Availability Center did not suppress alert Y's defined actions (that is, alert Y behaved as defined) because—even though alert X, the dominant alert, occurred before alert Y—alert Y occurred after its defined time limit expired.

- In example C, HP Business Availability Center did not suppress alert Y's defined actions (that is, alert Y behaved as defined) because the conditions that triggered alert X, the dominant alert, were no longer true by the time alert Y occurred. In this case, the time limit is irrelevant.
- In example D, HP Business Availability Center suppressed alert Y's defined actions because alert X, the dominant alert, occurred before alert Y and because alert Y occurred during its defined time limit. In addition, assuming follow-up alerts were defined for alerts X and Y, HP Business Availability Center sent a follow-up alert for alert X when its trigger conditions were no longer true. A follow-up alert for alert Y was not sent when its trigger conditions were no longer true, because the original alert Y was suppressed.

Define Alerts Dependency

HP Business Availability Center enables you to define alerts dependency. For details on alert dependencies, see "Alerts Dependency Overview" on page 397.

This task includes the following steps:

- "Plan the Feature" on page 401
- "Review Alert Dependencies" on page 402
- "Change the Cross-Profile Alerts Dependency Status" on page 402

1 Plan the Feature

To make optimal use of the alerts dependency feature, it is recommended that you map out an overall picture of your monitoring and alerting strategy before defining subordinate alerts. Further, you should decide whether you need cross-profile alerts dependency. For details on enabling cross-profile dependency, see "Change the Cross-Profile Alerts Dependency Status" on page 402.

After you have planned out your required alert dependencies and configured the needed cross-profile dependency setting, you can create or edit your dominant alerts to specify their subordinate alerts.

For details, see "Define Subordinate Alerts Dialog Box" on page 405.

2 Review Alert Dependencies

You can view an overall summary of all defined alert dependencies for all profiles. You can also determine whether a specific alert is defined as subordinate and view its dominant alerts. You can:

- **Review all defined alert dependencies.** In the Event-based Alerts tab, select the **View Dependencies** menu item. The Alerts Dependency Overview page displays a table that lists all existing dominant alerts, their subordinate alerts, their corresponding profiles, and the dependency time limit. For details, see "View Dominating Alerts Dialog Box" on page 407.
- **Verify whether an alert is defined as subordinate or as a dominant alerts.** In the Alerts page, click the Edit button for the relevant alert. The Alert Wizard opens. In the Alert Description area in the Trigger Criteria tab, check if one of the following is displayed:
  - **Make the following alert(s) subordinate to this alert: <specified alerts>.** Indicates that the current alert is a dominant alert for the specified alerts. For details, see "Alert Wizard" on page 287.
  - **This alert is subordinate to the alert(s): <specified alert>.** Indicates that the current alert is subordinate to the specified alert. For details, see "Alert Wizard" on page 287.

3 Change the Cross-Profile Alerts Dependency Status

Cross-profile alerts dependency is disabled by default. Enabling cross-profile alerts dependency has the following implications:

- **You can define more complex alert dependencies.** However, managing complex dependencies may require an advanced level of administration.

➤ **Permissions have an impact on the alert dependencies you can define.** When defining alert dependencies with cross-profile alerts dependency enabled, keep in mind that you do not have permissions to modify alerts defined in profiles to which you do not have permissions. Thus, if a subordinate alert belongs to a profile to which the you do not have permissions, you cannot unassociate it from its dominant alert, even if the dominant alert belongs to a profile to which you do have permissions. Further, if a dominant alert belongs to a profile to which you do not have permissions, you cannot edit the alert at all (that is, cannot add or remove dependencies).

If you require cross-profile alerts dependency, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **Alerting**, and change the **Enable cross profile alert dependencies** entry from **false** (default) to **true** in the Alerting - Triggered Alerts table.

Note: If you have defined cross-profile alert dependencies and you select not to support the feature, and set **Enable cross profile alert dependencies** entry back to **false**, the cross-profile alert dependencies are not disabled automatically; you must remove them manually.

Event-Based Alerts Dependencies User Interface

This section describes:

Alerts Dependency Overview Page

Description	Enables you to view an overall summary of all defined alert dependencies for all profiles. You can also determine whether a specific alert is defined as subordinate and view its dominant alerts. **To access:** Select **Admin** > **Alerts** > **Event-Based Alerts** > **View Dependencies**.
Important Information	For details on subordinate alerts, see "Define Subordinate Alerts Dialog Box" on page 405. To verify that an alert is defined as subordinate, look for the following line in the bottom window of any page in the Alert Wizard: **This alert is subordinate to the alert(s):** <alert_names>
Included in Tasks	"Define Alerts Dependency" on page 401

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Dominant Alert	The name of the dominant alert.
Dominant Alert Profile	The profile of the dominant alert.
Subordinate Alert	The name of the subordinate alert. Click the name of the alert to view the alert's dominant alerts. The View Dominating Alerts dialog box opens. For details, see "View Dominating Alerts Dialog Box" on page 407
Subordinate Alert Profile	The profile of the subordinate alert.
Time Limit	The amount of time HP Business Availability Center suppresses instances of the current alert after the dominant alert is triggered.

Define Subordinate Alerts Dialog Box

Description	Enables you to define subordinate alerts. **To access:** Click the link in **Make the following alert(s) subordinate to this alert:** <specify alerts> in the Alert definitions area in the Actions tab in the Alert wizard.
Important Information	To make optimal use of the alerts dependency feature, it is recommended that you map out an overall picture of your monitoring and alerting strategy before defining subordinate alerts. For details, see "Define Alerts Dependency" on page 401. Further, you should decide whether you need cross-profile alerts dependency. For details on enabling cross-profile dependency, see "Change the Cross-Profile Alerts Dependency Status" on page 402. After you have planned out your required alert dependencies and configured the needed cross-profile dependency setting, you can create or edit your dominant alerts to specify their subordinate alerts.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Click to edit the existing subordinate alert.
	Click to delete the relevant subordinate alert.
Alert	The name of the subordinate alert. If you are editing a current subordinate alert definition, or if you have clicked **New**, in the **Alert** list, select the alert that you want to subordinate to the alert you are defining.

GUI Element (A-Z)	Description
New	Click the **New** button to add a row to the table and display a list of available alerts that you can select to be subordinate to the alert you are defining. HP Business Availability Center also displays time limit selection lists. If cross-profile dependency is enabled, in the Profile list, select the profile in which the subordinate alert is defined. For details on enabling cross-profile dependency, see "Change the Cross-Profile Alerts Dependency Status" on page 402.
Profile	The profile corresponding to the subordinate alert.
Time Limit	The time limit of the subordinate alert. If you are editing a current subordinate alert definition, or if you have clicked **New**, in the **Time Limit** list, select the time limit of the subordinate alert.

View Dominating Alerts Dialog Box

Description	Enables you to view the dominating alerts for the current alert. **To access:** Select **Make specified alert subordinate to this alert** in the Alert definitions area in the Actions tab in the Alert wizard, and click the link in **This alert is subordinate to the alert(s):** <alert_name>.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Alert	The name of the subordinate alert. If you are editing a current subordinate alert definition, or if you have clicked **New** in the **Alert** list, select the alert that you want to be subordinate to the alert you are defining.
Profile	The profile corresponding to the subordinate alert.
Time Limit	The time limit of the subordinate alert. If you are editing a current subordinate alert definition, or if you have clicked **New** in the **Time Limit** list, select the time limit of the subordinate alert.

Part V

Send Alerts to Third-Party Applications

13

Integrate HP Business Availability Center Alerts Into an EMS Console

EMS adapters enable you to integrate alerts generated by HP Business Availability Center into your EMS console. These alerts can then be used in the standard alert-processing procedure used in the EMS application.

Note to HP Software-as-a-Service customers: For details on acquiring EMS adapters, contact HP Software-as-a-Service Support.

You can send HP Business Availability Center alerts to EMS applications with the following adapters:

- **BMC PATROL Adapter.** For details, see Chapter 14, "Send HP Business Availability Center Alerts to BMC PATROL."
- **CA Unicenter Adapter.** For details, see Chapter 15, "Send HP Business Availability Center Alerts to CA Unicenter."
- **IBM Tivoli Enterprise Console (TEC) Adapter.** For details, see Chapter 16, "Send HP Business Availability Center Alerts to Tivoli TEC."

Note: For details on assigning alerts in HP Business Availability Center, see "Set Up an Alert Delivery System – Workflow" on page 18.

14

Send HP Business Availability Center Alerts to BMC PATROL

This chapter explains how to configure HP Business Availability Center to send alerts to BMC PATROL.

This chapter includes:

Concepts

Tasks

About Sending HP Business Availability Center Alerts to BMC PATROL

You install the HP Business Availability Center SNMP Adapter on the BMC PATROL Agents to which you want to send alerts. You then direct SNMP traps generated by the Data Processing Server to the BMC PATROL Agents. For details on directing SNMP traps, see "Configure SMTP Mails" on page 262.

You do not have to install the SNMP Adapter on every BMC PATROL Agent in the BMC PATROL domain: a single agent per domain should suffice. However, if required, you can install the SNMP Adapter on several agents, to achieve higher availability.

Install the HP Business Availability Center SNMP Adapter on the BMC PATROL Agents

Once installed, the SNMP Adapter receives alerts (in the form of SNMP traps) from HP Business Availability Center and forwards them to the event management engine of the BMC PATROL Agents on which the SNMP Adapter operates.

To install the HP Business Availability Center adapter on BMC PATROL:

1. Copy the HP Business Availability Center SNMP Adapter Knowledge Module (TOPAZ_SNMP_ADAPTER.km) to the knowledge module location of both the BMC PATROL Console and BMC PATROL Agents.

   TOPAZ_SNMP_ADAPTER.km is included in the Adapter files. The file is located on the HP Business Availability Center Documentation and Utilities DVD in the \tools_and_utilities\EMS\BmcPatrol\TSA folder. Once the knowledge module is loaded into BMC PATROL, TOPAZ_SNMP_ADAPTER.km is accessible with the BMC PATROL developer console.

2. Load the HP Business Availability Center SNMP Adapter on the BMC PATROL Agents using the BMC PATROL Developer Console. For exact details, see the BMC PATROL documentation.

Troubleshooting and Limitations for BMC PATROL

BMC PATROL Agents output the following system message (numbers on the left may vary):

➤ **20040502153419 SNMP NOT ACTIVE.**

The SNMP Trap service is not enabled on the BMC PATROL Agent on which the SNMP Adapter is installed. Enable the SNMP Trap service on that agent, or use a different BMC PATROL Agent. See the BMC PATROL documentation for details on installing and enabling the SNMP trap service on BMC PATROL Agents.

➤ **20040502154044 SnmpListener, Line# 130: snmp_trap_listen: cannot open socket for listening 20040502154044 Listen status = ERR, Errno = 94.**

Another SNMP trap service is using the SNMP trap port. Disable that service or change the UDP port that is used for trap reception (in that case, you must reconfigure HP Business Availability Center).

➤ **20040502154044 Error: Can't recognize Alert Type Id X (where X is a number).**

The HP Business Availability Center SNMP Adapter receives an SNMP trap that is not recognized as a valid HP Business Availability Center alert. This is normal behavior.

Note: For testing purposes, you may want to enable auxiliary SNMP traps to be processed. This can be achieved by changing the KM environment variable **RAW_DATA** to **TRUE**.

15

Send HP Business Availability Center Alerts to CA Unicenter

This chapter explains how to configure HP Business Availability Center to send alerts to CA Unicenter.

This chapter includes:

Concepts

Tasks

About Sending HP Business Availability Center Alerts to CA Unicenter

To send alerts to the CA Unicenter application, you can use one of the following methods:

- Send an HP Business Availability Center Alert as an SNMP Trap
- Send an HP Business Availability Center Alert Using the Unicenter cawto Command

For details on directing SNMP traps, see "Configure SMTP Mails" on page 262.

Send an HP Business Availability Center Alert as an SNMP Trap

The following procedure explains how to configure Unicenter to pick up the SNMP traps sent to the Event Management host.

This task includes the following steps:

- "Configure Unicenter" on page 419
- "Configure the Management Server Host" on page 419
- "Configure HP Business Availability Center" on page 420

1 Configure Unicenter

To configure Unicenter:

a Enable the Unicenter **CATrapD** (SNMP trap daemon) to pick up the raw SNMP traps.

b Configure Event Management (Message Records and Actions) to format the traps according to the HP Business Availability Center MIB. This requires knowledge of the HP Business Availability Center MIB that is part of the Data Processing Server installation. The file resides on the HP Business Availability Center Documentation and Utilities DVD in the \tools_and_utilities\SNMP_MIBS\amAlerts5.mib folder.

2 Configure the Management Server Host

You must create a message record to fit the SNMP trap sent by HP Business Availability Center.

a Create a **[file name].def** file and save the following line in it:

```
define msgrec msgid="%CATD_I_060, SNMPTRAP: -c * 5233 * * 6 1 * *" type="MSG"
msgnode="*" desc="AM Alert Transaction Response Time" cont='N' msgact='Y'
wcsingle='?' wcmany='*' case="y" regexp="n"
```

b Load the file as part of the message records in Event Management by using the command:

```
cautil –f [file name].def
oprcmd opreload
```

c To receive and display SNMP traps from third party devices in the Unicenter Event Console, you must enable the SNMP Trap Service. Select **Unicenter Enterprise Management** > **Configuration** > **Settings**. Change the **SNMP Trap Server Activated** flag to **Yes**.

3 Configure HP Business Availability Center

To configure the alerts that are to be sent to the Unicenter Event Management host:

a Access the Alert Wizard: Select **Admin** > **Alerts** > **Event Based Alerts** > **Event Based Alerts configuration**.

b Create an alert according to the instructions in "Alert Schemes" on page 253.

c Select the **Send SNMP trap** check box and define the EMS IPs. For details, see "Actions Tab" on page 321.

Send an HP Business Availability Center Alert Using the Unicenter cawto Command

---

Note to HP Software-as-a-Service customers: This procedure is not relevant for HP Software-as-a-Service customers. Instead, HP Software-as-a-Service customers should use the SiteScope command line monitor. To use that monitor, consult HP Software-as-a-Service Support.

This command line utility is available after you install the Unicenter Event Management Agent on the HP Business Availability Center machine.

Note: You use the **cawto** command to send a message to the Windows console or the system console without waiting for a reply. To send a message and wait for a reply, use the Event Management **cawtor** command.

This task includes the following steps:

- "Configure the CA Unicenter Console" on page 421
- "Configure HP Business Availability Center" on page 421

1 Configure the CA Unicenter Console

You do not need to configure the Unicenter Event Management host. Verify that the **cawto** command is sent to the Unicenter Event Management node which must handle it: open the Event Management Console and look for the event that was sent with the **cawto** command.

2 Configure HP Business Availability Center

To configure the alerts that are to be sent to the Unicenter Event Management host:

a Access the Alert Wizard: Select **Admin** > **Alerts** > **Event Based Alerts** > **Event Based Alerts configuration**.

b Create an alert according to the instructions in "Alert Schemes" on page 253.

c Continue to the section "Run Executable File Dialog Box" on page 363. During this procedure, you must select the **Run executable file** check box and define the alert action in the Alert Wizard. When asked to enter the command line required to run the executable file, use the Unicenter **cawto** command line.

Note: Consult the Unicenter documentation about the parameters for the **cawto** command line and how they can be activated.

The following example shows how to create a **cawto** command that sends the HP Business Availability Center alert to Unicenter:

```
C:\tng\bin\cawto.exe –s "" –v W –n <node> "Alert <AlertName> for <ProfileName> was triggered because: <TriggerCause>"
```

where:

-s <source> – Identifies the application that is the source of the event. In the above example, **<source>** is **HP Business Availability Center**.

-v <value> – Severity of the event. When viewing events in the CA Message console, icons are displayed to the left of the events indicating the severity status. In the above example, **<value>** is **W** (Warning). Severity values can be one of the following:

Informational	I
Success	S
Warning	W
Error	E
Failure	F

You can set up the translation from HP Business Availability Center severity to Unicenter severity according to the following rules:

	Unicenter
OK	I
Warning	W
Minor	E
Major	E
Critical	F

-n <node> – Node to which the message is directed if the node is not the node the user is on.

<AlertName>, **<ProfileName>**, **<TriggerCause>** are HP Business Availability Center alert variables.

Troubleshooting and Limitations for CA Unicenter

What functionality is added when loading a custom or third party MIB on the DSM, using the LDMIB command

Products:

- Unicenter NSM

  Version: 3.0

  OS: WIN/NT, WIN2000, HP, AIX, SUN, LINUX, SCO, SINIX, TRU64

- Unicenter TNG

  Version: 2.2, 2.4, 2.4.2

  OS: WIN/NT, WIN2000, HP, AIX, SUN, LINUX, SCO, SINIX, TRU64

Solution:

Run **ldmib** on a custom MIB to give the following functionality:

- the ability to run **objectview** against that MIB. This requires that the MIB also be copied into the **%AGENTWORKS_DIR%\services\config\mibs** directory on the machine from which **objview** is being run.
- the ability to run **mibbrowse** against that MIB.

  Please note that no trap translation automatically occurs by loading an MIB. This requires DSM policy. You could use message records and actions to translate the **CATrapD** messages on the EM console to work around the need for DSM policy. This would then require enabling **CATrapD** by accessing the EM settings and turning on **SNMP trap server activated**.

Unreadable message formats on the event console ('%CATD_I_060, SNMPTRAP: -c public 791 172.20.0.18 mail.npc.net 2 0.')

Products:

- Unicenter NSM

  Version: 3.0

  OS: WIN/NT, WIN2000

➤ Unicenter TNG

Version: 2.2, 2.4, 2.4.2

OS: WIN/NT, WIN2000

Solution:

These are raw SNMP traps that the **CATrapD** daemon picks up. They may be generated by any SNMP enabled device or agent. **CATrapD** is enabled when you access the EM settings and enable **SNMP trap server activated**. Normally the DSM interprets the important ones but others do not warrant a separate translated message in the console. The reference guide lists the numbers at the end of these traps and what they stand for.

They are:

0	Coldstart	The sending SNMP entity has reinitialized itself, indicating that the agent's configuration may be changed This is typically a restart due to a crash or major fault.
1	WarmStart	The sending SNMP entity has reinitialized itself, but the agent's configuration has not been altered. This is typically a routine restart.
2	linkDown	The communications link has failed.
3	linkUp	The communications link has come up.
4	Authentication	The agent has received an incorrect community name. Failure from a manager.
5	EGP Neighbor	The external gateway protocol (EGP) neighbor is down. Loss.
6	Enterprise	An enterprise-specific event has occurred. Specific (Requires a specific trap type to identify).

Receive and display SNMP traps from third party devices in the Event Console

Products:

Unicenter TNG

Version: 2.1, 2.2, 2.4

OS: WIN/NT, WIN2000

Solution:

To receive and display SNMP traps from third party devices in the Unicenter Event Console, you must enable the SNMP Trap Service. Select **Unicenter Enterprise Management** > **Configuration** > **Settings**. Change the **SNMP Trap Server Activated** flag to **Yes**.

16

Send HP Business Availability Center Alerts to Tivoli TEC

This chapter explains how to configure HP Business Availability Center to send alerts to Tivoli TEC.

This chapter includes:

Concepts

Tasks

About Sending HP Business Availability Center Alerts to Tivoli TEC

You can integrate alerts with the IBM Tivoli Enterprise Console (TEC) application.

To send alerts to the Tivoli TEC management server, HP Business Availability Center utilizes Tivoli's **postzmsg, postemsg, wpostzmsg, or wpostemsg** commands. For details on these commands, see the Tivoli Web site (http://publib.boulder.ibm.com/tividd/td/tec/SC32-1232-00/en_US/HTML/ecormst02.htm). The recommended command to use is **postzmsg** as it can be copied to and run from any machine and it buffers events if the TEC server is unavailable.

wpostzmsg and **wpostemsg** are commands used by the managed node to communicate with the management server. Therefore the HP Business Availability Center server must be a Tivoli End Point (that is, the Tivoli software agent must be installed on the machine).

The command used is called from the **run_exe** command.

Set Up Tivoli TEC

To send alerts to Tivoli TEC, you must verify that:

- Tivoli End Point is installed on the Data Processing Server host, if using the **wpostzmsg** or **wpostemsg** commands.
- An ACP profile has been distributed to the Tivoli End Point on the Data Processing Server host.
- The command being used is located on the machine from which the alert is being sent. If using the **postzmsg** or **postemsg** command, it can be located anywhere on the machine. You can verify that the command is present by running the following:

```
Usage: postzmsg { -S <server> | -f <config_file> } [-r <severity>]
[-m <message> ] [<slot_name=value>, ...] <class> <source>
```

➤ If using the **wpostzmsg** or **wpostemsg** command, it should be located under the directory **<Drive>:\Program Files\Tivoli\lcf\bin\<platform>\bin**. Using one these commands requires the Tivoli environment to be sourced, so the command must be run from a batch file.

To send an alert to Tivoli TEC:

1. Create a **baroc** file which describes the event class of the alert, and deploy it on your Tivoli Tec. For more information on the baroc file format, see the Tivoli TEC documentation.
2. Copy the **postzmsg** or **postemsg** command to the HP Business Availability Center server. If using the **wpostzmsg** or **wpostemsg** command, install a Tivoli End Point on the HP Business Availability Center server (the End Point brings the **wpostzmsg** and **wpostemsg** executables with it).
3. Run the command by creating the appropriate command line. For example, if using the **postzmsg** command:

```
postzmsg -S server -r CRITICAL description="<AlertDescription>"
triggerCause="<TriggerCause>" hostname="cookie"
topazProfileName="<ProfileName>" Topaz_Alert Topaz
```

You can create and use a configuration file to specify various parameters. For details on running the commands, see the Tivoli Web site (http://publib.boulder.ibm.com/tividd/td/tec/SC32-1232-00/en_US/HTML/ecormst02.htm).

Send an HP Business Availability Center Alert Using the Tivoli End Point postemsg Command

---

Note to HP Software-as-a-Service customers: This procedure is not relevant for HP Software-as-a-Service customers. Instead, HP Software-as-a-Service customers should use the SiteScope command line monitor. To use that monitor, consult HP Software-as-a-Service Support.

This command line utility is available after you install Tivoli End Point on the HP Business Availability Center Data Processing Server machine.

You use the postemsg command to send a message to the Windows console or the system console without waiting for a reply.

To configure HP Business Availability Center:

1. To configure the alerts that are to be sent to the Tivoli TEC host, access the Alert Wizard: Select **Admin** > **Alerts** > **Event Based Alerts** > **Event Based Alerts Configuration**.
2. Create an alert according to the instructions in "Alert Schemes" on page 253.
3. Continue to the section "Run Executable File Dialog Box" on page 363. During this procedure, you must select the **Run executable file** check box and define the alert action in the Alert Wizard. When asked to enter the command line required to run the executable file, use the Tivoli End Point postemsg command line:

```
postemsg { -S <server> | -f <config_file> } [-r <severity>]
[-m <message> ] [<slot_name=value>, ...] <class> <source>
```

Index

A

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W