

HP Business Service Management

For the Windows and Linux operating systems operating systems

Software Version: 9.13

Using Service Health Analyzer 9.10

Document Release Date: July 2012

Software Release Date: March 2012



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2011 Hewlett-Packard Development Company, L.P.

Trademark Notices

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

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

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

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

iPod is a trademark of Apple Computer, Inc.

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

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

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

UNIX® is a registered trademark of The Open Group.

Acknowledgements

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

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

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

Documentation Updates

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

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

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

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

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

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

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

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

Support

Visit the HP Software Support Online web site at:

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

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

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

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

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

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

To find more information about access levels, go to:

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

Disclaimer for PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format.

Note: Some topics do not convert properly to PDF, causing format problems. Some elements of online help are completely removed from the PDF version. Those problem topics can be successfully printed from within the online help.

Contents

Using Service Health Analyzer 9.10.....	1
Contents.....	6
Welcome to Service Health Analyzer.....	9
Service Health Analyzer Overview.....	10
Setting Up and Configuring Service Health Analyzer - Overview.....	12
How to Set Up and Configure SHA in a New Deployment of BSM 9.12.....	13
How to Set Up and Configure SHA after an Upgrade from BSM 9.10 to BSM 9.12.....	16
How to Install the Analytics Server.....	19
How to Install the SHA Network Node Manager i (NNMi) Data Collector.....	21
Administering Service Health Analyzer.....	23
Selecting CIs to be Monitored by SHA Overview.....	24
How to Select CIs to be Monitored by Service Health Analyzer.....	25
CI Selection Tab.....	26
Event Template Overview.....	29
How to Configure the Service Health Analyzer Event Template.....	30
Event Template Tab.....	31
Configuring Verification Tools Overview.....	37
Service Health Analyzer SiteScope Templates.....	38
How to Configure Verification Tools.....	39
SiteScope Template Tab.....	40
Template Mapping Configuration Wizard.....	42
Select CI Type Page.....	43
Select Templates Page.....	45
Configure Parameters Page.....	47
Select Topology Dialog Box.....	50
Verification Tools Tab.....	52
Analyzing Service Health Analyzer Statistics.....	53
SHA Statistics Tab.....	54

Automatic Detection Overview	57
How a Metric is Added to an Anomaly.....	59
The Anomaly Life Cycle.....	62
Identifying Similar Anomalies.....	63
Identifying Similar Patterns.....	64
How To Process a Service Health Analyzer Event.....	65
How to Filter SHA Events.....	69
How to Investigate an Anomaly.....	70
Anomaly Highlights Page.....	71
Investigating with the Topology View Overview	77
Topology Map Layout Modes.....	79
Default Layers in Topology Map.....	80
Learn About the CI Node in a Topology Map.....	81
Location of a Manually Added CI.....	84
Drilling Down in the Topology View.....	85
How to Use the Topology View.....	88
How to Use the Reveal Mode.....	90
Topology View Tab.....	91
Investigating with Metrics Overview	101
Metric Correlation.....	103
Algorithms.....	103
Best Practice.....	104
Drilling Down in the Metrics View.....	105
How to Use the Metrics View.....	106
How to Use the Metrics Histogram.....	108
How to Correlate Metrics.....	109
Metrics View Tab.....	111
Using Service Health Analyzer Investigations	128
How to Create an Investigation.....	129
Investigation Properties Dialog Box.....	130
SHA Investigation Page.....	133
Managing SHA Databases — Overview	135

How to Configure a User Schema on an Oracle Server.....	136
How to Configure an SHA Database on a Microsoft SQL Server.....	138
SHA Database Management Page.....	139
SHA User Schema Properties — Oracle Server Page.....	140
SHA Database Properties — MS SQL Server Page.....	142
Advanced Configuration Overview.....	144
How to Edit the SHA Metric Selection XML Files for Baselining.....	145
How To Add and Remove Metric Types in the SiteScope, Diagnostics and PA XML... Files.....	146
How To Add and Remove Metric Types in the BPM, RUM, and NNM XML Files.....	148
How to Reload Metadata.....	151
How to Control the Amount of Data Stored in the Aggregation Database.....	154
How to Create a TQL Drilldown.....	156
How to Edit an SHA Infrastructure Setting.....	157
Build a Business CI Model.....	158

Welcome to Service Health Analyzer

The Service Health Analyzer guide describes how to install, configure and use the Service Health Analyzer (SHA) application in HP Business Service Management.

This guide includes the following sections:

- ["Setting Up and Configuring Service Health Analyzer - Overview" \(on page 12\)](#) - Describes how to install and configure SHA.
- ["Administering Service Health Analyzer" \(on page 23\)](#) - Describes SHA administration procedures that should be carried out before using SHA, and for ongoing maintenance.
- ["Automatic Detection Overview" \(on page 57\)](#) - Describes the SHA automatic detection process and concepts, and how to process an SHA event.
- ["Investigating with the Topology View Overview" \(on page 77\)](#) - Describes how to use the SHA Topology View to analyze an anomaly generated by SHA.
- ["Investigating with Metrics Overview" \(on page 101\)](#) - Describes how to use the SHA Metrics View to analyze an anomaly generated by SHA.
- ["Using Service Health Analyzer Investigations" \(on page 128\)](#) - Describes how to create and save an SHA investigation.
- ["Managing SHA Databases — Overview " \(on page 135\)](#) - Describes how to create or connect to an Oracle or SQL SHA database.
- ["Advanced Configuration Overview" \(on page 144\)](#) - Describes advanced SHA configuration procedures.

Service Health Analyzer Overview

HP Service Health Analyzer (SHA) enables you to be more proactive in managing your data center's physical and logical infrastructure, with very low overhead. It uses a self learning algorithm to analyze historical and current data, and if certain criteria are met, reports on the current state of abnormal IT services and their topology location. SHA uses a run-time analytics engine that can anticipate IT problems before they occur, by analyzing abnormal service behavior and alerting IT managers of real service degradation before an issue impacts their business.

SHA uses the Run-Time Service Model (RTSM) and enables you to analyze SHA anomalies using the familiar topology and metric views.

Key Features of Service Health Analyzer

Service Health Analyzer offers the following key features:

- **Anticipates potential IT problems before they occur** - Using various algorithms, abnormal metric values are examined to identify if they contribute to a potential IT issue.
- **Prevents or reduces downtime** - Potential issues are identified, and reported to an operator before their full effects are felt in the IT systems. This gives an operator vital time to take action before IT systems and services are impaired.
- **Compares between current and historical anomalies** - This can result in the filtering out of non-critical or self repairing issues that can for example reflect system noise, or can link to other anomalies that bear a resemblance to the current anomaly. Often the solution to the historical anomaly, might point you a solution for the current issue.
- **Provides an improved way to monitor and manage metric thresholds** - Metric baseline threshold sleeves are automatically calculated and updated. This gives you a truer reflection of seasonal changes in metric thresholds, saves time manually configuring thresholds, and reduces false alarms that may occur when non-dynamic thresholds are used.
- **Enables you to investigate an anomaly using information from the RTSM** - Presents anomalies using information from RTSM, displaying affected IT components in their associated topologies. This assists in the remediation of SHA events.

Note: The RTSM automatically discovers and updates the topology of an IT environment, allowing customers to have current views of their business services and all the underlying dependencies on the IT infrastructure, across physical, virtual, and cloud-based environments

- **Supports the following BSM data collectors** - Business Process Monitor (BPM), Real User Monitor (RUM), Diagnostics, SiteScope, Network Node Manager i (NNMi), and HP Performance Agent (PA).

For more information, see "[Drilling Down in the Topology View](#)" (on page 85), and "[Drilling Down in the Metrics View](#)" (on page 105).

- **Enables you to compare and correlate metrics in an anomaly** - You can automatically correlate business and infrastructure metrics to produce a meaningful SHA event. This is accomplished using RTSM modeling. Using various algorithms SHA can assess the criticality

of an event, and only report events that directly impact your business.

- **Enables you to calculate your potential return of investment** - You can calculate the savings your organization can make using Service Health Analyzer, based on cost parameters you input.

How SHA Works

- SHA correlates current and historical data with topology information to forecast future events.
- SHA analyzes historical data, learns normal behavior, creates baseline thresholds, prioritizes issues by business impact, and reduces alert “noise”. Baseline thresholds are regularly updated and therefore dynamic, providing a truer picture of real thresholds.
- SHA detects an anomaly and sends out an SHA event. Using abnormal metrics and topology information, SHA where relevant also identifies lead suspects for the issue.

Note: SHA anomaly detection can be reported in the Operations Management Event Browser as an event, in Service Health as a KPI, and with user notification such as email.

- SHA produces an Anomaly Highlights report that provides details for an anomaly, such as:
 - Lead suspects, and links to associated reports
 - The business impact
 - Affected applications and services
 - Geographical locations impacted
 - Links to similar historical anomalies, and where relevant, associated tickets

For more information, see ["How To Process a Service Health Analyzer Event" \(on page 65\)](#), and ["Anomaly Highlights Page" \(on page 71\)](#).

- SHA enables you to investigate anomalies in greater detail using the Topology and Metrics views.

For more information, see ["How to Use the Topology View" \(on page 88\)](#), and ["How to Use the Metrics View" \(on page 106\)](#).

Setting Up and Configuring Service Health Analyzer - Overview

Service Health Analyzer is part of the Business Service Management (BSM) solution running on the BSM servers. SHA requires the following components:

- **Analytics server** - Runs the baseline engine, and the analytics data collector.
- **Data Sources** - Provide metric data for analysis.
- **Database server** - An Oracle or Microsoft SQL server that stores metric and baseline data.

This section includes:

How to Set Up and Configure SHA in a New Deployment of BSM 9.12	13
How to Set Up and Configure SHA after an Upgrade from BSM 9.10 to BSM 9.12	16
How to Install the Analytics Server	19
How to Install the SHA Network Node Manager i (NNMi) Data Collector	21

How to Set Up and Configure SHA in a New Deployment of BSM 9.12

This task describes how to install and configure Service Health Analyzer in a new deployment of BSM 9.12.

1. Prerequisites

The following prerequisites are required to set up Service Health Analyzer.

- a. BSM version 9.12.

For more information, see the *BSM 9.12 Deployment Guide*.

- b. A Service Health Analyzer license.
- c. An Analytics server that must have a resolvable Fully Qualified Domain Name.

The Analytics server has the following hardware requirements:

- o **Memory:** 4 GB
- o **CPU:** 8 CPUs

Note:

The following CPU types are supported:

- 1) Intel Dual Core Xeon Processor 2.4 GHz or higher
- 2) AMD Opteron Dual Core Processor 2.4 GHz or higher

- o **Virtual Memory/Swap Space:** 4 GB

2. Enable the Service Health Analyzer application in BSM

Select **Admin > Platform > Setup and Maintenance > Server Deployment**, select Service Health Analyzer, and then click **Save**.

3. Add a Service Health Analyzer license

- a. Log in to BSM as an administrator and go to **Admin > Platform > Setup and Maintenance > License Management**.
- b. Select **Service Health Analyzer**, click the plus sign, and add a Service Health Analyzer license by navigating to and selecting the Service Health Analyzer license file.

Note: After selecting the file, the License Management page is refreshed and includes the new license. Allow 5 minutes for all processes/servers to refresh their license caches. Logout and re-login is required for the update to take effect in the current session.

4. Stop BSM on all BSM servers in the domain

On the Windows taskbar, click **Start > All Programs > HP Business Service Manager >**

Administration > Disable HP Business Service Management.

You can verify that the HP Business Service Management Server is stopped as follows:

- a. On the Windows taskbar, click **Start > All Programs > HP Business Service Manager > Administration > HP Business Service Management Server Status**.
- b. Verify that the Naming Status column is empty, or that the "Cannot check status" message appears.

Note:

To start or stop HP Business Service Management in Linux, run
/opt/HP/BSM/scripts/run_hpbsm start | stop.

To start, stop, or restart HP Business Service Management using a daemon script, run
/etc/init.d/hpbsmd {start| stop | restart}.

5. Install the Analytics server

Install the Analytics server, as described in ["How to Install the Analytics Server" \(on page 19\)](#).

6. Start BSM on all BSM servers in the domain

On the Windows taskbar, click **Start > All Programs > HP Business Service Manager > Administration > Enable HP Business Service Management**.

You can verify that the HP Business Service Management Server is started as follows:

- a. On the Windows taskbar, click **Start > All Programs > HP Business Service Manager > Administration > HP Business Service Management Server Status**.
- b. Verify that the `basel_engine`, and `analytics_dc` appear, and that nothing is listed under HAC Status.

Note:

To start or stop HP Business Service Management in Linux, run
/opt/HP/BSM/scripts/run_hpbsm start | stop.

To start, stop, or restart HP Business Service Management using a daemon script, run
/etc/init.d/hpbsmd {start| stop | restart}.

7. Start the SHA processes on the Analytics server

When all the BSM servers are started, on the Analytics server, on the Windows taskbar, click **Start > All Programs > HP Business Service Manager > Administration > Enable HP Business Service Management**.

You can verify that the SHA processes were started as follows:

- a. On the Windows taskbar, click **Start > All Programs > HP Business Service Manager > Administration > HP Business Service Management Server Status**.

- b. Verify that the `basel_engine`, and `analytics_dc` processes appear, and that nothing is listed under HAC Status.

Note:

To start or stop HP Business Service Management in Linux, run `/opt/HP/BSM/scripts/run_hpbsm start | stop`.

To start, stop, or restart HP Business Service Management using a daemon script, run `/etc/init.d/hpbsmd {start| stop | restart}`.

8. Create an SHA database

You can manually create and populate an SHA database, or create it in BSM.

- To manually create and populate an SHA database, see the instructions in the SHA Analytics User Schemas or the Creating the SHA Objects sections in the *HP Business Service Management Database Guide*.
- To automatically create and populate the SHA database, in BSM select **Admin > Platform > Manage SHA Databases**, and follow the instructions in ["How to Configure a User Schema on an Oracle Server" \(on page 136\)](#) for an Oracle user schema, or ["How to Configure an SHA Database on a Microsoft SQL Server" \(on page 138\)](#) for a Microsoft SQL Server database.

9. Configure Service Health Analyzer in BSM

- a. You must create business CI models between infrastructure CIs and application CIs. For more information, see ["Build a Business CI Model" \(on page 158\)](#).
- b. You must add CIs in the CI Selection tab. For more information, see ["How to Select CIs to be Monitored by Service Health Analyzer" \(on page 25\)](#).
- c. Map SiteScope templates to CIs, and configure verification tools. For more information, see ["How to Configure Verification Tools" \(on page 39\)](#).

The Analytics server has the following hardware requirements:

- **Memory:** 4 GB
- **CPU:** 8 CPUs

Note:

The CPUs have the following minimum requirements:

Intel Dual Core Xeon Processor 2.4 GHz or higher

AMD Opteron Dual Core Processor 2.4 GHz or higher

- **Virtual Memory/Swap Space:** 4 GB

How to Set Up and Configure SHA after an Upgrade from BSM 9.10 to BSM 9.12

This task describes how to install and configure Service Health Analyzer after upgrading from BSM 9.10 to BSM 9.12.

1. Prerequisites

The following prerequisites are required to set up Service Health Analyzer.

- a. BSM version 9.12.

For more information, see the *BSM 9.12 Deployment Guide*.

- b. A Service Health Analyzer license.
- c. An Analytics server that must have a resolvable Fully Qualified Domain Name.

The Analytics server has the following hardware requirements:

- o **Memory:** 4 GB
- o **CPU:** 8 CPUs

Note:

The following CPU types are supported:

- 1) Intel Dual Core Xeon Processor 2.4 GHz or higher
- 2) AMD Opteron Dual Core Processor 2.4 GHz or higher

- o **Virtual Memory/Swap Space:** 4 GB

2. Stop BSM on all BSM servers in the domain

On the Windows taskbar, click **Start > All Programs > HP Business Service Manager > Administration > Disable HP Business Service Management**.

You can verify that the HP Business Service Management Server is stopped as follows:

- a. On the Windows taskbar, click **Start > All Programs > HP Business Service Manager > Administration > HP Business Service Management Server Status**.
- b. Verify that the Naming Status column is empty, or that the "Cannot check status" message appears.

Note:

To start or stop HP Business Service Management in Linux, run `/opt/HP/BSM/scripts/run_hpbsm start | stop`.

To start, stop, or restart HP Business Service Management using a daemon script, run `/etc/init.d/hpbsmd {start| stop | restart}`.

3. Perform SHA specific upgrade from 9.10 to 9.12 steps

Perform the following steps on a BSM Data Processing Server machine, or a Typical machine:

- a. Run `\<HPBSMInstalldirectory>\ldbverify\bin\run_schema_upgrade.bat`.
- b. On the Windows taskbar, click **Start > All Programs > HP Business Service Manager > Administration > Configure HP Business Service Management**.
- c. Click **Next** until you reach the License screen and add an SHA license, or click **Next** to receive a 60 day evaluation license.
- d. Click **Next** until the Server Deployment screen and select **Service Health Analyzer**.
- e. Complete the wizard.

4. Run the configuration manager on each BSM Gateway server

On each BSM Gateway server, click **Start > All Programs > HP Business Service Manager > Administration > Configure HP Business Service Management**, and click **Next** until you complete the wizard.

5. Install the Analytics server

Install the Analytics server, as described in ["How to Install the Analytics Server" \(on page 19\)](#).

6. Start BSM on all BSM servers in the domain

On the Windows taskbar, click **Start > All Programs > HP Business Service Manager > Administration > Enable HP Business Service Management**.

You can verify that the HP Business Service Management Server is started as follows:

- a. On the Windows taskbar, click **Start > All Programs > HP Business Service Manager > Administration > HP Business Service Management Server Status**.
- b. Verify that the `basel_engine`, and `analytics_dc` appear, and that nothing is listed under HAC Status.

Note:

To start or stop HP Business Service Management in Linux, run `/opt/HP/BSM/scripts/run_hpbsm start | stop`.

To start, stop, or restart HP Business Service Management using a daemon script, run `/etc/init.d/hpbsmd {start| stop | restart}`.

7. Start the SHA processes on the Analytics server

When all the BSM servers are started, on the Analytics server, on the Windows taskbar, click **Start > All Programs > HP Business Service Manager > Administration > Enable HP Business Service Management**.

You can verify that the SHA processes were started as follows:

- a. On the Windows taskbar, click **Start > All Programs > HP Business Service Manager > Administration > HP Business Service Management Server Status**.

- b. Verify that the `basel_engine`, and `analytics_dc` processes appear, and that nothing is listed under HAC Status.

Note:

To start or stop HP Business Service Management in Linux, run `/opt/HP/BSM/scripts/run_hpbsm start | stop`.

To start, stop, or restart HP Business Service Management using a daemon script, run `/etc/init.d/hpbsmd {start| stop | restart}`.

8. Create an SHA database

You can manually create and populate an SHA database, or create it in BSM.

- To manually create and populate an SHA database, see the instructions in the SHA Analytics User Schemas or the Creating the SHA Objects sections in the *HP Business Service Management Database Guide*.
- To automatically create and populate the SHA database, in BSM, select **Admin > Platform > Manage SHA Databases**, and follow the instructions in ["How to Configure a User Schema on an Oracle Server" \(on page 136\)](#) for an Oracle user schema, or ["How to Configure an SHA Database on a Microsoft SQL Server" \(on page 138\)](#) for a Microsoft SQL Server database.

9. Configure Service Health Analyzer in BSM

- a. You must create a business CI model between infrastructure CIs and application CIs. For more information, see ["Build a Business CI Model" \(on page 158\)](#).
 - b. You must add CIs in the CI Selection tab. For more information, see ["How to Select CIs to be Monitored by Service Health Analyzer" \(on page 25\)](#).
 - c. Map SiteScope templates to CIs, and configure verification tools. For more information, see ["How to Configure Verification Tools" \(on page 39\)](#).
1. An Analytics server. The Analytics server must have a resolvable Fully Qualified Domain Name.

The Analytics server has the following hardware requirements:

- **Memory:** 4 GB
- **CPU:** 8 CPUs

Note:

The following CPU types are supported:

- 1) Intel Dual Core Xeon Processor 2.4 GHz or higher
- 2) AMD Opteron Dual Core Processor 2.4 GHz or higher

- **Virtual Memory/Swap Space:** 4 GB

How to Install the Analytics Server

The baseline engine runs on the Analytics server. This task describes how to install an Analytics server.

1. Insert the Analytics server installation DVD for your operating system, and run the Analytics server installation as follows:

For Windows, run <DVD1_ROOT>\Windows_Setup\HPSHA_9.10_setup.exe.

For Linux, log into the server as user root, and run the <DVD2_ROOT>\Linux_Setup\HPSHA_9.10_setup.bin script.

2. On the Choose Locale screen, click **OK** to continue with the installation. The Initialization screen appears.
3. If the Installer detects any anti-virus program running on your system, it prompts you to examine the warnings before you continue with the installation. Read the warnings, if any, that appear in the Application requirement check warnings screen and follow the instructions as described in the screen.

Click **Continue** to continue with the installation.

4. On the Introduction (Install) screen, click **Next**.
5. On the License Agreement screen, read the License Agreement.

To continue the installation, you must accept the terms of the license agreement, and then click **Next**.

6. On the Group Selection screen, select **HP Business Service Management - Analytics server**, and then click **Next**.
7. On the Choose the Folders screen, click **Next** to accept the default locations, or change the folder locations, and then click **Next**.
8. On the Install Checks screen ensure that all the checks were successful. If a check fails, you will be given specific information on the failure. The installation might not continue until the problem is rectified.
9. On the Pre-Install Summary screen, click **Install**.
10. Click **Next** until the Management Schema - Management Database Server Type screen appears, select a database server type, and then click **Next**.
11. Depending on the Server Type selected the following appears:

For Microsoft SQL Server

On the Management Schema - MS SQL Settings screen:

- a. Enter the Host name, Port name, Database name, and the Authentication method.

Note:

The database name cannot contain: /, \, :, *, ?, \", <, >, |, spaces, and cannot start with a digit.

The host name cannot contain /, :, *, ?, \", <, >, |, or any spaces.

- b. If you select **SQL server authentication**, enter a username and password for a user with administrator permissions, and then click **Next**.

For Oracle

On the Management Schema - Management Oracle Schema Settings screen:

Enter the Host name, Port, SID, Schema name and Schema password, and then click **Next**.

Note:

The schema name cannot contain: /, \, :, *, ?, \", <, >, |, spaces, and cannot start with a digit.

The host name cannot contain /, :, *, ?, \", <, >, |, or any spaces.

12. On the Management Summary screen, if the management database or user schema configuration was successful, click **Next**.
13. On the Login Settings screen, enter and confirm a JMX password for the Analytics server.
14. On the Summary screen, verify that the installation was completed successfully, and then click **Finish**.

How to Install the SHA Network Node Manager i (NNMi) Data Collector

The SHA NNMi data collector, collects utilization input and output metrics from NNMi that are stored in CSV format, and converts them to BSM metrics. These metrics are for a CI node and CI interface combination.

NNMi is installed on a standalone server. The Network Performance Smart Plug-In (PerfSpi) can be installed on the NNMi server or on a separate server. To use NNMi data with Service Health Analyzer, you must install the SHA NNMi data collector on the same server where PerfSpi is installed. PerfSpi converts the NNMi data to CSV format.

BSM samples contain information such as the CI node, CI Interface and the metric value, and are sent for the CIs you select in the CI Selection feature of the Service Health Analyzer Administration.

For more information, see ["How to Select CIs to be Monitored by Service Health Analyzer" \(on page 25\)](#).

Note: NNMi metric baseline information is calculated by NNMi, and not by the Analytics engine.

This task describes how to install the SHA NNMi data collector.

1. On the server where the Network Performance Smart Plug-In (PerfSpi) is installed, insert the Service Health Analyzer installation DVD for your operating system, and run the following:

For Windows, run `<DVD1_ROOT>\Windows_Setup\HPSHA_9.10_setup.exe`

For Linux, log into the server as user root, and run the `<DVD2_ROOT>\Linux_Setup\HPSHA_9.10_setup.bin` script.

2. On the Choose Locale screen, click **OK** to continue with the installation. The Initialization screen appears.
3. If the Installer detects any anti-virus program running on your system, it prompts you to examine the warnings before you continue with the installation. Read the warnings, if any, that appear in the Application requirement check warnings screen and follow the instructions as described in the screen.

Click **Continue** to continue with the installation.

4. On the Introduction (Install) screen, click **Next**.
5. On the License Agreement screen, read the License Agreement.
To continue the installation, you must accept the terms of the license agreement, and then click **Next**.
6. On the Group Selection screen, select **HP Business Service Management - Analytics NNM data collector**, and click **Next**.
7. On the Choose the Folders screen, click **Next** to accept the default locations, or change the folder locations, and then click **Next**.

8. On the Install Checks screen ensure that all the checks were successful. If a check fails, the installation might not continue until the problem is rectified.
9. On the Pre-Install Summary screen, click **Install**.
10. Click **Next** until the Management Schema - Management Database Server Type screen appears, select a database server type, and then click **Next**.
11. Depending on the Server Type selected the following appears:
For Microsoft SQL Server:
On the Management Schema - MS SQL Settings screen:
 - a. Enter the Host name, port name, database name, and the authentication method.
 - b. If you select **SQL server authentication**, enter a username and password for a user with the administrator permissions, and then click **Next**.**For Oracle:**
On the Management Schema - Management Oracle Schema Settings screen:
Enter the Host name, Port, SID, Schema name and Schema password, and then click **Next**.
12. On the Management Summary screen, if the management database or user schema configuration was successful, click **Next**.
13. On the Login Settings screen, enter and confirm a JMX password for the Analytics server.
14. On the Summary screen, verify that the installation was completed successfully, and then click **Finish**.
15. On the server where PerfSpi is installed, create a folder **C:\NPSExportData** that will hold the CSV files.
 - a. Create a folder **C:\NPSExportData** that will hold the CSV files.
 - b. From a command prompt, run **configurecsvexport.ovpl -p interface_health -a "LIVE, C:\NPSExportData"**.

Administering Service Health Analyzer

This section includes:

Selecting CIs to be Monitored by SHA Overview	24
How to Select CIs to be Monitored by Service Health Analyzer.....	25
CI Selection Tab.....	26
Event Template Overview	29
How to Configure the Service Health Analyzer Event Template.....	30
Event Template Tab.....	31
Configuring Verification Tools Overview	37
Service Health Analyzer SiteScope Templates.....	38
How to Configure Verification Tools.....	39
SiteScope Template Tab.....	40
Template Mapping Configuration Wizard.....	42
Verification Tools Tab.....	52
Analyzing Service Health Analyzer Statistics	53
SHA Statistics Tab.....	54

Selecting CIs to be Monitored by SHA Overview

SHA monitors CIs that are specifically selected by the SHA administrator. You can choose from CIs that are part of the views specified in the **Views Selector Filter** setting of the **Service Health Analyzer - General Settings**. The default views are End User Applications, Business Services, and System Software Monitoring.

For more information on how to edit infrastructure settings, see "[How to Edit an SHA Infrastructure Setting](#)" (on page 157).

Note: Contents of views can be seen in the RTSM IT Universe Manager.

When CIs are selected, the process of collecting metric samples begins. Once there are sufficient metric samples to create the baseline, a batch process creating baseline information runs, and the CIs and their metrics are included in the anomaly detection process.

Metrics that are collected for a CI are based on the contents of out-of-box SHA XML files stored on the Analytics server. The Business Process Monitor (BPM), Real User Monitor (RUM), Diagnostics, SiteScope, Network Node Manager i (NNMi), and HP Performance Agent (PA) data collectors each have a separate XML file that contain a list of metrics to be collected for each CI Type. Only metrics included in the XML file have metric baselines created.

Service Health Analyzer License

You can apply an evaluation (60 day), temporary, or permanent license to SHA. You must purchase a license for each managed node (CI Type of node that SHA monitors). The number of monitored managed nodes is a combination of :

- Managed nodes that are children of CIs selected in the CI Selection feature.
- Manged nodes created from TQLs stored in the Service Health Analyzer\Analytic CIs folder in RTSM.


When you save CI selections, if you exceed the number of node licenses purchased, you will receive a warning message that you have exceeded your license count.

When using an evaluation license, the license management screen displays that you have one SHA license. In the evaluation version, when you save CI selections, and you exceed the number of node licenses, you receive no warning.



For information on how to select CIs, see "[How to Select CIs to be Monitored by Service Health Analyzer](#)" (on page 25).

How to Select CIs to be Monitored by Service Health Analyzer

This task describes how to select CIs to be monitored by Service Health Analyzer.

1. (Optional) Create new views containing CIs you want to be monitored. For more information, see "View Formats" in the *RTSM Modeling Guide*.
2. (Optional) Add the the views to the filter.
 - a. Select **Admin > Platform > Infrastructure Settings**.
 - b. In **Applications**, select **Service Health Analyzer**, and in the **Service Health Analyzer - General** section, edit the **Views Service Filter** settings.
3. Add a CI for monitoring.
 - a. Select **Admin > Service Health Analyzer**, and then click the **CI Selection** tab.
 - b. Select a view from the drop down box, select a CI Type, and then click  to move the CI to the Selected CIs pane.

Note: If you select a CI with descendants, all the CI descendants are also selected. CI descendents are not visible in the Selected CIs pane.

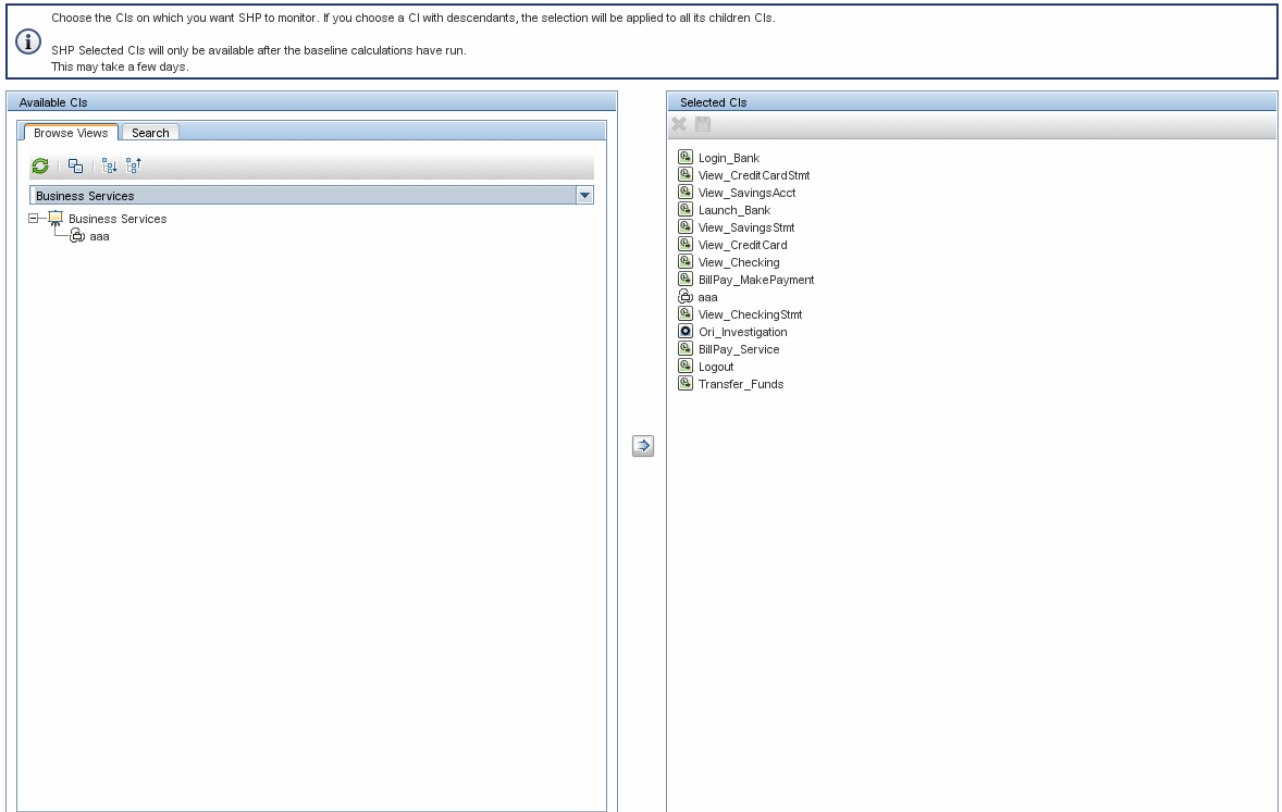
4. To remove a CI from monitoring, click a CI in the Selected CIs pane, and then click .
5. Click  to save the changes.

The SHA engine starts collecting metric samples for the selected CIs. Once sufficient metric samples have been collected for a CI, and on a periodic basis, a process runs that calculates the baseline. Once the baseline has been calculated for a metric, the metric can be reported as part of an anomaly.

For information on which metrics are baselined and have values collected, see "[How to Edit the SHA Metric Selection XML Files for Baselining](#)" (on page 145).

CI Selection Tab

This tab enables you to select CIs that are monitored by Service Health Analyzer.








To Access	Select Admin > Service Health Analyzer , and then click the CI Selection tab.
Important information	<ul style="list-style-type: none"> You must define the SHA database schema before you can use the CI Selection Tab. Once a CI has been selected, it must complete its baseline calculation process before can be part of an anomaly. This process can take several days. It is highly recommended that you add CIs in the CI Selection tab, CIs can also be added in RTSM Admin. If CIs are added in RTSM Admin, they must be added to queries that are child resources of the Service Health Analyzer\Analytic CIs folder, or to the Example resource under the Analytic CIs folder. <p>CIs added to a child of the Analytic CIs resource, are not visible in the Selected CIs pane, but are still monitored by SHA.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p>Caution: Do not edit the SHA_TQL_FILTER_ADMIN_CIS TQL.</p> </div>
Relevant Tasks	"How to Select CIs to be Monitored by Service Health Analyzer" (on page 25)

Available CIs Area

The available CIs area lists the available CIs for each view. Available views are configured in the Service Health Analyzer - General section of the Service Health Analyzer Infrastructure settings. You can select a CIs in this area and move it to the Selected CIs area. Additionally you can search for a specific CI using the **Search** Tab in the Available CIs area.



Browse Views Tab

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element	Description
	Expand All. Expands all the CIs for the selected CI type.
	Collapse All. Collapses the CIs for the selected CI type.
	Refresh. Reloads the Available CI list.
	Clear All. Clears current selection in the Browse View Tab.
View	Displays views that contain the CIs you want SHA to monitor. Views are separated by a line. Those below the line have not been selected in this session.
<CIs>	The CIs that belong to the selected CI type.
	Click to move the selected CI from the Available CIs area to the Selected CIs area. Note: You can select and move multiple CIs simultaneously.

Search Tab

User interface elements are described below (unlabeled elements are shown in angle brackets):




UI Element	Description
	Enables you to edit the fields listed in the search results table.
Name	The name of the CI you want to transfer to the Selected CIs area. Click Search to search for the CI in the CI tree.
<column filter>	<ul style="list-style-type: none"> After entering a string in a column's filter, press Enter, or click another element on the page to generate the list of matching records for the currently selected view. If a column's filter is empty, all records for the currently selected view are displayed. You can use the asterisk (*) wildcard as part of a string in a column's filter.
	Move to selected CIs. Click to move transfer the selected CI from the Available CIs area to the Selected CIs area.

UI Element	Description
	<p>Note: You can select and move multiple CIs simultaneously.</p>

Selected CIs Area

The Selected CIs area, displays the CIs that have been transferred from the Available CI area. Once changes are saved the process of collecting metric samples begins.

User interface elements are described below (unlabeled elements are shown in angle brackets>):

UI Element (A–Z)	Description
	<p>Delete. Removes a selected CI.</p>
	<p>Save. Saves any changes made. Once you save, metrics for the CI are recorded and used in the baseline calculation. The icon is enabled when a change is made.</p> <p>If you click , and the number of SHA managed nodes exceeds the amount of nodes in your license, you will receive a warning message that you have exceeded your limit.</p> <p>In evaluation mode you do not receive a warning message.</p>

Event Template Overview

The event template defines the structure of the SHA event that is sent to the Operations Management Event Browser. In the template, you define the format of the SHA event using attributes described in ["Event Template Tab" \(on page 31\)](#).

The Title and Description fields are used in all SHA events.

For every SHA event generated, ETI values are calculated and Severities are assigned using the following logic:

1. If there is only one pattern suspect for the anomaly, an ETI value is identified with the same name as the pattern name.

For example, if the pattern suspect is "Known Issue", an ETI value of "Known Issue" and severity "Minor" is assigned to the event.

2. If there are several pattern suspects for the anomaly, the ETI value (matching the pattern name) with the worst severity is selected.

For example, if there are 2 pattern suspects: "Known Issue" and "Reoccurrence", ETI value "Major" and severity "Major" is assigned to the event.

Note: If there are two suspect patterns with the same severity, the first suspect that appears in the anomaly suspect list is selected.

3. If there are no pattern suspects on the anomaly, or there are pattern suspects with no matching ETI values, the monitored CIs are checked for an infrastructure CI type. If monitored CIs have an infrastructure CI type, the ETI value is set to "Infrastructure" and severity to "Minor".
4. If none of the above checks apply, the default ETI and severity values configured in the Event Template are added to the SHA event. The default values set in the event template are an ETI value of "Major", and a severity of "Major".

This section includes:

How to Configure the Service Health Analyzer Event Template	30
Event Template Tab	31

How to Configure the Service Health Analyzer Event Template

This task describes how to configure the SHA event template, to create events when an anomaly is generated.

1. Configure the SHA Event Template


The out-of-the-box SHA template is configured with the attributes necessary to provide the required information for an SHA event. You can add to or edit the default attribute settings as follows:

- a. Select **Admin > Service Health Analyzer**, and then click the **Event Template** tab.
- b. From the Attributes pane, drag an attribute to the required field in the General pane.

You can also select an attribute in the Attributes pane, click inside the required field in the General pane, and then press <Alt> + i to insert the attribute.

You can add text to the template fields. For example in the Title field, you could enter: **This is the title of the event: <<eventTitle>> This is the event description : <<eventDecription>>**


2. If you want to add additional attributes that will appear in the Custom Attributes tab of the SHA event:

- a. Click the **Custom Attributes** tab.
- b. Click  to create a new key, and add a new key name or use one of the known key names. The new key appears in the Name column.
- c. For the new key, click inside the Value text box where you want to insert the attribute, and drag an attribute to the value field.

To edit an existing key/name, click inside the Value text box where you want to insert the attribute, and drag an attribute to the value field.

You can also select an attribute in the Attributes pane, click inside the required field in the Custom Attributes tab, and then press <Alt> + i to insert the attribute.

3. Click to save the changes.

You can restore the default event template values by clicking .

Event Template Tab




This tab enables you to configure the event template.

The screenshot shows the 'Event Templates Editor' window. It has a toolbar with a save icon and a refresh icon. Below the toolbar are two tabs: 'General' (selected) and 'Custom Attributes'. The 'General' tab is divided into three sections: 'General', 'Correlation', and 'Advanced Parameters'. The 'General' section contains fields for Title, Description, Severity (set to 'Critical'), Category, Subcategory, Log only (set to 'false'), and Event Type Indicator (set to 'Predictive_Health_ETI:Critical'). The 'Correlation' section has a 'Key' field and a checkbox for 'Submit close key condition' with a 'Close Key Pattern' field below it. The 'Advanced Parameters' section has fields for 'CI hint', 'Host hint', and 'Generating source hint'. To the right of the main editor is a list of attributes: <<anomalyHighlights>>, <<anomalyId>>, <<anomalyRelatedCI>>, <<businessEntities>>, <<eventDescription>>, <<eventTitle>>, <<investigateAnomalyURL>>, <<locations>>, <<shpEngineServerName>>, <<similarities>>, <<slas>>, <<suspects>>, and <<timeframe>>.

To access	Select Admin > Service Health Analyzer , and then click the Event Template tab.
Relevant tasks	"How to Configure the Service Health Analyzer Event Template" (on page 30)
See also	"Event Template Overview" (on page 29)

Event Template Editor Toolbar

This toolbar enables you to save or restore changes made to the event template. User interface elements are described below:

UI Element (A-Z)	Description
	Save. Saves the event template.
	Undo. Restores the event template to the last save.
	Restore Default. Restores the event template default values.

General Tab

This area enables you to define the Event Template.

Important information	Do not change the values of the of the Event Type Indicator, and Key fields.
------------------------------	--

User interface elements are described below:

UI Element (A-Z)	Description
Category	Used to organize or group events. You can specify your own categories.
CI hint	Information about the CI that is related to the event. This attribute is used for providing hints to enable the event processing to find the correct related CI. Default Value: <<anomalyRelatedCI>> It is recommended that you use the default value.
Close key pattern	Enables the event that is sent to close all the events whose Key attribute matches the Close Key Pattern expression. You can use wildcards (*).
Description	Detailed information describing the event. Default Value: <<investigateAnomalyURL>> <<anomalyHighlights>>
Event Type Indicator	Links between the event and the health indicator so information about the health indicator can be updated as a result of submitting the event. Default Value: Predictive_Health_ETI:Critical Caution: Do not change the default value.
Generating source hint	Information about the monitoring application and the corresponding probe/agent that is responsible for creating the event. Default Value: <<shaEngineServerName>> It is recommended that you use the default value.

UI Element (A-Z)	Description
Host hint	Information about the CI of type Node that is hosting the CI related to the event. Default Value: <<shaEngineServerName>> It is recommended that you use the default value.
Key	A unique string representing the type of event that occurred. Caution: Do not change the value in this field.
Log only	Assign the value: <ul style="list-style-type: none"> true to send the event to the history event browser as a close event. Such an event goes through the complete event processing, but has its Life Cycle State set to close from the beginning. false to send the event to the event channel if the alert is configured to send an event. Default value: False
Severity	The severity of the event. It represents the translation of the alert CI status into the event severity. The severity levels can be: Normal, Warning, Minor, Major, CriticalUnknown. Default value: Critical
Subcategory	More detailed organization of events that have the same category. Used for event standards and external event sources that are using subcategories.
Submit close key condition	When you select the option, you must enter a value in the Close key pattern box.
Title	Describes the occurrence represented by the event. The title should include information about what threshold has been crossed (or other trigger conditions), and the current values. Default Value: <<eventTitle>> <<eventDescription>> Note: Since the Title text is typically shown within a single line in the event browser, it is recommended that the most relevant information is placed at the beginning of the text.

Attributes Area

Select attributes from the Attribute area to be included in the event template.

Important information	<ul style="list-style-type: none"> • Select the relevant attribute in the Attributes area and drag it into the relevant box in the General tab. • You can also select a specific attribute and click CTRL+I while editing text to insert that attribute in the text. • The attributes represent useful information that can be inserted into the SHA event.
------------------------------	--

The table lists the attributes you can use in the General tab:

Attribute	Description
anomalyHighlights	The highlights of the anomaly. The anomaly highlight consists of all the highlights of the Title and Description fields and links to similar anomalies. For more on anomaly highlights, see " Anomaly Highlights Page " (on page 71).
anomalyId	The ID of the anomaly.
anomalyRelatedCI	The CIs related to the anomaly.
businessEntities	The affected business entities.
investigateAbnormalURL	The URL that you click to investigate the anomaly.
locations	The locations affected by the anomaly. A location is displayed because running transactions or SiteScope servers located there or at satellite locations, participate in the anomaly. Format: location: <tab>location value<new line>
shaEngineServerName	The name of the server on which the SHA engine is running.
similarities	The anomalies and the pattern investigations that are similar to the anomaly.
slas	Affected SLAs that include CIs that participate in the anomaly.
suspects	The anomaly suspect CIs.
timeframe	The anomaly time frame.



Custom Attributes Tab

Use this tab to add custom attributes.

You can also create custom attributes in the SHA Event Template dialog box. The output of a custom attribute is displayed in the Custom Attribute tab of the SHA event.

Important information	<p>A custom attribute consists of a key name and a value (both are strings). The value can be any string and is used by the Event Template mapping as any other value.</p> <p>Limitations:</p> <ul style="list-style-type: none"> • Make sure that the name of the custom attribute you are defining is unique and does not already exist in the list of constant attributes. For details of the constant attributes, see "Constant Attributes" (on page 35). • If you add to a template a custom attribute with a key similar to a constant attribute's key, the custom attribute is ignored. For details about the constant attributes, see Constant Attributes. • If you use, in the same template, more than one custom attribute with the same key, only one of these custom attributes is taken into account. • Event Template attributes are changed into the value of the relevant attribute of the triggered alert. When it is a custom attribute, the value specified in the Custom Attributes tab for the relevant attribute is used.
------------------------------	---

User interface elements are described below:

UI	
Element	Description
Name and Value	<p>Each event can have any number of custom attributes. You use custom attributes to provide additional event information that is not provided by any of the other Event Template attributes, or not contained in any of the other attributes. Each custom attribute consists of a Name and a Value.</p> <p>This feature may be used when you manage the environments of multiple customers using one instance of the product. Multiple customers might be handled by a custom attribute object. For details about the available attributes, see "Attributes Area" (on page 33).</p> <p>Example: Name = "Customer" ; Value = "XYZ Company"</p>
	<p>Lists the options available for creating a custom attribute, as follows:</p> <ul style="list-style-type: none"> • New key. To create a new key. A new row opens in the Name/Value table. • Known key. Opens a submenu with the known keys as options. You can select the relevant key. A new row opens in the Name/Value table, with the name of the selected key in the Name column. You can then enter the value of the key in the corresponding Value column. <p>Note: The known keys are defined in Operations Management. Such keys have additional capabilities. Keys defined in the SHA Event Template dialog box only have a value and are used as strings.</p>
	Deletes the selected attributes from the table.

Constant Attributes

The Event Template uses the constant attributes to represent the fields that appear in the General tab (title, category, subcategory, and more).

Note: Do not use these attribute's keys as the keys to custom attributes.

The constant attribute keys are:

- Category
- CiHint
- CloseKeyPattern
- DateOccurred
- Description
- EtiHint
- HostHint
- Key
- LogOnly
- OriginalData
- Severity
- SubmitCloseKey
- SourceHint
- SubCategory
- Title

Configuring Verification Tools Overview

Service Health Analyzer helps you find the root cause of a problem by enabling you to investigate enterprise problems discovered in BSM, and identifying likely suspect CIs. When an anomaly occurs and an SHA event is generated, part of the process includes running verification tools that assist in identifying suspect CIs.

To identify suspect CIs more accurately, you configure SHA SiteScope templates and verification tools. When an SHA event is generated, during the creation of the anomaly highlights, verification tools are run. If a verification tool fails, it is reported in the Anomaly Highlights page, and the rogue CI can be identified as suspect.

This section includes:

Service Health Analyzer SiteScope Templates	38
How to Configure Verification Tools	39
SiteScope Template Tab	40
Template Mapping Configuration Wizard	42
Select CI Type Page	43
Select Templates Page	45
Configure Parameters Page	47
Verification Tools Tab	52

Service Health Analyzer SiteScope Templates

SHA SiteScope templates gather in-depth data on system components, based on an anomaly's suspect CIs.

SiteScope provides out-of-the-box TQLs and SiteScope monitor templates, that are used in the SHA SiteScope template configuration.

When an anomaly is opened:

1. SHA determines which CIs are suspect in causing the anomaly. These CIs are called suspect CIs.
2. For each suspect CI, SHA determines by CI Type which SHA SiteScope templates are configured to run on each suspect CI.
3. If the relevant verification tool (that can be identified by the CI Type and the SiteScope template) has its **Executions Type** set to Automatic, the RTSM populates monitor variables from relevant CI attributes configured on the **Configure Parameters** page of the CI Type Mapping wizard, and runs the verification tool.
4. When a verification tool fails, the Anomaly Highlights reports the failed tool name.

Selectable SiteScope templates are displayed in the SiteScope Templates page. For user interface details, see "[SiteScope Template Tab](#)" (on page 40).

You can configure SHA to automatically run verification tools. For further information, see "[How to Configure Verification Tools](#)" (on page 39).

You create, or edit mappings between CI Types and SiteScope templates using the CI Type Mapping wizard. For user interface details, see "[Template Mapping Configuration Wizard](#)" (on page 42).

How to Configure Verification Tools

This task describes the flow for configuring verification tools.



1. (Optional) Configure additional SHA SiteScope templates

Out-of-box templates are provided with SiteScope. These templates monitor the data sources in Business Service Management.

- a. Select **Admin > System Availability Management**.
- b. Click the name of a SiteScope server, and then click **Templates**.
- c. Add an additional SiteScope template as described in the *Using SiteScope Guide*.

2. Map the templates and their parameters to the relevant CIs and their attributes.

Note: To see the available CI Types, select **Admin > RTSM**, click **CI Types**, and then expand **Configuration Items**.

- a. Select **Admin > Service Health Analyzer**, click the **SiteScope Templates** tab, and then click  to create a new mapping.
- b. In the Template Mapping Configuration wizard, select a CI Type that you want to map to a template. For user interface details, see "[Template Mapping Configuration Wizard](#)" (on [page 42](#)).
- c. In the Available Templates pane, select a template and click . The template moves to the Selected Templates pane.
- d. On the Configure Parameters screen, map the CI attributes to the template parameters, and if required enter default attribute values.

Note: If you wish to assign attributes from a CI in a different topology, click **Select**, select a topology, select the node to which the templates are mapped, and click **OK**. Additional CIs are now presented in the Configure Parameter screen.

- e. Click **Finish**, review the mapping, and then click **OK**.

3. Configure the verification tools

- a. Select **Admin > Service Health Analyzer**, and then click the **Verification Tools** tab.
- b. To automatically run the verification tool when the CI is suspect, select the mapped template, click the Execution Type, and then click **Automatic**.

Note: By default, the Execution Type is set to Disabled.

4. Result

When an anomaly occurs, the verification tool runs for CIs of the selected CI Type.

SiteScope Template Tab

This tab enables you to display all CI Types that are mapped to out-of-the-box SiteScope templates. The templates include the SiteScope monitors used to monitor the CI Types.

SiteScope monitors mapped on this page are available as verification tools.



To access	Select Admin > Service Health Analyzer , then click the SiteScope Templates tab.
Task	" How to Configure Verification Tools " (on page 39)

UI Element (A–Z)	Description
	New Mapping. Opens the Template Mapping Configuration wizard where you map SiteScope templates to a CI Type. For details, see " Template Mapping Configuration Wizard " (on page 42).
	Edit Mapping. Opens the Template Mapping Configuration wizard where you can edit the selected CI Type mapping. For details, " Template Mapping Configuration Wizard " (on page 42).
	Delete Mapping. Deletes the selected mapping between the CI Type and the SiteScope template.
	<p>Validate Mappings with SiteScope. Validates that the mappings are synchronized with the SiteScope machine.</p> <ul style="list-style-type: none"> When the mapping is successfully validated, a checkmark appears on the left of the Template name, and a tooltip provides further details. When the selecting mapping is not validated, an error icon appears on the

UI Element (A–Z)	Description
	<p>left of the template name, and a tooltip provides further details about the problem.</p> <p>For example, the validation will fail if the template no longer exists on the SiteScope machine, or a specific configuration setting of the template no longer exists.</p>
<column filter>	<ul style="list-style-type: none"> • After entering a string in a column's filter, press ENTER or click another element on the page to generate the list of matching records. • If a column's filter is empty, all records are matched for that column and are included in the generated list. • You can use the asterisk (*) wildcard to represent any part of a string in a column's filter. For example P* will return all items beginning with the letter P.
CI Type	The name of the CI Type in the topology.
Templates	The SiteScope templates mapped to the CI type.

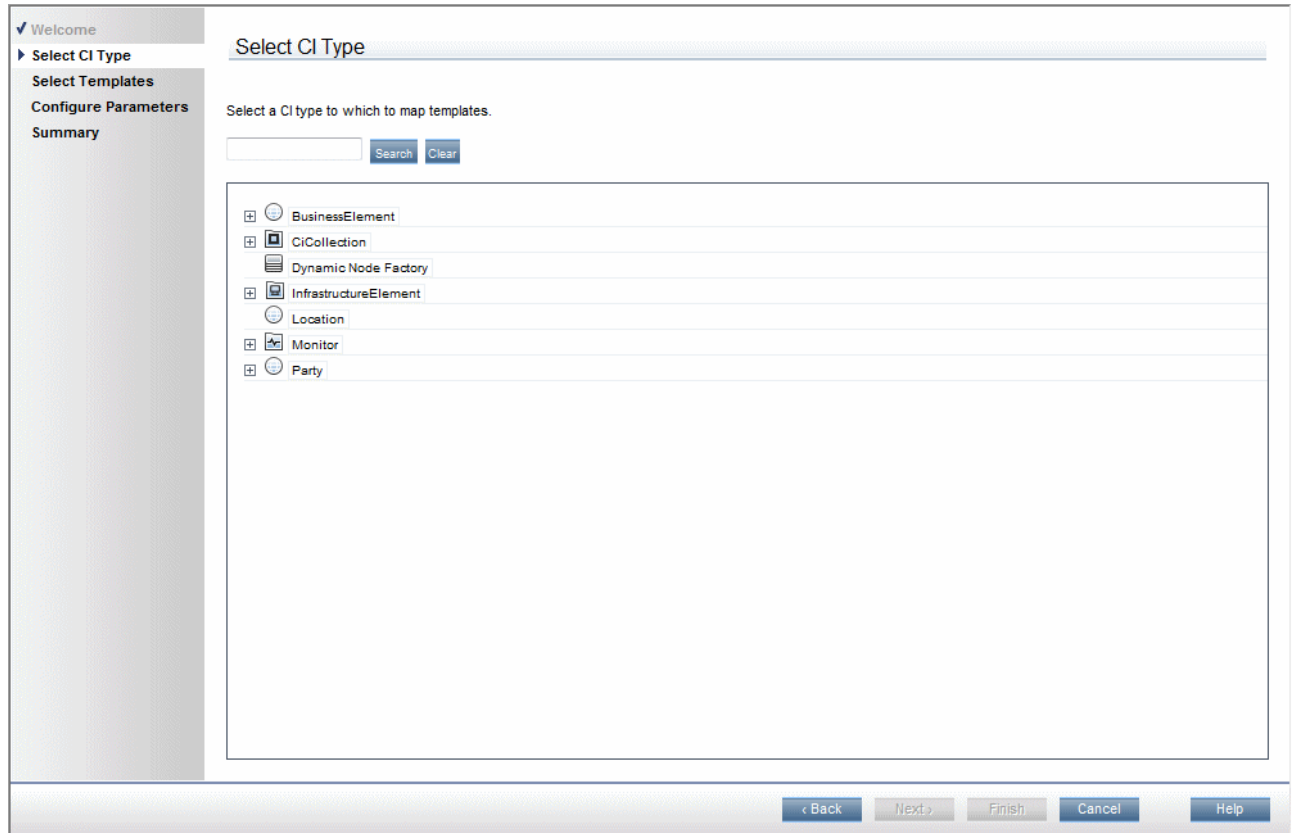
Template Mapping Configuration Wizard

This wizard enables you to configure mappings between CI Types and SiteScope templates.

<p>To access</p>	<p>Admin > Service Health Analyzer, and then click the SiteScope Templates tab.</p> <p>In the SiteScope Templates tab:</p> <ul style="list-style-type: none"> • Click  New Mapping to create a new mapping; OR • Select an existing suspect CI Type mapping, and click  Edit Mapping.
<p>Important information</p>	<ul style="list-style-type: none"> • Child CIs of a CI for which you assign a SiteScope template, are also assigned that SiteScope template. • When you add a new mapping you must complete each wizard screen in chronological order. • When you edit a previously configured mapping: <ul style="list-style-type: none"> ▪ The Welcome and Summary pages of the wizard are not displayed. ▪ You can also access wizard pages in any order by clicking a page name from the left menu. ▪ From any wizard page, click OK to save the configuration and exit the wizard.
<p>Relevant tasks</p>	<p>"How to Configure Verification Tools" (on page 39)</p>
<p>Wizard map</p>	<p>The Template Mapping Configuration wizard consists of the following:</p> <p>Welcome page > "Select CI Type Page" (on page 43) > "Select Templates Page" (on page 45) > "Configure Parameters Page" (on page 47) > Summary</p>

Select CI Type Page

This page enables you to select the CI Types to which you map the SiteScope templates.



Important information	<p>This page lists the CI Types available in the RTSM.</p> <p>General information about the wizard is available at "Template Mapping Configuration Wizard" (on page 42).</p>
Wizard map	<p>The Template Mapping Configuration wizard consists of the following:</p> <p>Welcome page > "Select CI Type Page" (on page 43) > "Select Templates Page" (on page 45) > "Configure Parameters Page" (on page 47) > Summary</p>

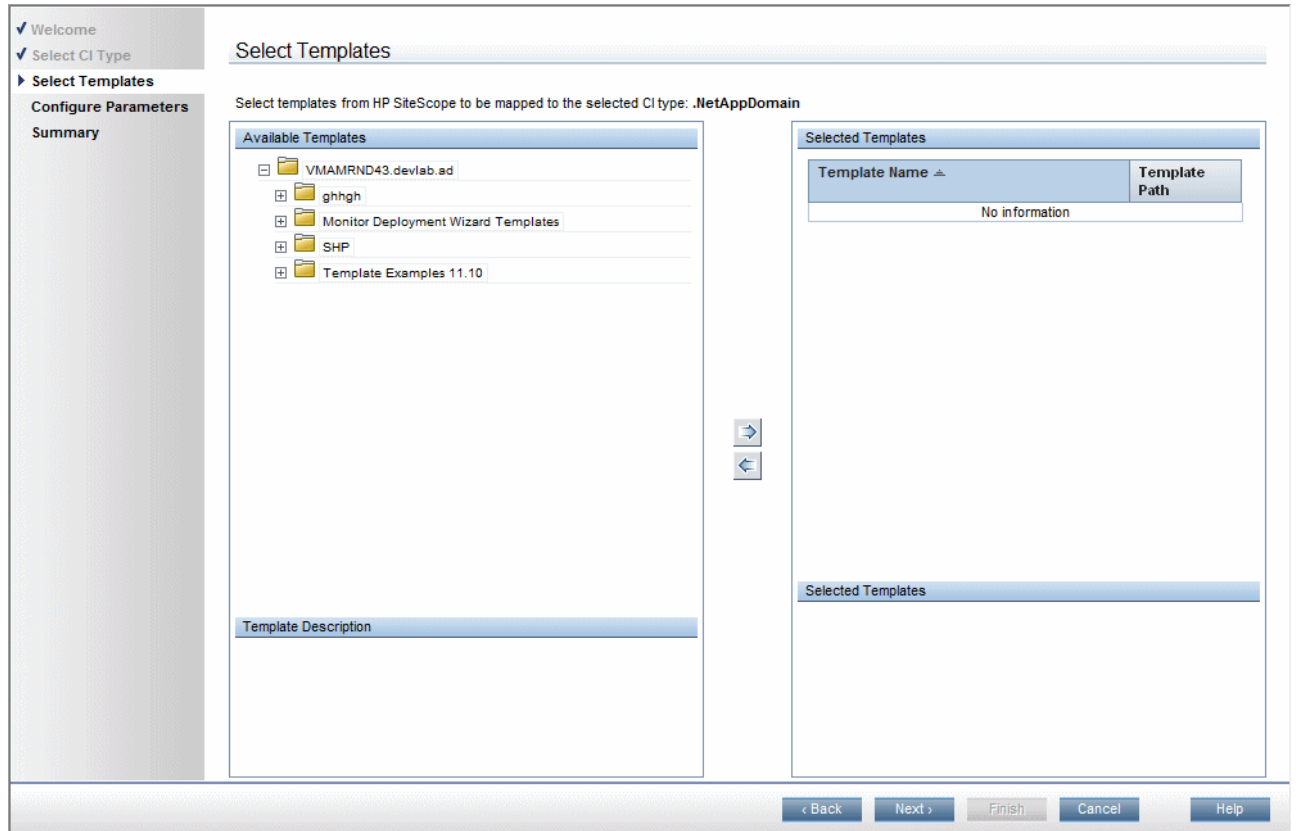
User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<CI type tree>	Displays a list of CI types from which you select the required CI type to which to map a SiteScope template. Select a CI type, and then click Next to move to the Select Templates page.
<Search string>	You can search for CI Types containing a specific string that you enter in the CI Type field, or Templates containing a specific string that you enter in the Templates field.

UI Element (A-Z)	Description
	The search returns matching results where the search string exactly matches the start of the CI Type or Template name, or matches an * wildcard followed by a text string. Note: The search is not case sensitive.
Clear	Clears the current search string and to display all CI Types.
Search	Displays CI Types that match the search string.



Select Templates Page

This page enables you to select SiteScope templates to map to the CI Type selected in the Select CI Type page.



Important information	This page displays the available templates defined on the SiteScope machine. General information about the wizard is available at " Template Mapping Configuration Wizard " (on page 42).
Wizard map	The Template Mapping Configuration wizard consists of the following: Welcome page > " Select CI Type Page " (on page 43) > " Select Templates Page " (on page 45) > " Configure Parameters Page " (on page 47) > Summary

User interface elements are described below:

UI Element (A-Z)	Description
	Select template to map. Adds the selected template from the Available Templates pane to the Selected Templates pane.
	Remove template from mapping. Removes the selected template from the Selected Templates pane.
Available Templates	Displays the available templates. You can expand a template to display its

UI Element (A-Z)	Description
	child templates. You can select multiple templates by selecting multiple templates while holding <Ctrl>.
Selected Templates	Displays a list of the SiteScope templates you selected for mapping to the CI Type, and the template path.
Selected Template Description	Displays a detailed description of a selected templates.
Template Description	Select a template to display a detailed description of the available template.

Configure Parameters Page

This page enables you to configure the settings and default values of the SiteScope template parameters.

Configure Parameters

Map CI attributes to template parameters and/or assign default values.

Selected CI: **.NetAppDomain**.

Topology for .NetAppDomain: **(None)** [Select](#)

Template Parameter Name	CI	CI Attribute	Default Value (Optional)
IIS Server			
application_ip *			
host_password *			*****
host_username *			
nt_domain *			
Windows basic template			
frequency *			800
host *			
password *			*****
user *			



* Mandatory SiteScope template parameter

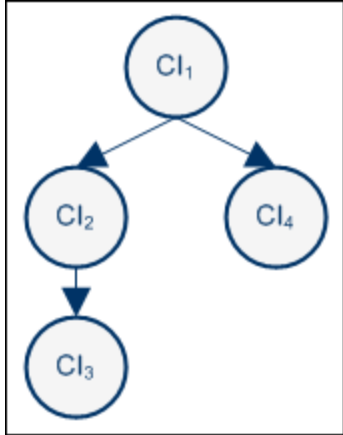
Back Next Finish Cancel Help

<p>Important information</p>	<p>When you click Next to go to the Summary page, the parameter mapping you selected is validated and you may receive the following message types:</p> <ul style="list-style-type: none"> • Informational messages: <ul style="list-style-type: none"> ▪ If a new parameter was added to the CI or to the SiteScope template. ▪ If the SiteScope is not activated. • Error messages: <ul style="list-style-type: none"> ▪ If the template was removed from SiteScope. ▪ If the parameter was removed from the template. ▪ If the SiteScope does not exist. ▪ If Business Service Management cannot communicate with System Availability Management. <p>General information about the wizard is available at "Template Mapping Configuration Wizard" (on page 42).</p>
<p>Wizard</p>	<p>The Template Mapping Configuration wizard consists of the following:</p>

map	Welcome page > "Select CI Type Page" (on page 43) > "Select Templates Page" (on page 45) > "Configure Parameters Page" (on page 47) > Summary
-----	---

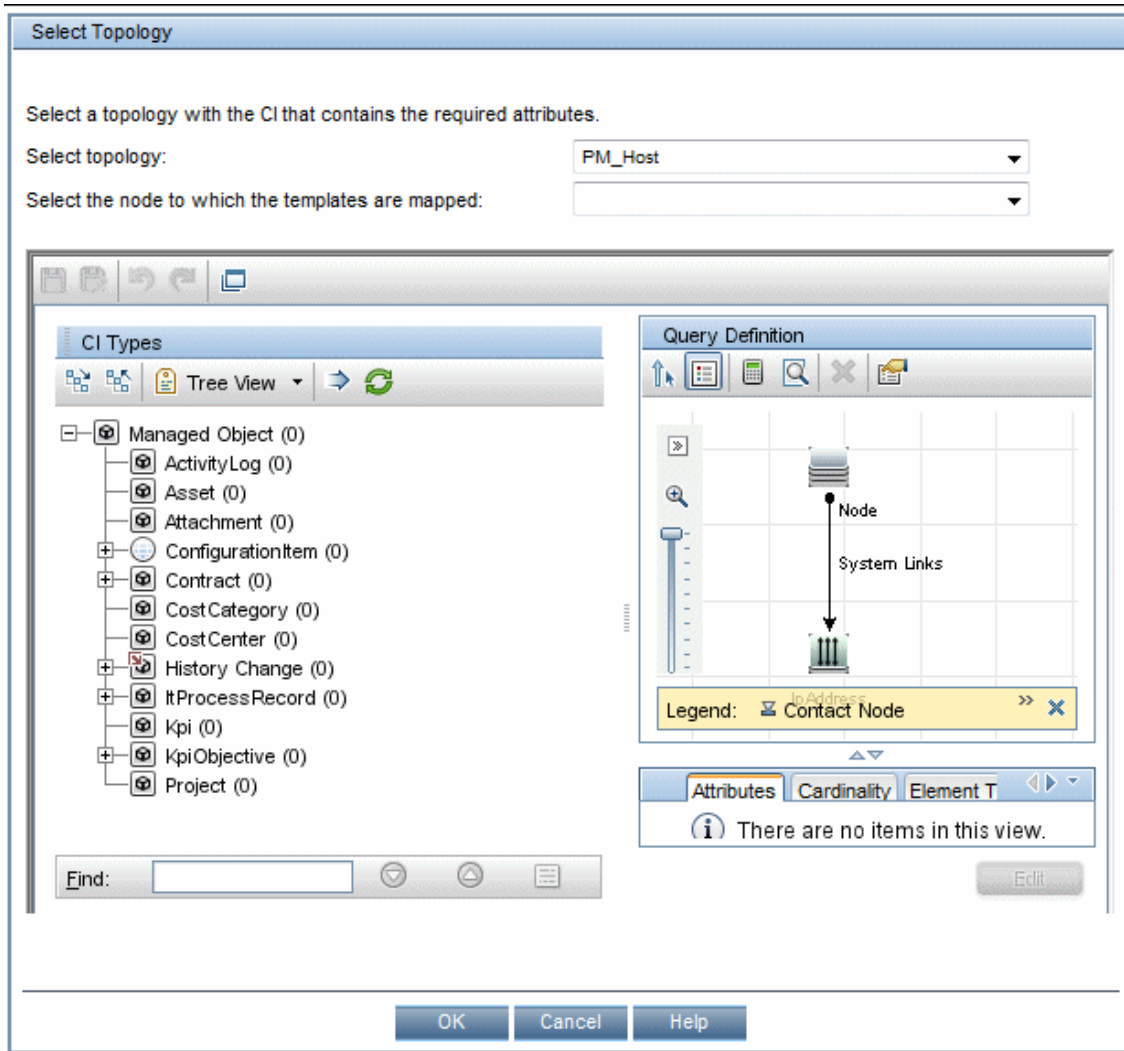
User interface elements are described below:

UI Element (A-Z)	Description
CI	<p>The default CI from the selected CI type topology to use as the source for the required SiteScope template parameter. Click the arrow to open a drop-down list of all the CIs included in the CI type topology. Select a different CI if required.</p> <p>Note: If there is no configured topology for the selected CI type, the CI corresponding to the selected CI type itself is the only available option.</p>
CI Attribute	<p>The default attribute of the selected CI that you use as the source for the selected SiteScope template parameter.</p> <p>Click the arrow to open a drop-down list of all the attributes for the selected CI. Select a different attribute if required.</p>
Default Value	<p>If the CI attribute is dynamically assigned a value, then this value is used. A default value can optionally be entered and is used when the CI attribute is not dynamically assigned a value.</p>
Template/Parameter Name	<p>A hierarchical list of the selected SiteScope templates, and the parameters that they require.</p> <p>Note:</p> <ul style="list-style-type: none"> • Mandatory parameters for which settings are required are denoted by a red asterisk. • A parameter included in an existing mapping, but that is not found in a template, is denoted by the  icon. • A parameter found in a template, but not included in an existing mapping, is denoted by the  icon. • Additional and deleted parameters are automatically added to, or removed from the mapping when you click the OK button on the wizard page. • Only parameters that are configured as flow input parameters for SiteScope templates are included.
To choose an attribute that is not part of the selected CI click here	<p>Click the link to open the Select Topology dialog box, where you can select a CI from a related topology to use as a source for a required SiteScope template parameter.</p> <p>For example, in the following image, if the selected CI is CI₄ you can</p>

UI Element (A-Z)	Description
	<p data-bbox="553 254 1162 281">select any attribute of all the other CIs in the topology.</p> <div data-bbox="553 306 894 737"><pre data-bbox="553 306 894 737">graph TD; CI1((CI1)) --> CI2((CI2)); CI1 --> CI4((CI4)); CI2 --> CI3((CI3));</pre></div> <p data-bbox="553 764 1357 831">For details on the user interface, see "Select Topology Dialog Box" (on page 50).</p> <p data-bbox="553 852 1373 982">Note: The available topologies are out-of-the-box. If you create your own topology, it should be located in the SiteScope On Demand Monitors folder in RTSM Modeling Studio. The topology should have the correlation or integration type.</p>

Select Topology Dialog Box

This page enables you to select a different CI Type or node CI from a topology related to the CI Type selected in the Template Mapping Configuration wizard. This CI is used as a source for a required SiteScope template parameter for the CI selected in the wizard.



To access	Click the Select link next to Topology for <CIType> in the Configure Parameters page in the Template Mapping Configuration wizard. For details on the user interface, see " Configure Parameters Page " (on page 47).
See Also	"Template Mapping Configuration Wizard" (on page 42)

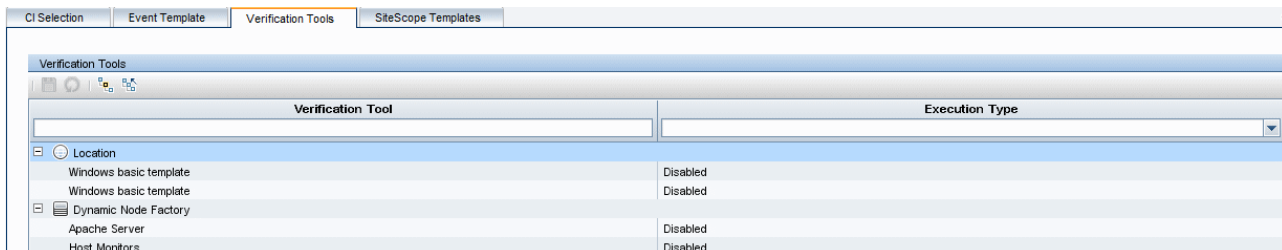
User interface elements are described below (unlabeled elements are shown in angle brackets>):

UI Element (A-Z)	Description
<Topology>	Displays a map of the selected CI topology.

UI Element (A-Z)	Description
map>	
Select the node to which the templates are mapped	Select a specific node from the selected topology to use as the source for a required SiteScope template parameter that is related to the CI type selected in the Template Mapping Configuration wizard. Available nodes are those applicable for the CI type selected in the wizard, and their descendants.
Select topology	<p>Select a topology from the drop-down list of topologies that are related to the CI Type selected in the Template Mapping Configuration wizard. Related topologies are those topologies in the SiteScope On Demand Monitors folder.</p> <p>Note:</p> <ul style="list-style-type: none">• Topology names in the On Demand Monitors folder cannot contain spaces.• You can create topologies using Query Manager (Admin >RTSM Administration > Modeling > Query Manager). For task details, see "Define a TQL Query" in the <i>Modeling Guide</i>.





Verification Tools Tab

The Verification Tools tab enables you to configure which of the SiteScope verification tools should run when an anomaly is created. Verification tools that fail on a CI are reported in the Anomaly Highlights page as suspect.



To access	Select Admin > Service Health Analyzer , and then click the Verification Tools tab.
See also	"How to Configure Verification Tools" (on page 39)

Verification Tools Toolbar

UI Element	Description
	Save. Saves changes made to the verification tool properties.
	Expand All. Expands the tree of CI Types and displays the verification tools configured for each CI Type.
	Collapse All. Collapses the tree of CI types.
	Reset. Resets changes made on this page, as long as the changes have not been saved.
Verification Tool	Lists the configured verification tools, categorized by CI Type.
Execution Type	Enables you to configure whether the verification tools will be run automatically or not. Choose from the following: <ul style="list-style-type: none"> • Disabled - The verification tool does not run when an anomaly is created. • Automatic - The verification tool runs automatically when an anomaly is created.
<column filter>	After entering a string in a column's filter, press Enter , or click another element on the page to generate the list of matching records. If a column's filter is empty, all records are displayed. You can use the asterisk (*) wildcard as part of a string in a column's filter. To filter Execution Types, click the Execution Type drop down arrow, and select the filter you require. If you select a blank line, both Automatic and Disabled verification tools are displayed.

Analyzing Service Health Analyzer Statistics

The Service Health Analyzer Statistics page enables you to view the current monthly return of investment as a result of using Service Health Analyzer, and is based on cost parameters that you input.

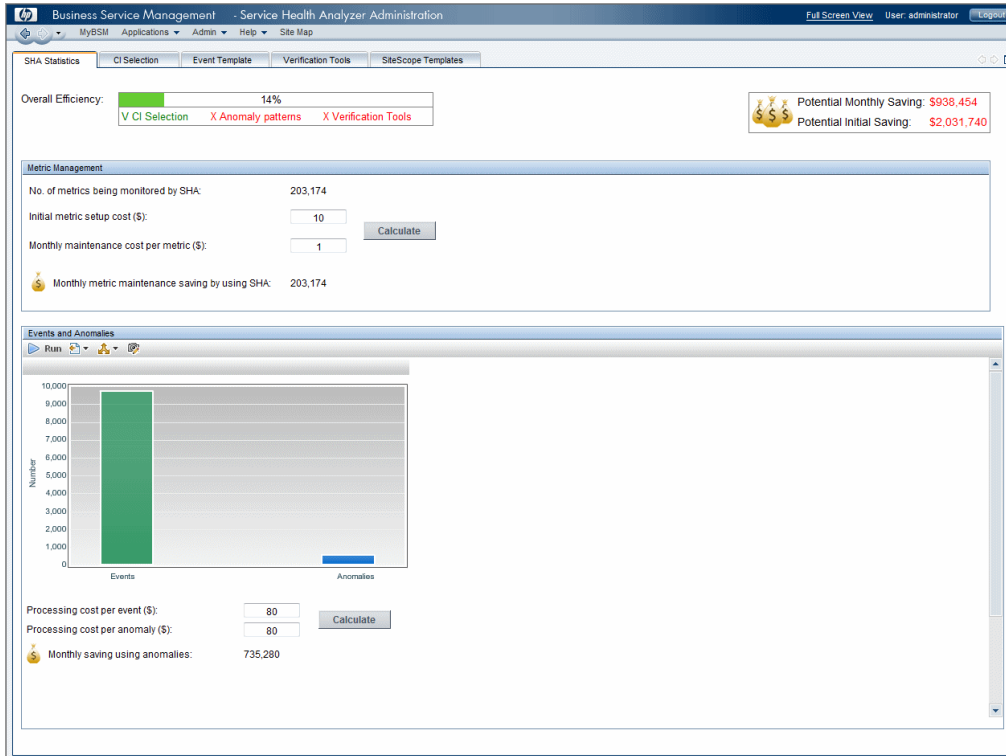
The SHA Statistics page:

- Recommends how to improve the efficiency of SHA.
- Displays the initial amount saved by using SHA, and the potential monthly savings.
- Compares the number of events to the number of anomalies and enables you to calculate the cost savings made by processing anomalies, and not regular events.

For more information, see "[SHA Statistics Tab](#)" (on page 54).

SHA Statistics Tab

This tab enables you to view monthly SHA statistics, and to calculate the current and potential savings you can make by using SHA.



To access	Select Admin > Service Health Analyzer , and then click the SHA Statistics tab.
Important Information	<ul style="list-style-type: none"> • The SHA Statistics tab can only be accessed by users assigned the BSM Administrator role. • Settings entered in this page are saved per user. • The figures on this page are based on a rolling month. • User inputted costs can be entered with a decimal point. The calculation results are rounded upwards.
Relevant tasks	<ul style="list-style-type: none"> • "How to Select CIs to be Monitored by Service Health Analyzer" (on page 25) • "How to Configure Verification Tools" (on page 39)

UI Element	Description
Overall Efficiency	Describes the overall efficiency of the SHA deployment as a percent. This figure is based on a combination of the following measurements:

UI Element	Description
	<ul style="list-style-type: none"> • CI Selection - The number of CIs selected in the CI Selection feature of Service Health Analyzer. It is recommended that you configure at least three CIs in the CI Selection feature. For more information, see "How to Select CIs to be Monitored by Service Health Analyzer" (on page 25). • Anomaly patterns - The number of anomalies that have been saved as investigations with a pattern type configured. It is recommended that you configure at least two investigations with patterns. For more information, see "Investigation Properties Dialog Box" (on page 130). • Verification Tools - The number of verification tools configured. It is recommended that you configure and set as automatic at least three verification tools. For more information, see "How to Configure Verification Tools" (on page 39). <p>Note: When a measurement complies with the minimum requirements, the measurement name appears in green. If a measurement does not comply, it appears in red.</p>
No. of Metrics being monitored by SHA	<p>The number of metric incidents being monitored by SHA. This is a combination of the CIs selected, the XML metadata files that contain the metric types that are collected for each data collector, and the metric instances. For more information, see "How to Select CIs to be Monitored by Service Health Analyzer" (on page 25).</p> <p>Note: This value is automatically calculated and cannot be edited.</p>
Initial setup cost per metric (\$)	<p>The initial cost of setting up or configuring a metric instance that is not managed by SHA. For example, analyzing metric instance behavior and then adjusting a static metric threshold.</p>
Monthly maintenance cost per metric (\$)	<p>The monthly maintenance cost of maintaining a metric instance that is not managed by SHA. For example, ongoing analysis of metric instance behavior, and then re-adjusting a static metric threshold.</p>
Calculate	<p>Click to calculate the "Monthly metric maintenance saving by using SHA".</p>
Monthly metric maintenance saving by using SHA	<p>The monthly metric maintenance saving. This is calculated as follows: No. of Metrics being monitored by SHA * Monthly maintenance cost per metric (\$).</p>
<Events and Anomalies Graph>	<p>The graph displays in bar format a comparison of the number of events sent to Operations Management Event Browser with the number of detected anomalies sent to the Operations Management Event Browser.</p>
Processing cost per	<p>The cost for processing a non-SHA event.</p>

UI Element	Description
event (\$)	Note: The cost of processing events and anomalies should be similar.
Processing cost per anomaly (\$)	The cost of processing an SHA event. Note: The cost of processing events and anomalies should be similar.
Calculate	Click to calculate the "Monthly saving using anomalies".
Monthly saving using anomalies	The monthly savings when only processing SHA events. This is calculated as follows: (No of events*Processing cost per event) – (No of anomalies*Processing cost per anomaly) .
Potential Monthly Saving	The potential monthly savings. This is calculated as follows: Monthly saving using anomalies + Monthly metric maintenance saving by using SHA.
Initial Saving	The initial amount saved. This is calculated as follows: Initial setup cost per metric (\$) * No. of Metrics being monitored by SHA.

Automatic Detection Overview

Service Health Analyzer (SHA) periodically receives data from samples that monitor enterprise components. The process of automatic detection of anomalies and the creation of SHA events is performed using the following:

- **Metrics**

A metric represents the time/value combinations provided for a specific field in a sample. Metric samples represent the behavior of the metric over time. The metric values are used to create and maintain a metric baseline, and to determine the mean and standard deviation values for the metric. Mean and standard deviation values for a metric are used to create a baseline sleeve, and to identify metrics that deviate from the baseline. The mean and standard deviation are a statistical way of estimating the normal behavior of a metric.

For more information, see ["How a Metric is Added to an Anomaly" \(on page 59\)](#).

- **Samples**

A sample is a collection of time stamped data that contains fields that represent specific metrics. SHA periodically receives samples that contain values of a metric at a specific time. Fields in a sample can include; Transaction from Location, Session ID, Transaction ID, Location ID, Server ID, Timestamp, Mean, Standard Deviation, Value, and Status. These fields identify the Metric ID, the value of the metric sample at the time the sample was taken, confirm whether a sample value was actually sent, and assist in identifying abnormal metrics.

- **A Metric Baseline Sleeve**

During the learning period, metric values are used to calculate the mean and standard deviations for a metric. The calculated mean and standard deviation values are then used to create the baseline sleeve that determines whether future metric values are normal. Once the baseline sleeve for a metric is created, a metric is considered to be abnormal when it's value is higher or lower than the metric's mean value + or - 3 times the standard deviation.

In addition, when calculating a metric's baseline, the baseline engine takes into account such things as seasonality and trends.

- **Seasonality** - When a repeated pattern at constant time intervals occurs, a metric has seasonality. For example a metric might have typical values at 8:00 every day when users log on, and different values at 12:00 when users take a break.
- **Trends** - When a metric's values have a consistent linear change over time, a trend is identified.

Seasonality and trends are considered to be part of the normal behavior of a metric, and the baseline sleeve is adjusted accordingly.

- **The Analytics Engine**

The Analytics engine, reads metrics from the SHA database at 5 minute intervals, and as part of an ongoing process, calculates the baseline sleeve for each metric.

- **Anomalies**

An anomaly represents anomalous behavior in a part of an IT system. An anomaly consists of

CIs, links between CIs, and metric values that are measured for the CIs. Links between CIs can represent a physical or logical dependency between the CIs. Metrics are measured for the CIs that had anomalous values during the anomaly time frame. When an anomaly is detected, an SHA event is generated which is used to alert an operator of an existing problem in the enterprise.

For more information, see ["The Anomaly Life Cycle" \(on page 62\)](#).

This section includes:

How a Metric is Added to an Anomaly	59
The Anomaly Life Cycle	62
Identifying Similar Anomalies	63
Identifying Similar Patterns	64
How To Process a Service Health Analyzer Event	65
How to Filter SHA Events	69
How to Investigate an Anomaly	70
Anomaly Highlights Page	71

How a Metric is Added to an Anomaly

The SHA engine continually monitors metrics for abnormal behavior. Service Health Analyzer uses specific behavior to change the status of a metric from a regular metric to a metric that takes part in an anomaly. An anomaly might indicate that there is a problem with the monitored enterprise component.

Once you select a CI to be monitored by SHA, metric values are collected for that CI, and a baseline is calculated for the metric. Once a baseline exists for a metric, it can be included in an anomaly.

A metric is added to an anomaly as follows:

1. **A metric becomes a traced metric.**

At specified intervals, SHA checks the value of a metric sample at each point in time (metric point) against the metric's predefined **baseline threshold** at that metric point.

If at a metric point, a metric sample and its value deviates from its predefined **baseline sleeve**, or the metric displays availability abnormality, the metric becomes a **traced metric**.

2. **A traced metric becomes a continuously abnormal metric.**

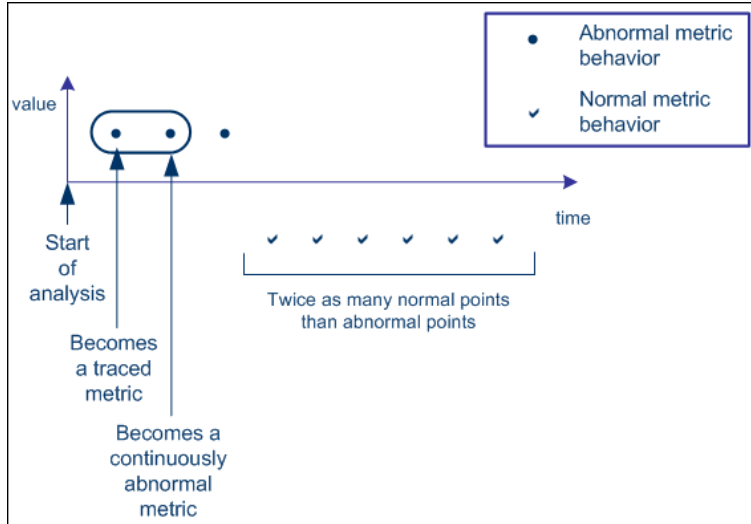
SHA also checks the behavior of a metric over time, and uses the **Abnormal event factor** infrastructure setting, a ratio between normal and abnormal sample values to determine how to classify the traced metric. For a metric to become continuously abnormal, its values must deviate from the baseline sleeve, or become unavailable, and have enough abnormal samples to be considered abnormal.

The minimum number of abnormal samples is calculated based on a learned value which represents the probability of a metric having an abnormal sample.

For example, if the **Abnormal event factor** infrastructure setting is 2 (the default setting), and the metric has two abnormal and one normal points, it is considered to be an **continuously abnormal metric**.

If the metric has two normal and one abnormal point, it is considered to be a normal metric.

In the example below, the first metric sample is abnormal, so the metric becomes a traced metric. The second point is abnormal, so the metric becomes a continuously abnormal metric. At that point the continuously abnormal metric is added to a new or to an existing anomaly. From the third point (abnormal) until the fifth normal point the metric continues to be a continuously abnormal metric.



The details of continuously abnormal metrics are stored in the online memory in the Analytics engine, until the metric behavior returns to normal. A metric is considered to be normal if the ratio between normal and abnormal samples is such that it satisfies one of the following:

- a. Normal samples > Abnormal Samples*Abnormal-event-factor
- b. The metric has a "normal tail". This means that the metric's time series ends with a series of sufficient consecutive normal samples.

Note: If a metric behaves abnormally but the time period between two abnormal metric points is longer than the time specified in the **Anomalies Time Cluster Distance** infrastructure setting, SHA ignores the first metric point, and the second metric point becomes a traced metric. Because such a metric never accumulates enough abnormal or normal metric points to calculate if its behavior is abnormal, it is considered as noise. If a metric is scheduled to report every x minutes where $x > \text{Anomalies Time Cluster Distance}$, it is never added to an anomaly.

3. **The SHA engine adds the continuously abnormal metric to an existing anomaly.**

The SHA engine creates a new anomaly, or adds a continuously abnormal metric to an existing anomaly as follows:

- **According to the start time.** If the start time of the continuously abnormal metric is close to the start time of an anomaly, and the metric belongs to the same RTSM model, the continuously abnormal metric is added to the anomaly. A close start time occurs when the difference between the time when the metric become continuously abnormal and the anomaly start time is less than the value of the **Anomalies Time Cluster Distance** setting defined in Infrastructure Settings.

Note:

- The SHA engine starts a new anomaly if there is no existing anomaly that fulfills the conditions described above.
- A metric is added to an anomaly only if the metric abnormal start time is within time cluster distance range after the anomaly start time.

4. **The SHA engine determines if the anomaly is significant.**

The engine calculates the probability of encountering the metric events if there was no anomaly. If it is determined that this probability is low, in other words there is a great probability that the detected anomaly represents a real problem, the anomaly is considered to be significant and is created.

For more information, see "[The Anomaly Life Cycle](#)" (on page 62).

For more information on how to edit infrastructure settings, see "[How to Edit an SHA Infrastructure Setting](#)" (on page 157).

The Anomaly Life Cycle

The following can occur in an anomaly life cycle:

1. Open Anomaly Event

When SHA creates an anomaly, an **Open Anomaly Event** corresponding to the anomaly is converted into an event using the Event Channel, and can be tracked in the Operations Management Event Browser, or in the HP ServiceCenter/HP Service Manager.

Several events may be sent to the Operations Management Event Browser for an anomaly, such as an event for each representative CI of the anomaly. The representative CI appears in the Operations Management Event Browser as a "related CI" of the event.

Example: If an anomaly contains several business application CIs, in some cases an event will be sent separately for each business application CI. Each event is however sent in the context of the same SHA anomaly.

The anomaly's metric information is stored in the Analytics engine as an anomaly during the whole time the anomaly is open. If the Analytics engine fails during that period, this data is lost.

2. Update Anomaly Event

During the following analysis cycles, SHA continues to analyze the metrics for abnormal behavior.

A metric is added to an anomaly when it becomes a continuously abnormal metric, its start time is close to an anomaly's start time, and it belongs to the same RTSM model.

SHA issues an **Update Anomaly Event** corresponding to the anomaly to the Event Channel. The event can be tracked in the Operations Management Event Browser, or in the HP ServiceCenter/HP Service Manager.

Note: Updated anomaly information can be viewed in the Anomaly Highlights page. For more information, see ["Anomaly Highlights Page" \(on page 71\)](#).

3. Close Anomaly Event

An anomaly can consist of several continuously abnormal metrics, as described in ["How a Metric is Added to an Anomaly" \(on page 59\)](#). When the last metric included in the anomaly returns to normal, the anomaly is closed. SHA issues a **Close Anomaly Event**. The anomaly and the metrics information are stored in the Profile database to be used in future investigations or as recent or historical anomalies used in the similarity analysis process.

For task details, see ["How To Process a Service Health Analyzer Event" \(on page 65\)](#).

Identifying Similar Anomalies

When Service Health Analyzer detects an anomaly, it uses a similarity analysis process to find similarities between the current anomaly and previously saved anomalies. By viewing similar anomalies you may be able to identify the causes and solutions of the current anomaly.

SHA compares different anomalies as described below, and when an anomaly fulfills the similarity requirements, it is added as a similar anomaly in the Anomaly Highlights page. The similar anomaly list may also contain hypertext links to the similar anomaly, and to its ticket ID. For more information, see "[Anomaly Highlights Page](#)" (on page 71).

You can customize the similarity analysis by modifying the defaults of the similarity analysis parameters in the **Service Health Analyzer - Similarity** section of the Infrastructure settings for Service Health Analyzer.

For more information on how to edit infrastructure settings, see "[How to Edit an SHA Infrastructure Setting](#)" (on page 157).

Comparison

The similarity analysis compares the current anomaly with another anomaly, and returns a similarity score. If the similarity score is higher than the configured **Similarity Threshold** parameter, the anomaly is added to the Anomaly Highlights page as a similar anomaly.

The similarity score is calculated using an algorithm that takes into account such things as matching CI Types and metrics, and common CI Types in each anomaly.

For example: when we compare Anomaly A1 with Anomaly A2 and Anomaly A3, the anomaly that is most similar to A1 is A3.

- **Anomaly A1:** 2 CIs of CI Type T1, 2 CIs of CI Type T2, 2 CIs of CI Type T3
- **Anomaly A2:** 2 CIs of CI Type T1, 2 CIs of CI Type T4, 2 CIs of CI Type T5
- **Anomaly A3:** 2 CIs of CI Type T1, 2 CIs of CI Type T2, 2 CIs of CI Type T6

Identifying Similar Patterns

A pattern investigation is an investigation that has been manually assigned a pre-defined pattern. You assign a pattern to an anomaly investigation in the Investigation Properties dialog box. For user interface details, see ["Investigation Properties Dialog Box" \(on page 130\)](#).

When Service Health Analyzer detects an anomaly, it compares the newly detected anomaly with the existing pattern investigation using the similarity analysis process on pattern investigations instead of on anomalies. The existing pattern investigations might provide solutions to the problem that caused the current anomaly.

Service Health Analyzer compares the newly detected anomaly with existing anomalies. For concept details, see ["Identifying Similar Anomalies" \(on page 63\)](#).

The similarity criteria processes the relevant similar pattern investigations and anomalies, and displays the selected elements in the Suspects area of the Anomalies Highlights page. For user interface details, see ["Anomaly Highlights Page" \(on page 71\)](#).

Suspect Pattern Investigation

During the investigation process, the existing pattern investigations are examined. While running, the similarity analysis process calculates a similar pattern score based on the similarity criteria for each existing pattern investigation. Service Health Analyzer compares the similar pattern scores with a pre-defined threshold. If the score is above the threshold, the pattern investigation is considered a suspect and is listed in the Suspects area in the ["Anomaly Highlights Page" \(on page 71\)](#).

The threshold is configurable in the **Pattern Suspect Similarity Threshold** infrastructure setting.

For more information on how to edit infrastructure settings, see ["How to Edit an SHA Infrastructure Setting" \(on page 157\)](#).

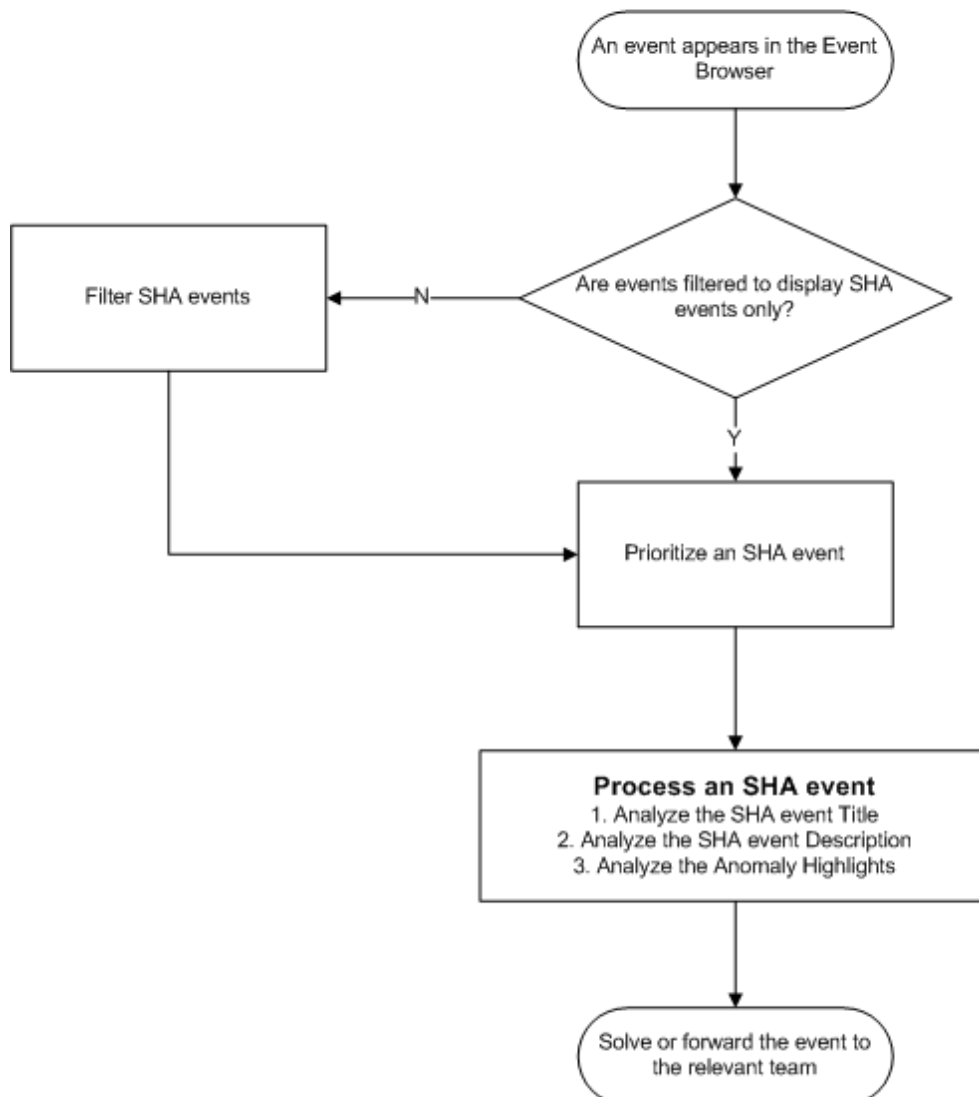
How To Process a Service Health Analyzer Event

Service Health Analyzer (SHA) events are predictive, and can act as an early warning for an operator who can process an event before the full impact is felt by the business. An SHA event or anomaly is generated based on several algorithms that determine whether a particular metric has consistently deviated from baseline thresholds over a period of time. An SHA event details can be used by the operator to analyze the root cause of the SHA event, and to either provide a solution, or forward the event to a relevant subject matter expert (SME) to process.

SHA events differ from regular Operations Management events because they are predictive and are the result of a combination of many metrics. Because of this, an SHA event might warn you of an anomaly in a metric that needs addressing, but still not categorize the anomaly as requiring immediate attention, because that particular anomaly has no effect on the business application.

The following is a typical workflow that describes how to process an SHA event.

SHA Event Operator Workflow



1. Identify an SHA event

Operations Management processes events from a number of data sources. You must first identify an SHA event.

- On the **General** tab of the Event Details pane, the **Event Type Indicator** field has a format of Predictive health: <Value>.
- (Optional) Create a filter to display SHA events only, and then select the filter. For more information, see ["How to Filter SHA Events" \(on page 69\)](#).

Tip: It is best practice to create a filter that only displays SHA events.

2. Prioritize an event

Once an SHA event has been identified, you can prioritize the SHA event as explained below. An SHA event is a result of an analysis of abnormal metrics and their effect on application performance and availability.

- a. Check the severity of the SHA event.
- b. Check the Event Type Indicator (ETI) value.

Note: An ETI value is aligned to a Severity type in the Server Health application. The correlation between ETI values and Severities, can be viewed in **Admin > Service Health > Repositories**, when you select the **Predictive Health** indicator .

- c. Based on a combination of the ETI value and the Severity, you can prioritize an SHA event as described in the following table.

Event Type Indicator and Severity Table

Event Type Indicator value	Severity	Description
Critical	Critical	Business metrics are affected, and the SHA event requires immediate attention.
Infrastructure	Minor	There is abnormal behavior in the infrastructure layer, however the application is still functioning satisfactorily, and the business layer remains unaffected. For example if a server in a server farm crashes, the application layer may still function satisfactorily even though the server farm is running one server short. The Severity level in such a case is minor which indicates the SHA event requires attention, but not necessarily immediate.
Known Issue	Minor	The anomaly is similar to a previous anomaly that was assigned a pattern of known issue by an SME, and a solution to the problem may be available.

Event Type Indicator value	Severity	Description
		The SHA event requires attention, but not necessarily immediate.
Noise	Normal	<p>The anomaly is similar to a previous anomaly that was assigned a pattern of noise by an SME. These types of anomalies can normally be ignored.</p> <p>For example, you can configure an anomaly with a noise pattern, if you know that a particular resource usage of a CI will be high at a particular time of the day, and that it does not require immediate attention. Once configured as noise the CI will still generate an event, but it will be assigned a severity of Normal.</p>
Reoccurrence	Major	The anomaly is similar to a previous anomaly that was assigned a pattern of Reoccurrence by an SME. These type of events require immediate attention, and a solution to the problem may also be available.
Warning	Warning	The SHA event requires immediate attention.

3. Use the event title to analyze an event

On the **General** tab of the Event Details pane, the **Title** field contains either specific information on the root cause of the SHA event, or provides information that assists you in isolating the root cause of the SHA event.

This information is used to solve the problem, or to decide to whom the SHA event should be forwarded.

In the **Title** field, the following information if available is displayed:

- The name of the Related CI, and if available an additional identifier of the CI, for example its IP address or FQDN.
- **Suspects** - The following types of suspects are displayed:
 - **Pattern** - An anomaly can be manually assigned a pre-defined pattern. During the analysis, the similarity analysis process compares the similar pattern score with a pre-defined threshold. If the pattern score is above the threshold, the pattern is included as a suspect.
 - **Downtime** - When one of the affected CIs been configured as having downtime.
 - **Verification** - When an automatically executed verification tool failed for one of the affected CIs.

Note: By default, up to five items comprised of the above suspect types are listed.

The listing order is in the same order as the suspect types above.

- **Layers** - Abnormal metrics are divided per layer. If 90% of the abnormal metrics belong to a single layer, the layer is included in the additional information.

- **Additional Information** – The following is displayed:

Abnormal Metrics - By default, the first five abnormal metrics included in the specified layer are displayed.

- **Business Impact** – Lists the applications that might be affected, and the effect on users and SLAs.

4. Use the description to analyze an event

On the **Additional Info** tab of the Event Details pane, the **Description** field contains the contents of the event title and the following additional information that may assist in processing the SHA event.

- A link to the Anomaly Highlights Window.
- **Timeframe** – The start time and end time of the anomaly.
- **Location** - Locations affected.
- **Similarities** – Other SHA events that were similar to the currently selected one. Similar SHA events are given a closeness percentage to the current SHA event score, where 100% is identical.

5. Use the Anomaly Highlights to analyze an event

On the **Additional Info** tab of the Event Details pane, the **Description** field content contains a link to the Anomaly Highlights window. Information in the Anomaly Highlight page, is used to assist in identifying the root cause of the anomaly, or help determine which support team is responsible for further investigation of the anomaly.



The Anomaly Highlights window:

- Includes the details of the anomaly in an easy to read format.
- Enables you to link to similar SHA events (anomalies) by the timestamp of the anomaly, or by its ticket number.
- The **Investigate Further** button, acts as a portal for SMEs who wish to further investigate an SHA event.
- May include links to more detailed reports for various suspects, additional information, and business impact items.

For more information on the Anomaly Highlight window, see "[Anomaly Highlights Page](#)" (on [page 71](#)).

How to Filter SHA Events

This task describes how to filter Service Health Analyzer events in the Operations Management Event Browser.

1. From the Event Browser, open the Select an Event Filter dialog box using the **Event Filter**  button.
2. From the Select an Event Filter dialog box, open the Filter Configuration dialog box using the New Item  button and select **Advanced Filter**.
The Filter Configuration dialog box opens.
3. Enter a name and description for the new filter.
4. Assemble the SHA filter by dragging the ETI Resolution Hint Advanced Property to the Filter Definition pane.
5. In the Edit Expression Dialog box, from the drop down, select **Contains**, enter *Predictive_Health_ETI* in the text box, and then click **OK**.
6. To filter SHA events, use this filter.

How to Investigate an Anomaly

This task describes the workflow for investigating an anomaly.

1. Process the Service Health Analyzer event.

For more information, see ["How To Process a Service Health Analyzer Event" \(on page 65\)](#)

2. Investigate the anomaly further.

- a. Use the Topology View.

For more information, see ["How to Use the Topology View" \(on page 88\)](#).

- b. Use the Metrics View.

For more information, see ["How to Use the Metrics View" \(on page 106\)](#)

Note: Once you save an anomaly from the Topology or Metrics views, it becomes an investigation. When you save an anomaly, it is recommended that you add investigation properties to the anomaly. Investigation properties are used when Service Health Analyzer creates the Anomaly Highlights, and can provide useful information for solving future anomalies.

Anomaly Highlights Page

This page displays the details of the selected anomaly, and links to other similar anomalies.

Timeframe:

- Started at 10/18/11 9:54 AM, no end date.

Suspects:

- Known Issue
Suspect due to Known Issue
- Downtime
Suspect due to downtime: Exchange server planned downtime
[Downtime](#)
- vmamind87.devlab.ad (Windows/Infrastructure)
Failing tools: dataCollector-CPU, dataCollector-...
- Suspect Layer: NETWORK
Abnormal transaction behavior.

Additional Information:

- HR Portal (BusinessApplication/application_and_services)
Abnormal metric: CPU Utilization
[Run Books](#)

Business Impact:
Status of relevant SLA as of 11/9/11 10:15 AM:

- OLA - Failed
[SLM Report](#)

1 applications/services that might be affected:

- HR Portal
89 users out of 107 are experiencing problems as of 11/9/11 10:15 AM
[RUM Report](#)

3 locations are affected:

- New York (2 locations)
- London (1 location)

Similarities:

- 11/8/11 12:20 PM Similarity score: 91%
- 11/8/11 7:50 PM Similarity score: 78%

Note: The details are not yet final since the information is still being gathered. Try to reinvoke later for final results.

Close Investigate Further Copy to Clipboard Help

To access	<ul style="list-style-type: none"> In Operations Management, select an SHA event. On the Additional Info tab of the event, in Description click the hyperlink to open the Anomaly Highlights window. In Service Health, in the 360° View Hierarchy, click the down arrow, or right-click on a name instance, navigate to Go To, click Go to Service Health Analyzer.
Relevant tasks	"How To Process a Service Health Analyzer Event" (on page 65)

User interface elements are described below (unlabeled elements are shown in angle brackets>):

UI Element	Description
<areas>	The Anomaly Highlights window displays the following areas: <ul style="list-style-type: none"> • "Timeframe Area" (on page 72) • "Suspects Area" (on page 72) • "Additional Information Area" (on page 74) • "Business Impact Area" (on page 74) • "Similarities Area" (on page 75)
Copy to Clipboard	Copies the anomaly highlights information to the user clipboard.
Investigate Further	Opens the SHA Topology view. For more information, see "Topology View Tab" (on page 91) , and "Metrics View Tab" (on page 111) .
Close	Closes the Anomaly Highlights page.

Timeframe Area

This area displays information about the start and when relevant the end of the anomaly's time frame.

Suspects Area

This area displays the anomaly's suspects. Up to five suspects are listed in the suspects area. Suspects are ordered as follows: Pattern Suspects, Downtime, Failed Verification Tools and associated CIs. For more information, see [Suspect Types](#).

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element	Description
<Pattern suspects>	Lists pattern suspects that are similar to the current anomaly. A pattern becomes suspect when the similarity between the current anomaly, and a previous anomaly that was defined with a pattern, breaches the predefined Pattern Suspect Similarity Threshold . For information on editing infrastructure settings, see "How to Edit an SHA Infrastructure Setting" (on page 157) .
<Pattern suspect> <link>	This link is associated with a <Pattern> entry. Opens a window that displays the following information: <ul style="list-style-type: none"> • <Pattern>. The name of the pattern. • Description. The description of the investigation as entered in the Description field in the Save Investigation dialog box.

UI Element	Description
	<ul style="list-style-type: none"> • Modified By. The name of the user who assigned the pattern to the investigation. • Date. The date the investigation was created. • Investigation Id. The ID of the investigation. • Comments. The comments entered by the user.
Downtime	Lists CIs with downtime status that are part of the anomaly, followed by information about the specific downtime. For more information about downtime, see "Downtime Management" in <i>Platform Administration</i> .
Downtime <link>	<p>This link is associated with a Downtime entry.</p> <p>Displays the downtime properties. The link appears on the right of the downtime entry. A downtime entry is listed when at least one of the anomaly CIs has a downtime configuration. The Downtime Properties dialog box displays details about the relevant downtime. For details about downtime, see "Downtime Management" in <i>Platform Administration</i>.</p> <div data-bbox="459 884 1385 1350" style="border: 1px solid black; padding: 10px;"> <p>Downtime Properties</p> <p>Name: Application Maintenance Description: Service Maintenance Is Planned: Yes Category: Maintenance Timeframe: Started at Sun Jan 03 10:32:31 PST 2010 TimeZone: Pacific Standard Time</p> <p style="text-align: center;">Close</p> </div>
Verification Tool	Lists the name the failed verification tools followed by the SiteScope template name. The verification tools are ordered according to the start of their verification time. For user interface details, see " Verification Tools Tab " (on page 52).
<Layer name>	<p>Lists the name of a problematic layer and its metrics if the percentile of metrics in the problematic layer of the CI topology is larger than The percentile to determine distinct layers infrastructure setting.</p> <p>For information on editing infrastructure settings, see "How to Edit an SHA Infrastructure Setting" (on page 157).</p> <p>The default percentile is 0.9, meaning that 90% of the abnormal metrics must belong to a distinct layer for a layer to be displayed in the Suspects area.</p> <p>One of the following layers can be reported: Database, Network, Application,</p>

UI Element	Description
	<p>Client, or Infrastructure.</p> <p>Example: Suspect Layer: Network</p>

Additional Information Area

This area displays Additional Information of the anomaly, and includes whether a specific layer is prominent in the anomaly, the affected CIs and the abnormal metrics.

UI Element	Description
<CI name>	Lists the CIs that have abnormal metrics, and the first abnormal metric for the specified CI. The default layers are Infrastructure and Software, and can be edited in The Layers that the suspects should be collected from infrastructure setting for Service Health Analyzer.

Business Impact Area

This area displays SLAs, Application or Service CIs and the locations affected by the anomaly.

UI Element	Description
<SLA>	Lists the current SLAs that are affected by the anomaly. Each SLA is followed by the worst status of the SLA. This information is independent from the anomaly's time frame.
SLM Report <link>	<p>This link is associated with an <SLA> entry.</p> <p>This link opens the SLA Summary report for the relevant SLAs. The report displays the list of SLAs and their current worst status in the SLA Summary report. For user interface details, see "SLAs Summary Report" in <i>Using Service Level Management</i>.</p>
<nn> applications/services	<p>Displays the number (nn) of Application or Service CIs that might be affected by the problem detected by the anomaly, and the following information:</p> <ul style="list-style-type: none"> • A list of each application or service CI. • The number of Real User Monitor users using the impacted applications or services. • The timestamp when the anomaly started and the users were impacted.
RUM Report <link>	<p>This link is associated with an <application/services> entry.</p> <p>This link opens the RUM Application Health report for the relevant Application or Service CI. The report displays the general status of a selected application by viewing different aspects of its performance,</p>

UI Element	Description
	availability, load, and impact on end users. For user interface details, see "Application Health Report" in <i>Using End User Management</i> .
<Locations>	<p>By default, lists up to 5 main locations that participated in the anomaly. A location is followed by the number of satellite locations.</p> <p>Note:</p> <ul style="list-style-type: none"> You can edit The number of locations to calculate infrastructure setting. <p>For information on editing infrastructure settings, see "How to Edit an SHA Infrastructure Setting" (on page 157).</p> <ul style="list-style-type: none"> To manage the satellite location information, see "Location Manager Page" in <i>Platform Administration</i>.

Similarities Area

This area displays the past anomalies, that have characteristics similar to this anomaly. The similar past anomalies might help you solve the problem associated with the active anomaly.

UI Element (A–Z)	Description
Similar Past Anomalies	<p>By default, lists up to 5 previous anomalies that have characteristics similar to this one, and their similarity value is greater than the Similarity Threshold infrastructure setting.</p> <p>With each anomaly, where relevant, the following Links are provided:</p> <ul style="list-style-type: none"> The hyperlink link on the timestamp, links to the Topology and Metric views. The hyperlink on the Ticket ID, links to the Ticket ID associated with an existing HP Service Manager incident. The ticket might contain information on how to solve the problem. <p>Note: Hyperlinks on a ticket ID only appear when HP Service Manager is integrated with BSM.</p> <p>Past anomalies that are listed, were associated with events or Service Manager incidents.</p> <p>Various settings relating to similar anomalies can be found in the Infrastructure Settings Manager in the Service Health Analyzer - Similarity Analysis section. They include the Similarity Threshold, Number of Similar Anomalies, Modifying the Ticket System URL, and Maximum Capacity for Similarity Anomalies.</p>

UI Element (A–Z)	Description
	<p>For information on editing infrastructure settings, see "How to Edit an SHA Infrastructure Setting" (on page 157).</p> <p>For more conceptual information, see "Identifying Similar Anomalies " (on page 63).</p> <p>For details on configuring HP Service Manager and HP Business Service Management integration, see <i>Solutions and Integrations</i>.</p>

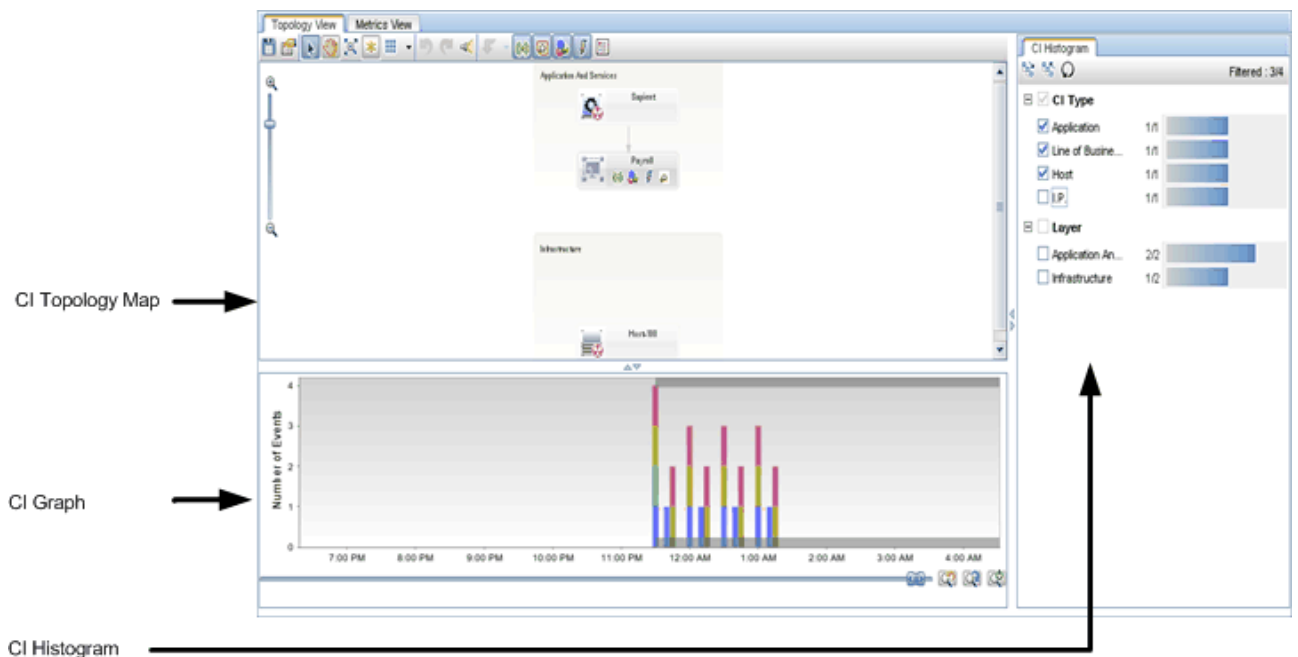
Investigating with the Topology View Overview

You can use the Topology View to investigate the root cause of an anomaly. The Topology View is most likely to be used by an infrastructure owner or an application manager who wants to analyze in greater detail the causes of an anomaly, and solve potential business performance and systems issues before they escalate.

Note: If you access the Topology View from a previously saved investigation, the view might also include manually revealed CIs that are related to CIs in the anomaly.

The Topology View consists of the following:

- **CI Topology Map** - Provides you with an interactive graphic representation of CIs that are associated with an anomaly. Connecting lines between CI nodes, represent the relationships between the CIs.
- **CI Graph** - Displays a stacked bar graphical representation of special events that occurred in a given time frame. You can change the time frame, and drill down on each special event for further details. Special events include: OM events, Discovered Changes, Downtime, and Incidents.
- **CI Histogram** - Provides a means to quickly view the distribution of CIs in the Topology Map by selecting CI Types and Layer properties.



This section includes:

Topology Map Layout Modes	79
Default Layers in Topology Map	80

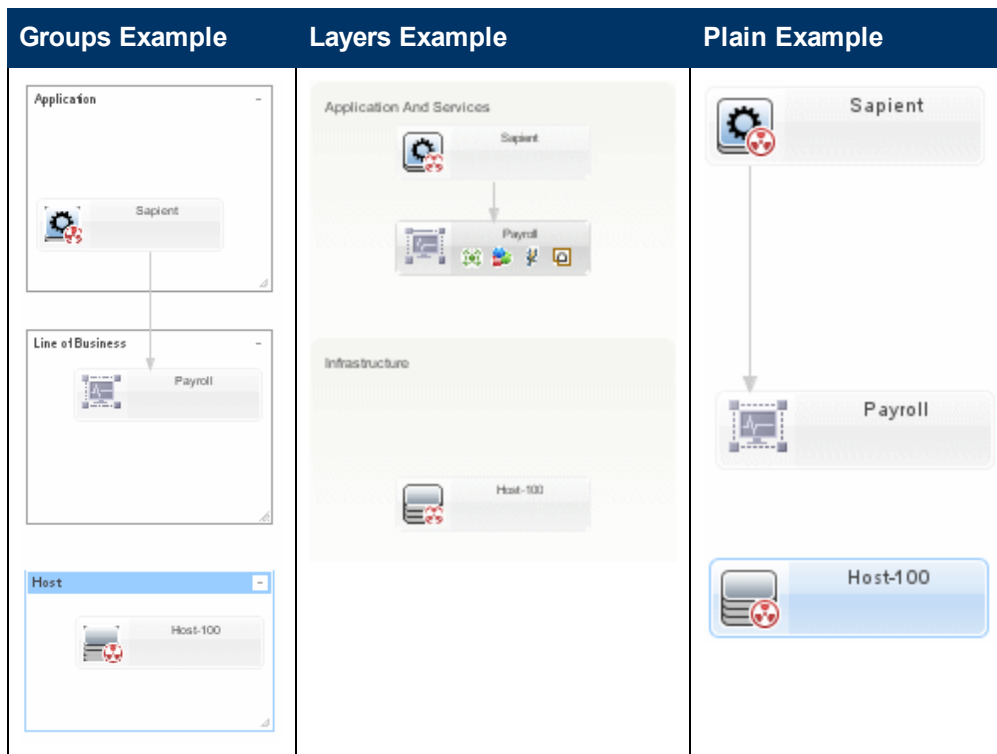
Learn About the CI Node in a Topology Map.....	81
Location of a Manually Added CI.....	84
Drilling Down in the Topology View.....	85
How to Use the Topology View.....	88
How to Use the Reveal Mode.....	90
Topology View Tab.....	91

Topology Map Layout Modes

The different layout modes enable you to customize the visual layout of the CIs in the Topology Map pane.

You can customize your layout using the following layout modes:

- **Groups** - Displays CIs inside their respective group boxes. CIs are assigned to groups in the RTSM.
- **Layers** - Displays CIs grouped into functional layers, such as **Facilities, Applications and Services, Software, Business Enablement, and Infrastructure**. Layer contents are static, and CIs cannot be removed from or added to a layer in the Topology Map. Within the layer mode, CIs are assigned to default layers based on their CI Type attributes defined in the RTSM. For more details on layers, see "[Default Layers in Topology Map](#)" (on page 80).
- **Plain** - Displays CIs, and is not grouped by groups or layers. This layout enables you to freely move CIs anywhere in the Topology Map pane according to your needs.



Default Layers in Topology Map

Within the layer mode, CIs are assigned to default layers based on their CIT attributes within the RTSM. The following section describes each of the layers that are defined out-of-the-box.

- **Business Enablement** - This layer contains business services, processes, and activities. These include both business services which a business provides to another business (or one organization provides to another within a business), and IT services which an IT organization provides to support business services or IT operations.

A Business Service typically has an associated end-user or customer, a business application, and a service level agreement. Examples include payment processing, backup and recovery, and self-service help desk.

- **Application and Services** - This layer contains applications and their core components, not including elements that are deployable. An application is a set of components which supports a business activity, which is seen as a whole, and is known by a specific name.

The Application and Services layer also includes business transactions, as well as infrastructure services that support business services and processes. Examples include voice and network services, database services, backup and restore services, desktop services, and Windows administration services.

- **Software** - This layer includes individual installations of software elements. These are executables that can be deployed, or are deployed, on a logical system.
- **Infrastructure** - This layer includes logical systems such as virtualization and clustering, and physical systems such as storage devices, network devices, and servers.
- **Facilities** - This layer includes locations, sites, buildings, rooms, racks, and so on.

Learn About the CI Node in a Topology Map

Event type icons are displayed on a CI node when an event type is associated with a CI in the anomaly. Only events that occurred in the selected time frame in the CI Graph pane are represented on the CI node. The event types include; incidents, events, discovered changes, downtime, and planned changes. If a CI is associated with an abnormal metric, the abnormal metric icon is also displayed on the CI.



Event type icons behave as follows:

- Event type icons are displayed for the currently selected time frame in the CI Graph pane.
- Event type icons are only displayed for the selected CI nodes in the Topology Map. When you click out of selected CI nodes, event icons are re-displayed for all CI nodes.
- A maximum number of discovered Changes, events, and incidents can be displayed in the Topology View or CI Graph at any one time. The values are held in the **Max number of Discovered changes to fetch for the UI**, **Max number of events to fetch for the UI**, and **Max number of incidents to fetch for the UI** infrastructure settings. Their default values are 300.

For more information on how to edit infrastructure settings, see ["How to Edit an SHA Infrastructure Setting" \(on page 157\)](#).






Caution: If one of the special events exceeds the Max number configured, none of that type of special event will be displayed in the UI.

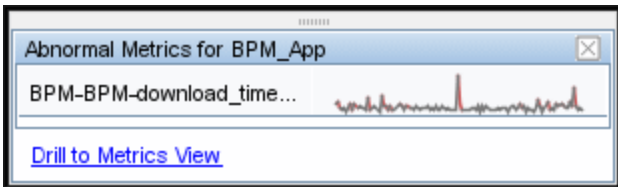
If you do not want to change the infrastructure setting, you can alternately select a shorter time frame, or select in the Topology Map to display events for specific CIs only.






- By default closed events are not displayed in the UI. To display closed events, change the **Show closed events in UI** in the Service Health Analyzer Infrastructure settings to true.
- By default events with a severity status of Critical, or Major are displayed in the UI. To display events with other severity statuses, change the **Events severities to show in SHA UI** in the Infrastructure settings.
- You can edit the fields displayed in the Incidents, Event, and Planned Change tables by editing the Displayable Attributes for Incident, Displayable Attributes for Event, and the Displayable Attributes for Planned Change in the Service Health Analyzer Infrastructure settings.
- When you click an icon on a CI node, a relevant event type table opens displaying relevant information, as detailed in the examples below.

Note: Clicking a column header in an event type table will sort the relevant column.

The following table describes the event types and icons.

Icon	Event Type																								
	<p>Incidents. Indicates that the CI is associated with incidents received from the HP Service Manager. Incidents are represented by a purple bar in the CI Graph pane.</p> <p>To display incidents, BSM must be integrated with HP ServiceCenter/HP Service Manager.</p> <table border="1"> <caption>Incidents for Gold Employee Service</caption> <thead> <tr> <th>Description</th> <th>Open Time</th> <th>Close Time</th> <th>Status</th> <th>Solution</th> <th>Urgency</th> </tr> </thead> <tbody> <tr> <td>IM2004 Sales reps complain that it takes long time to place new orders</td> <td>7/20/11 4:40 PM</td> <td>7/20/11 4:40 PM</td> <td>open</td> <td></td> <td>2_high</td> </tr> <tr> <td>IM2006 Sales reps complain that it takes long time to place new orders</td> <td>7/21/11 10:45 AM</td> <td>7/21/11 10:45 AM</td> <td>open</td> <td></td> <td>2_high</td> </tr> <tr> <td>IM2007 Users experience problems with the HR Portal</td> <td>7/21/11 12:30 PM</td> <td>7/21/11 12:30 PM</td> <td>open</td> <td></td> <td>2_high</td> </tr> </tbody> </table>	Description	Open Time	Close Time	Status	Solution	Urgency	IM2004 Sales reps complain that it takes long time to place new orders	7/20/11 4:40 PM	7/20/11 4:40 PM	open		2_high	IM2006 Sales reps complain that it takes long time to place new orders	7/21/11 10:45 AM	7/21/11 10:45 AM	open		2_high	IM2007 Users experience problems with the HR Portal	7/21/11 12:30 PM	7/21/11 12:30 PM	open		2_high
Description	Open Time	Close Time	Status	Solution	Urgency																				
IM2004 Sales reps complain that it takes long time to place new orders	7/20/11 4:40 PM	7/20/11 4:40 PM	open		2_high																				
IM2006 Sales reps complain that it takes long time to place new orders	7/21/11 10:45 AM	7/21/11 10:45 AM	open		2_high																				
IM2007 Users experience problems with the HR Portal	7/21/11 12:30 PM	7/21/11 12:30 PM	open		2_high																				
	<p>Events. Indicates that the CI is associated with events from Operations Manager <i>i</i>. Events are represented by a green bar in the CI Graph pane.</p> <p>To display events in Operations Management, you need an OMi license.</p> <table border="1"> <caption>Events for Gold Employee Service</caption> <thead> <tr> <th>Title</th> <th>Description</th> <th>Severity</th> <th>Type</th> <th>Category</th> <th>Date</th> </tr> </thead> <tbody> <tr> <td>Gold Employee Service experiences a problem related to...</td> <td>Follow this link to open the anomaly highlights window...</td> <td>critical</td> <td></td> <td></td> <td>7/21/11 9:56 AM</td> </tr> </tbody> </table>	Title	Description	Severity	Type	Category	Date	Gold Employee Service experiences a problem related to...	Follow this link to open the anomaly highlights window...	critical			7/21/11 9:56 AM												
Title	Description	Severity	Type	Category	Date																				
Gold Employee Service experiences a problem related to...	Follow this link to open the anomaly highlights window...	critical			7/21/11 9:56 AM																				
	<p>Discovered Changes. Indicates that the CI is associated with discovered changes. Discovered Changes are represented by a blue bar in the CI Graph pane.</p> <p>To display discovered Changes, BSM must be integrated with HP Universal CMDB.</p> <table border="1"> <caption>Discovered Changes for scdam085</caption> <thead> <tr> <th>Date</th> <th>Changer</th> <th>Change Type</th> <th>Attribute</th> <th>Old Value</th> <th>New Value</th> </tr> </thead> <tbody> <tr> <td>7/21/11 9:41 AM</td> <td>Admin</td> <td>Added Relation to Hypervisor 25</td> <td></td> <td></td> <td></td> </tr> <tr> <td>7/21/11 9:40 AM</td> <td>Admin</td> <td>Removed Relation to Hypervisor 12</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Date	Changer	Change Type	Attribute	Old Value	New Value	7/21/11 9:41 AM	Admin	Added Relation to Hypervisor 25				7/21/11 9:40 AM	Admin	Removed Relation to Hypervisor 12									
Date	Changer	Change Type	Attribute	Old Value	New Value																				
7/21/11 9:41 AM	Admin	Added Relation to Hypervisor 25																							
7/21/11 9:40 AM	Admin	Removed Relation to Hypervisor 12																							
	<p>Planned Changes. Indicates that the CI is associated with planned changes events defined in HP ServiceCenter/HP Service Manager. Planned Changes are represented by a turquoise bar in the CI Graph pane.</p> <p>To display planned Changes, BSM must be integrated with HP ServiceCenter/HP Service Manager.</p> <table border="1"> <caption>Planned Changes for Gold Employee Service</caption> <thead> <tr> <th>Description</th> <th>Status</th> <th>Priority</th> <th>Start Time</th> <th>End Time</th> </tr> </thead> <tbody> <tr> <td>CR5003 Move scdam055 from Hypervisor 12 to Hypervisor 25</td> <td></td> <td>2_high</td> <td>7/21/11 9:30 AM</td> <td>7/21/11 9:30 AM</td> </tr> </tbody> </table>	Description	Status	Priority	Start Time	End Time	CR5003 Move scdam055 from Hypervisor 12 to Hypervisor 25		2_high	7/21/11 9:30 AM	7/21/11 9:30 AM														
Description	Status	Priority	Start Time	End Time																					
CR5003 Move scdam055 from Hypervisor 12 to Hypervisor 25		2_high	7/21/11 9:30 AM	7/21/11 9:30 AM																					
	<p>Abnormal Metrics associated. Indicates that the CI is associated with abnormal metrics.</p> <p>The abnormal table displays the names of the abnormal metrics and previews of the metrics data. The preview includes metric data from 5 hours before the anomaly start time, and up to 5 hours from the anomaly start time.</p> <p>A metric is associated with a CI when one of the metric's dimensions is the CI.</p>																								

Icon	Event Type
	 <p>Click Drill to Metrics View to display the listed metrics in the Metrics View.</p>

Icon	Event Type	Required Integration	Bar Color in Histogram
	Incidents	HP Service Manager	red
	Events	Operations Manager <i>i</i>	green
	Discovered Changes	HP Universal CMDB	blue
	Planned Changes	HP ServiceCenter/HP Service Manager	turquoise
	Abnormal Metrics associated	N/A	N/A

Location of a Manually Added CI

When you add a CI to the Topology Map using the **Reveal Mode** feature, the default location of the added CI in the Topology Map depends on the display layout type selected as follows:

- **Layers** - The revealed CI is added to its configured layer. Arrows indicate its parent and child CIs.

The default location of a revealed CI in the layout does not depend on the parent and child CI relationships, but on the layer the CI belongs to.

- **Plain** - Revealed CIs are located in proximity to their parent and child CIs as follows:
 - In proximity to its parent CI, if the added CI's parent CI is already displayed in the Topology Map.
 - In proximity to its child CI, if the added CI's child CI is already displayed in the Topology Map.
 - In proximity to its parent CI, if the added CI's parent and child CIs are already displayed in the Topology Map.

Arrows indicate the parent and child relationships.

- **Group** - Revealed CIs belonging to a specific group are located in that group in the Topology Map.

If the CI does not belong to a group, it is located according to the Plain layout logic.

For user interface details, see ["Topology View Tab" \(on page 91\)](#). For task details, see ["How to Use the Reveal Mode" \(on page 90\)](#).

Drilling Down in the Topology View

Drill downs in the Topology Map, provide a shortcut to a selection of domain reports for CIs that are part of the anomaly.

The drill down options available are determined by the CI Type.

Note: To drill down, in the Topology Map, right-click a CI and select an available drilldown.

The drill down options are as follows:

Drill down to	Data Collector	CI Types	Further Details
Application Health	BPM, RUM	business_application, business_transaction_flow, business_transaction	See Application Health Report in <i>Using End User Management</i>
RUM Event Summary	RUM	business_application, business_transaction_flow, business_transaction	For details, see RUM Event Summary Report in <i>Using End User Management</i> .
RUM Session Analyzer	RUM	business_application, business_transaction_flow, business_transaction	For details, see RUM Session Analyzer Report in <i>Using End User Management</i>
BPM Error Summary	BPM	business_application, business_transaction_flow, business_transaction	For details, see BPM Error Summary Report in <i>Using End User Management</i>
BPM Transaction Validation	BPM	business_application, business_transaction_flow, business_transaction	For details, see BPM Transaction Invocation in <i>Using End User Management</i>
CI Properties	All	All managed objects	Reports the properties of the selected CI.
KPIs Over Time	All	Configuration_item	For details, see "KPIs Over Time Report" in <i>Using Service Health</i> .
Performance Graphs	PA	host_node, exchangemailserver, j2eeserver, database, domaincontroller, globalcatalogserver, business_application, business_transaction	Displays performance graphs for the selected CI.
SLA Summary	All	Configuration_item	For CIs associated with SLAs

Drill down to	Data Collector	CI Types	Further Details
			For details, see SLAs Summary Report in <i>Using Service Level Management</i> .
Operations Management Tools	SiteScope, PA	Infrastructure element	Displays Operations Management tools for the selected CI.
SiteScope	SiteScope, NNMi, PA	Infrastructure element	Included in the dimensions of metrics collected by a SiteScope data collector. Displays a list of all the SiteScope servers that monitor the metrics or the CIs.
Diagnostics Layers View	All	business_transaction, node, running_software, j2eeapplication, mqchannel, mqqueue, mqqueuemanager, sqldatabase, sap_r3_server, sqlserver	For details, see Enabling Diagnostics Integration with BSM's Service Health Analyzer in the <i>HP Diagnostics Installation and Configuration Guide</i> .
Run Books	All	Infrastructure element	Requires HP Operations Orchestration application to be integrated with BSM. For user interface details about the run books, see Run Books Configuration Page in <i>Solutions and Integrations</i> .
NNMi	NNMi	Network node	For details see, " How to Install the SHA Network Node Manager i (NNMi) Data Collector " (on page 21).
Ping	All	Network node	For metrics whose dimensions include a CI with the Node type. This drill down pings the host instance represented by the CI.
Run TQL on <CI_name>			This drill down lists all the available TQLs. You can select to run a specific TQL to merge the topology configured in the TQL, to the active topology. For details, see " How to Create a TQL Drilldown " (on page 156).

How to Use the Topology View

Use the various tools in the Topology View to assist you in investigating the root causes of the anomaly.

Note:

- The default Topology Map displays associated CIs identified in the anomaly.
- The CI Graph and the Topology Map, display special events of selected CIs for the current time frame. For a new anomaly, the time frame of the anomaly is the default.
- If you select specific CIs in the Topology Map, or specific attributes or attribute values in the CI Histogram, the selections are reflected in the CI Graph.

The suggested flow is as follows:


1. Use the Topology Map

- a. View the Topology Map to and assess if its contents point to an obvious problem.

For example if a CI displays one or more event icons, then that CI might be a suspect for further investigation. For more information on event icons, see ["Learn About the CI Node in a Topology Map" \(on page 81\)](#).

- b. If several CIs display event icons, examine if they have a common parent.

If there is no visible common parent, you can use the reveal mode to identify and add associated CIs to the Topology Map.

For example, if two applications are having problems at around the same time, but at first glance, the Topology View does not display a link between these two applications, you can use the **Reveal Mode** icon  to display related CIs that were not included in the original Topology Map. For more information, see ["How to Use the Reveal Mode" \(on page 90\)](#).

Once you use the Reveal Mode, you may see in the Topology Map a link between the two applications and a virtual machine CI on which two applications are running.

- c. View the topology using different layout types to assess if the problematic CIs are common to a layer or group. For more information, see ["Topology Map Layout Modes" \(on page 79\)](#).
- d. Use the drill down functionality to access relevant domain reports, and get more information about the CI. For more information, see ["Drilling Down in the Topology View" \(on page 85\)](#).
- e. For a CI, when available, run TQLs that can add related CIs to the Topology Map.

For more information, see ["CI Topology Map Pane" \(on page 95\)](#).

2. Use the CI Graph

- a. Look for events that occur during, or in the minutes preceding the anomaly.

For example, if two events occurred before the anomaly, then these two events may be connected to the anomaly you are investigating.

- b. To improve the event focus, select CIs, or groups of CIs in the Topology Map, and look for events that occur during, or in the minutes preceding the anomaly.

When you select specific CIs in the Topology Map, events not involving the specific CI are removed from the CI Graph.

- c. Click on an specific event in the CI Graph to display more details about the event. When you click on an event, the CI the event belongs to becomes the focused CI in in the Topology Map.

For more information, see ["CI Graph Pane" \(on page 96\)](#)

3. **Use the CI Histogram**



The Topology Map and CI Graph contents, reflect the selections you make in the CI Histogram, and enable you to investigate in a more focused manner.

Select a CI attribute or attribute value, to display the CIs that belong to the selected categories.

For more information, see ["CI Histogram Pane" \(on page 98\)](#).


4. **Save an Investigation**

To save an anomaly as an investigation, or to save changes you made to an existing investigation, do as follows:


- a. On the Topology Toolbar, click  **Investigation Properties**, and add relevant investigation properties.
- b. Click Save  to save the investigation.

Note: If you make changes to the Topology Map within an existing investigation, for example you add CIs using the Reveal Mode feature, and then save those changes. The original investigation is overwritten by the current investigation.


How to Use the Reveal Mode

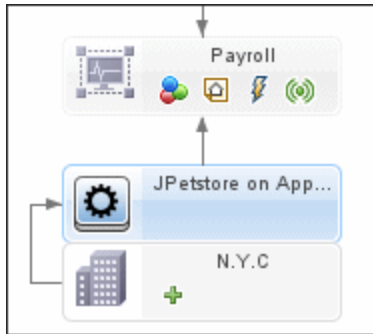
If two applications are having problems at about the same time, but the Topology View does not display a link between these two applications, you can use the **Reveal Mode** icon  to display related CIs that were not included in the original Topology Map.



Note: Added CIs will not have display baseline information or abnormal metrics.

1. Click **Reveal Mode** . This enables you to display CIs that are not part of the anomaly, but are connected to CIs that are part of the anomaly. Relationships between CIs are defined in RTSM Administration.
2. Click a CI, to reveal its neighboring CIs.



3. If the revealed CI displays a , you can click the revealed CI to reveal its connected CIs. If you click one of these child CIs, its child CIs are displayed, and its sibling CIs are no longer displayed.



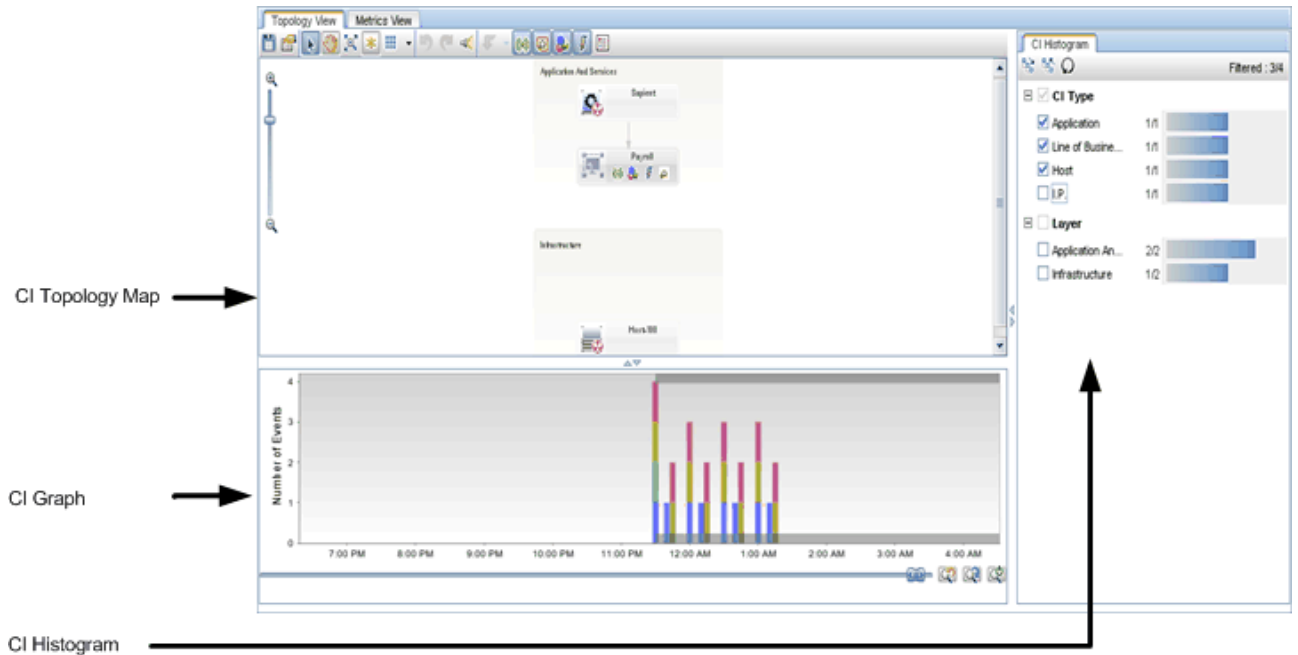
4. Click  on a revealed CI to add the CI and its parent CIs (up to the original CI clicked in the reveal process) to the Topology Map.
5. Click **Save Investigation** , to save the investigation to the database.

Note: You can retrieve a saved investigation by selecting **Applications > Service Health Analyzer**, and then double-clicking on the saved investigation.

Topology View Tab

The Topology View, displays the topology of the anomaly or saved investigation and consists of the following:

- The Topology Map pane displays a topology of the CIs associated with the anomaly.
- The CI Graph pane displays for a specified time frame special events that are related to the CIs in the topology.
- The CI Histogram pane displays CIs from the Topology Map categorized by CI Type and Layer.



<p>To access</p>	<p>Use one of the following:</p> <ul style="list-style-type: none"> • In Operations Management, select an SHA event. On the Additional Info tab of the event, in Description, click the hyperlink to the Anomaly Highlights window, and then on the Anomaly Highlights page, click Investigate Further. • In Service Health, in the 360° View Hierarchy, click the down arrow, or right-click on a name instance, navigate to Go To, click Go to Service Health Analyzer, and click Investigate Further. • For an existing investigation, select Applications > Service Health Analyzer, and double-click the relevant investigation. • You can access the Anomaly Highlights page via a link sent in an email alert, and then click Investigate Further.
<p>Important information</p>	<ul style="list-style-type: none"> • The CIs in the Topology Map are static. Icon representation of event types varies according to the selected time frame or the selected CI.











	<ul style="list-style-type: none"> • Only events that occurred in the selected time frame are visible in the Topology Map, and CI Graph. • When you select a CI in the Topology Map, the CI Graph displays only the event types associated with the selected CI. Event type icons for other CIs are not visible. <p>Note: To re-select all the CIs in the Topology Map, click out of the selected CI.</p> <ul style="list-style-type: none"> • When an event is selected in the CI Graph, the focus in the Topology Map changes to the CI that owns the selected event. • When an attribute, or attribute value is selected in the CI Histogram, the Topology Map and the CI Graph only display CI and event information relevant to the selected attribute or attribute value. • CIs that appear faded in the Topology Map, are not associated with events that occurred in the time frame that is currently displayed. • A maximum number of discovered changes, events, and incidents can be displayed in the Topology View or CI Graph at any one time. The values are held in the Max number of Discovered changes to fetch for the UI, Max number of events to fetch for the UI, and Max number of incidents to fetch for the UI infrastructure settings. Their default values are 300. <p>For more information on how to edit infrastructure settings, see "How to Edit an SHA Infrastructure Setting" (on page 157).</p> <p>Caution: If one of the special events exceeds the Max number configured, none of that type of special event will be displayed in the UI.</p> <p>Note: If you do not want to change the infrastructure setting, you can alternately select a shorter time frame, or select specific CIs until the maximum value is not reached.</p> <ul style="list-style-type: none"> • By default closed events are not displayed in the UI. To display closed events, change the SHA Infrastructure setting Show closed events in UI to true. • When you drill down from Service Health, if more than one anomaly is currently open for the selected CI, the anomaly for the CI with the highest severity is opened.
<p>Relevant tasks</p>	<ul style="list-style-type: none"> • "How to Use the Topology View" (on page 88) • "How to Use the Reveal Mode" (on page 90)






The Topology View page consists of the following:



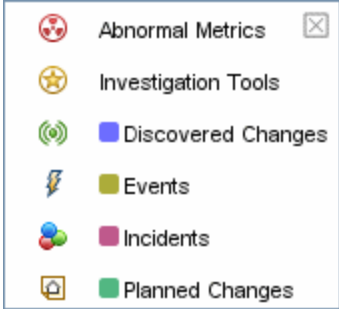






- ["Topology View Toolbar" \(on page 93\)](#)
- ["CI Topology Map Pane" \(on page 95\)](#)
- ["CI Graph Pane" \(on page 96\)](#)
- ["CI Histogram Pane" \(on page 98\)](#)

Topology View Toolbar

User interface elements are described below (unlabeled elements are shown in angle brackets>):

UI Element	Description
	<p>Save Investigation. Saves changes made to the Topology Map. For example if you:</p> <ul style="list-style-type: none"> • Manually change the location of a CI node in the topology. • Manually add a CI node in the topology, using the reveal mode, or using a TQL drill down. • Change the layout of the CI nodes in the Topology Map. • Group one or more CI nodes into groups (sub-topology). <p>Note: One investigation can be saved per anomaly. This means that when two users are working simultaneously on an investigation, the last save becomes the currently saved investigation for the anomaly.</p>
	<p>Investigation Properties. Enables you to add properties for the investigation. For details, see "Investigation Properties Dialog Box" (on page 130).</p>
	<p>Select. Enables you to select CIs or groups, and perform actions on the selected elements.</p> <p>Note: Click  to return to Select mode after using Pan.</p>
	<p>Pan. Enables you to drag the Topology Map within the Topology Map pane.</p> <p>Note: The pan works when the Topology Map is not set to Fit to screen mode.</p>
	<p>Fit to screen. Fits the Topology Map to the Topology Map pane, by expanding or reducing it. Relative proportions of the images are maintained.</p>
	<p>Show Links. Click, to toggle between hide, or display relationship links between CIs in the Topology Map.</p>
	<p>Layout. Enables you to view the topology map in different layouts. For more details, see "Topology Map Layout Modes" (on page 79).</p>
 	<p>Undo and Redo. Use to undo or redo operations you performed on the Topology View. Undo and Redo only works for changes made before you save the changes.</p>


UI Element	Description
	<p>Reveal Mode. Enables you to display neighboring CIs that are associated to CIs that are part of the current anomaly. Additional layers neighboring CIs can also be displayed. For details, see "How to Use the Reveal Mode" (on page 90).</p> <p>For details on the location of revealed CIs in the Topology Map, see "Location of a Manually Added CI " (on page 84).</p>
	<p>Drilldown to. Displays the list of drill down options available for the selected CI. The Drilldown to options vary depending on the data collector. For details, see "Drilling Down in the Topology View" (on page 85).</p>
	<p>Discovered changes. Displays in the CI Graph, discovered changes that occurred in CIs that are part of the anomaly, and that occurred during the currently selected time frame. Discovered changes are represented by a blue bar in the CI Graph.</p> <p>To display discovered changes, BSM must be integrated with HP Universal CMDB .</p> <p>When you click a blue bar in the CI Graph, a table consisting of CIs that contain discovered changes in the currently selected time frame is displayed, and the relevant CIs are highlighted in the Topology Map.</p> <p>When you hover above a section of a bar in the graph a tooltip that contains information about discovered changes that occurred at that time appears.</p>
	<p>Planned changes. Displays in the CI Graph, planned changes that occurred in CIs that are part of the anomaly, and that occurred during the currently selected time frame. Planned changes are represented by a turquoise bar in the CI Graph.</p> <p>To display planned changes, the BSM planned changes component must be integrated with HP ServiceCenter/HP Service Manager.</p> <p>When you click a turquoise bar in the CI Graph, a table consisting of CIs that contain planned changes in the currently selected time frame is displayed, and the relevant CIs are highlighted in the Topology Map.</p> <p>When you hover above a section of a bar in the graph a tooltip that contains information about planned changes that occurred at that time appears.</p>
	<p>Incidents. Displays in the CI Graph, HP Service Manager incidents that occurred in CIs that are part of the anomaly, and that occurred during the currently selected time frame. Incidents are represented by a red bar in the CI Graph.</p> <p>To display incidents, BSM must be integrated with HP ServiceCenter/HP Service Manager.</p> <p>When you click a red bar in the CI Graph, a table consisting of CIs that contain incidents in the currently selected time frame is displayed, and the relevant CIs are highlighted in the Topology Map.</p> <p>When you hover above a section of a bar in the graph a tooltip that contains information about incidents that occurred at that time appears.</p>

UI	
Element	Description
	<p>Events. Displays in the CI Graph, Operations Management (OMi), and external events added using the Events API that occurred in CIs during the currently selected time frame. Events are represented by a green bar in the CI Graph.</p> <p>To display events, BSM must be integrated with OMi.</p> <p>When you click a green bar in the CI Graph, a table consisting of CIs that contain events in the currently selected time frame is displayed, and the relevant CIs are highlighted in the Topology Map.</p> <p>When you hover above a section of a bar in the graph a tooltip that contains information about events that occurred at that time appears.</p>
	<p>Legend. Displays the legend for the icons in the topology map, and the CI Graph pane.</p> <p>You can drag the legend box to any location on the Topology Map.</p> <div data-bbox="414 827 750 1134" style="border: 1px solid gray; padding: 5px; margin: 10px 0;">  <ul style="list-style-type: none">  Abnormal Metrics ✕  Investigation Tools  Discovered Changes  Events  Incidents  Planned Changes </div>

CI Topology Map Pane

The CI Topology Map pane, displays a Topology Map that includes the CIs that the anomaly detection process associates with the anomaly.

User interface elements are described below (unlabeled elements are shown in angle brackets>):

UI	
Element (A–Z)	Description
	<p>Zoom. Move the slider up and down to zoom in (enlarge), or to zoom out (reduce the size) of the Topology Map.</p>
<CI node>	Represents a CI in the Topology Map, and includes the following elements:




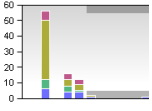

UI Element (A–Z)	Description
	<ul style="list-style-type: none"> The name of the CI. The left most icon displays the type of CI as it is represented in the RTSM. <p>Note: When you hover over a CI, the CI Name and the CI Type are displayed.</p> <ul style="list-style-type: none"> An Abnormal Metrics associated icon, if the CI is associated to an abnormal metric. An event type icon is displayed on a CI node when the CI is associated with an event that occurred during the time frame selected in the CI Graph pane. For details, see "Learn About the CI Node in a Topology Map" (on page 81). <p>Drilldowns: Right-click the CI to display a list of available drill downs. For details, see "Drilling Down in the Topology View" (on page 85).</p>
<Map>	<p>Displays the topology of CIs that are part of the anomaly you are investigating.</p> <p>CIs that are part of the anomaly can be:</p> <ul style="list-style-type: none"> CIs with abnormal metrics. CIs that are linked in the RTSM, to abnormal CIs.


CI Graph Pane

The CI Graph pane displays in stacked bar format discovered changes, planned changes, incidents, or events associated with CIs in the Topology Map. Each event type is represented by a color in the stacked bar.

Important information	<ul style="list-style-type: none"> The CI Graph, displays events for CIs currently selected in the Topology Map, that occurred during the selected time frame. <p>Note: If you select a CI with no event icons, the graph pane will be empty.</p> <ul style="list-style-type: none"> The CI Graph displays at any time up to one week of event types, and holds by default 60 days of historical data for the CIs that appear in the anomaly. Event type icons appear on a CI node in the Topology map when the event occurs in the selected timeframe for the CI Graph.
See also	"Topology View Toolbar" (on page 93) .

User interface elements are described below (unlabeled elements are shown in angle brackets):

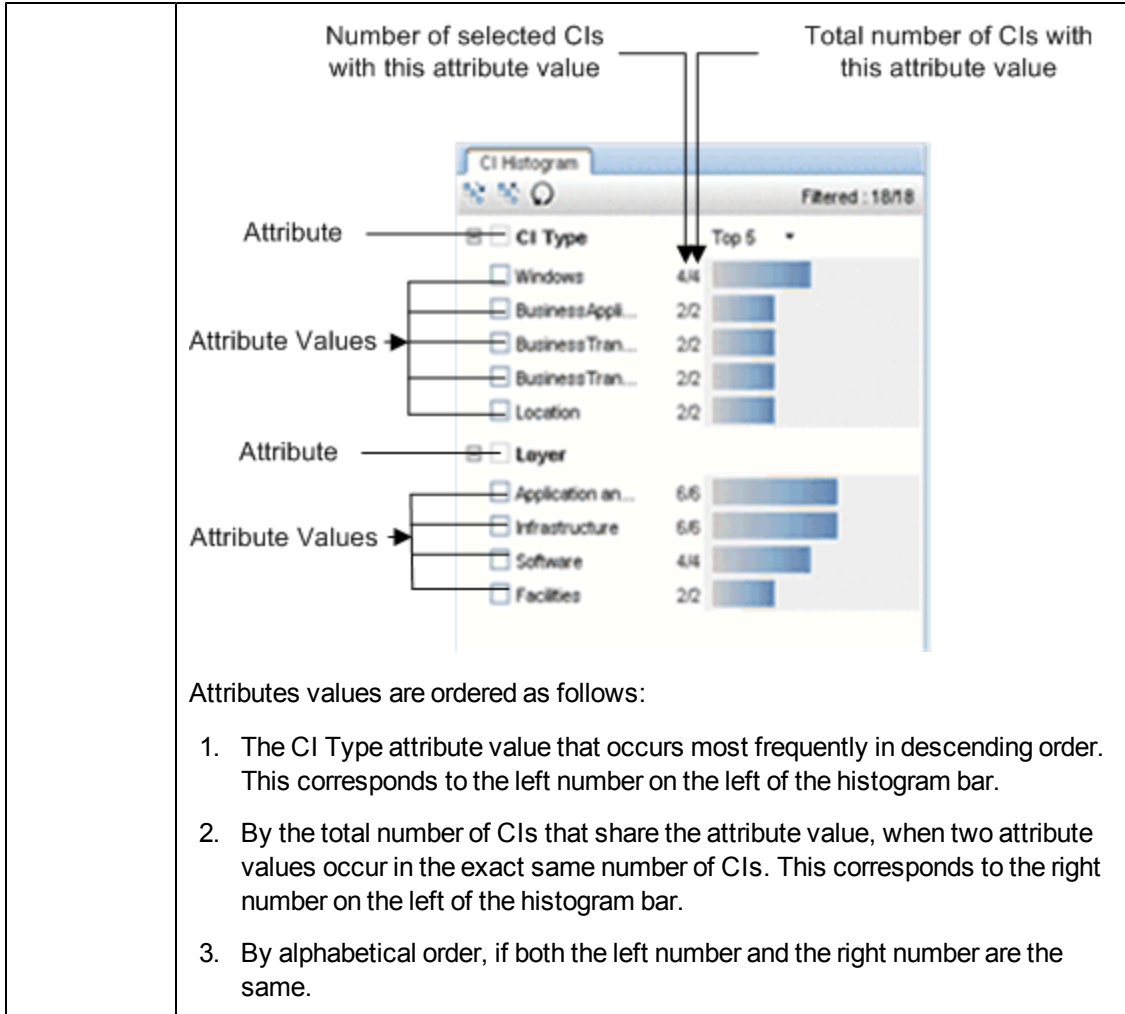
UI Element (A–Z)	Description
	<p>Previous Zoom. Restores the previous zoom definition to the graph.</p>
	<p>Next Zoom. Restores the zoom definition of the graph to the next definition.</p> <p>Note: This button is enabled only when you have previously clicked the Previous Zoom button.</p>
	<p>Reset Zoom. Restores the zoom definition of the graph to the initial time frame of the anomaly.</p>
	<p>Gray bars that appear at the top and bottom of the CI Graph pane indicate the time frame of the anomaly.</p> <p>Note: If you hover over the gray bar, a tooltip with the start time, and if relevant the finish time of the anomaly is displayed.</p>
	<p>Move the ends of the slider to define the time frame that you want to display in the graph. A maximum of one week's data can be displayed at any one time.</p> <p>Note:</p> <ul style="list-style-type: none"> To move the whole graph, click on the middle of the slider and drag, or right-click in the graph and drag. To focus on a selected time frame, on the CI Graph, drag the mouse over the range you want to focus on.
<p><Stacked bar></p>	<p>Stacked bars have the following properties:</p> <ul style="list-style-type: none"> A stacked bar corresponds to events related to a CI or a group of CIs that occurred in the selected time frame. The size of each bar corresponds to the number of events that occurred at the time displayed on the x-axis. The color of each bar corresponds to an event type. The CI Graph displays events that are filtered by the CIs selected in the Topology Map, that occurred in the selected time frame. <p>When you click a section of the stacked bar in the CI Graph View:</p> <ul style="list-style-type: none"> CIs that correspond to the selected group of events/incidents/planned changes/discovered changes are highlighted in the Topology Map.

UI Element (A–Z)	Description
	<ul style="list-style-type: none"> A table displays the events/incidents/planned changes/discovered changes represented by the clicked section of the bar, and the CIs that are affected. <p>For details on the data listed in the popups, see "Learn About the CI Node in a Topology Map" (on page 81).</p> <p>Note: You can click a column name to sort a column.</p>
<Tooltip>	<p>Hover above a section of a bar in the graph to display a tooltip that includes the type of event, the time when the event occurred, and the number of events of this type that occurred at that time.</p> 
X-axis	The scale of the x-axis depends on the selected zoom. The smallest unit is minutes, and the largest unit is days.
Y-axis	The y-axis displays the number of events.

CI Histogram Pane

The CI Histogram categorizes the CIs displayed in the Topology Map according to the CI Type and Layer properties.

Important information	<p>The pane lists, under each attribute, the attribute values, and the number of occurrences of the attribute value for CIs in the Topology Map.</p> <p>When you select CIs in the Topology Map to view their attribute value distribution, the attribute values of the selected CIs are highlighted. When you select specific attribute values in the CI Histogram, non related CIs are removed in the Topology Map.</p>
------------------------------	---



User interface elements are described below (unlabeled elements are shown in angle brackets>):

UI Element (A-Z)	Description
	Expand all. Expands the histogram so that attribute values are displayed under the relevant attributes.
	Collapse all. Collapses the histogram so that only the attributes are listed.
	Reset. Refreshes the CI histogram display.
<Attribute>	The CI attribute (CI Type or Layer) that is displayed in the histogram.
<Attribute Value> <mm/tt>	The specific value of the CI attribute. mm (the number on the left) indicates the number of CIs that are displayed in the Topology Map whose attribute has the specific value.

UI Element (A–Z)	Description
	<p>tt (the number on the right) represents the total number of CIs in the Topology Map, whose attribute has the displayed value. For example, if the Topology Map includes 4 CIs of type Windows, the number on the right is 4. The number of the left can be between 0 and 4 because all 4 CIs, may or may not be selected in the Topology Map.</p> <p>mm and tt are both affected when you add CIs in the Topology Map.</p> <p>Note:</p> <ul style="list-style-type: none"> • If you select CI attribute values in the CI Histogram, only CIs with the selected attribute values are displayed in the CI Topology Map. To restore all the CIs in the map, clear the attribute values box in the CI Histogram. • If you select a CI in the Topology Map, the histogram bars of the attribute values of the selected CI are orange.
<p>Filtered: <nn/rr></p>	<p>nn indicates the number of CIs that are selected in the CI Histogram.</p> <p>rr indicates the total number of CIs that participate in the investigation.</p>
<p>Top 5, 10, 20, Show All</p>	<ul style="list-style-type: none"> • Top 5, Top 10, or Top 20 . Lists the first 5, 10, or 20 values of the selected attribute. • Show All. Display all values for attributes. <p>Attributes and attribute values are displayed as described in "Important information" (on page 98).</p>

Investigating with Metrics Overview

You use the Metrics View to investigate the root cause of an anomaly. The Metrics View is most likely to be used by an infrastructure owner or an application manager who wants to analyze in greater detail the causes of an anomaly, and solve potential performance business and infrastructure issues before they escalate.

When you access the Metrics View of an anomaly, the view displays the set of anomaly related metrics that show abnormal behavior over time. You can alter the time frame to display past behavior for selected metrics.

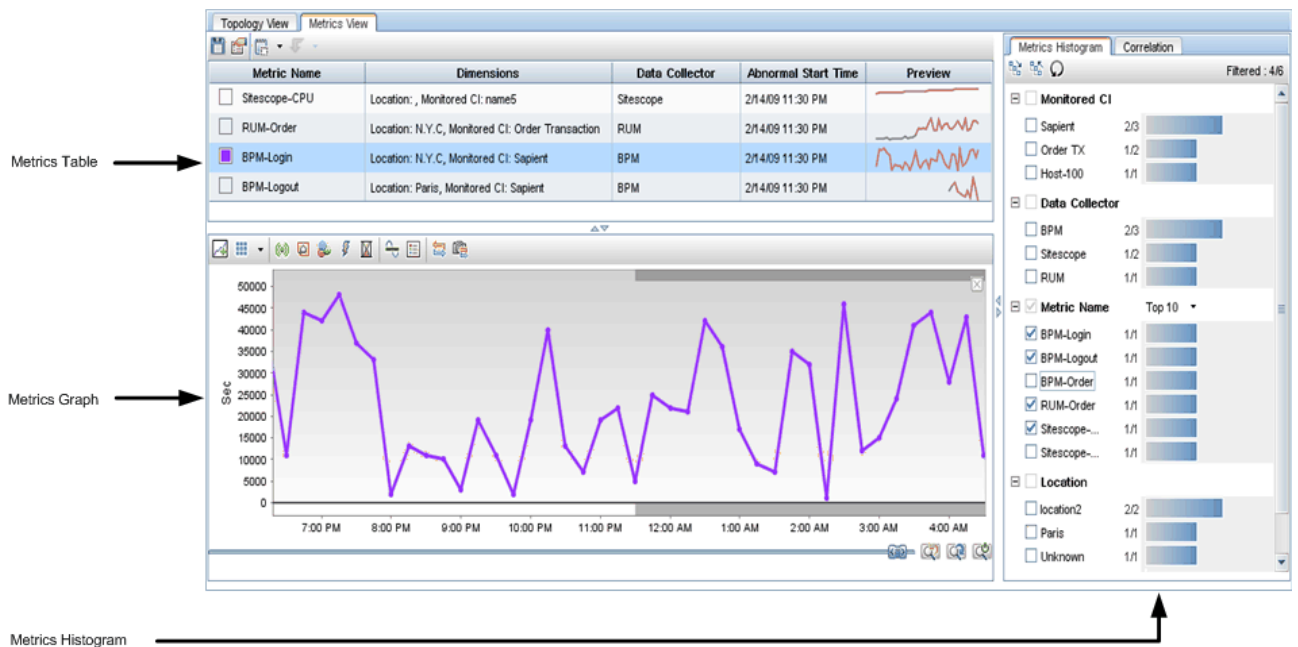
The Metrics View tab, consists of the following:

Metrics Table - Lists in tabular format the abnormal metrics in an anomaly.

Metrics Graph - Enables you to view and compare metric data and event-correlated metric data in graphical format, for a selected time frame.

Metric Histogram Tab - Lists metric data categorized by attributes and attribute value.

Correlation Tab - Enables you to calculate the correlation between metrics.

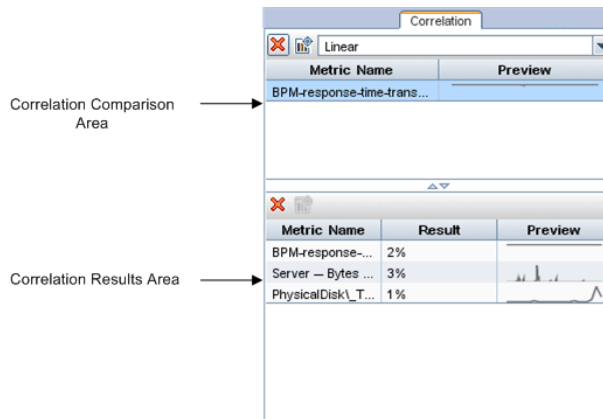


This section includes:

Metric Correlation	103
Drilling Down in the Metrics View	105
How to Use the Metrics View	106
How to Use the Metrics Histogram	108

How to Correlate Metrics	109
Metrics View Tab	111

Metric Correlation



The metric correlation feature enables you to find parallels between different metrics for a specific time frame. There is no limit to the number of metrics you can correlate with each other.

Metric correlations are calculated by comparing selected base metrics that you can view in the Correlation Comparison area, with other selected metrics that can be viewed in the Correlation Results area. A single base metric is correlated with all other selected metrics on a one to one basis. If you select more than one base metric, each base metric is simultaneously correlated with selected metrics, and the mean result of the correlations of all base metrics with a selected metric is calculated.

For user interface details, see ["Correlation Tab" \(on page 124\)](#).

This section includes the following:

- ["Algorithms" \(on page 103\)](#)
- ["Best Practice" \(on page 104\)](#)

Algorithms

Metric correlations can be calculated using the following algorithms:

- **Statistical**

A statistical correlation compares the good behavior and bad behavior of metrics to calculate the correlation. Use this type of correlation when the selected time frame displays enough good and bad samples.

The statistical correlation compares the base metrics in the Comparison area with its own baseline and splits the correlation time frame into good behavior time-slots and bad behavior time-slots. It checks how the metrics in the Correlation Results area behave during the good and bad behavior time-slots and builds a statistical model of the behavior. It then uses the model to calculate the correlation.

Note: To ensure that a statistical correlation is significant, ensure that you select a time frame that includes good and bad behavior. If the samples in your selected time frame do

not satisfactorily represent both good and bad samples, you will be unable to perform a correlation using a statistical algorithm.

- **Event-to-Event**

An event-to-event correlation compares the behavior of the base metrics metric with its own baseline to find good and bad behavior time-slots. Use this type of correlation to find metrics that are reporting either good or bad statuses at the same time.

Note: It is useful to compare metrics that are bad in all the time frames or good in all time frames and to look for other metrics with a similar behavior.

The event-to-event correlation compares the base metric in the Correlation Comparison area with its own baseline and finds the good behavior time-slots and bad behavior time-slots. It aligns the metrics in the Correlation Results area with the base metrics in the Correlation Comparison area, and checks if they are reporting either good or bad statuses at the same time. It then compares how similar their behavior is, and then calculates the correlation.

- **Linear**

The linear correlation searches for metrics whose values go up or down at more or less the same rate and time. Use this algorithm when you don't have a baseline or when you want to investigate a metric that has an anomaly but does not breach the baseline thresholds.

The linear correlation compares a metric's behavior with its baseline because it might miss recurrent problems. Recurrent problems are usually absorbed into the baseline.

Best Practice

If you have metrics representing business elements that are behaving abnormally, you may want to know what system elements might be causing the problem. If a system metric correlates strongly with the business metric that you are currently studying, that system metric might be the cause of the abnormality in the business metric.

For example, when the database query response time metric deviates from the baseline, and you correlate it with the Disk I/O response time metric, you might see that there is a direct correlation between the two metrics. This would suggest that the abnormal behavior might be connected to disk performance and that this should be checked.

Drilling Down in the Metrics View

Metric drill downs provide a shortcut to domain reports for the CIs that own the abnormal metrics.

Drill down options are determined by the data collector that provides the metrics used in creating the anomaly.

Note: To drill down, select a metric in the Metric Table, click the  Drill Down icon, and select a drill down.

The Drill down options are as follows:

Data Collector	Drilldown to
BPM	<ul style="list-style-type: none">• BPM Error Summary. For details, see "BPM Error Summary Report" in <i>Using End User Management</i>• BPM Transaction Validation. For details, see "BPM Transaction Invocation" in <i>Using End User Management</i>.• Application Health. For details, see "Application Health Report" in <i>Using End User Management</i>.
RUM	<ul style="list-style-type: none">• RUM Session Analyzer. For details, see "RUM Session Analyzer Report" in <i>Using End User Management</i>.• RUM Event Summary. For details, see "RUM Event Summary Report" in <i>Using End User Management</i>.• Application Health. For details, see "Application Health Report" in <i>Using End User Management</i>.
SiteScope	A list of all the SiteScope monitors that monitor the metrics or the CIs.
SiteScope, Performance Agents	A selection of Operations Management tools.

How to Use the Metrics View

This task describes how to use the various tools in the Metrics View to assist you investigate the root causes of an anomaly.

As you become familiar with the various tools, you may decide to use the Metrics View in a different manner to the suggested flow that follows:

1. Use the Metrics Table

In the Metrics table, examine the behavior of an abnormal metric.

For example:

- a. Different metrics might exhibit abnormal behavior at about the same time, indicating that the abnormal metrics are symptoms of the same problem.
- b. Other metrics might be connected logically. For example they may be part of the same data collector, application or location.

2. Use the Metrics Histogram

Using the Metrics View Histogram, display the distribution of metrics by attribute (for example by data collection source), and by attribute value.

For more information, see ["How to Use the Metrics Histogram" \(on page 108\)](#).

3. Use the Metrics Graph

Drag relevant metrics from the Metrics Table into the Metrics Graph area. Use the various Metric Graph icons to display discovered changes, planned changes, incidents, events, and downtime that occurred to the CIs during the selected time frame.

In the Metric Graph, you can display historical metric behavior, and view the baseline sleeve for a selected metric. You can use the baseline sleeve and the metric graph line to identify when the metric deviated from the baseline.

4. Use the Correlation Feature

Using the Correlation Tab, examine more closely the correlation between different metrics. Close correlation results between base metrics and selected metrics, might indicate that the selected metric is an additional symptom of the same problem, or it might be a metric that you should investigate further to find the root cause of the problem.

For more information, see ["How to Correlate Metrics" \(on page 109\)](#).

5. Drill Down to Application Reports


You can also drill down on a metric to access relevant application reports (for example RUM, BPM, SiteScope) filtered for the CIs attached to the metrics, and get more information about the metric.

For more information, see ["Drilling Down in the Metrics View" \(on page 105\)](#).

6. Add Investigation Properties

If you want to add or edit investigation property details, on the Metric toolbar, click 

Investigation Properties, and add relevant investigation properties.

7. Click  to save the investigation.

How to Use the Metrics Histogram

The Metrics Histogram categorizes attributes and attribute values of metrics listed in the Metrics Table pane. Example of attributes are: Application, Transaction, Data Collector, Metric Name, and Location.

The amount of data in the Metrics table can often be difficult to analyze at first glance. To assist you to analyze metric data, you can use the Metrics Histogram feature to filter attributes and attribute values, and investigate the abnormal metrics you think are the most significant ones in the anomaly.

By selecting only the most significant attribute values in the histogram you can filter out the less significant metrics shown in the Metrics Table. This helps you to focus on the problem, and simplifies and speeds up the investigation process.

This task describes how to use the Metrics Histogram.

1. Open the Metrics View tab

For more information on accessing the Metrics View, see ["To access" \(on page 111\)](#).

2. Filter Out Metrics by Selecting Attributes and Attribute Values

In the Metrics Histogram tab, select attributes or attribute values that display significant activity in the Metrics Histogram.

The Metrics Table only displays metrics that are associated to the selected attributes and attribute values that you select. The result is a more focused Metrics Table.

Example: To display a more focused Metrics Table, you might select the top two data collectors, and a location.

3. Drag Metrics to the Metrics Graph

Drag and drop metrics for comparison from the Metric Table to the Metrics Graph area.

4. Isolate the Problem

Use the tools available in the Metrics Graph area to isolate the problem, and the metrics that caused it.

Example: You can select a time frame that includes troublesome metrics, and then analyze metric behavior for that time frame.

For details about the Metrics Graph, see ["Metric Graph Pane" \(on page 114\)](#).

How to Correlate Metrics

This task describes how to perform a correlation between metrics.

For concept details, see ["Metric Correlation" \(on page 103\)](#)

To correlate metrics:

- 1. Open the Metrics View tab**

For more information on accessing the Metrics View, see ["To access" \(on page 111\)](#).

- 2. Drag and Drop metrics from the Metric Table Pane to the Metric Graph Pane**

Only metrics that have been dragged and dropped in the Metric Graph pane can be used as base metrics for correlation calculations.

- 3. Capture a Correlation Time Frame**

For each metric in the Metric Graph pane that you want to use as a correlation base metric, select a time frame by clicking and dragging the mouse over the time frame you want to select,

and then click  **Capture Correlation Time Frame**.

The selected pane expands to occupy the whole Metrics Graph pane, and the name of the metric with a preview of the graph for the metric are displayed in the Correlation Comparison pane of the Correlation tab. For details about the Comparison Pane, see ["Correlation Comparison Area" \(on page 125\)](#).

- 4. Drag Metrics to the Correlation Results Pane**

Drag metrics you want to correlate with the base metrics, from the Metrics Table pane into the Correlation Results pane. The correlation calculates and the results are displayed in the Correlation Results pane. For details about the Comparison pane, see ["Correlation Results Area" \(on page 126\)](#). For details on how correlations results are calculated, see ["Metric Correlation" \(on page 103\)](#).


- 5. Select a Correlated Metric**

Select the metric that has a high correlation, and select it in the Metrics Histogram to see which CI is problematic. Once you find the relevant CI, go to the corresponding Topology View to find the other CIs that are part of the same topology, and see if you can identify common issues.


- 6. Result**

By analyzing the correlation results for different combinations of metrics, you can get clearer indications of what might be causing the problem.

Note:

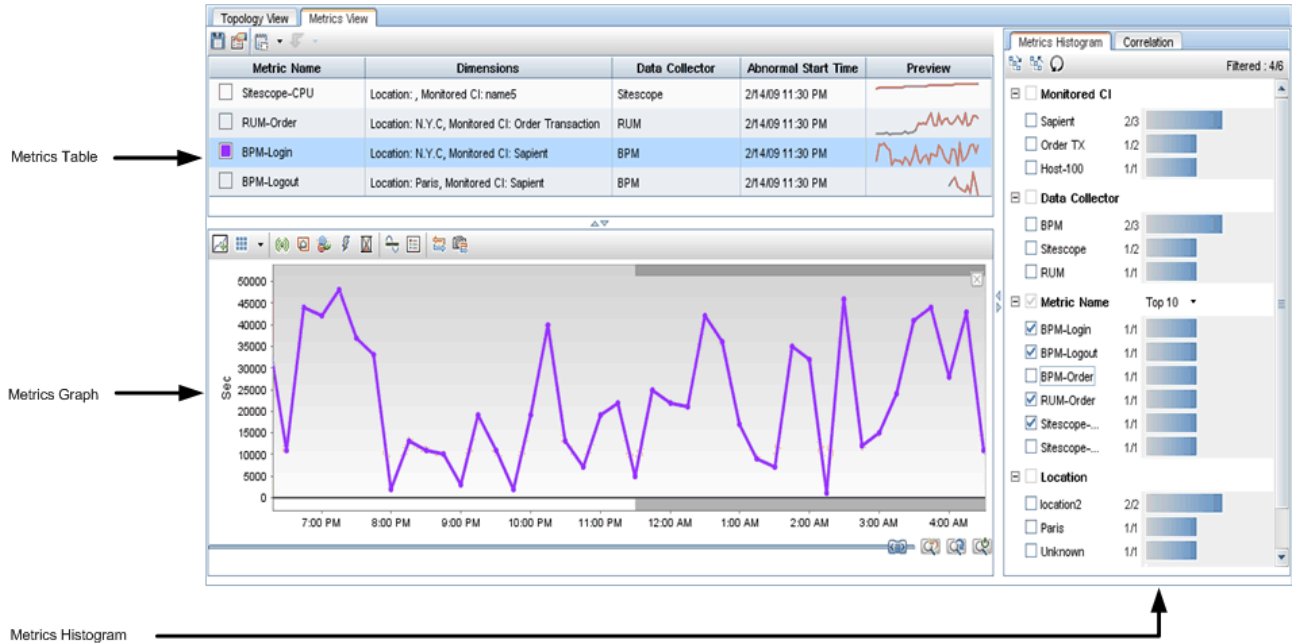
- You can capture several time frames for the same correlation base metric name.
- When you click **Capture Correlation time Frame** , the Correlation tab becomes the


default tab.

- To view the correlation time frames you selected, in the Metrics Graph pane, select a metric and click the **Show Correlation Time Frames** . The correlation time frames are indicated by vertical bars with a shaded background.

Metrics View Tab

The Metrics View tab, contains tools that enable you to investigate the root causes of an anomaly, by analyzing the anomaly CI's metric related data.



<p>To access</p>	<p>Use one of the following:</p> <ul style="list-style-type: none"> • In Operations Management, select an SHA event. On the Additional Info tab of the event, in Description, click the hyperlink to the Anomaly Highlights window, and then on the Anomaly Highlights page, click Investigate Further, and then click the Metrics View tab. • In Service Health, in the 360° View Hierarchy, click the down arrow, or right-click on a name instance, navigate to Go To, click Go to Service Health Analyzer, on the Anomaly Highlights page, click Investigate Further, and then click the Metrics View tab. • In the Topology View, click an abnormal metric icon  to open an Abnormal Metric table for the selected CI, and then click Drill to Metrics View. This opens the Metrics view for the selected metrics. • Applications > Service Health Analyzer, double-click the relevant investigation, and click the Metrics View tab.
<p>Important Information</p>	<ul style="list-style-type: none"> • A maximum number of discovered changes, events, and incidents can be displayed in the Metrics Graph at any one time. The values are held in the Max number of Discovered changes to fetch for the UI, Max number of events to fetch for the UI, and Max number of incidents to fetch for the UI infrastructure settings. Their default values are 300.




	<p>For more information on how to edit infrastructure settings, see "How to Edit an SHA Infrastructure Setting" (on page 157).</p> <p>Caution: If one of the special events exceeds the maximum number configured, none of that type of special event are displayed in the UI.</p> <p>If you do not want to change the infrastructure setting, you can alternately select a shorter time frame.</p> <ul style="list-style-type: none"> • By default, closed events are not displayed in the UI. To display closed events, change the Show closed events in UI setting to True.
<p>Relevant tasks</p>	<ul style="list-style-type: none"> • "How to Use the Metrics View" (on page 106) • "How to Use the Metrics Histogram" (on page 108) • "How to Correlate Metrics" (on page 109)

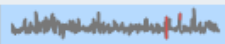
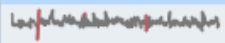
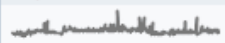
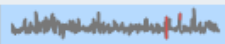
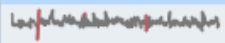
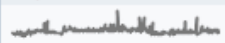
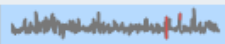
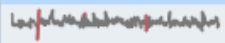
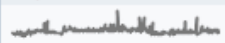

The Metrics View page consists of the following:

- ["Metrics Table Pane" \(on page 112\)](#)
- ["Metric Graph Pane" \(on page 114\)](#)
- ["Metrics Histogram Pane" \(on page 122\)](#)
- ["Correlation Tab" \(on page 124\)](#)

Metrics Table Pane

User interface elements are described below (unlabeled elements are shown in angle brackets>):

UI Element (A–Z)	Description
	<p>Save. Opens the Save Investigation dialog box where you can enter a name for the investigation and save it.</p> <p>Note: One investigation can be saved per anomaly. This means that when two users are working simultaneously on an investigation, the last save becomes the currently saved anomaly.</p>
	<p>Investigation Properties. Opens the Investigation Properties Dialog box. For details, see "Investigation Properties Dialog Box" (on page 130).</p>
	<p>Group metrics by. Select the element you want to use to group the metrics:</p> <ul style="list-style-type: none"> • None. - Click to display the metrics without grouping. • Metric Name. - Click to display the metrics grouped by metric name. • Data Collector. - Click to display the metrics grouped by data collector.

UI Element (A–Z)	Description																								
	<ul style="list-style-type: none"> • Abnormal Start Time. - Click to display the metrics grouped by abnormal start time. • Advanced. - Click to open the Advanced dialog box where you can group metrics by metric name, abnormal start time and data collector. <p>Example: The image shows a grouping by data collector followed by a grouping by Abnormal Start Time.</p> <table border="1" data-bbox="456 590 1382 842"> <thead> <tr> <th>Metric Name</th> <th>Data Collector</th> <th>Abnormal Start Time</th> <th>Preview</th> </tr> </thead> <tbody> <tr> <td colspan="4">[-] BPM</td> </tr> <tr> <td colspan="4">[-] Tue, 5 Feb 2008 22:14:45</td> </tr> <tr> <td><input type="checkbox"/> cild704 [CA</td> <td>BPM</td> <td>Tue, 5 Feb 2008 22:14:45</td> <td></td> </tr> <tr> <td><input type="checkbox"/> cild703 [CA</td> <td>BPM</td> <td>Tue, 5 Feb 2008 22:14:45</td> <td></td> </tr> <tr> <td><input type="checkbox"/> cild702 [CA</td> <td>BPM</td> <td>Tue, 5 Feb 2008 22:14:45</td> <td></td> </tr> </tbody> </table>	Metric Name	Data Collector	Abnormal Start Time	Preview	[-] BPM				[-] Tue, 5 Feb 2008 22:14:45				<input type="checkbox"/> cild704 [CA	BPM	Tue, 5 Feb 2008 22:14:45		<input type="checkbox"/> cild703 [CA	BPM	Tue, 5 Feb 2008 22:14:45		<input type="checkbox"/> cild702 [CA	BPM	Tue, 5 Feb 2008 22:14:45	
Metric Name	Data Collector	Abnormal Start Time	Preview																						
[-] BPM																									
[-] Tue, 5 Feb 2008 22:14:45																									
<input type="checkbox"/> cild704 [CA	BPM	Tue, 5 Feb 2008 22:14:45																							
<input type="checkbox"/> cild703 [CA	BPM	Tue, 5 Feb 2008 22:14:45																							
<input type="checkbox"/> cild702 [CA	BPM	Tue, 5 Feb 2008 22:14:45																							
	<p>Displays a list of drill downs. The available drill downs depend on the type of data collector used to gather the metric data.</p> <p>For details, see "Drilling Down in the Metrics View" (on page 105).</p>																								
<p>Abnormal Start Time</p>	<p>The time when the abnormality started.</p>																								
<p>Data Collector</p>	<p>The data collector that collected the selected metric. Data collectors include: SiteScope, Real User Monitor, Business Process Monitor, Performance Agent, and NNMi.</p>																								
<p>Dimension</p>	<p>Lists all the dimensions (attributes) of the metric as they appear in the PMDB.</p>																								
<p>Metric Name</p> <input type="checkbox"/>	<p>The name of the abnormal metric that contributed to the anomaly. The column also displays a thumbnail of the color that represents the metric in the Metric Graph.</p> <p>Note: Colors are automatically assigned and cannot be changed.</p>																								
<p>Preview</p>	<p>Displays as a sparkline the value of the abnormal metric over a specific time frame.</p> <p>drag and drop. To view a metric's data in a higher resolution, select the metric in the Preview column, and drag and drop it to the Metrics Graph area. For details on the Graph area, see "Metric Graph Pane" (on page 114).</p> <p>Note:</p>																								


UI Element (A–Z)	Description
	<ul style="list-style-type: none"> • The time frame starts 5 hours before the beginning of the anomaly, and ends 5 hours after the beginning of the anomaly. If the current time is less than the beginning of the investigation plus 5 hours the time frame ends at the current time. • The time frame for all the metrics displayed in the Preview column is the same. • The preview of some metrics may be empty if the metric does not have data for that time frame.




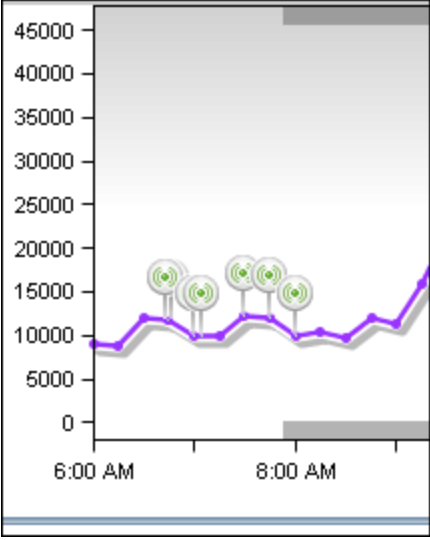
Metric Graph Pane



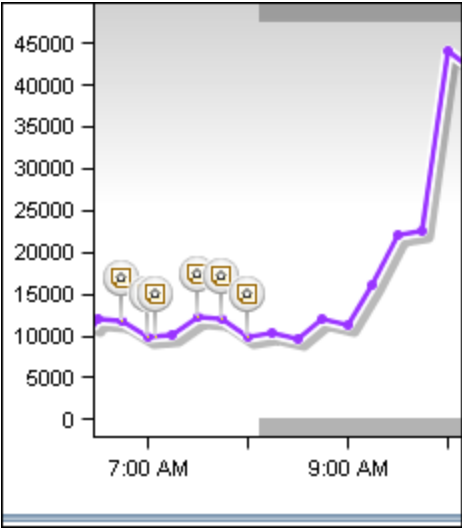


The pane enables you to graphically view metric data and event-correlated metric data, for a selected time frame. For each metric where relevant, you can also display special events that occurred to the CIs for the selected time frame.

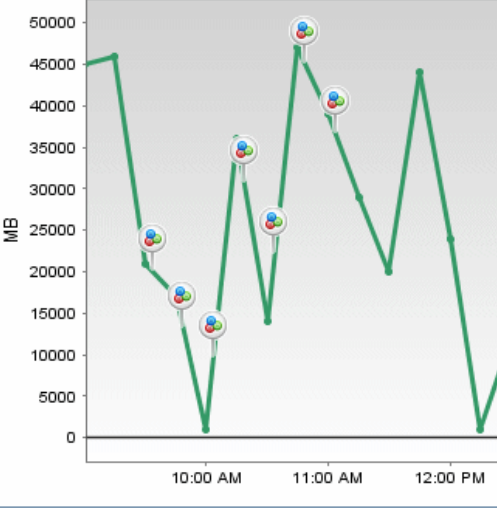





Important information	<ul style="list-style-type: none"> • The Metric Graph Pane displays at any time up to one week of data for selected metrics, and holds by default up to 60 days of historical data. • When multiple metrics are dragged to a graph, the currently active metric line is thicker and more prominent, and the x-axis is calibrated according to the active metric.
------------------------------	--

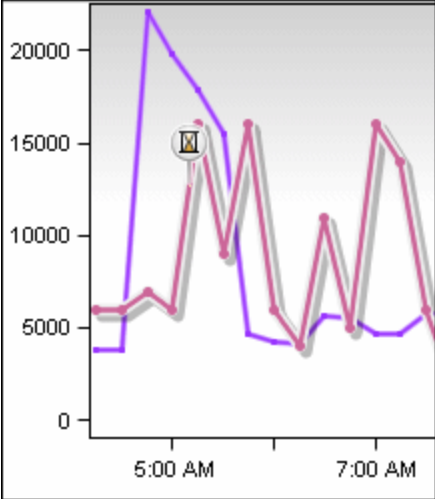

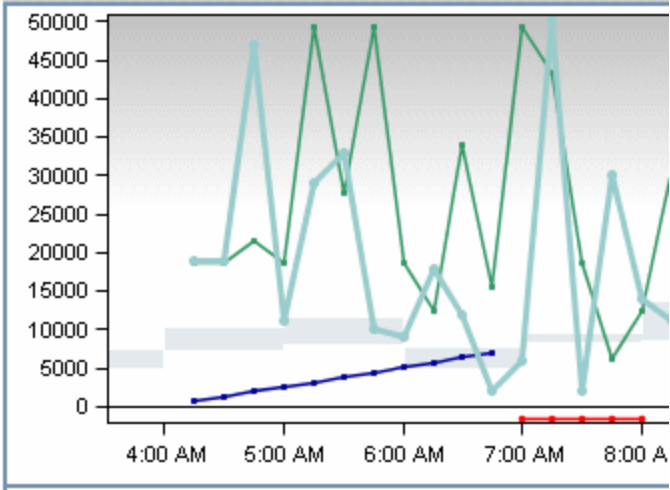

User interface elements are described below (unlabeled elements are shown in angle brackets>):

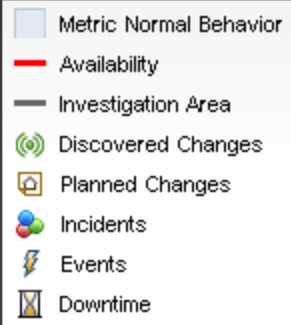









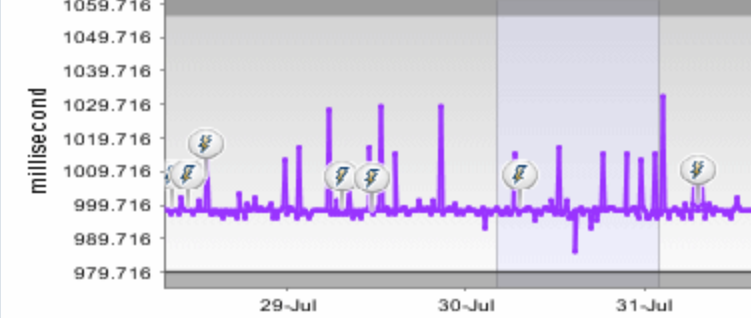





UI Element	Description
	<p>Add graph. Adds a new graph area in the Metrics Graph pane.</p> <p>You can add up to four graph panes, and add up to four metrics to each graph pane. For details, see the Layout button description.</p> <p>When displaying several graph panes, the X-axis (time frame) is consistent in all graph panes. This is true if a specific area of a graph is selected, or if you use the slider to change the time frame.</p>

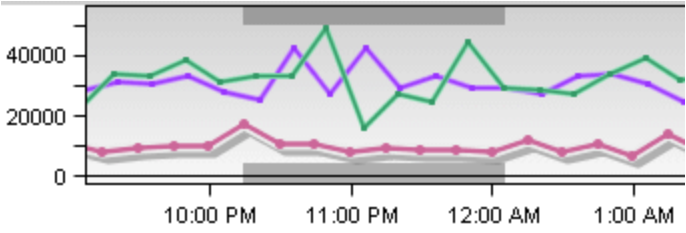



UI Element	Description
	<p>Layout. The layouts available when displaying multiple graph panes in the metric graph area. Depending on the number of graph panes you open, you can display them as Horizontal, Vertical, or Grid. Every time you click the Layout icon, the next layout method is automatically applied.</p> <p>Note:</p> <ul style="list-style-type: none"> • The Y-axis of the graph pane displays a metric specific value. If you have more than one metric in a graph, the Y-axis values are for the currently focused metric sparkline. • The slider of the graph pane works simultaneously for all the Metric Graphs. This means that the X-axis in all graphs is identical. • The zoom functionality affects all graph panes.
	<p>Discovered changes. Displays in the Metric Graph pane, discovered changes that occurred in the CIs that correspond to the selected metric displayed in the graph. Each discovered change is indicated by . A discovered change icon is displayed for each CI at the time the discovered change occurred.</p> <p>This information is displayed only when Business Service Management is integrated with HP Universal CMDB.</p> <p>Example:</p>  <p>The above graph shows discovered change events occurring before the start of the anomaly (indicated by the grey horizontal bar). In such a case, the anomaly may be a direct result of the discovered changes, and they are therefore worth further investigation.</p>

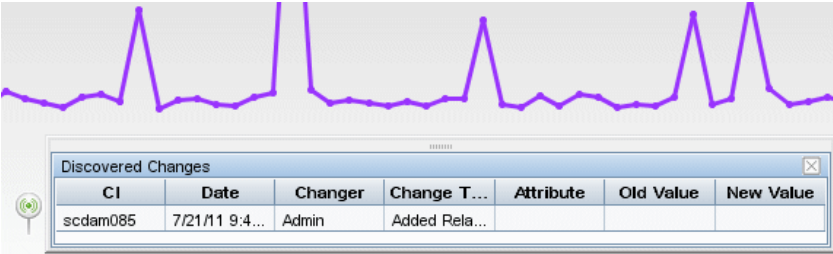
UI Element	Description
	<p>Planned changes. Displays in the Metric Graph pane, planned changes that occurred in the CIs that correspond to the selected metric displayed in the graph. Each planned change event is indicated by . A planned change icon is displayed for each CI at the time the planned change occurred.</p> <p>This information is displayed only when Business Service Management planned changes component is integrated with HP ServiceCenter/HP Service Manager.</p> <p>Example:</p>  <p>The above graph shows planned change events occurring before the start of the anomaly (indicated by the grey horizontal bar). In such a case, the anomaly may be a direct result of the planned changes, and they are therefore worth further investigation.</p>
	<p>Incidents. Displays in the Metric Graph pane, incidents that occurred in the CIs that correspond to the selected metric displayed in the graph. Each incident is indicated by . An incident icon is displayed for each CI at the time the incident occurred.</p> <p>This information is displayed only when BSM is integrated with HP ServiceCenter/HP Service Manager. For details about the integration, see "How to Integrate HP Service Manager with Business Service Management Components" in <i>Solutions and Integrations</i>.</p> <p>Example:</p>

UI Element	Description
	
	<p>Events. Displays in the Metric Graph pane, the following type of events that occurred in the CIs that correspond to the selected metric displayed in the graph:</p> <ul style="list-style-type: none"> • Operations Management (OMi) events. This information is displayed only when you have an OMi license installed. • External events added using the Events API. <p>Each event is indicated by . An event icon is displayed for each CI at the time the event occurred.</p> <p>Example:</p> 
	<p>Downtime. When selected, displays in the Metric Graph pane, downtime events that occurred in the CIs that correspond to the selected metric displayed in the graph. Each downtime event is indicated by . A downtime icon is displayed for each CI at the time the downtime event occurred.</p>

UI Element	Description
	<p>For details, see "Downtime Management" in <i>Platform Administration</i>.</p> <p>Example:</p> 
	<p>Metric Baseline. Displays the baseline of the selected metric. The baseline is represented by continuous gray rectangles. The vertical measurement of the rectangle represents the normal baseline range of the metric during the selected time frame. The time frame is represented by the horizontal side of the rectangle.</p> <p>Example:</p> 
	<p>Legend. Displays the graph's legend.</p> <p>You can drag the legend box to any location on the Metrics Graph pane.</p> <p>Example:</p>

UI Element	Description
	 <ul style="list-style-type: none">  Metric Normal Behavior  Availability  Investigation Area  Discovered Changes  Planned Changes  Incidents  Events  Downtime
	<p>Show Correlation Time Frames. Enables you to display the correlation time frames you selected for the active metric. The correlation time frames are indicated by vertical bars with a colored background. For user interface details, see "Correlation Tab" (on page 124).</p>  <p>The graph displays a purple line representing a metric over time, with vertical bars indicating correlation time frames. The y-axis is labeled 'millisecond' and ranges from 979.716 to 1059.716. The x-axis shows dates from 29-Jul to 31-Jul. A shaded area highlights a specific time frame.</p>
	<p>Capture Correlation Time Frame. Moves the metric you want to use as a base metric for the correlation, from the Metrics Graph pane to the Correlation Comparison area. In the Metrics Graph pane, click and drag to select the time frame you want to use for the correlation, and then click . The metric in the selected time frame is added to the Correlation Comparison area. For user interface details, see "Correlation Tab" (on page 124).</p>
	<p>Previous Zoom. Restores the previous zoom definition to the graph.</p>
	<p>Next Zoom. Restores the last zoom definition of the graph to the next definition.</p> <p>Note: Next Zoom is enabled only when you have previously clicked the Previous Zoom button.</p>
	<p>Reset Zoom. Restores to the default zoom definition of the graph.</p>
<p><Range of the anomaly></p>	<p>The gray upper and lower bars indicate the time frame of the anomaly.</p>

UI Element	Description
	<p>Note: If you hover over the gray line, a tooltip with the start time, and if relevant the finish time of the anomaly is displayed.</p> <p>Example:</p> 
	<p>Move the ends of the slider to define the time frame that you want to display in the graph. A maximum of one week's data can be displayed at any one time.</p> <p>Note:</p> <ul style="list-style-type: none"> To move the whole graph, click on the middle of the slider and drag, or right-click in the graph and drag. To focus in on a selected time frame, drag the mouse over the range you want to focus on.
	<p>Red dots above the X-axis indicate an availability problem in the currently focused metric in the Metric Graph.</p> <p>Tooltip: If you hover on the dots, you see a tooltip with more details about the metric that is unavailable.</p>
	<p>Close graph. Closes a Metric Graph pane.</p>
<p><Drag and drop></p>	<p>Select a metric in the table, then drag and drop it into a metric graph pane.</p> <p>Note:</p> <ul style="list-style-type: none"> You cannot change the color of a line representing a metric. To remove a metric from a Metric graph pane, right-click the line, and then select Remove.
<p><Metrics Graph pane></p>	<p>The area where a Metric graph is displayed.</p> <p>To horizontally scroll the contents of the Metric Graph, right-click anywhere on the graph and drag the graph to the left or right.</p>

UI Element	Description
<Tooltip>	<p>Regular tooltip: Hover above a dot on a line in the metrics graph to display a tooltip that includes the metric name, value and time the metric value was collected.</p> <p>On-demand tooltip: Click an event type icon to display tabular information about the event associated with the metric at that time.</p> <p>The information displayed in the tooltip depends on the type of event/incident/change.</p> <p>Example:</p> <div data-bbox="565 594 1068 688" style="border: 1px solid black; padding: 5px; background-color: #ffffcc;"> PhysicalDisk_TotalAvg. Disk Read Queue Length Time: 7/27/11 6:25 AM Value: 0.046 </div> <p>Example:</p> 
<zoom>	<p>Zoom in:</p> <p>Left-click in the relevant area of the graph and drag. When you release the button, the area you selected expands to fit the graph space.</p>
X-axis	<p>The scale of the x-axis depends on the selected zoom. The smallest unit is minutes, and the largest unit is days.</p>
Y-axis	<p>The Y-axis displays the scale for the currently selected metric. A selected metric's sparkline is thicker and is therefore more prominent.</p> <p>Example:</p> <p>In the first graph the blue metric is selected and the Y-axis range is calibrated using the metric values that the blue line represents.</p> <p>In the second graph the yellow metric is selected and the Y-axis range is calibrated using the metric values that the yellow line represents.</p>

UI Element	Description

Metrics Histogram Pane

The Metrics Histogram tab enables you to filter metrics listed in the Metrics View pane by attribute type and attribute value.

<p>Important information</p>	<p>The Metrics Histogram pane lists, under each attribute, the attribute values, the number of occurrences of the attribute value in the selected metrics, and in all the metrics in the anomaly.</p> <p>If you select a metric in the Metrics Table their attribute value distribution is highlighted in the Metrics Histogram. When you select specific attribute values, only metrics relevant to the attribute values are displayed in the Metrics Table.</p>
-------------------------------------	---

The screenshot shows a 'Metrics Histogram' interface with a 'Filtered : 1/2' indicator. It displays several attributes with their respective values and counts:

- Application:** Gold Employee... (0/1), HR Portal (0/1)
- Data Collector:** SIS (1/10), BPM (0/2)
- Metric Name (Top 5):** PhysicalDisk\... (1/1), Processor\Tot... (0/4), BPM-respons... (0/2), Processor\cp... (0/2), % of physical ... (0/1)
- Transaction:** (None listed)
- Measurement ID (Top 5):** (None listed)
- Node (Top 10):** (None listed)
- Location:** Atlanta (0/1), Austin (0/1)

Attribute values are ordered as follows:

1. From the attribute value that occurs most frequently in the metrics in descending order. This corresponds to the left number on the left of the histogram bar.
2. By the total number of metrics that share the attribute's value, if two values occur in the exact same number of metrics. This corresponds to the right number on the left of the histogram bar.
3. By alphabetical order, if both the left number and the right number are the same.

User interface elements are described below (unlabeled elements are shown in angle brackets>):


UI Element (A–Z)	Description
	Expand All. Expands all the attributes displayed in the histogram, and displays their attribute values.
	Collapse All. Collapses the histogram so that only attributes are displayed.
	Reset. Resets all the selections in the histogram to the default display.

UI	
Element (A–Z)	Description
<Attribute>	<ul style="list-style-type: none"> • Application. Lists applications involved in the anomaly. • Data Collector. Lists the data collectors used to collect metrics. For example: BPM, SiteScope. • Metric Name. Lists the names of the metrics included in the anomaly. • Transaction. List specific transactions involved in the anomaly. • Measurement ID. • Node. Lists nodes involves in the anomaly. • Location. Lists the metrics collected by location. • Monitored CI. Lists all metrics having the monitored CI as an attribute.
<Metrics>	<p>The length of the bar and the first number on the left of the bar indicate the number of metrics in the anomaly that are related to the selected attribute value. The second number on the left of the bar provides the total number of metrics that include the attribute value.</p> <p>When you select a metric in the Metrics Table, the Histogram bars for related attribute values change color to orange.</p> <p>For details about the Metrics Table area, see "Metrics Table Pane" (on page 112).</p> <p>Select different metrics to help you isolate the problem that caused the anomaly. For details, see "How to Use the Metrics Histogram" (on page 108).</p>
<nn/tn> at the top right-hand side of the histogram	<p>nn indicates the number of metrics that are filtered by the histogram.</p> <p>tn indicates the total number of metrics that participate in the investigation.</p>
Top 5, 10, 20, Show All	<ul style="list-style-type: none"> • Top 5, Top 10, or Top 20. Lists the first 5, 10, or 20 metrics attribute values for the selected metrics. • Show All. Display all metrics with the relevant attribute <p>For more information, see "Important information" (on page 122).</p>

Correlation Tab

The Correlation tab enables you to display the correlation between selected metrics for a selected time frame.



Important information	The metrics in the Correlation Comparison Area, are used as the base metrics for the correlation. The metrics in the Correlation Results Area are correlated with the base metrics.
------------------------------	---

	<p>You can see the selected correlation time frames for the currently selected metric when you click Show Correlation Time Frames  in the Metrics Graph. For more details, see "Metric Graph Pane" (on page 114).</p> <p>There is no limit to the number of metrics that you can correlate.</p> <p>The correlation results in the Correlation Results area, are calculated using all the all the metrics in the Correlation Comparison area.</p> <p>Best Practices:</p> <ul style="list-style-type: none"> • You can for example, correlate system metrics (Correlation Results area) with business metrics (Comparison area). You may also correlate infrastructure metrics (Correlation Results area) with database performance metrics (Comparison area). • Add to the Comparison area, metrics that represent the same problem (recurrent problem) or the same metric for different time frames. • It is recommended to include in the time frame, both "good" and "bad" behavior, to get better Correlation Results. Drag into the correlation bottom section, metrics that seem to have similar behavior. • Select the metric that has the best correlation and go to the histogram to see which CI is problematic. Once you find the relevant CI, go to the corresponding Topology View to find the other CIs that are part of the same topology. These CIs may help you solve the problem.
<p>See also</p>	<p>"Metric Correlation" (on page 103)</p> <p>"How to Correlate Metrics" (on page 109)</p>

Correlation Comparison Area

The Comparison area displays metrics you select as base metrics for a correlation operation. Metrics listed in the Correlation Results area are correlated with metrics in the Correlation comparison area.

User interface elements are described below (unlabeled elements are shown in angle brackets>):



UI Element (A–Z)	Description
	<p>Delete Correlation Time Frame. Removes the selected metric from the Correlation Comparison area.</p>
	<p>Set Focus. Displays the selected metric for its correlation time frame in the Metric Graph pane.</p> <p>Note: You can also double-click the metric in the Correlation Comparison area for the same result.</p>

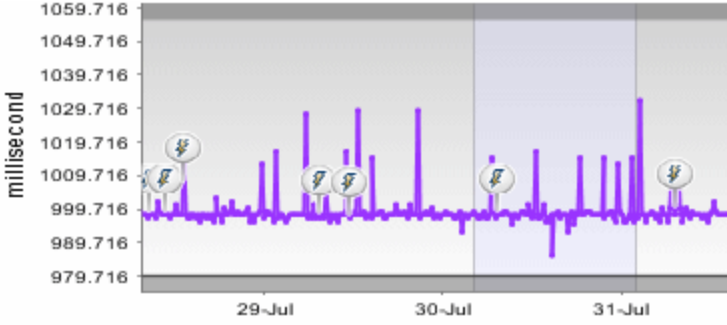
UI Element (A–Z)	Description
Algorithms	<p>Depending on the metrics you want to correlate, you can select different types of algorithms:</p> <ul style="list-style-type: none"> • Statistical • Event to event • Linear <p>For details about the different types of algorithms, see "Algorithms" (on page 103).</p> <p>All base correlation metrics are correlated with metrics in the Correlation Results area using the selected algorithm. A percentage correlation for each metric is displayed in the Result column of the Correlation Results area.</p>
Metric Name	The name of a metric you select to be used as a base for the comparison with the metrics listed in the Correlation Results Area.
Preview	<p>A preview of the metric over the comparison time frame you selected in the Metrics Graph pane. When you perform multiple time frame selection on the same base metric, the Comparison area displays each time frame as a separate entry.</p> <p>The correlation with the metrics in the Correlation Results are performed only for the time frame displayed in the Comparison area's Preview column.</p>

Correlation Results Area

The Correlation Results area holds metrics that are correlated with the base metrics in the Correlation Comparison area.

User interface elements are described below (unlabeled elements are shown in angle brackets>):

UI Element (A–Z)	Description
	Delete Correlation Time Frame. Deletes the selected metrics.
	Set Focus. Click the button and then click the relevant metric in the list, or double-click the metric to change the focus to the selected metric in the Metrics Graph pane and display the time frames selected for the correlation.

UI Element (A–Z)	Description
	 <p>The correlation time frames are indicated by vertical bars with a shaded background.</p>
Metric Name	The name of the metric you selected to be correlated with base metrics.
Preview	<p>Displays a preview of the compared metric in the correlation results area in the same time frame as the focused base metric.</p> <p>The correlation is performed for the time frame displayed in the Preview column of the metrics in the Comparison area. This is the correlation time frame you selected for the base metric .</p>
Result	The percentage correlation between the metrics in the Comparison area and each metric in the Correlation Results area. The closer the result is to 100%, the greater the correlation between the metrics.

Using Service Health Analyzer Investigations

Once an anomaly has been created, you can investigate the causes of the anomaly using features such as the Topology and Metrics Views.

In certain instances, you might want to save an anomaly, for example if you are in the middle of an investigation and you have made changes to the Topology Map, or you want to assign a pattern to an anomaly.

A saved SHA investigation, contains the details of the anomaly at the time it was saved. The contents of an anomaly may change after you save an investigation. To see the latest metric and topology information for an anomaly, you can access it through the Anomaly Highlights page. You can only save one investigation per anomaly. If you save the updated anomaly as an investigation, you will be prompted to overwrite the existing investigation for the anomaly.

This section includes:

How to Create an Investigation	129
Investigation Properties Dialog Box	130
SHA Investigation Page	133


How to Create an Investigation

This task describes how to create an investigation.

1. Investigate an anomaly with the Topology or Metrics views, until you are ready to save the anomaly.


For more information on how to get to the Topology or Metrics Views, see ["Topology View Tab" \(on page 91\)](#), or ["Metrics View Tab" \(on page 111\)](#).

2. It is recommended that before you save an anomaly, that you assign Investigation properties to the anomaly. On the Topology View, or Metrics View toolbar, click the **Investigation**

Properties  icon, and enter relevant investigation properties.

For more information on Investigation properties, see ["Investigation Properties Dialog Box" \(on page 130\)](#).

Note: In the Investigation Properties Dialog, you can associate a pattern with an investigation.


3. To save the anomaly, click , and in the Save Investigation Dialog box, enter an Investigation name.

Note: You can save one investigation per anomaly. This means that when two users are working simultaneously on an investigation, the last save becomes the currently saved investigation for the anomaly.



If you want to use an existing investigation, select **Applications > Service Health Analyzer**. For more information, see ["SHA Investigation Page" \(on page 133\)](#).


Investigation Properties Dialog Box


This dialog box, enables you to add Investigation property details to an SHA event. Adding details in the Investigation Properties dialog box, can assist in the classification and solving of future anomalies. After updating the Investigation properties, you must save the investigation.

<p>To access</p>	<ul style="list-style-type: none"> • Applications > Service Health Analyzer, double-click an investigation in the Investigation List, and in the Topology View, or the Metrics View, click  Investigation Properties. • From the Anomaly Highlights page, click Investigate Further, and in the Topology View or Metric View, click  Investigation Properties.
<p>Relevant tasks</p>	<p>"How to Create an Investigation" (on page 129)</p>

User interface elements are described below:

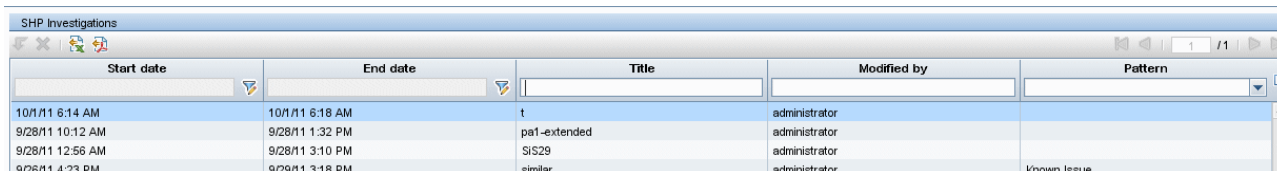
UI Element	Description
	<p>Associate new ticket. Opens the Associate new ticket dialog box where you can enter the ticket data.</p>
	<p>Detach ticket. Select the relevant tickets and click the button to remove the manual link between the selected tickets and the investigation.</p>
<p>Description</p>	<p>A description of the investigation.</p>

UI Element	Description
Time-frame	<p>The time frame of the investigation.</p> <p>Note: If the anomaly is still open, the last time value displays the current server time.</p>
Created by	The first user to save the investigation.
Last modified by	The name of the last user to modify the investigation.
Ticket ID	<p>The Ticket IDs that you want to associate with the investigation.</p> <p>You manually enter Ticket IDs, and this connects the Ticket ID to an anomaly.</p>
No pattern/ Pattern of type	<p>Select to associate the investigation with a pattern. You can select from the list of available patterns.</p> <p>To add or remove pattern selections:</p> <ol style="list-style-type: none"> 1. Select Admin > Platform > Infrastructure Settings: 2. Select Application, and then select Service Health Analyzer. 3. In the Service Health Analyzer - UI table, locate the Anomaly Pattern Type field. Modify the default patterns. <p>Note: Once an investigation is assigned a pattern, it can be included as a suspect in the Anomaly Highlights window.</p> <p>Pattern investigations are compared with anomalies to help you determine the cause of the anomaly. For concept details, see "Identifying Similar Patterns" (on page 64).</p>
Comments	<p>Click  to add your comments to the investigation description. Your user name and the timestamp are automatically added. For example:</p>

UI Element	Description
	<div data-bbox="467 254 1096 300">Comments</div> <div data-bbox="467 310 1096 357"></div> <div data-bbox="467 367 1096 756"><p>admin 1/7/10 3:36 PM: The table space is almost full. Not sure if this is the cause. Need further investigation by the DBA together with the application team.</p><p>admin 1/7/10 3:37 PM: We were able to pinpoint this to an asynchronous process that is filling the DB at a very high rate. This is a known error - see IM2975 for details.</p></div> <div data-bbox="467 787 1372 898"><p>Note: Adding comments is very important, as they can be used later to assist in solving anomalies.</p></div>

SHA Investigation Page




When you save an anomaly, you can access it later as an SHA investigation. This page displays a list of saved investigations .



Start date	End date	Title	Modified by	Pattern
10/1/11 6:14 AM	10/1/11 6:18 AM	t	administrator	
9/28/11 10:12 AM	9/28/11 1:32 PM	pa1-extended	administrator	
9/28/11 12:56 AM	9/28/11 3:10 PM	SIS29	administrator	
9/28/11 4:23 PM	9/29/11 3:18 PM	similar	administrator	Known Issue

To access	Select Applications > Service Health Analyzer
Relevant tasks	"How to Create an Investigation" (on page 129)

User interface elements are described below:

UI Element (A–Z)	Description
	Excel. Saves the investigation list in Excel format.
	PDF. Saves the investigation list in PDF format.
	Delete. Deletes the selected investigations.
Anomaly ID	The number of the anomaly associated with the investigation. The automatic detection automatically assigns an ID number to the anomaly. Note: Click an anomaly to access Advanced Analytics and display all the metrics of the selected anomaly. For details, see "Anomaly Highlights Page" (on page 71) .
Created by	The user who first saved the investigation.
Creation Date	The date the investigation was saved.
End Date	The time when the investigation ended.
Investigation ID	The investigation ID of the investigation.
Modified by	The name of the user who last saved the investigation.
Pattern	The type of pattern that fits the anomaly/investigation; for example: <code>Known problem</code> , <code>Noise</code> , <code>Other</code> . For details, see the patterns available in the Investigation Properties tab. For details, see "Investigation Properties Dialog Box" (on page 130) . Pattern investigations are compared with anomalies to help you solve the problem. For concept details, see "Identifying Similar Patterns" (on page 64) .

UI Element (A–Z)	Description
Start Date	The time when the investigation started.
Tickets	The ID of the tickets manually entered in the Investigation Properties dialog box. Only one ticket ID is stored for an anomaly. For user interface details, see "Investigation Properties Dialog Box" (on page 130) .
Title	The title of the investigation entered by the user when saving the investigation.

Managing SHA Databases — Overview

You can maintain and administer the databases BSM uses to store monitoring data. You can create and manage SHA databases directly from Platform Administration.

Before you configure your monitoring environment, you must configure the database into which you want monitoring data saved.

Note: The term database is used to refer to a database in Microsoft SQL server. The term user schema refers to a database in Oracle server.

SHA supports two database types:

- **Microsoft SQL server** - This database runs on Windows operating systems only. For details on how to configure a database on a Microsoft SQL server, see ["How to Configure an SHA Database on a Microsoft SQL Server" \(on page 138\)](#).
- **Oracle server** - This database runs on any BSM supported operating system. An Oracle server database is referred to as a user schema. For details on how to configure a database on an Oracle server user schema, see ["How to Configure a User Schema on an Oracle Server" \(on page 136\)](#).

For more information on BSM and databases, see the *HP Business Service Management Database Guide*.

This section includes:

How to Configure a User Schema on an Oracle Server	136
How to Configure an SHA Database on a Microsoft SQL Server	138
SHA Database Management Pag	139
SHA User Schema Properties — Oracle Server Page	140
SHA Database Properties — MS SQL Server Page	142

How to Configure a User Schema on an Oracle Server

This task describes how to configure one or more SHA user schemas on your Oracle server.

This task includes the following steps:

- ["Prerequisites" \(on page 136\)](#)
- ["Gather Connection Parameters" \(on page 136\)](#)
- ["Add a User Schema" \(on page 136\)](#)

1. Prerequisites

Before you begin, make sure that:

- a. You have created a dedicated default tablespace for SHA user schemas (and a dedicated temporary tablespace, if required).
- b. You are using a secure network connection if you do not want to submit database administrator connection parameters over a non-secure connection. If you do not want to submit database administrator connection parameters using your Web browser at all, you can manually create SHA user schemas and then connect to them from the Database Management page.

2. Gather Connection Parameters

Make sure that you have the following connection parameters to the database server:

- a. **Host name.** The name of the machine on which the Oracle server is installed.
- b. **SID.** The Oracle instance name that uniquely identifies the instance of the Oracle database being used, if different from the default value, **orcl**.
- c. **Port.** The Oracle listener port, if different from the default value, **1521**.
- d. **Database administrator user name and password.** The name and password of a user with administrative permissions on the Oracle server. These parameters are used to create the BSM user, and are not stored in the system.
- e. **Default tablespace.** The name of the dedicated default tablespace you created for SHA user schemas (for details on creating a dedicated tablespace, see Overview of Oracle Server Deployment in the Business Service Management Database Guide). If you did not create, and do not require, a dedicated default tablespace, specify an alternate tablespace. The default Oracle tablespace is called **users**.
- f. **Temporary tablespace.** The name of the dedicated temporary tablespace you created for SHA user schemas. If you did not create, and do not require, a dedicated temporary tablespace, specify an alternate tablespace. The default Oracle temporary tablespace is called **temp**.

If required, consult with your organization's database administrator to obtain this information.

3. Add a User Schema

- a. Access the Database Management page, located at **Admin > Platform > Setup and**

Maintenance > Manage SHA Databases.

- b. Select **Oracle** from the dropdown list, and click **Add**.
- c. Enter the parameters of your user schema on the **SHA Database Properties - Oracle Server** page. For user interface details, see ["SHA User Schema Properties — Oracle Server Page" \(on page 140\)](#).

If your SHA database is part of Oracle Real Application Cluster (RAC), see Support for Oracle Real Application Cluster in the Business Service Management Database Guide.

How to Configure an SHA Database on a Microsoft SQL Server

This task describes how to configure one or more SHA databases on a Microsoft SQL server.

This task includes the following steps:

- ["Prerequisites" \(on page 138\)](#)
- ["Add a Database" \(on page 138\)](#)

1. Prerequisites

Before you begin, make sure that you have the following connection parameters to the database server:

- a. **Server name.** The name of the machine on which a Microsoft SQL server is installed. If you are connecting to a non-default Microsoft SQL server instance in dynamic mode, enter the server name in the following format:

```
<host_name>\<instance_name>
```

- b. **Database user name and password.** The user name and password of a user with administrative rights on a Microsoft SQL server (if using SQL server authentication).
- c. **Server port.** The Microsoft SQL server's TCP/IP port. The default port, 1433, is automatically displayed. You must change the port number in one of the following instances:
 - The default Microsoft SQL server instance listens to a port other than 1433.
 - You connect to a non-default Microsoft SQL server instance in static mode.
 - You connect to a non-default Microsoft SQL server instance in dynamic mode. In this case, enter port number 1434.

If required, consult with your organization's DBA to obtain this information.

2. Add a Database

- a. Access the Database Management page, located at **Admin > Platform > Setup and Maintenance > Manage SHA Databases**.
- b. Select **MS SQL** from the dropdown list, and click **Add**.
- c. Enter the parameters of your database on the **SHA Database Properties - MS SQL Server** page. For user interface details, see ["SHA Database Properties — MS SQL Server Page" \(on page 142\)](#).

How to Delete Analytics Databases

You can delete all the analytics databases. For example, if you are replacing a server, you may need to delete all the databases from the old server and reconfigure them on the new server. Databases are deleted using the BSM Browser.

Caution: This procedure will delete **all** analytics databases. There is no way to delete a single database.

1. On the server, open BSM Browser located in the following directory:
<BSM_INSTALL_DIR>\tools\bsmbrowser
2. In the BSM Browser, select **File > Topaz Connect**.
3. Select the required Database and click **Ok**.
4. Enter the following command: `delete from ANALYTICS_DATABASES`
5. In BSM, Select **Admin > Platform > Setup and Maintenance > Manage Analytics Databases** and refresh the page to confirm that all analytics databases have been deleted.


Once you have deleted the databases you need to manually configure new databases. For details, see [How to Configure an SHA Database on a Microsoft SQL Server \(on page 138\)](#) or [How to Configure a User Schema on an Oracle Server \(on page 136\)](#) and then restart BSM.

SHA Database Management Page

This page enables you to maintain and administer the databases used to store SHA data.

To access	Select Admin > Platform > Setup and Maintenance > Manage SHA Databases
Relevant Tasks	<ul style="list-style-type: none">• How to Configure a User Schema on an Oracle Server"(onpage136)• How to Configure an SHA Database on a Microsoft SQL Server" (on page 138)

User interface elements are described below:

UI Element (A-Z)	Description
	Click to edit the properties of the Microsoft SQL server database or Oracle server user schema.
Add	Adds a Microsoft SQL server database or Oracle server user schema, as specified in the dropdown database list.
Db Name	The name of the database.
Db Type	The type of database, either Microsoft SQL or Oracle.
Host	The name of the server on which the database is running.

SHA User Schema Properties — Oracle Server Page

This page enables you to configure one or more SHA user schemas on your Oracle server.

To access	Select Admin > Platform > Setup and Maintenance > Manage SHA Databases , select Oracle from the dropdown database list and click Add .
Important information	<ul style="list-style-type: none"> It is recommended that you configure Oracle server user schemas manually, and then connect to them in the Database Management page. For details on manually configuring Oracle server user schemas, see Overview of Oracle Server Deployment in the Business Service Management Database Guide. User schema creation can take several minutes. The browser might time out before the creation process is completed. However, the creation process continues on the server side. <p>If a timeout occurs before you get a confirmation message, verify that the user schema name appears in the database list on the Database Management page to ensure that the user schema was successfully created.</p>
Relevant tasks	"How to Configure a User Schema on an Oracle Server" (on page 136)
See also	"Managing SHA Databases — Overview " (on page 135)

User interface elements are described below:

UI Element (A-Z)	Description
Create database and/or tables	<p>Select or clear as required.</p> <ul style="list-style-type: none"> To create a new user schema, or connect to an existing, empty user schema and populate it with SHA tables, select the check box. To connect to an existing user schema already populated with SHA tables, clear the check box. <p>Note: Clearing this check box disables the database administrator connection parameter and tablespace fields on the page, and instructs the platform to ignore the information in these fields when connecting to the Oracle server machine.</p>
Database administrator password	<p>Enter the password of a user with administrative permissions on Oracle server.</p> <p>Note: This field is enabled only if you selected the Create database and/or tables check box.</p>
Database administrator user name	<p>Enter the user name and password of a user with administrative permissions on Oracle server.</p>

UI Element (A-Z)	Description
	<p>Note: This field is enabled only if you selected the Create database and/or tables check box.</p>
Default tablespace	Enter the name of the default tablespace designated for use with SHA user schemas.
Host name	Enter the name of the machine on which the Oracle server is installed.
Port	Enter the required Oracle listener port, or accept the default value.
Retype password	Retype the user schema password.
SID	Enter the required Oracle instance name, or accept the default value.
Temporary tablespace	Enter the name of the temporary tablespace designated for use with SHA user schemas. Default Value: temp
User schema name	<ul style="list-style-type: none"> • If you are configuring a new user schema, enter a descriptive name for the user schema. • If you are connecting to a user schema that was previously created, enter the name of the existing user schema.
User schema password	<ul style="list-style-type: none"> • If you are configuring a new user schema, enter a password that enables access to the user schema. • If you are connecting to a user schema that was previously created, enter the password of the existing user schema. <p>Note: You must specify a unique user schema name for each user schema you create for SHA on the Oracle server.</p>

SHA Database Properties — MS SQL Server Page

This page enables you to configure a new or existing SHA database on Microsoft SQL server.

To access	Select Admin > Platform > Setup and Maintenance > Manage SHA Databases , select Microsoft SQL from the dropdown database list and click Add .
Important information	<ul style="list-style-type: none"> It is recommended that you configure Microsoft SQL server databases manually, and then connect to them in the Database Management page. For details on manually configuring Microsoft SQL server databases, see "Overview of Microsoft SQL server Deployment" in the Business Service Management Database Guide. Database creation can take several minutes.
Relevant tasks	"How to Configure an SHA Database on a Microsoft SQL Server" (on page 138)
See also	"Managing SHA Databases — Overview " (on page 135)

User interface elements are described below:

UI Element (A-Z)	Description
Create database and/or tables	Select or clear as required. <ul style="list-style-type: none"> To create a new database, or connect to an existing, empty database and populate it with SHA tables, select the check box. To connect to an existing database already populated with SHA tables, clear the check box.
Database name	<ul style="list-style-type: none"> If you are configuring a new database, type a descriptive name for the database. If you are connecting to a database that was previously created, type the name of the existing database.
Password	<ul style="list-style-type: none"> Should remain empty if you are using Windows authentication. Make sure the BSM service logs in with a windows user configured in the database server as an authorized windows login. If you are using SQL server authentication, enter the password of a user with administrative rights on Microsoft SQL server.
Port	Enter the port number if: <ul style="list-style-type: none"> The Microsoft SQL server's TCP/IP port is configured to work on a port different from the default (1433). You use a non-default port in static mode. You use a non-default port in dynamic mode. In this case, enter port 1434.

UI Element (A-Z)	Description
Server name	Enter the name of the machine on which the Microsoft SQL server is installed. If you are using a non-default instance in dynamic mode, enter the server name in the following format: <my_server\my_instance>
SQL server authentication	Select if the Microsoft SQL server is using SQL server authentication.
User name	<ul style="list-style-type: none">• Should remain empty if you are using Windows authentication.• If you are using SQL server authentication, enter the user name of a user with administrative rights on Microsoft SQL server.
Windows authentication	Select if the Microsoft SQL server is using Windows authentication.

Advanced Configuration Overview

The advanced configuration section, contains procedures that enable you to customize parts of the SHA operations.

The procedures in this section should only be carried out by someone who is expert in the relevant area.

Caution: Incorrectly carrying out advanced configuration procedures can damage SHA. It is therefore recommended that you back up files before editing them.

This section includes:

How to Edit the SHA Metric Selection XML Files for Baselining	145
How to Control the Amount of Data Stored in the Aggregation Database	154
How to Create a TQL Drilldown	156
How to Edit an SHA Infrastructure Setting	157
Build a Business CI Model	158

How to Edit the SHA Metric Selection XML Files for Baselining

SHA collects metrics and calculates metric baselines for a CI based on a combination of the CIs selected in the CI selection feature of SHA, and the contents of out-of-box SHA XML files. The XML files, are stored on the Analytics server in **\<BSM installation Directory>\confanalytics\metadata\Default**. Each supported data collector (SiteScope, NNMI, BPM, RUM, PA and Diagnostics) has a separate XML file that contains a list of metric types that are baselined. Only metric types included in the XML file have metric baselines created.

Caution: Only subject matter experts should edit these files. It is recommended that you edit these files using an XML editor, and that you take a backup of a file before editing it.

The following tasks describe how to edit XML files and reload any changes:

How To Add and Remove Metric Types in the SiteScope, Diagnostics and PA XML Files.....	146
How To Add and Remove Metric Types in the BPM, RUM, and NNM XML Files.....	148
How to Reload Metadata.....	151

How To Add and Remove Metric Types in the SiteScope, Diagnostics and PA XML Files

Baselined metric types are specified within the <Matches> tag of the relevant data collector XML file. Each **match value** represents a metric type that has a baseline that is built and periodically maintained. You might want to add a metric type that is not included in the out-of-box data collector specific XML file, or comment out a metric type that is not required. This task describes how to edit SiteScope Diagnostics, and PA XML files.

Note: In the Diagnostics XML file, only match values of under 81 characters can be processed.

To add a new metric type for baselining

1. Open the relevant SiS, Diagnostics, or PA .xml file in an XML editor.
2. Inside the <Matches> tag, add an additional match value in the following format:

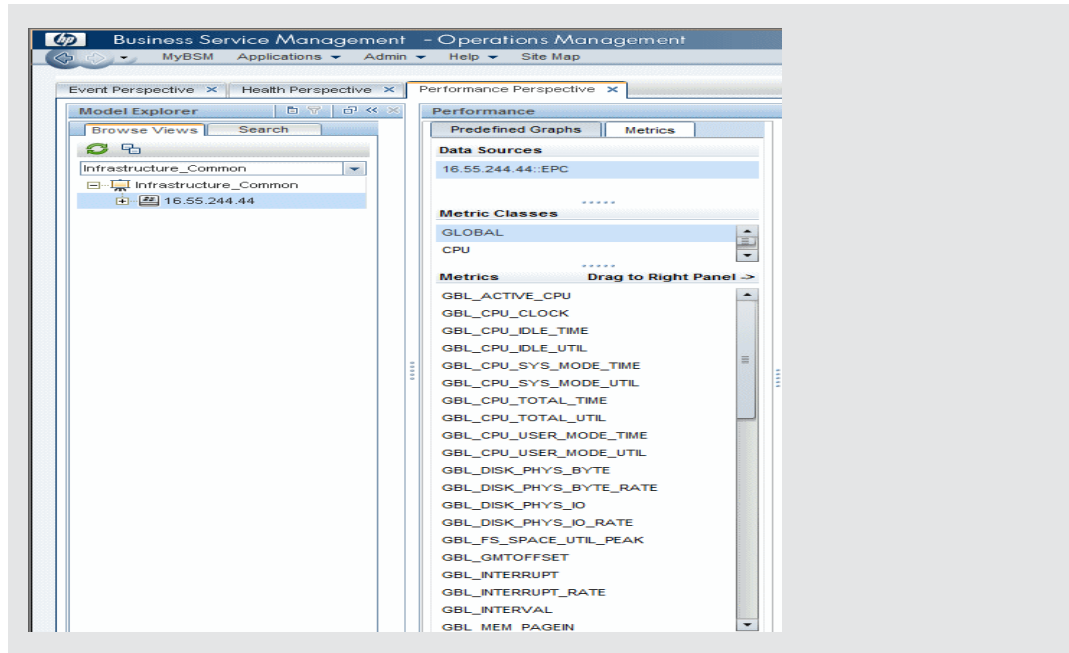
<match value="<Metric type name>" />, where <Metric type name> is the name as defined in the relevant metric table.

Example:

To add a metric called newmetric, in the list of metric values, add another line <match value="newmetric" />

Example:

To identify Performance Agent (PA) metric types, select **Operations Management > Performance Perspective**. In the Browse Views tab, select Infrastructure_common, and in the Performance pane, click the Metrics tab. A list of the available PA metrics is displayed.



3. Save the changes, and reload the metadata. For more information, see ["How to Reload Metadata" \(on page 151\)](#).

To comment out a metric type currently being baselined.

1. Open the relevant SiS, Diagnostics, or PA .xml file in an XML editor.
2. Comment out a <Match value="<metric to be deleted>" /> line, by adding !-- after the < character, and -- before > in the line for the metric you no longer want to baseline. To return the metric for baselining, remove the !--, and the -- for the specific Match value line in the relevant XML file.

Example:

The following example shows how to comment out the Total Accesses metric type.

```
<!-- match value="Total Accesses" /-->
```

3. Save the changes, and reload the metadata. For more information, see ["How to Reload Metadata" \(on page 151\)](#).

How To Add and Remove Metric Types in the BPM, RUM, and NNM XML Files

Baselined metric types are specified within the <Metric-type> tag of the relevant data collector XML file. Values within the <Metric-type> tag, represent different elements of the metric type that has a baseline that is built and periodically maintained. You might want to add a metric type that is not included in the out-of-box data collector specific XML file, or comment out a metric type that is not required. This task describes how to edit BPM, RUM, and NNM XML files.

Note: RUM metrics are not location aware by default.

To add a new metric type for baselining

1. Open the BPM, RUM, or NNM .xml file in an XML editor.
2. Copy the "Example metric-type tag configuration" section in the XML file, beginning with <!-- Metric-type and ending with </metric-type -->, to a location in the file immediately after a </metric-type> tag.

Note: Ensure that you do not copy the description of the example metric-type line, beginning with <!-- This is an example metric-type tag, and ending with "change_me" places -->.

3. Remove the !-- from the beginning of the copied example metric configuration, and the -- from the end of the example.

Note: Ensure that there are no other commented out lines within the Metric-type tag.

4. Change the values indicated in the copied example with a "change_me" string to reflect the new metric that you want to be baselined.
 - a. To identify mapped-to names for BPM, in an XML editor, open the <BSM-install-dir>\dat\metadata\bpm_trans_t.xml file, and under the <MD_SAMPLE> tag where NAME="trans_t", identify the <MD_FIELD> tags with the NAME values for the measurement, mean and standard deviation. Copy those <MD_FIELD> NAME values to the relevant mapped-to value in the copied sample text.

Enter meaningful strings for the Metric-type name, measurement name and measurement unit.

- b. To identify mapped-to names for RUM, in an XML editor, open the <BSM-install-dir>\dat\metadata\rum_trans_t.xml file, and under the MD_SAMPLE tag where NAME="rum_trans_t", identify the <MD_FIELD> tags with the NAME values for the measurement, mean and standard deviation. Copy those <MD_FIELD> NAME values to the relevant mapped-to value in the copied sample text.

Enter meaningful strings for the Metric-type name, measurement name and measurement unit.

- c. To identify mapped-to names for NNM, in an XML editor, open the <BSM-install-

dir>\dat\metadata\analytics_nnm_metric_t.xml file, and under the MD_SAMPLE tag where NAME="nnm_metric_t" identify the <MD_FIELD> tags with the NAME values for the measurement, mean and standard deviation. Copy those <MD_FIELD> NAME values to the relevant mapped-to value in the copied sample text. Only one MD_SAMPLE tag exists in this file.

Enter meaningful strings for the Metric-type name, measurement name and measurement unit.

5. For the BPM and NNM XML files, if you want the suspect metric to be associated with a specific layer name, add a <layer name> value. This can however add a processing overhead to the Analytics server.

Example: To configure a metric to report as part the Network suspect layer that appears in the anomaly Highlights page, add the tag and value **<layer name="Network" />** below the <status mapped-to="u_iStatus" available="0" /> line.

6. Save the changes, and reload the metadata. For more information, see ["How to Reload Metadata" \(on page 151\)](#).

To comment out a metric type currently being baselined.

1. Open the BPM, RUM, or NNM xml file in a text editor.
2. For the specific metric, comment out the contents of the <metric-type> tag until </ metric-type>, by adding ! – after the < of the metric-type tag, and – before the > of the /metric type tag close. As shown in the following example:

Example:

```
<!-- metric-type name="ssl-time-transaction" mapped-to="trans_t">
- <consumers>
<consumer name="SHA" />
</consumers>
<time-stamp mapped-to="time_stamp" />
<mean mapped-to="baseline_ssl_time_loc_mean" />
<std-dev mapped-to="baseline_ssl_time_loc_std" />
<measurement name="SSL Time" unit="millisecond" mapped-to="u_iWSSLTime" />
- <dimensions>
<dimension name="Transaction" mapped-to="u_iTransactionId"
type="CITYPE:business_transaction" />
<dimension name="Application" mapped-to="application_id" type="CITYPE:business_
application" />
<dimension name="Location" mapped-to="u_iLocationId" type="CITYPE:location" />
```

```
</dimensions>  
<status mapped-to="u_iStatus" available="0" />  
<layer name="SSL" />  
<filters />  
<downtime mapped-to="application_id" />  
</metric-type >
```

Note: Ensure that there are no other commented out lines within the Metric-type tag.

3. Save the changes, and reload the metadata. For more information, see ["How to Reload Metadata" \(on page 151\)](#).

How to Reload Metadata

To activate saved changes to the data collector XML files, you must reload the metadata.

This task describes methods on how to reload metadata. You can use either method to reload metadata.

Method 1 - How to reload metadata by restarting BSM on the Gateway, Data Processing, and Analytics servers

1. Log on as administrator to the JMX console on the Analytics server, and click **Reload**.
2. Under `java.lang.string.reloadmetadata`, enter the value **False**, and then click **Invoke**.
3. On all Data Processing servers (DPS), restart BSM as follows:

Select **Start > Programs > HP Business Service Management > Administration > Disable | Enable Business Service Management**

Note: First Disable and then Enable

4. On all BSM Gateway servers, restart BSM as follows:

Select **Start > Programs > HP Business Service Management > Administration > Disable | Enable Business Service Management**

Note: First Disable and then Enable BSM

5. On the Analytics server, restart BSM as follows:

Select **Start > Programs > HP Business Service Management > Administration > Disable | Enable Business Service Management**

Note: First Disable and then Enable BSM

Note:

- To start or stop HP Business Service Management in Linux, run `/opt/HP/BSM/scripts/run_hpbsm start | stop`
- To start, stop, or restart HP Business Service Management using a daemon script, run `/etc/init.d/hpbsmd {start| stop | restart}`

Method 2 - How to reload metadata by restarting processes

1. Log on as administrator to the JMX console on the Analytics server as follows:

In your Web browser address bar, enter:

`http://<analytic_server_fqdn>:29924/mbean?objectname=Topaz%3AService%3DAnalyticsMetadata`, where `<analytic_server_fqdn>` is the fully qualified domain name of your analytics server.

- In java.lang.string.reloadmetadata, Under Value, click **False**, and then click **Invoke**.

java.lang.String reloadMetaData

reload metadata from XML files into the database

Parameters

Name	Class	Value	Description
validateChanges	boolean	<input checked="" type="radio"/> true <input type="radio"/> false	whether to check for conflicts between current (stored in DB) and new meta-data settings before overwriting the current settings

- On all Data Processing servers (DPS), restart the pi_engine process as follows:

In your Web browser address bar, enter:

http://<Each DPS

fqdn>:11021/invoke?operation=showServiceInfoAsHTML&objectname=Foundations

%3Atype%3DNannyManager, and click the **Restart** link of the **pi_engine** process.

<Each DPS fqdn>, should be replaced with the fully qualified domain name of a Data Processing server. This must be performed on each DPS.

pi_engine	hpbsm_pi_engine	STARTED	16:58:26 3/Nov/2011	1	40	Click Here	Thread dump , Restart , Start , Stop
-----------	-----------------	---------	---------------------	---	----	----------------------------	--

Note: Refresh the screen and confirm that the pi_engine process has a Status of STARTED, before continuing to the next step.

- On all BSM Gateway servers, restart the analytics_loader process as follows:

In your Web browser address bar, enter:

http://<each GW

fqdn>:11021/invoke?operation=showServiceInfoAsHTML&objectname=Foundations

%3Atype%3DNannyManage, and click the **Restart** link of the analytics_loader process.

<each GW fqdn>, should be replaced with the fully qualified domain name of a BSM Gateway server. This must be performed on each Gateway server.

analytics_loader	hpbsm_analytics_loader	STARTED	16:18:14 6/Nov/2011	1	17	Click Here	Thread dump , Restart , Start , Stop
------------------	------------------------	---------	---------------------	---	----	----------------------------	--

Note: Refresh the screen and confirm that the analytics_loader process has has a Status of STARTED, before continuing to the next step.

- On the Analytics server, restart the basel_engine and analytics_datacollector processes.

In your Web browser address bar, enter:

http://<analytics_server_host_

name>:11021/invoke?operation=showServiceInfoAsHTML&objectname=Foundations

%3Atype%3DNannyManager and and click the **Restart** links of the **basel_engine** and the **analytics_datacollector** processes.

<analytics_server_host_name>, should be replaced with the fully qualified domain name of your Analytics server.

Service name	Process name	Status	Status since	Restart count	Order	JMX	Operations
basel_engine	hpbsm_basel_engine	STARTED	13:58:16 26/Oct/2011	5	24	Click Here	Thread dump , Restart , Start , Stop
analytics_dc	hpbsm_analytics_dc	STARTED	18:38:08 24/Oct/2011	2	40	Click Here	Thread dump , Restart , Start , Stop

[Refresh](#)

Note: Refresh the screen and confirm that the basel_engine and analytics_dc processes have a Status of STARTED.

How to Control the Amount of Data Stored in the Aggregation Database

By default, Service Health Analyzer is configured to store up to 60 days of aggregated historical metric data. For each aggregated metric, SHA stores, the metric value, mean value, standard deviation value, and an unavailable value. These values are aggregated at 5 minute intervals.

This topic describes how to control the amount of data stored to the aggregated database.

You can reduce the amount of data stored in the Aggregated database by controlling how aggregated data is stored by:

- Reducing the number of days that aggregated historical data is stored.

If you reduce the number of days of stored aggregated data, then only aggregated historical data for the specified time is presented in the Metric Graph pane in the Metrics View Tab.

- Storing only the aggregated metric value field.

The following limitations exist if you choose to only store the aggregated metric value field:

- You can only view a metric baseline sleeve for up to the previous 2 days. Any older historical data older cannot be displayed with its metric baseline.
- Unavailability data is only available for up to the previous 2 days. Any older historical unavailability data cannot be displayed for the metric.

How to reduce the historical aggregated data period

1. Open the \\<GW>\<HPBSM>\conf\pmanager\aa_pmconfig.properties file with a text editor.
2. In the [AA_AGGR_VAL], [AA_AGGR_MEAN], [AA_AGGR_STDDEV], and [AA_AGGR_STATUS] sections, change the values of the **Range** and **Lifetime** parameters to the number of days of historical aggregated data that you want to store in the Aggregated database.

Note: This setting should be the same as the **Investigation Past days** infrastructure setting .

For more information on how to edit infrastructure settings, see ["How to Edit an SHA Infrastructure Setting" \(on page 157\)](#).

3. Save the file.

How to only store the aggregated metric value field contents

1. In your Internet browser address bar, Enter **http://<GW>:8080/jmx-console/HtmlAdaptor?action=inspectMBean&name=Foundations%3Aservice%3DInfrastructure+Settings+Manager** where <GW> is the FQDN of your BSM gateway.
2. If required, login to the JMX Console.
3. Locate the setGlobalSettingValue() setting, enter the following values, and then click **Invoke**:
context = **pi-settings**;
setting = **noa.analytics.aggr.values.only**;


new value = **true**

Note: The default value is False.

How to Create a TQL Drilldown

Using a TQL drill down, you can merge the topology configured in the TQL, to the active topology.


This task describes how to create a TQL drill down that you can access from the Topology View.

1. Select **Admin > RTSM Administration > Modeling Studio**.
2. Click the **Resource** tab, right-click **Service Health Analyzer**, click **New**, and then click **Query**.
3. Drag a node to the Query Definition Pane, right-click the node, click **Query Node Properties**, and then rename the node to **CI_ID**.
4. Drag another node to the Query Definition Pane, right-click the node, click **Query Node Properties**, and then rename the node to **RETRIEVED_ITEM**.
5. Create the relevant link between the nodes.
6. Click  **Save**, to save the query.

When you right click a CI node in the Topology view that has a relationship to the TQL, the Run TQL option appears.

How to Edit an SHA Infrastructure Setting

This task describes how to change an Service Health Analyzer infrastructure setting.

1. Select **Admin > Platform > Infrastructure Settings**.
2. In **Applications**, select **Service Health Analyzer**
3. For the relevant infrastructure setting, click  **Edit Setting**, and modify the value.

Build a Business CI Model

SHA creates by default events on software element, business service, and business application CI Types. You must create Business CI models that connect those CI types to other non-default CI types for example, infrastructure CI or other business CI types in order to receive SHA events for the non-default CI Types. Business CI models enable SHA to correlate between end-user applications and the underlying infrastructure that supports those applications.

For more information on how to build a business CI model, see "Build a Business CI Model - Scenario" in the *Modeling Guide*.

Note: When you build an SHA CI business model ensure that you add within the model, infrastructure and end-user monitors.

