



# Operations Bridge Analytics

Software Version: 3.00

# Operations Bridge Analytics Help

Document Release Date: January 2017

Software Release Date: January 2017



**Hewlett Packard**  
Enterprise

## Legal Notices

### Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise 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 Hewlett Packard Enterprise 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

© 2016 - 2017 Hewlett Packard Enterprise Development LP

### Trademark Notices

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

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

Citrix® and XenDesktop® are registered trademarks of Citrix Systems, Inc. and/or one more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

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.

iPad® and iPhone® are trademarks of Apple Inc.

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

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft®, Windows®, Lync®, Windows NT®, Windows® XP, Windows Vista® and Windows Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NVIDIA® is a trademark and/or registered trademark of NVIDIA Corporation in the U.S. and other countries.

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

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

SAP® is the trademark or registered trademark of SAP SE in Germany and in several other countries.

UNIX® is a registered trademark of The Open Group.

## Documentation Updates

To check for recent updates or to verify that you are using the most recent edition of a document, go to: <https://softwaresupport.hpe.com/>.

This site requires that you register for an HPE Passport and to sign in. To register for an HPE Passport ID, click **Register** on the HPE Software Support site or click **Create an Account** on the HPE Passport login page.

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

## Support

Visit the HPE Software Support site at: <https://softwaresupport.hpe.com/>.

Most of the support areas require that you register as an HPE Passport user and to sign in. Many also require a support contract. To register for an HPE Passport ID, click **Register** on the HPE Support site or click **Create an Account** on the HPE Passport login page.

To find more information about access levels, go to: <https://softwaresupport.hpe.com/web/softwaresupport/access-levels>.

**HPE Software Solutions Now** accesses the Solution and Integration Portal website. This site enables you to explore HPE product solutions to meet your business needs, includes a full list of integrations between HPE products, as well as a listing of ITIL processes. The URL for this website is <https://softwaresupport.hpe.com/km/KM01702731>.

# Contents

Features .....	6
Chapter 1: Dashboards .....	8
Chapter 2: Search Tool .....	32
Filter Search Query Results .....	35
Text Search .....	37
Track Message Groups and Parameters .....	51
Log and Event Analytics .....	53
Chapter 4: Play Back History .....	57
Chapter 5: Predictive Analytics .....	59
Chapter 6: Alerts .....	61
Chapter 7: Correlate Metrics .....	71
UI Description .....	72
Chapter 8: Topology Manager .....	74
Chapter 9: About the Analytics Query Language (AQL) .....	77
Chapter 10: Anomaly Detection .....	78
Collections .....	81
Chapter 11: General Collection Information .....	82
Chapter 12: Installing and Configuring a Third-Party Agent .....	91
Chapter 13: Adding a New Source Type — Command Line Method .....	93
Important Prerequisite Steps .....	94
Configuration Steps .....	97
Troubleshooting the Custom CSV Collection .....	106
Removing the Registration and Data for a Custom CSV Collection .....	107
Detailed Configuration Steps .....	111
Generating and Configuring Templates (Custom SiteScope Collection) .....	112
Configuring SiteScope for Integrating Data with Operations Bridge Analytics(Manual Method) .....	121
Task 1: Creating a SiteScope Tag .....	121
Task 2: Using the New SiteScope Tag to Mark the Monitor or	122

Monitor Groups .....	
Task 3: Creating a New Data Integration Preference .....	123
Chapter 14: Troubleshooting Source Type Manager Error Messages .....	126
Chapter 15: Managing the Content for Data Source Types .....	133
Chapter 16: Using Tags for Source Types .....	136
User Tasks .....	139
Command Line Usage Examples for Creating Tags .....	139
Chapter 17: Communicating Collection Names and Meta Data Information to your Users .....	147
<b>Integrations .....</b>	<b>148</b>
Chapter 18: BSM and OMi Integrations .....	149
Chapter 19: Configure Log Integrations .....	159
Map Arcsight Logger Data .....	160
Reference .....	166
Map Splunk Data .....	167
<b>Administration .....</b>	<b>171</b>
Chapter 20: Administering Operations Bridge Analytics Performance .....	172
Improving Log Analytics Collection Performance .....	172
Increasing JVM Memory to Improve Collection Performance .....	173
Increasing the Index Entity Cache Size .....	173
Managing Collected Data File Usage with Existing Delete Policies .....	174
Monitoring Operations Bridge Analytics Processes .....	175
Restarting Operations Bridge Analytics Processes .....	177
Restarting Operations Bridge Analytics Processes after a Vertica Shutdown .....	178
Restarting the Operations Bridge Analytics Server and Operations Bridge Analytics Collector Host .....	180
Throttling Operations Bridge Analytics Network Traffic .....	180
Tuning Apache Kafka Processes .....	182
Expanding the Apache Kafka Cluster in Operations Bridge Analytics ...	182
Tuning Apache Kafka Disk Partition Capacity .....	186
Chapter 21: Adding More Operations Bridge Analytics Servers .....	187
Chapter 22: Changing the Password of an Operations Bridge Analytics Collector Host .....	188
Chapter 23: Checking the Status of Operations And Operations Bridge	189

Analytics Servers .....	
Chapter 24: Configuring LDAP Server Authentication for Operations Bridge Analytics .....	193
Chapter 25: Content Packs .....	197
Chapter 26: Daylight Savings Time Codes .....	199
Chapter 27: Log Files in Operations Bridge Analytics .....	211
Using and Maintaining Audit Log Files .....	211
Chapter 28: Maintaining the Operations Bridge Analytics Database .....	214
Backing up and Restoring Data .....	214
Managing Vertica Data .....	214
Resetting the Vertica Database Password .....	215
Setting Collection Retention Periods .....	218
Chapter 29: Manage Users and Tenants .....	219
Important Tenant Information .....	228
Chapter 30: Modifying Unit Scaling on Collected Data .....	233
Chapter 31: Registering Operations Bridge Analytics Collector Hosts .....	235
Removing a Collection Registration for a Tenant .....	236
Chapter 32: Resolve Host Aliases .....	239
Chapter 33: Using Parametric Dashboards .....	242
Troubleshooting .....	249
Chapter 34: Collection Troubleshooting Topics .....	249
Chapter 34: General Troubleshooting Tips .....	253
Chapter 34: Integration Troubleshooting Topics .....	255
Send documentation feedback .....	258

# Features

This section contains the following topics:

["Dashboards" on page 8](#)

["Search Tool" on page 32](#)

["Play Back History" on page 57](#)

["Predictive Analytics" on page 59](#)

["Alerts" on page 61](#)

["Correlate Metrics" on page 71](#)

["Topology Manager" on page 74](#)

["About the Analytics Query Language \(AQL\)" on page 77](#)

["Anomaly Detection" on page 78](#)

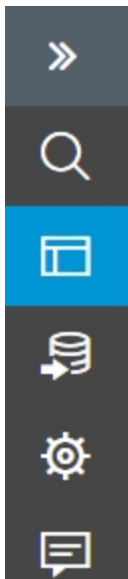


# Chapter 1: Dashboards

A dashboard is a graphical display of your data in one or more Query Panes. Dashboards can be custom-defined or you can use one of the out-of-the-box dashboards. Dashboards are automatically updated with the latest incoming data and can be shared with other users.

To access

From the main toolbar on the left, select the Dashboard icon.



## Learn About

### Dashboards Overview

A dashboard is the graphical user interface for troubleshooting your IT operations problems.

Dashboards are collections of Query Panes defined in a specific layout. Dashboards allow you to customize your user interface and save the settings.



The first time you access Operations Bridge Analytics, it displays the **LogsOverview** dashboard. This dashboard lists all of the log messages from the log files that have been configured to be collected in your IT environment. Use this dashboard as a starting point to look for errors that might have occurred.

You can only edit dashboards that created by your Operations Bridge Analytics user. To edit other dashboards, you can save a copy under a different name.

## Default Visualizations

If you select a visualization unsupported by your Analytics Query Language (AQL) search query, Operations Bridge Analytics uses the visualizations described in "[Default Visualizations by Types of Analytic Functions](#)" below. See [Dashboards and Query Panes](#) for more information about selecting a visualization in a dashboard query pane. See the AQL Developer Guide for more information about AQL.

### Default Visualizations by Types of Analytic Functions

AQL Query	Default Visualization	Valid Visualizations
Includes a Moving Aggregate (Time Series) Analytic Function	Line Chart	Line chart, heat map, bar chart, and pie chart
Includes an Overall Aggregate (Summary) Analytic Function	Table	Table, bar chart, and pie chart

**Tip:** When using the topN or bottomN analytic function, Operations Bridge Analytics displays a bar chart by default. You can also use topN and bottomN analytic functions to visualize pie charts and tables.

## Data Types

### Moving Aggregate Data Visualizations

Operations Bridge Analytics presents moving aggregate (time series) data as line charts, heat maps, bar charts, and pie charts. Moving aggregate (time series) data is data displayed according to a time interval within a specified time range.

This data might include the total, average, minimum, or maximum values calculated at each interval over the specified time range. It might also include the count of unique instances or values. For example, you might want to view CPU utilization for each unique host in a specified domain at 1-hour intervals for the last 24 hours.

Operations Bridge Analytics shows time series (moving aggregate) data as a line chart by default.

## Overall Aggregate Data Visualizations

Operations Bridge Analytics presents overall aggregate data as bar charts, pie charts, or tables.

Overall aggregate data is data grouped by total, average, minimum, or maximum values within a specified time range.

Operations Bridge Analytics shows overall aggregate (summary of totals, counts, averages, maximum values, or minimum values) data in table format by default.

### About Bar Charts

You can use both moving aggregate (time series) and overall aggregate (summary) analytic functions to display your results as a bar chart.

Group the Results and Select the Items to Display

- You can group the items in a bar chart by entities or metrics. Entities are defined as any items measured by your metrics. To do so, select **Group by Entity** or **Group by Metric**.
- Select the entities or metrics to appear by using the drop-down menu.
- Select the group to appear by using the **Go To Page** menu or the arrows at the bottom of the pane.

### About Heat Maps

You can use moving aggregate (time series) analytic functions to display your results as a heat map.

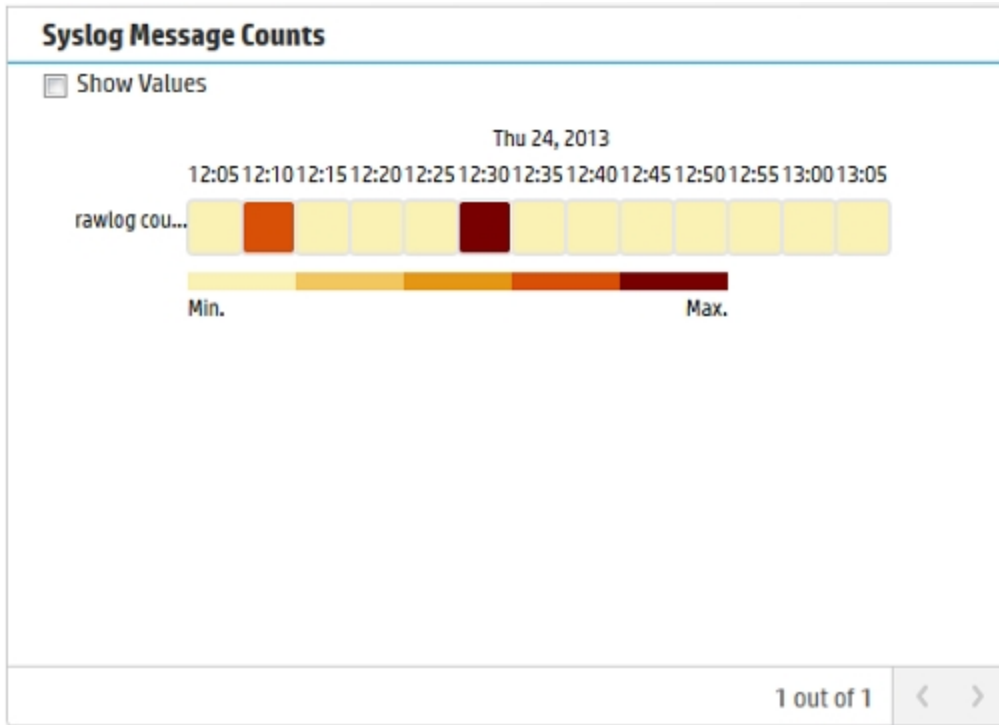
Moving aggregate (time series) analytic functions show results according to a time interval within a specified time range. This data might include actual metric values or total, average, minimum, or maximum values calculated at each interval over the specified time range. For example, you might want to view CPU utilization for each unique host in a specified domain at 1-hour intervals for the last 24 hours.

Heat maps use a series of color-coded rectangles to map returned values to a scale based on the minimum and maximum values. Each cell color is determined as follows:

- Operations Bridge Analytics identifies the minimum and maximum value per the group by entity for the selected metric. The minimum and maximum values are identified in the available results for the selected duration.
- Operations Bridge Analytics calculates the percentage of each cell value in relation to the minimum and maximum value.

- The calculated percentage value is associated with a pre-determined color shade. For example, a value of 50 percent might be associated with a medium shade of orange.

The following heat map example displays the number of syslog log file messages generated over a specified time period:

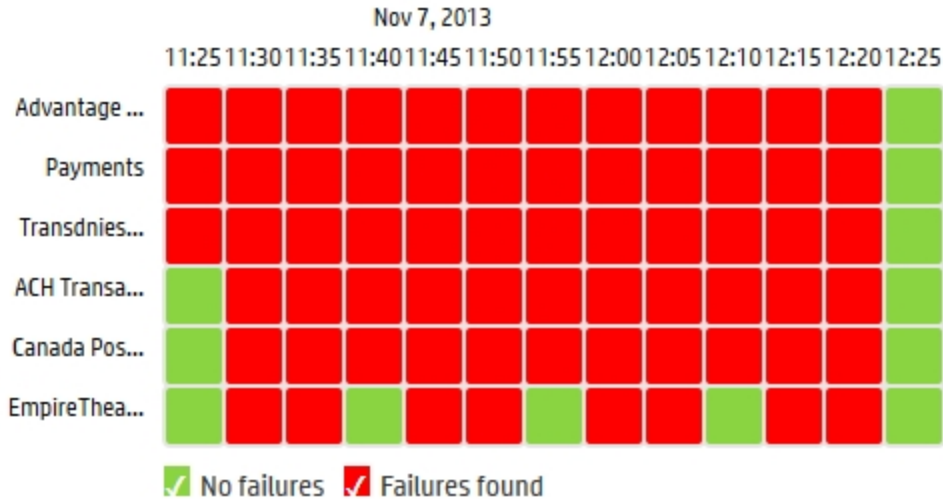


When using the heat map legend, note the following:

- The legend describes the minimum to maximum value ranges represented by each color used in the map.
- A clear rectangle indicates that no data is available.
- If there are more than four digits in the value, the units are scaled to allow them to fit in the box. For example, 0.046 second appears as 46 m.
- Some dashboards provided by Operations Bridge Analytics use heat maps to show metrics that indicate some type of failure. Operations Bridge Analytics uses green to indicate **No failures** and red to indicate the **Failures found**.

For example:

### **MOVING\_DISTINCT\_COUNT(Transaction)**




You can perform the following operations on heat maps:

Display the value within each heat map cell

Click **Show Values** to show the first few characters of the value that is represented within each heat map cell.

Calculate the percentage values using the minimum and maximum values for the entire matrix, per row, or per column



**To recalculate percentage values in a heat map:**

1. Mouse over the query pane toolbar for the query pane you want to change.
2. Click  to edit the query pane.
3. Navigate to the **Visualization** tab.
4. Select **Heat**.
5. Do either of the following:
  - a. Select **Matrix** to calculate the heat percentages using the minimum and maximum values of the entire data set (matrix).


- b. Select **Row** to calculate the heat percentages using the minimum and maximum values per row.
  - c. Select **Column** to calculate the heat percentages using the minimum and maximum values per column.
6. Click **OK**.

Operations Bridge Analytics recalculates the heat colors based on the new minimum and maximum values.

## View more heat maps in a query pane

Operations Bridge Analytics enables you to navigate through a series of heat maps by using the  and  buttons.

## Modify the color scheme

Operations Bridge Analytics enables you to choose from a number of different color schemes for heat maps. To do so, click the Settings  button and select **Color Scheme**.

## About Line Charts

You can use moving aggregate (time series) analytic functions to display your results as a line chart.

When using line charts, note the following:

- Operations Bridge Analytics shows multiple line charts in a single query pane when the Analytic Query Language (AQL) search query requests in multiple line charts.
- Operations Bridge Analytics shows time series information in line chart format by default.
- When creating BPM line charts, if you want to see data gaps (for when an application status was unavailable), add `i.status` to the AQL query.

Example: In the following example, add the bold text to the AQL Query.

```
from i in (bpm_application_performance) let analytic_interval=between($starttime, $endtime)
let interval=$interval select i.application, moving_avg(i.transaction_response_time), i.status
```

You can perform the following operations on line charts:

- To change the order that items appear in the list, select **Group by Entity** or **Group by Metric**.
- To show different entities or metrics, select the check boxes next to the items in the list.
- To copy a metric to a different line chart (or to an empty pane), drag the desired metric to any pane with the following symbol:



## About Pie Charts

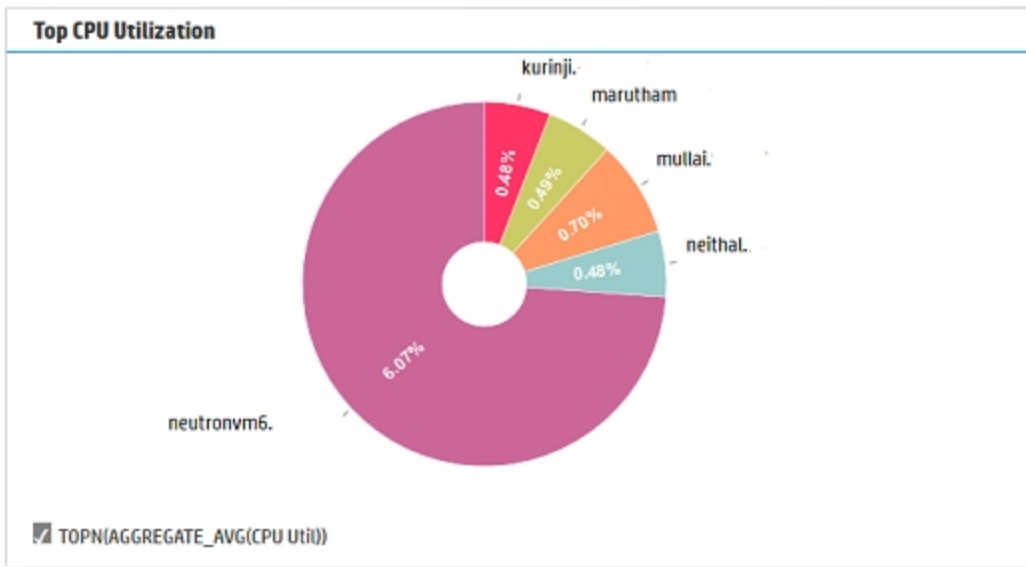
You can use both moving aggregate (time series) and overall aggregate (summary) analytic functions to display your results as a pie chart.

Moving aggregate (time series) analytic functions show results according to a time interval within a specified time range. This data might include the total, average, minimum, or maximum values calculated at each interval over the specified time range. For example, you might want to view CPU utilization for each unique host in a specified domain at 1-hour intervals for the last 24 hours.

Each moving aggregate value shown represents a recomputed value using each data point per interval within the specified time segment. For example, the `moving_avg` analytic function calculates the average of all average values returned for the specified time frame and metric or attribute. Operations Bridge Analytics shows each of these recalculated values, one per pie chart segment.

Overall aggregate (summary) data is data grouped by total, average, minimum, or maximum values within a specified time range. For example, you might want to view the total number of log messages generated by each host within a specified domain within the last hour.

Operations Bridge Analytics displays the values for each pie segment as shown in the following example:



Select items in the chart to generate a new dashboard focusing on the selected item.

## About Sunburst Charts


Sunburst charts display the hierarchy you defined using the topology manager. They show services, their associated groups, their associated hosts, and the top metrics for each host.

To interpret the data in a sunburst chart, note the following:

- The root or center of a sunburst chart does not represent an object.
- Sunburst charts use color ranges to show the relative weight of a metric among the set of objects rather than to show status. Operations Bridge Analytics uses a darker color to indicate that there is more of a particular value. It uses a lighter shade of the same color to indicate that there is less of a value.
- Gray indicates that no values are available.
- Operations Bridge Analytics calculates the color fill for each parent node using the average color of all child nodes. When determining the average, It ignores any node with a fill color of gray.

You can perform the following operations on a sunburst chart:

- To select a metric to appear, use the drop-down menu.
- To return the sunburst chart to its original detail, click the center of the chart.

- To drill into any of the elements in the chart, click the element.
- To modify the color scheme, click the Settings  button and select **Color Scheme**.

## About Table Data

Operations Bridge Analytics presents overall aggregate data as bar charts, pie charts, or tables. Overall aggregate data is data grouped by total, average, minimum, or maximum values within a specified time range.

Operations Bridge Analytics shows overall aggregate (summary of totals, counts, or averages) data in table format by default.

**Note:** Operations Bridge Analytics also shows log file information in table format by default.





When viewing table data, note the following:

- You can use an AQL query to specify the column names to appear. Operations Bridge Analytics displays each column name in the order in which it appears in the AQL query.
- If you do not specify column names in your query, Operations Bridge Analytics initially displays a maximum of eight columns.
- If more than eight columns are returned from the search, Operations Bridge Analytics displays the set of columns that are determined to be of the most value. Examples of these "preferred" columns include **raw**, **message**, **title**, **severity**, and **host**.
- Operations Bridge Analytics does not display identification columns that are for internal use only.

You can perform the following operations on table data:

- To filter the results, enter a string in the text field.

**Note:** For log data, when filtering the message field, strings that include special characters must be contained in quotation marks.

- To restore the original column settings, select the **Columns** drop-down menu and select **Restore original**.
- To sort the data, use the up  and down  buttons at the top of each column.
- To get more details about a row, click . To hide the details, click .
- To show or hide columns, select the **Columns** drop-down menu and use the check boxes next to the column names.



## About Log and Event Analytics


You can show messages sorted according to significance by using the Log and Event Analytics visualization. Log and Event Analytics is a forensic tool that scans your messages over a given time range and generates a list of the most significant ones.

This visualization is only available for specified AQL queries. For details, see ["Log and Event Analytics" on page 53](#).

## Predefined Dashboards Provided by Operations Analytics

Some dashboards do not contain data until specific collections are configured. For example, the BPM Applications Overview dashboard contains empty panes until a BPM collection is configured and has collected data.

Name	Description
Anomalies	Displays all anomalies and allows you to drill down to each anomaly for more details. For more details about anomalies, see <a href="#">"Anomaly Detection" on page 78</a> .
BPM Applications Overview	<p><b>Note:</b> See Configuring Collections for the configuration steps required to display this dashboard information.</p> <p>Use the BPM Applications Overview to view the following:</p> <ul style="list-style-type: none"> <li>• Application Availability Over Time The heat map value in this dashboard is the number of failed transactions.</li> <li>• Application Performance Over Time</li> <li>• Application Layer Performance Over Time</li> <li>• Top 10 Transactions Performance</li> <li>• Top 10 Locations Performance</li> </ul>
Logs Search	<p>Shown by default when you initially log on to Operations Bridge Analytics. This dashboard provides an overview of the following information for the log messages in your IT environment:</p> <ul style="list-style-type: none"> <li>• Log Messages — All</li> <li>• Log Messages — Syslog Only</li> </ul> <p><b>Note:</b> You can change the sort order of the message displayed in the</p>

Name	Description
	<p>log messages panes by modifying the AQL query. For details, see the <i>AQL Developer Guide</i>.</p>
NNMi Network SPI	<p>Displays the following information:</p> <ul style="list-style-type: none"> <li>• Top 10 Network Interfaces with Utilization In</li> <li>• Top 10 Network Interfaces with Utilization Out</li> <li>• Top 10 network interfaces based on highest error percentages</li> <li>• Top 10 network interfaces based on highest discard percentages</li> <li>• Top 10 network interfaces based on highest in and out throughput</li> <li>• Top 10 network devices based on highest CPU utilization</li> <li>• Top 10 network devices based on highest memory utilization</li> <li>• Top 10 unavailable nodes</li> <li>• Top 10 network devices based on highest SNMP response times</li> </ul>
OA Environment Overview	<p><b>Note:</b> See Configuring Collections for the configuration steps required to display this dashboard information.</p> <p>This dashboard provides an overview of the following information for the hosts in your IT environment:</p> <ul style="list-style-type: none"> <li>• Top 10 CPU utilization (cpu_util)</li> <li>• Top 10 disk utilization (disk_io_rate)</li> <li>• Top 10 memory utilization (mem_util)</li> <li>• Top 10 network utilization (net_packet_rate)</li> </ul> <p>Use this dashboard to help determine, at a glance, problem areas to investigate more closely in your network environment.</p> <p>To return to this dashboard, click .</p>
OA Microsoft ActiveDirectory Server	<p>This dashboard provides information from a selection of metrics taken from the Operations MP for MS ActiveDirectory Collection.</p>
OA Microsoft Exchange Server	<p>This dashboard provides information from a selection of metrics taken from the Operations MP for MS Exchange Collection.</p>
OA Microsoft SQL Server	<p>This dashboard provides information from a selection of metrics taken from the Operations MP for MS SQL Server Collection.</p>
OA Oracle Database	<p>This dashboard provides information from a selection of metrics taken from</p>

Name	Description
MP	the Operations MP for Oracle Database Collection.
OA Oracle Database SPI	This dashboard provides information from metrics taken from the Operations SPI for Oracle Collection.
OM Events	<p><b>Note:</b> See Configuring Collections for the configuration steps required to display this dashboard information.</p> <p>Use this dashboard to view the following information:</p> <ul style="list-style-type: none"> <li>• Event Count Over Time</li> <li>• Top 10 Hosts with Event Count Over Time</li> <li>• Event Count by Host — Current Week</li> <li>• Event Count by Host — Previous Week</li> <li>• Event Count by Severity — Current Week</li> <li>• Event Count by Severity — Previous Week</li> <li>• Table of the first 500 OM events</li> </ul>
OMi Events	<p><b>Note:</b> See Configuring Collections for the configuration steps required to display this dashboard information.</p> <p>Use this dashboard to view the following information:</p> <ul style="list-style-type: none"> <li>• Total count of the OMi events over time</li> <li>• Percentage of OMi events by host</li> <li>• Total count of OMi events by State</li> <li>• Top hosts that have highest number of OMi events</li> <li>• Percentage of OMi events by application</li> <li>• Event count by the host</li> <li>• Event count by host from the previous week</li> <li>• Event count by severity</li> <li>• Event count by severity from the previous week</li> <li>• Table of the first 500 OMi events</li> </ul>
OpsA Alerts	<p>Displays all instances of triggered alerts going back three months by default.</p> <p>You can drill down to open extra dashboards showing more details about an alert instance or time period surrounding an alert . To the time period or alert name of an alert instance.</p>
OpsA Health	Displays the metrics, topology, and log information available for the

Name	Description
	<p>following Operations Bridge Analytics servers and appliances:</p> <ul style="list-style-type: none"> <li>• Operations Bridge Analytics Collector Appliance</li> <li>• Operations Bridge Analytics Server Appliance</li> <li>• List of configured collections that Operations Bridge Analytics is collecting data for.</li> </ul> <p>This dashboard provides current details about Operations Bridge Analytics system health. See <a href="#">"Checking the Status of Operations And Operations Bridge Analytics Servers"</a> on page 189 for more information.</p>
OpsA Meta Info	<p>Displays the following information for the collections in your IT environment:</p> <ul style="list-style-type: none"> <li>• Collections and any tags for each collection</li> <li>• Columns (metrics) per collection and tag names per column</li> <li>• Columns defined as keys.</li> </ul> <p>See <a href="#">"How to View Collection Information"</a> on page 90 for more information.</p>
SiteScope Environment Overview	<p>Displays the following information monitored by SiteScope:</p> <ul style="list-style-type: none"> <li>• Top CPU Utilization</li> <li>• Top Disk Utilization</li> <li>• Top Memory Utilization</li> <li>• Top 10 Hosts with Ping Roundtrip Time</li> <li>• Top 10 Hosts with URL Content Roundtrip Time</li> <li>• Top 10 Hosts with JMX Physical Memory</li> </ul>
Tracked Logs	<p>shows data collected from tracked logs and parameters.</p> <p>Contains log and parameter count over time, and data distribution query panes.</p>

## Tasks


### How to Save a Dashboard

Dashboards are automatically saved when you add/remove Query Panes or modify the dashboard layout.

To copy a dashboard and save it under a new name, see ["How to Copy a Dashboard"](#) below .

**Tip:** If you want to experiment with different dashboard layouts, save a copy of the original layout under a different name. Otherwise, Operations Bridge Analytics overwrites the original dashboards as it automatically saves any changes you make.


## How to Copy a Dashboard

1. Navigate to the **Dashboard** user interface.
2. Select the triple bar icon  and select **Manage**.
3. Click the check box  for the dashboard you want to copy.
4. Click **Copy**.
5. In the **Specify a new name** dialog, enter the name of the copied dashboard.
6. Click **OK**.


The copied dashboard appears in the **Dashboards** menu.

## How to Copy a Pane

You can copy any pane to a custom dashboard of your choice.


1. From the desired pane, click **More Pane Actions** .
2. Hover over **Copy Pane to**, and select the target dashboard.
3. If you duplicated the dashboard to the original dashboard it was in, you must refresh your browser to view the changes..

## How to Delete a Dashboard

1. Navigate to the **Dashboard** user interface.
2. Select the triple bar icon  and select **Manage**.
3. Click the check box  for each dashboard you want to delete.
4. Click **Delete**.
5. Click **OK**.

The dashboard name is removed from the **Dashboards** menu.


## How to Share a Dashboard

1. Navigate to the **Dashboard** user interface.
2. Select the triple bar icon  and select **Manage**.
3. Click the check box  for each dashboard you want to share.
4. Click **Share**.

Each dashboard you select is available to all users in the same tenant.

**Note:** Shared dashboards that have been provided by other members of your user community are appended with the name of the user who provided the dashboard.

## How to Stop Sharing a Dashboard


1. Navigate to the **Dashboard** user interface.
2. Select the triple bar icon  and select **Manage**.
3. Click the check box  for each dashboard you want to unshare.
4. Click **Unshare**.

**Note:** Each dashboard you select is removed from the dashboard menu of other users in your user community (tenant).

## How to Export Viewed Data to a CSV File

You can export the result from a pane you are viewing in the Operations Bridge Analytics console to a CSV file. This enables you to import the data from this CSV file into a MS Excel spreadsheet for further analysis.

To export the data from a pane into a CSV file, do the following:

1. From an Operations Bridge Analytics dashboard, click **More Pane Actions** .
2. Click **Export to CSV** to export the pane results to a CSV file.

## How to Export and Import Dashboards

After you create new dashboards or modify existing ones, you might want to export these dashboards to a file, then import them for use among tenants.

**Caution:** Do not edit the dashboard file (shown as `mydashboard.xml` file in the examples in this section) after you export it, then attempt to import the file. Manually editing an exported dashboard file is not supported.

**Note:** If you choose to add spaces to your dashboard names, such as using two or more words in your dashboard names, you must always use quotation marks when working with these dashboards.

## Exporting and Importing Dashboards Among Operations Bridge Analytics Tenants

Suppose that you created a new dashboard, `dashboard1`, and want to export this dashboard and share it with another Operations Bridge Analytics tenant. You can use the instructions in this section to import these dashboards to another tenant.

To accomplish this, do the following:

1. From the Operations Bridge Analytics console, navigate to the **Dashboards** menu.
2. While viewing the dashboards, make a list of the dashboards that you want to export. For this example, you have `dashboard1` and `dashboard2` on your list.

**Note:** Dashboards can be **shared** with other users in your user community. See *Share a dashboard with other users in your user community* in the *Operations Bridge Analytics help* for more information. The instructions in this section work for both shared and non-shared dashboards.

3. Run the following command to export `dashboard1`:

```
opsa-dashboard-manager.sh -u <the user that will own the dashboard> -  
e dashboard1 -f <mydashboardfile>
```

**Note:** To export more than one dashboard, use `-e dashboard1 dashboard2`.

**Note:** The `opsa-dashboard-manager.sh` script exports the dashboard to the current directory. For example, if you run the `opsa-dashboard-manager.sh` script from the `$OPSA_HOME/bin` directory, look for the exported dashboards in the `$OPSA_HOME/bin` directory.

**Note:** You can use variations of the `opsa-dashboard-manager.sh` to export specific dashboards or all dashboards. See the `opsa-dashboard-manager.sh` reference page (or the

Linux man page) for more information.

**Note:** If you create dashboard names that include spaces, you must wrap those dashboard names in double quotation marks. For example, wrap any dashboard names that include white space as shown in the bold font: `opsa-dashboard-manager.sh -u opsa -p opsa -e "metrics dashboard" -f mydashboardfile`.

4. To import your exported dashboard or dashboards to another Operations Bridge Analytics installation, run the following command from the Operations Analytics Server on which you want to import your dashboards:

```
opsa-dashboard-manager.sh -u <the user that owns the dashboard or dashboards> -i -f <mydashboardfile>
```

**Note:** The `opsa-dashboard-manager.sh` script prompts you for the password for the `opsatenantadmin` password, which you set during installation.

**Note:** Before you import dashboards, it is a good practice to create a backup copy of any dashboards you plan to import. See *Copy a dashboard* in the *Operations Bridge Analytics help* for more information.

5. To see the newly imported dashboards, you must run the following command from the Operations Analytics Server on which you imported the dashboards:

```
$OPSA_HOME/bin/opsa-server restart
```

**Note:** After running an `opsa-server restart` command, information logged in the `/opt/HP/opsa/log/opsa-server.log` file is removed. To view the files that retain this information across restarts, see the log files located in the `/opt/HP/opsa/jboss/standalone/log` directory. Look for log file names that begin with `server.log`.

See the *opsa-server* reference page (or the Linux man page) for more information.

After you successfully import a dashboard, users associated with the tenant you used for the import see data using the imported dashboard.

## How to Add or Edit a Query Pane

1. Click  next to the Dashboard menu to add a new pane.



Click  on the top of any pane to edit.

2. In the **Query** tab, do one of the following:

- In the **(NEW PANE)** attribute, enter the AQL query, AQL function name, or AQL expression for the new query pane.

**OR**

- Select an AQL function.

Enter values for any of the AQL function arguments that apply.

Note the following:

- Your Operations Bridge Analytics administrator can provide descriptions for the arguments required for each AQL Function provided. See ["Add / Edit Query Pane - Query Tab" on page 29](#) for information about how to view these descriptions.
- If descriptions are not provided, you can also view the collection information configured for your IT environment. This collection information might also assist you in providing values for the arguments required.

Click **Show Properties** to view a new query pane that displays the collections (property group uid) and columns (property uid). It also shows whether the column contains metric or attribute values.

Also see ["How to View Collection Information" on page 90](#) for more information about how to view the meta data stored for your collections.

Click [here](#) for a brief description of the possible AQL function argument types. See the AQL Developer Guide for more information.

Argument Type	Description
analytic	Specifies an analytic function that can be applied to overall aggregate analytic functions, moving aggregate analytic functions, or raw metrics. These analytic functions include: topN, bottomN, inverse_pctile, pctile, outlier, or rank. See the AQL Developer Guide for more information.
collection	Specifies the name of the collection for which Operations Bridge Analytics returns search results.
custom	Indicates that Operations Bridge Analytics cannot identify the argument type.  Check the description for the AQL function that appears in the Query tab when adding or editing a query pane. Also, check with your Operations Bridge

Argument Type	Description
	Analytics administrator for assistance with providing values for these arguments.
entity	Specifies the type of entity attribute on which you want to filter. For example, host_name.
filter	Specifies the filter value to use in the where clause of the AQL function.  For example, when used with host name, you might enter the following filter value to return data for only the servers in the co.usa.enterprise.com domain: \"*\.co.usa.enterprise.com".
grouping	Specifies an argument required for the group by clause.
function	Specify the overall aggregate or moving aggregate analytic function you want Operations Bridge Analytics to use. See the AQL Developer Guide for more information.
metric	Either of the following: <ul style="list-style-type: none"> <li>Name of the metric column.</li> <li>Tag that represents the metric column.</li> </ul>
ordering	Specifies an argument required for the order by clause.

3. *Optional.* Use the **Visualization** tab to change the visualization that appears.

- a. Navigate to the **Visualizations** tab.
- b. Navigate to the Visualizations options:



- c. Select the visualization you want to use.
- d. Navigate to another tab or click **OK**.
- e. **Note:** If you select a visualization that is not valid for the data displayed, Operations Bridge Analytics displays the default visualization for the AQL query.

See [Working with Query Panes](#) for more information about visualizations.

4. Use the **Parameters** tab to provide the parameter values, if any, to the selected AQL function.

**Note:** Any parameter value you provide overrides the associated value selected using another method in the Operations Bridge Analytics console. For example, if you specify a

time interval using the `$interval` parameter, Operations Bridge Analytics uses the value for `$interval` rather than the time line segment selected. See "[Filter Search Query Results](#)" on [page 35](#) for more information about time line segments.

- a. Navigate to the **Parameters** tab.
- b. Provide the parameter values you want to use.


**Tip:** Mouse over a parameter to view its description.

To restore the parameter values to their original default values, click **Defaults**.

**Note:** If you want to use these parameters to write an AQL to define a pane, you must add "\$" before the parameter.

- c. Navigate to another tab or click **Save** to save your changes.

## How to Resize a Query Pane

Navigate to the query pane you want to change. Click the Resize button  in the upper right corner of the query pane.

## How to Delete a Query Pane from the Dashboard

Click **x** in the upper right corner of the pane to close the query pane and remove it from your dashboard.

## How to Modify the Scale of Data Displayed in a Pane

To modify the scale that data is displayed (for example, to display kb instead of bytes) see "[Modifying Unit Scaling on Collected Data](#)" on [page 233](#).

## How to Copy a Metric from One Query Pane to another Query Pane

You can copy a metric from one line chart to another one or to an empty pane by dragging the metric to any pane with the following symbol:



**Note:** Copying metrics is not fully supported if the AQL in the source pane uses one of the following elements:

- aqlrawlogcount
- pctile
- inverse\_pctile
- rank
- topN
- bottom
- Breach AQL

In this case, the metric may be copied to the new pane temporarily but will not remain after refreshing the browser.

Copying metrics is not supported to panes that are actively using predictive analytics.

## User Interface

### Dashboard Menu

Item	Description
Dashboard Name List	Operations Bridge Analytics lists all of the dashboards available for your use. These dashboards include: <ul style="list-style-type: none"><li>• Dashboards created by the current user.</li><li>• Dashboards shared by other users in the same user community (tenant).</li></ul>
New	Creates a dashboard.
Save As	If you are in an unsaved dashboard as a result of a search, Save As saves the search results as a dashboard.  If you are in a saved dashboard, Save As creates a copy with a new name.
Manage	Enables you to copy, share, unshare, or delete a dashboard that you no longer need from the <b>Dashboards</b> menu.

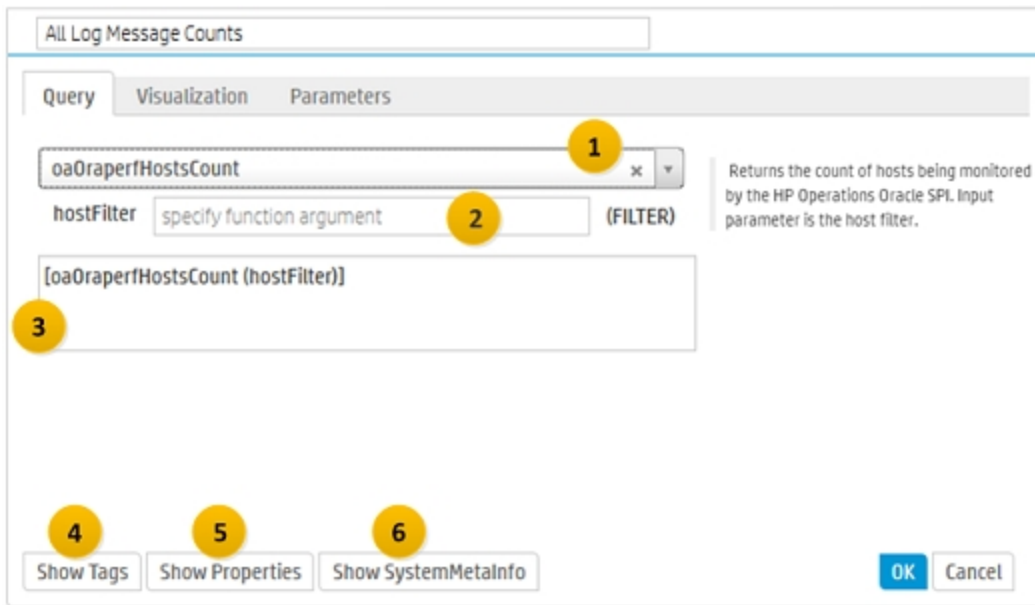
Item	Description
	<b>Note:</b> You can delete only dashboards that you created.

## Add / Edit Query Pane - Query Tab

When adding a new query pane, you can use the **Query** tab to specify the pre-defined AQL function you want to use as your search query.

**Note:** You can also choose to enter your own AQL query. If you want to use an AQL function, either select one from the list or create the function using a text editor. See the AQL Developer Guide for more information.

The following illustration highlights the main features of the Query tab.



### 1. Select an AQL Function

Enables you to create a new query pane by selecting an existing AQL function.

These functions are provided by Operations Bridge Analytics and your Operations Bridge Analytics administrator.

Your Operations Bridge Analytics administrator has the option to provide a description for each AQL function he or she creates.

Any description information appears to the right of the AQL function's argument information.

## 2. Specify Argument Values

Operations Bridge Analytics requires argument names as part of the syntax for an AQL function.

Each name represents a value that must be passed to the AQL function when it is executed.

These arguments should appear in the associated AQL function displayed in the pane below the required argument list.

If you do not know the value to provide for each argument name in the list, contact your Operations Bridge Analytics administrator.

Argument values are usually stored as meta data for your Operations Bridge Analytics collection.

Use the **Dashboards** menu to navigate to the **SystemMetalInfo** dashboard and view the meta data stored for your collections. Also see the *AQL Developer Guide* for more information.

## 3. View the AQL Function

After you select an AQL function from the list, Operations Bridge Analytics displays the AQL function below the list of arguments.

To view the AQL query associated with this AQL function, navigate to the one of the following directories on the Operations Bridge Analytics server:

- \$OPSA\_HOME/inventory/lib/hp/aql
- \$OPSA\_HOME/inventory/lib/user/aql

**Tip:** Your Operations Bridge Analytics administrator might have chosen to create AQL functions in a different directory.

## 4. View Tag Information

Enables you to view the following information for the collection that is included in your query:

- The name of the collection (**property group uid**)
- Tag assigned to each column in the collection (**tag name**)
- Column name that is assigned to each tag (**property uid**)

## 5. View Collection Column Information

Enables you to view the following information for the collection that is included in your query:

- The name of the collection (**property group uid**)
- Column name and its associated tag (**property uid**)
- Type of data (metric or attribute) that is stored in the associated column.

## 6. View the SystemMetalInfo Dashboard


Enables you to view the SystemMetalInfo dashboard. This dashboard includes the following information:

- Collections and any tags for each collection
- Columns per collection and tag names per column
- Columns defined as keys as well as whether the data stored in the column is a metric or attribute

See ["How to View Collection Information" on page 90](#) for more information.

## Chapter 2: Search Tool

The search tool enables you to search for elements in your environment, and for text in logs and events. For more detailed information on text search, see ["Text Search" on page 37](#).

The search tool is opened by selecting the search icon  from the main toolbar on the left of the user interface.

### Learn About

#### Using Search Operators

You can use prefixes called search operators to specify what you are searching for.

Operator	Results
Host:	A search for a host. The result is displayed in a dynamic dashboard, including visualizations of all the data that was found for that host, like metrics, logs, and anomalies.
Service:	A search for a service. The result is displayed in a dynamic dashboard including visualizations of all the data that was found for that service, like metrics, logs, and anomalies.
Application:	A search for an application. The result is displayed in a dynamic dashboard, including visualizations of all the data that was found for that application, like metrics, logs, and anomalies.
Text:	A text search. The results of a text search display messages and statistics about the particular passage of text.

#### Example queries

The following examples show how you can use search operators to search for hosts, services, and applications.




**Note:** If a prefix search operator, like Host:, is not specified, then a tag search is performed. All information in OBA is annotated with a tag value. For example, if you search for `cpu`, then all metrics that have been tagged with the value `cpu` are displayed. The list of available tags is shown in the OpsA Meta Info dashboard.

Query	Results
Host: *	Displays metrics, log messages, events and anomalies for all hosts.
Host:"server.example.com"	Displays data for the specified host.
Host:"server.example.com" cpu	Displays cpu related data for the specified host.
Host:"server.example.com" disk FocusOn:"volume1"	Displays data related to the disk "volume 1".
Service:"productionEurope"	Displays data for the specified service.
Service:"productionEurope" DrillTo:groups FocusOn:"web1"	Displays data for the "web1" group of the specified service.
Application:"online banking"	Displays data for the specified application.
Text: error	Displays log messages and events that contain "error".
Text: error hostname=server.example.com	Displays log messages and events of the specified host that contain "error".
Text: error   top hostname	Displays a list of hosts sorted by number of times "error" was found

## Tasks

### How to use the search tool

1. Select the search icon  from the main toolbar on the left of the user interface. Use the search field to specify your query. You can select suggested items or manually type at any time. If you are searching log and event messages, see ["Text Search " on page 37](#)

**Note:** The search tool only suggests mandatory parameters for an operator. If an operator

supports optional parameters, the search tool only offers suggestions for a mandatory parameter if an optional parameter is not specified. The search tool does not offer suggestions for optional parameters.

2. Press the space bar to view additional modifiers for your query. The modifiers are based on the actual data in your system. For details about the syntax, see above.

3. Results:

The results of each search is a dashboard. Operations Bridge Analytics uses its default dashboard layout and populates the dashboard with the data requested by your search.

# Filter Search Query Results

Operations Bridge Analytics enables you to filter your search query results using the following methods:

Use the Time Line to fine tune the Time Range selected.

Operations Bridge Analytics enables you to focus on a specified time segment using the slide bar that appears above the metrics, log file and event data displayed. For example, you might want to focus on a particular day or a particular peak period.

**Note:** The time range attribute that appears next to the search query initially defines the x-axis for the bar, line or plot diagram shown as well as the time frame for the log file and event information that is shown.

Changing the Time Line segment, changes the information displayed in visualizations and tables for all metric and log file and event data.

## To filter your analysis by time segment:

Slide each end of the time line to the beginning and end point of the time you want to use:

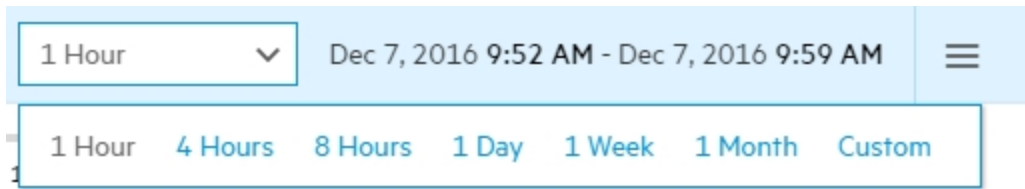


Operations Bridge Analytics filters the information available to focus only on the time segment you selected in each of the metric visualizations displayed. The log file and event information is also filtered based on the time segment you specify.

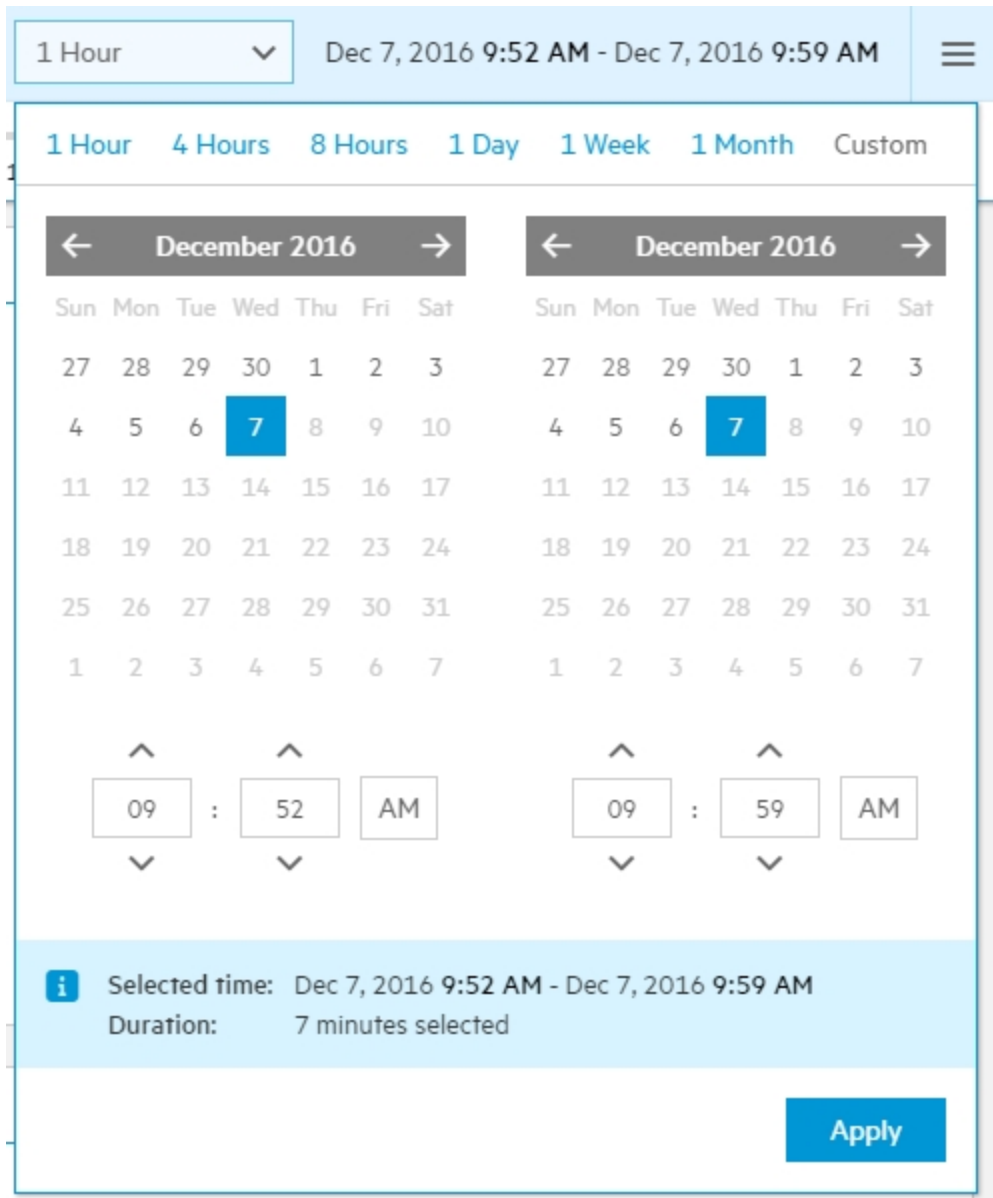
Use the Time Range option to filter the results by a specified time period.

## To change the time range for the data displayed, by doing either of the following:

- Refine your search query to narrow the information presented.
- Change the time range value from the Time Range drop-down menu to narrow or broaden the time range for which the data is shown:



Use the **Custom Time** option when you want to specify a start and end date using the Operations Bridge Analytics calendar:



Use the Filter option to filter the results by words or phrases.



The **Filter** option enables you to filter the results according to a word or phrase.

**Note:** The word or phrase you enter must be an exact match in the results displayed.

See "[Search Tool](#)" on page 32 for more information.

## Text Search

The text search user interface allows you to search all logs and events and filter the results in many ways. Text search results display information about messages, fields, and topology associated with the query. You can narrow your results by clicking on almost any item in the user interface or by modifying the search statement at the top of the page.

To access

From the Search  tool, select or type **Text**:

## Learn About

### User Interface


**Timeline.** The timeline displays the total number of messages returned and the number of messages per time segment. The total span of time displayed can be selected using the drop down menu or using the slider. Selecting a time segment filters the results.


**Fields.** The fields section displays a list of different fields identified in any of the message results. For example, *hostname(3)* indicates that the field *hostname* was identified with three unique values. Selecting the fields allows you to view more details such as the distribution of different values, and filter by field values.

**Topology.** The topology section displays a list of the different groups and services associated with the returned results. You can filter by specific groups and services and view more information by selecting those items.

**Message List.** The message list in the middle of the text search dashboard displays all the messages that contain the text from the search query. Click on a message to display more details.

**Parameters.** Parameters are displayed as underlined text in a message. Click a parameter to see the distribution of parameter values. To filter by parameter values, extract the parameter as a field and filter by the field using the Fields area of the user interface. You can also track parameters, as described in ["Track Message Groups and Parameters" on page 51](#).

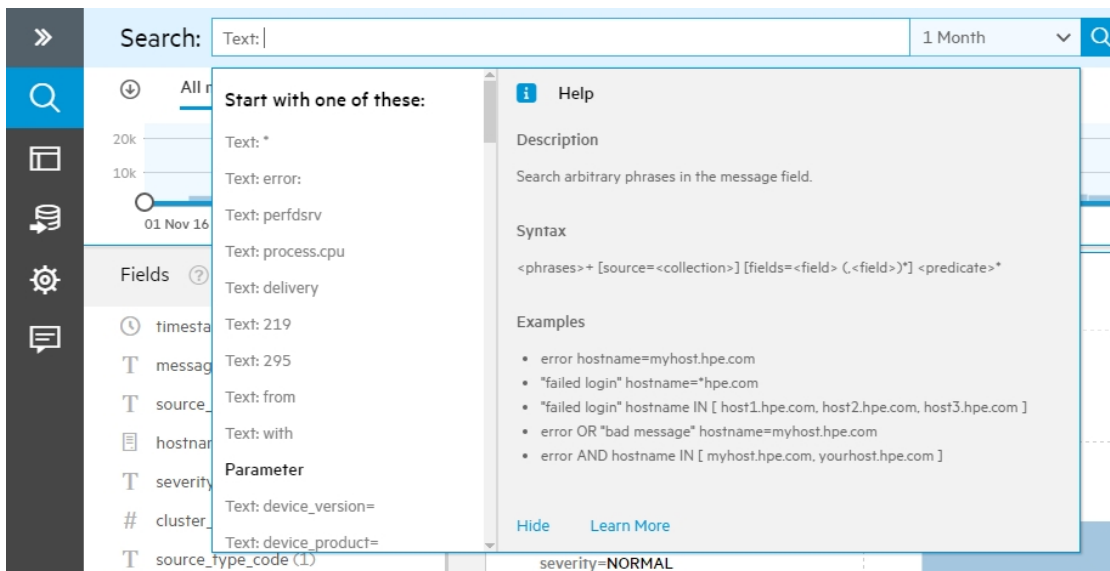
**Like.** Click the like  button in a message to indicate that this message group is significant to you. This information is used in future calculations to determine message significance.

**Ignore** Click the ignore  button to ignore a message group. This removes the message group from the log viewer list and the Top Unusual Messages chart. You can later restore these items by using the **Ignored Messages** button.

## Tasks

### How to Perform a Text Search

1. Type *Text:* into the search bar. Then type the text for which you want to search. Use the search operators to refine your search. For information on search syntax, see ["Text Search Syntax Reference" on the next page](#).



**Note:** When running a Text Search involving **hostname=** with a server having a hyphenated name, consider the following:

Running a Text Search such as **hostname=server-name.<domain>.com** might result in an empty list of messages.

For a better result, enclose the server name in quotes. For example, running a Text Search such as **hostname="server-name.<domain>.com"** results in an accurate list of messages.

## How to Create a Field from a Parameter or Selected Text

The message list in a search query displays all messages that contain the text specified in a query. To create a field from a parameter or fragment of text in a message, do the following:

1. Click a message to display more message details.
2. To create a field from a parameter, click a parameter in the message. Parameters are displayed as underlined text in the message. Then, click **Create Field from Parameter**.
3. To create a field from a text fragment in a message, highlight the text with your cursor, and click **Create Field from Selected Text**.

## Text Search Syntax Reference

### General Syntax

The OBA search process uses an optimized search language that allows you to specify multiple search criteria in a pipeline format. The pipe (|) symbol connects different processes in the pipeline, passing the results of each process from left to right, thus refining the search as it goes. Operators are used to perform additional manipulation of the data, including sorting, filtering, or extracting information based on a specific set of results. Each operator can have various parameters and predicates to further refine the search.

```
<fulltextsearch> | <operator1> | <operator2> | ... | <operatorN>
```

```
fulltextsearch: (<term>)+ (<filter predicate>)* // error hostname=*hpe.com
```

```
operator: <operator name> (<parameter>)* (<filter predicate>)* // movingCount
severity interval=30
```

**Note:** When searching for strings that contain special characters (such as \*-%\$) you might receive error messages. To resolve this issue place the entire string in quotes. If the special

character is a quotation mark, place the entire string in quotes, and replace any quotation marks with \". For example, if you are searching for the string **my "host"**, you would enter **"my \"host\""**.

For a more complex example, as in looking for a service in addition to the term `error-message`, you might use **((`*service*` OR `*database*`) AND `"*error-message*"`)**.

### Examples:

- Count all messages that contains the words `jdbc` and `error` for the `opsa-db` over time:

```
error jdbc hostname=opsa-db.example.com | movingcount
```

- All example hosts in the top 20 list of HTTP 404 errors:

```
404 source_type=apache | top 20 hostname | filter hostname=*.example.com
```

### Operators:

#### top

**Syntax:** `top [<limit>] (<field>)+`

**Description:** Lists search results of the most frequent values of the specified field(s), from highest to lowest.

- limit:** (*optional*) Limits the maximum displayed number of messages. The default limit is 500.
- field(s):** Field name to use the `top` operator on. Use the space character as a separator for multiple fields.

**Examples:** `top 2 data_source hostname`

#### bottom

**Syntax:** `bottom [<limit>] (<field>)+`

**Description:** Lists search results of the least common values for the specified field(s), from lowest to highest.

- limit:** (*optional*) Limits the maximum displayed number of messages. The default limit is 500.
- field(s):** Field name to use the `bottom` operator on. Use the space character as separator for several fields.

**Examples:** `bottom 2 data_source hostname`



## movingCount

**Syntax:** `movingcount [<field>+] [interval=<interval>] [timeunit=<timeunit>]`

**Description:** Total count of rows per time interval (default: column counts per 5 minutes). If a field is provided the operator counts the non-null values.

- **field:** (*optional*) Counts the non-null values of this field.
- **interval:** (*optional*) Can be a positive number. Default interval is 5.
- **timeunit:** (*optional*) The unit of the interval. Can be one of the following: hour, minute, second, millisecond. The default value is minute.

**Examples:** `movingCount hostname interval=5 timeunit=minutes`

## movingAverage

**Syntax:** `movingaverage <field>+[interval=<interval>] [timeunit=<timeunit>]`

**Description:** Accumulated average of the values in the specified field, per time period over a specified time window.

- **field(s):** Name of the fields for the average. The selected fields must contain numeric values.
- **interval:** (*optional*) Can be a positive number. The default interval is 5.
- **timeunit:** (*optional*) The unit of the interval. Can be one of the following: hour, minute, second, millisecond. The default timeunit is minute.

### Examples:

1. `error | movingaverage aNumericField`
2. `error | movingaverage aNumericField 1 hour`
3. `error | rex "%{DATA}HTTP 1.1" %{INT:code} %{INT:bytes}" | movingaverage bytes`

## rex

**Syntax:** `rex [strict] [field=<sourcefield>] <regexPattern>`

**Description:** Extracts additional fields based on the given regex pattern for each row. These fields are not stored in the database and are only visible in the query results. The operator can be used in a regular

or strict mode. If the operator is in regular mode and the pattern does not match, the fields will be null. If the operator is in strict mode and the pattern does not match, the affected rows will be filtered out.

### RegexPattern:

The regex uses GROK regex patterns and extractions. The extractions will create a new field with the specified alias in the form `%{SYNTAX:ALIAS}`.

**field:** The field to be used as input. By default, this is the message text.

**Syntax:** WORD, TIMESTAMP, INT, WORD, DATA, IP, IPV4, IPV6, MAC, HOST, ... (see more on GROK documentation)

**alias:** The field name of the extracted field.

### Examples:

1. `rex strict "This ${WORD:verb} a test."`  
Filters and extracts a field named "verb"
2. `rex "Flushing \[%{INT:number}\]"`  
Split up a row into fields and escaping the brackets.

sort

**Syntax:** `sort [<limit>] ([<order>] <field>)+`

**Description:** Sorts the result by the defined fields.

- **limit:** (*optional*) Default is 10.000
- **order:** (*optional*) Can be asc (ascending) or desc (descending). The default is asc.
- **order/column:** Can be repeated for additional sorting in case the previous fields have the same value.

### Examples:

1. `sort desc hostname`
2. `sort asc hostname desc timestamp`
3. `sort 10 desc hostname`

## head

**Syntax:** head [*<limit>*]

**Description:** Displays the first lines of the search results.

- **limit:** (*optional*) limits the number of results. The default is 10.

**Examples:** head 100

## tail

**Syntax:** tail [*<limit>*]

**Description:** Displays the last lines of the search results.

- **limit:** (*optional*) Limits the number of results. The default is 10.

**Examples:** tail 100

## between

**Syntax:** between *<starttime>* *<endtime>*

**Description:** Delivers results within a time frame from start time to end time. Both values are time values and can contain different formats. If a time value contains more than one word, it needs to be enclosed in double quotes (") or single quotes (').

### Time supported formats & examples:

- **Formal dates:** "2015-01-28" (YYYY-MM-DD), "2015/04/02" (YYYY/MM/DD), "1/02/1980" (M/DD/YYYY), "2/28/79" (m/DD/YY), "28.2.1977" (DD.MM.YYYY), 1437572023
- **Relaxed dates:** "Fri, 21 Nov 1997", "Jan 21, '97", "Sun, Nov 21", "jan 1st", "february twenty-eighth"
- **Relative times and dates:** now, tomorrow, yesterday, "30 seconds ago", "5 mins ago", "3 weeks ago"
- **Time** (most dates can be prefixed or suffixed with time information): "5:30 am", "12:59:10", "23:59"

### Examples:

1. error | between "25 minutes ago" now
2. error | between 1437568723 1437572023

3. error | between "2015-07-21 12:14" "1 week ago"

## dedup

**Syntax:** dedup [*<limit>*] (*<column>*)<sup>+</sup>

**Description:** Filters out rows that contain the same values in the given fields. If the parameter limit is used, it shows a limited amount of rows per field.

- **limit:** (*optional*) Limits the number of allowed duplicates. The default is 1.
- **field:** The field name for the field(s) to use dedup on. Multiple fields should be separated by spaces.

### Examples:

1. error | dedup 5 hostname
2. error | dedup hostname message

## lasthour

**Syntax:** lasthour

**Description:** Delivers all entries between the last hour and now.

**Examples:** error | lasthour

## count

**Syntax:** count [*<field>*]

**Description:** Counts all values. If a field is specified, only non-null values in the field are counted.

- **field:** (*optional*) The field name for the field to be counting non-null values on.

### Examples:

1. error | count
2. error | count hostname

## countBy

**Syntax:** countby *<field>*<sup>+</sup>

**Description:** Groups and counts all values in the specified field.

- **field:** The field name for the field to group and count.

**Examples:** error | countby hostname

## distinctCount

**Syntax:** distinctcount [approximate=true|false] [tolerance=<number>] <field>+

**Description:** Counts all distinct values for each field in the specified list.

- **field:** The field name for the field to count the distinct values.
- **approximate:** (*optional*) true|false (false is default), if true, use Vertica built-in function `approximate_count_distinct (field, tolerance)` for sql query, if false, the `count(distinct field)` is used.
- **tolerance:** (*optional*) Decimal number (1.0 default), ignored if `approximate=false`

**Note:** For the `approximate_count_distinct` see the Vertica documentation.

**Examples:** error | distinctcount hostname datasource

## max/min

**Syntax:**

max <field>

min <field>

**Description:** Displays the maximum/minimum value of the field.

- **field:** the field name for the field with the max/min value. The selected field has to be a numeric type.

**Examples:**

1. error | max aNumericField
2. error | min aNumericField
3. error | rex "%{DATA}HTTP 1.1" %{INT:code} %{INT:bytes}" | min bytes
4. error | rex "%{DATA}HTTP 1.1" %{INT:code} %{INT:bytes}" | max bytes

where

**Syntax:** `where <predicate>+`

**Description:** Displays the results that match the filter expression. The two keywords NOT and ISNULL can be used independently.

**Predicates:**

[NOT] <filter rule> ([AND | OR] <filter rule>)\*

filter rule: <field> <operator> <value> | <field> ISNULL | <field> IN [<value>(<value>)\*]

NOT: (*optional*) Keyword for negating the result.

ISNULL: (*optional*) Keyword for null values. Cannot be used with operator + value.

**Note:** Empty values are different from null values

- **field:** The field name to apply the filter expression on.
- **operator:** One of the following operators: =, <, >, <=, >=
- **value:** The value to apply the filter expression on. The data type has to be the same of the column type.

**Host lookup**

Predicates that refer to fields that are tagged `host_name` are extended with all known aliases to the given value. By default, this applies to the field `hostname`.

The original value of the field is preserved in a new field in the result table. The new field is named `<hostfieldname>_original`.

This feature can be disabled by specifying `disableHostLookup=true`

**Examples:**

1. `where hostname=www1.shop.com`

In this example, "hostname=www1.shop.com" is actually extended with all known aliases to www1.shop.com, since hostname is actually tagged with the "host\_name" tag

2. `where NOT hostname=www1.shop.com AND (severity = high OR severity = critical)`

3. `where NOT hostname ISNULL`

## lastmessage

**Syntax:** lastmessage

**Description:** Finds the last message in time and displays all messages found between the last message time and one hour before the last message time.

**Example:** error | lastmessage

## significant

**Syntax:** significant [problemtime=<problemtime>]

**Description:** Calculates and displays message significance for a given problemtime.

**problemtime:** Time in milliseconds. The calculation emphasizes messages closer to the given problem time.

**Example:\*** | significant problemtime=1437572023

## eval

**Syntax:** eval (<field> = <arithmetic expression>)+

**Description:** Executes SQL functions and arithmetics that are available from vSQL and UDX.

- **field:** The field name for the result of your calculation.
- **arithmetic expression:** Includes simple calculations and/or functions.
- **simple calculation:** [<parenthesis>] <number> <operator> <number> [<parenthesis>]  
 <existing field> <operator> <number>  
 <existing field> <operator> <existing field>
- **existing field:** Field name whose value can be converted into a number.
- **number:** 0-9
- **operator:** One of the following operators: +, -, \*, /, %, ^
- **parenthesis ():** Provide additional information through encapsulation. Always used in pairs.

### Examples:

```
eval failedPercent = count(failedLogin) / count(login) * 100
```

```
eval newResult = newVerticaFunction(significantmessage)
```

## topology

### Syntax:

topology <category> = <field>

topology <category> IN [<field>, <field>+]

**Description:** This operator can only be used at the beginning of the pipeline. It shows the current topology for the specified category.

- **category:** host\_name, group\_name, or service\_name
- **field:** Name(s) of the specified category.

### Examples:

1. topology group\_name = "group\_1"
2. topology host\_name IN [www3.shop.com, www2.shop.com]

## topologyfilter

**Syntax:** topologyfilter <category> = <field> [, <field>+] [<category> = <field> [, <field>+] ]

**Description:** Filters the results based on the specified topology.

- **category:** group\_name or service\_name
- **field:** Name(s) of the specified category.

### Examples:

1. \* | topologyfilter service = "service\_1"
2. \* | topologyfilter group = "group\_1" service = "service\_1"

## topologycount

### Syntax:

topologycount

topologycount <category>



**Description:** Shows the distinct count of results per category or all instances of the specified category and their distinct count of results.

- **category:** host\_name, group\_name, tier, service\_name

**Examples:**

1. \* | topologycount
2. error | topologycount group\_name

## field

**Syntax:** field (<field>[=hidden])+

**Description:** Filter the results so that they will only contain the given fields in the given order. If a field is marked as "hidden" the field is still included in the results, but will not show up in the user interface. Hidden fields can be used for internal purposes.

- **field:** List of selected fields to be displayed in the given order. Each field can be marked as hidden. Fields not available in the result set will be ignored.

**Examples:**

1. \* | field hostname severity
2. \* | field id=hidden hostname severity

## startswith / endswith

**Syntax:** startswith <phrase>

startswith <phrase>

endswith <phrase>

**Description:** Return messages that begin or end with the given phrase.

**Examples:**

1. startswith "Sql Connection Error:"
2. endswith "has failed connection"

## ntile

**Syntax:** `ntile <field> <#tiles>`

**Description:** Calculates and displays the statistical percentile for each value in the given field. The second parameter gives the granularity of percentiles that are resolved.

For example, the median value would have a percentile of 50. A percentile of 90 means 90% of the values are less than this value.

- **field:** Must be a numeric field. The field will be used as input to calculate the percentiles
- **#tiles:** Optional number of percentiles that will be distinguished. By default 10 percentiles are assumed.

### Examples:

1. `ntile failedLogin 10`
2. `ntile significance 100`

## movingsum

**Syntax:** `movingsum [<field>] [interval=<interval>] [timeunit=<timeunit>]`

**Description:** Accumulated sum of the values in the specified field, per time period over a specified time window.

- **field:** Numeric field to be summed up.
- **interval:** (*optional*) Can be a positive number. Default interval is 5.
- **timeunit:** (*optional*) The unit of the interval. Can be one of the following: hour, minute, second, millisecond. Default timeunit is minute.

**Examples:** `*http* | rex "%{DATA:data}HTTP 1.1 %{INT:code} %{INT:bytes}" | movingsum bytes`

## sum

**Syntax:** `sum <field>+`

**Description:** Running total of all values in the given field. If a field is specified, only non-null values in the field are summed.

- **field:** The field name for the field to be counting non-null values on.

**Examples:**\* | sum error\_count field\_length

cast

**Syntax:** cast [*<field>*=*<type>*]+

**Description:** Changes the type of field if needed for a follow up operators. For example, this is needed if a number has been extracted from a text field and should be treated as a number instead of a string. Also can be used to specify a host column. The advantage of host columns is that a hostname in that column will mapped to alias names if necessary.

- **field:** Field that needs to be casted
- **type:** integer, numeric, string, timestamp, host

**Examples:**cast error\_count=integer sourcehost=host

hideignored

**Syntax:** hideignored

**Description:** Hide all log analytic messages that are set to be ignored by the user.

**Examples:**error | hideignored

## Track Message Groups and Parameters

You can select message groups or parameters within a group to track. Message groups are groups of similar logs and events. Data is collected and displayed in the Tracked Logs and Events dashboard.

## Learn About

About Tracking Message Groups and Parameters

You can specify individual message groups and parameters within those groups to focus on. Once selected, Operations Bridge Analytics will collect and display data about frequency over time. You can view the data in the Tracked Logs and Events dashboard, any custom dashboards you specify, and search results.



Tracking parameter distribution enables you to display the values of a parameter over time as well as the relative prevalence of each value.

After the data is collected, you can apply analytic tools to the data as you would any other metric. For example, you can use Predictive Analytics and perform correlations on the collected data.

## User Tasks

### How to Track a Message Group or Parameter

To track a message group or parameter, do the following:

1. Click a message in the search dashboard to view more details. If viewing a message in another dashboard, click **Go to Search** to view the message in the search dashboard.
2. To track a message group, click  **Track Message Group**.
3. To track a parameter, click a parameter, then click  **Track Parameter**.
4. Complete the user interface:
  - a. Specify a message group name if this group was not already named. For parameters, specify a parameter name.
  - b. The tracked data will always be visible in the Tracked Logs and Events dashboard, but you can also include the data in custom dashboards. Specify them in the **Add to custom dashboards** field.
  - c. Use the checkbox to specify if you want to display data about the tracked message group or parameter in search results when searching for related hosts.
  - d. You can add tags to the tracked message group or parameter to show its data in search results when searching for the specified tags.

**Note:** It may take a minute for tracked data to be visible in the user interface.

5. You can manage your tracked items by going to Settings  > Tracked Logs and Events.

### How to Manage Tracked Message Groups and Parameters

1. Go to the Settings  Menu.


2. Go to Tracked Logs and Events.
3. You can activate and deactivate tracked message groups and parameters, as well as edit the tracking settings.

**Note:** You cannot deactivate a message group if you are actively tracking parameters from that group.

## Log and Event Analytics

Log and Event Analytics are forensic tools that scan your log messages over a given time range and generates a list of the most significant Logs and Events.

To Access:

Search for a host, group of hosts, or service using the Search Tool . Locate the **Log and Event Analytics - Most Significant Messages** Query Pane. For information on this procedure, see "[Log and Event Analytics Dashboard Workflow](#)" on the next page. Alternatively, you can investigate significant messages in the Text Search user interface. For details on this procedure, see "[Log and Event Analytics Text Search Workflow](#)" on page 55.

## Learn About

### About Message Significance

Searching for the root cause of a problem can be daunting and knowing where to start can be difficult. Operations Bridge Analytics has designed powerful Log and Event Analytics algorithms that create a list of the top suspected log messages and events and show them visually in a pane. This algorithm runs over a user-defined time range for a host or a user defined group of hosts (a service). The Log and Event Analytics algorithms use a number of different parameters to calculate message and event significance, such as:

- Distance from problem time (user defined)
- Severity
- Specific keywords (for example: Exception)

- Repetition and seasonality (to identify insignificant messages)
- User feedback

The results can be viewed as a graph or in a list format.

## About Message Groups

Operations Bridge Analytics automatically analyzes your messages and creates message groups. Message groups are comprised of messages with very similar texts. These groups can later be liked, ignored, and analyzed as one unit. For details, see the tasks below.

## Tasks

### Log and Event Analytics Dashboard Workflow

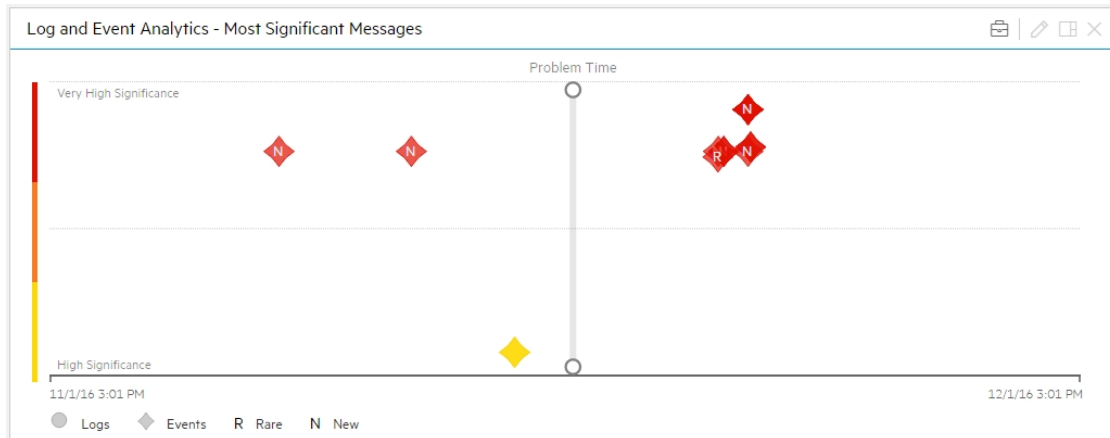
1. Make sure that log and event data is coming into Operations Bridge Analytics.
2. Search for a host, groups of hosts, or a service using the search tool.



The image shows a search bar with the text "Host:myhost123" entered. To the right of the search bar is a dropdown menu currently set to "1 Month" with a downward arrow. Further right is a blue search button with a magnifying glass icon.

Alternatively, you can add the Top Unusual Log Messages query pane to a custom dashboard.

3. Locate the **Log and Event Analytics - Most Significant Messages** query pane and define the time the problem started in the query pane by sliding the **Problem Time** indicator to the appropriate time. Operations Bridge Analytics then recalculates the most significant messages based on the problem time you select.



4. Hover over the diamonds in the graph to view the tooltips. Click a diamond to investigate the message in the text search user interface.

## Log and Event Analytics Text Search Workflow

1. Make sure that Log and Event data is coming into Operations Bridge Analytics.
2. Search for any string using the Text Search user interface.
3. Switch to **Significant messages** at the top of the Text Search user interface. Use the filtering and other search capabilities to investigate the significant messages.

## Modifying the Significant Message Calculation Model


Log and Event Analytics use a number of different criteria to calculate which messages and events are significant. You can affect this calculation in the following ways:

- **Problem time**

In the **Log and Event Analytics - Most Significant Messages** Query Pane, move the problem time indicator to the location that you believe the problem occurred. The significance of messages and events are calculated based on proximity to this time.

- **Keywords**


Operations Bridge Analytics uses certain keywords such as **Exception** to determine significance for log messages. You can add and remove additional keywords and set their importance.

- a. Click the Settings  button and select **Keywords Settings**.
- b. Enter a display name and your keyword in the **Expressions** field.


**Note:** You can use a variety of custom expressions in this field. For details, see below.

- c. Indicate the relative importance of this expression in the **Importance** drop down menu.
- d. Click **Add**.

- **Likes**

In the text search user interface, click the like  button to indicate that this message group is significant to you. This information is used in future calculations to determine message significance.

- **Ignore**

In the text search user interface, click the ignore  button to ignore a message group. This removes the message group from the log viewer list and the Top Unusual Messages chart. You can later restore these items by using the **Ignored Messages** button.

## How to Add a Log and Event Analytics Query Pane to a Custom Dashboard


Add a query pane with the following AQL query to a custom dashboard:

```
aqllogsummary(<aqlit></aqlit>, $starttime, $endtime, $problemtime)
```

For details about creating custom query panes, see [How to Add or Edit a Query Pane](#).



## Chapter 4: Play Back History

Operations Bridge Analytics enables you to play back your dashboard results using the  Play feature.










Use this feature when you want to view the most recent changes in data over time or when you want to note the point at which a problem began to occur.

When using this feature, note the following:

- Operations Bridge Analytics uses the start and end time specified in the time line.
- Operations Bridge Analytics selects the optimum time segment within the specified start and end time in which to show the results. For example, if the time line specifies 1 day, Operations Bridge Analytics might choose a time interval of 1 hour. If the time line specifies 1 hour, Operations Bridge Analytics might choose a time interval of 5 minutes.

**Note:** If you provide an \$interval parameter value in a query pane, Operations Bridge Analytics uses the \$interval value you specify for the time segment for only that query pane. See [Dashboards and Query Panes](#) for more information.


### To play back your search query results:


1. Click  Playback .
2. Click  (Play).
3. Do any of the following:
  - To pause the recording, click  (Pause) or press the spacebar. To unpaue press the spacebar again.
  - To fast forward to a new location, click  (Pause), then  (Fast Forward).
  - To rewind to a new location, click  (Pause), then  (Rewind).
  - To reverse play, click  (Back).

**Note:** If a query pane shows multiple pages of data, Operations Bridge Analytics replays only the results for the current query pane.

As Operations Bridge Analytics replays the results, it indicates each point in time for which data appears as shown in the following example:

12<sup>Mar</sup> 2015 4:01<sup>PM</sup> - 12<sup>Mar</sup> 2015 4:31<sup>PM</sup>


When you finish viewing the playback results, click  (Pause).


To exit playback mode, click .

# Chapter 5: Predictive Analytics

Predictive analytics enables you to generate a prediction line for one or more metrics based on past behavior and seasonal trends.

## To Access


To turn on predictive analytics in a Metric Data query pane, click **More Pane Actions**  and select **Predict**.

Click **1 Day**  to specify the length of the prediction line. By default, the prediction line runs for one day.

## Learn About

### About Predictive Analytics

Operations Bridge Analytics can predict the future behavior of some metrics and show this information in a query pane. The prediction line is shown as a dashed line, with the option of adding a prediction sleeve to show the margin of error.

Typically it takes about 2-3 hours to gather enough information to enable the prediction feature. The prediction confidence indicates the strength of the prediction and can be viewed in the tooltip over the  icon. Confidence increases as more data is collected for a given metric.

The tooltip also shows the trend of the prediction over time. For example, if the prediction is that the value will decrease from the current time until the end of the prediction time, the tooltip will indicate that there is a descending trend line.

To calculate the prediction, Operations Bridge Analytics makes use of the following items:

- Previous metric data and trends. For example, the data is steadily increasing or decreasing over time.
- Seasonal patterns (up to one week). For example, every morning at 8:30 there is a peak as employees arrive at the office.

Predictive analytics presents different displays depending on whether you are viewing one metric or more than one metric.

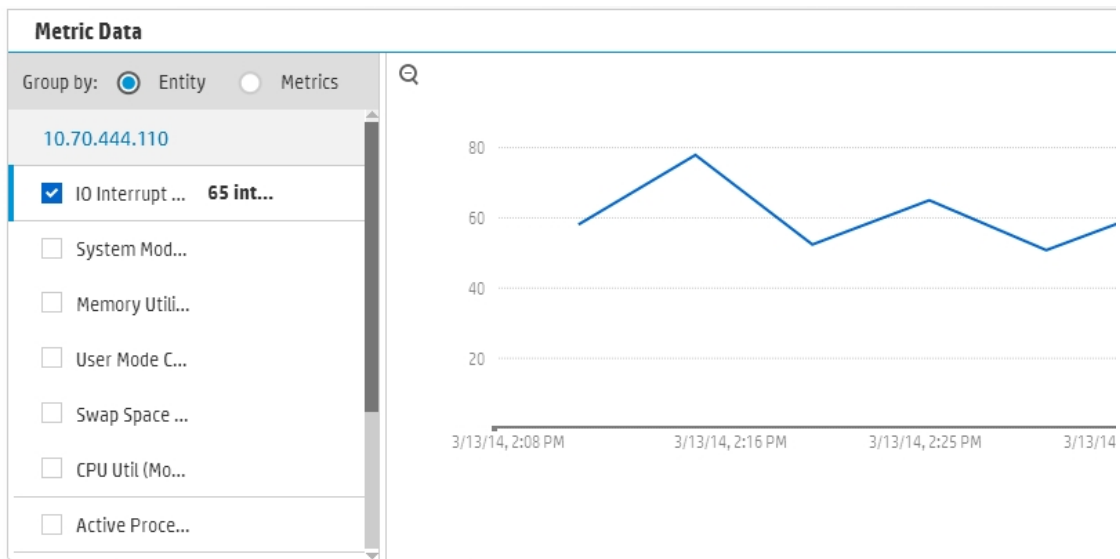
### Limitations:






- While the prediction feature is generally accurate, inaccurate predictions can occur at times due to unexpected events.
- Most AQL statements are supported with the prediction feature, but a limited number are not.

## Tasks

### Using Predictive Analytics

1. Select the check boxes next to the items you want to view.



2. Click **More Pane Actions**  and select **Predict**.
3. To edit the time period the prediction is active for, click **1 Day** .
4. To view the strength of the prediction, mouse over the  icon. To view the prediction sleeve, which shows the margin of error, click .
5. To remove the prediction lines, click **Disable Predict**  **Predict**.

## Chapter 6: Alerts

Alerts allow you to trigger different actions based on conditions and time intervals that you specify. This feature allows you to use Operations Bridge Analytics as a pro-active monitoring tool, in addition to its strong forensic capabilities.

### Learn About

#### About Alerts

Alerts are based on the results of an AQL query. You can configure the alert to send an email, run a script, send an SNMP trap, or create an event in OMi.

Alerts are created based on AQL queries. The query is taken from a pane, but can be modified in the alerts wizard. After the alert is created, the AQL defined in the alert is no longer connected to the AQL in the source pane (modifying one does not affect the other).

The history of triggered alerts can be viewed in the OpsA Alerts dashboard provided by Operations Bridge Analytics. This dashboard shows you all instances of triggered alerts going back three months by default.

You can drill down to open additional dashboards showing more details about an alert instance or time period surrounding an alert by clicking the time period or alert name of an alert instance.

#### About Alert Types

**Abnormality based Alerts.** Operations Bridge Analytics automatically calculates a dynamic baseline for a metric. Results that deviate from the baseline are defined as abnormal and may trigger alerts depending on other trigger conditions. This type of alert is only supported on line charts.

As soon as the alert is defined, data from the previous 90 days is used to calculate the baseline. The baseline requires a minimum of 12 data points to function.

**Threshold based Alerts.** You use an AQL to define a static threshold that is used to trigger the alerts. The trigger can only be based on the number of results of the query over a given time, so care must be taken to select a meaningful AQL. For example, if you want to see an alert every time CPU utilization

exceeds 80%, you must use an AQL that only displays instances in which the CPU utilization is 80% or higher.

This type of alert is supported on multiple types of panes. For example, in the BPM Overview dashboard, you can create an alert on the Application Overview Unavailability Over Time pane to let you know if the number of applications that were unavailable is greater than a number you specify in the alerts wizard.

## About Ownership

Alerts are defined per Operations Bridge Analytics tenant. Any user can create an alert. The creator of the alert and users with tenant admin permissions can edit and delete an alert. Other users can view, activate, deactivate, and add email recipients to alerts.

### Best Practices - Defining Alert Schedules

Alert schedules are defined primarily by the **Check data in the last** and **Run Every** settings in the Create Alerts Wizard. These settings specify how often to check the alert parameters, and on how much data to use when checking. Sometimes, there can be inconsistencies in time stamps on data and this can result in some data not being checked if the two values are equal (for example, Check data in the last hour and run every hour). To prevent this from happening, we recommend making sure that the value for **Run Every** be at least ten minutes less than the value for **Check data in the last**.

However, this can result in the same data being checked more than once, and generating redundant alerts. To prevent the alert actions from happening too frequently, use the **Perform action at most once every** setting.

## Limitations

You can create a maximum of 100 alerts per Operations Bridge Analytics environment. For options about how to increase this maximum number, speak to HP Software Support.


Alerts cannot be created from Log and Event Analytics panes.

# User Tasks

## How to Configure a New Alert

1. Before this procedure can be performed, your administrator must set up the alert action

capabilities. For details, see below.

2. From a query pane, click **More Pane Actions** , then select **Create Alert**.
3. Specify the type of alert. If relevant, select the metrics you want to use for the alert calculation. For details about alert types, see ["About Alert Types" on page 61](#).
4. Complete the **Create Alerts Wizard**. Details of selected user interface elements are described below.

#### First Page

UI Element	Description
<b>Alert Type</b>	<p>For details about the different alert types, see <a href="#">"About Alert Types" on page 61</a>.</p> <ul style="list-style-type: none"> <li>○ <b>Abnormality based alert on selected metrics.</b> Create an abnormality based alert. Select up to ten metrics to use.</li> <li>○ <b>Abnormality based alert on all metrics.</b> Create an abnormality based alert using all metrics.</li> <li>○ <b>Threshold based alert on selected metrics.</b> Create a threshold based alert. Select up to ten metrics to use.</li> <li>○ <b>Threshold based alert on all metrics.</b> Create a threshold based alert using all metrics.</li> </ul> <p><b>Note:</b> Alerts defined on all metrics will not trigger alert actions if the maximum number of metrics is exceeded.</p>
<b>Select Metrics</b>	Select up to ten metrics. This option is only relevant for some alert types.
<b>Define Alert</b>	After you click <b>Define Alert</b> , you will not be able to return to this page of the wizard.

#### Details Page

UI Element	Description
<b>Severity</b>	Select the severity you would like to associate with instances of this alert.
<b>AQL</b>	<p>The AQL query that will be used to calculate when to trigger an alert. This query is originally taken from a query pane, but can be modified. For example queries, see below.</p> <p>After the alert is created, there is no connection between the query in the original</p>

UI Element	Description
	pane and the query in the alert. This means that if the query changes in the host pane, this will not change the definition of the query in the alert.
<b>Check data in the last..</b>	When calculating whether to trigger an alert, the query is run over this time period.
<b>Test AQL</b>	Tests the query and returns and error if the query is not valid. Also returns the number of results for the query using the time period you specified above. Triggers are based on the number of query results.

## Schedule and Trigger Page

UI Element	Description
<b>Run every</b> <b>Run weekly</b> <b>Run monthly</b>	<p>Determines how often to check if an alert should be triggered.</p> <p><b>Note:</b> This schedule is determined by the client time zone, not the server time zone.</p> <p>We recommend making sure this value is less than the value for the Check data in the last setting. For details, see <a href="#">"Best Practices - Defining Alert Schedules"</a> on page 62.</p>
<b>Abnormal Results Definition</b>	<p>This section is only visible for Abnormality based alerts. Define the normal and abnormal range for AQL results. Abnormal results will be aggregated to potentially trigger results depending on the other trigger conditions.</p> <p>You can see a graphic representation of the abnormal and normal ranges as you modify your selections.</p> <ul style="list-style-type: none"> <li>◦ <b>Normal Range.</b> The size of the sleeve surrounding the dynamically generated threshold that defines a normal AQL results.</li> <li>◦ <b>Value is</b> The location that results can be considered abnormal.</li> <li>◦ <b>and also</b> In addition defining abnormal results based on the normal range which changes over time, you can define them based on a static value such as "above 5". In this case, both conditions must be met for a result to be considered abnormal (it must be in the defined abnormal range and above 5).</li> </ul> <p><b>For example:</b> If you defined a wide normal range, the normal range is calculated to within 5 standard deviations of the dynamically calculated baseline average. If you also wanted to make sure that the value is always above a static number, such as 50% CPU utilization, you would specify</p>



UI Element	Description
	“and also above 50”. In this case, the range must be more than 5 standard deviations away from the baseline average AND over 50% .
<b>Trigger if number of results</b>	Determines the condition to trigger the alert. The trigger is based on the number of query results over the time period defined in the Details page.

## Action Page

UI Element	Description
<b>Send email</b>	<p>Specify the email recipients and email subject. If there is more than one recipient, separate them using commas. For example:</p> <p>email1@abc.com,email2@abc.com</p> <p>You must specify which domains are permitted in the Alerts Settings.</p>
<b>Run script</b>	<p>This option is disabled if there are no scripts in the /opt/HP/opsa/inventory/lib/user/alerts/scripts/&lt;tenant_name&gt; directory.</p> <p>Input script parameters separated by commas. You can use any script parameters, as well as the following Operations Bridge Analytics variables as parameters:</p> <p><b>&lt;&lt;AlertLink&gt;&gt;</b>: A link to an Operations Bridge Analytics dashboard focusing on the alert instance.</p> <p><b>&lt;&lt;AlertId&gt;&gt;</b> - The alert ID.</p> <p><b>&lt;&lt;AqlDefinition&gt;&gt;</b> - The alert AQL query.</p> <p><b>&lt;&lt;AlertName&gt;&gt;</b> - The alert name.</p> <p><b>&lt;&lt;AlertUserId&gt;&gt;</b> - The user ID of the alert owner.</p> <p><b>&lt;&lt;AlertTrigger&gt;&gt;</b> - The alert trigger condition.</p> <p><b>&lt;&lt;AlertTimeFrame&gt;&gt;</b> - The alert calculation time period.</p> <p><b>&lt;&lt;AlertSeverity&gt;&gt;</b> - The alert severity.</p> <p><b>&lt;&lt;AlertAqlResultCount&gt;&gt;</b> - The number of results of the alert query over the defined time period.</p> <p><b>&lt;&lt;AlertDescription&gt;&gt;</b> - The alert description.</p> <p><b>&lt;&lt;AlertID&gt;&gt;</b> - The ID of the alert.</p> <p><b>&lt;&lt;AlertType&gt;</b> - The type of the alert.</p> <p><b>Note:</b> You can configure OBA to run alert scripts using only one specified</p>

UI Element	Description
	operating system user for security purposes. For details, see <a href="#">"How to Run Alert Scripts Using a Specific Operating System User"</a> on page 69.
<b>Encrypt</b>	Encrypts the script parameters. This is recommended when passwords are included in the parameters.
<b>SNMP</b>	Define the SNMP server settings. If you select Default from Alerts Settings, this takes the settings from the Alerts Settings user interface. If you select Custom, you define the settings here.
<b>Send to OMi</b>	Creates an event in OMi every time an alert is triggered. This action will not occur until you complete the procedure: <a href="#">"Sending Events to HPE Operations Manager i (OMi)"</a> on page 157.
<b>Perform action on every trigger</b>	Perform the alert action every time an alert is triggered.
<b>Perform action at most once every</b>	This prevents the alert action from happening too frequently.  <b>Note:</b> You can use this action to prevent notifications from redundant alerts, for details, see <a href="#">"Best Practices - Defining Alert Schedules"</a> on page 62.
<b>Run Test Alert</b>	This triggers a test alert with the name <b>TestAlert&lt;alertname&gt;</b> . It can be viewed in the alerts dashboard. Additionally, if you configured an action the action is performed. The test alert trigger is displayed as -1.

5. Manage and edit the alerts using the **Alerts Manager** user interface. This user interface can be

found by selecting Settings  from the main menu on the left.

- Filter the results by using the **Alert Name**, **Severity**, **Type**, and **Column** column headings.
- You can temporarily deactivate alerts you don't need right now and activate them again at any time. Select the desired alert and click **Activate** or **Deactivate**.
- Click the alert name to open a dashboard showing recent instances of this alert.

## How to View Alerts


A summary of your alerts can be viewed in the OpsA Alerts dashboard provided by Operations Bridge Analytics. This dashboard shows you all instances of triggered alerts going back three months by default.

You can drill down to open additional dashboards showing more details about an alert instance or time period surrounding an alert by clicking the time period or alert name of an alert instance.


You can search for an alert by using the search tool. Type **Alert** and hit space. Alert names located in your environment are displayed.

**Note:** The drill feature can sometimes take up to 30 minutes to function for newly created items. For example, alerts created in the last 30 minutes may return empty dashboards when attempting to click the alert name from the alerts dashboard.

## How to Activate or Deactivate Alerts

You can activate and deactivate alerts using the **Alerts Manager** user interface. This user interface can be found by selecting Settings  from the main menu on the left. If an alert is inactive, it is saved but no alerts are triggered and no actions are taken. Active alerts are fully functional.

## How to Edit an Alert


You can edit alert definitions using the **Alerts Manager** user interface. This user interface can be found by selecting Settings  from the main menu on the left.

# Administrator Tasks

## How to Set up Alert Action Capabilities

Before you can configure alerts to trigger an action, an Operations Bridge Analytics user with at least tenant administrator permissions must configure the desired action in the Alerts Settings dialog box. The settings in this dialog box are shared by all tenants in the Operations Bridge Analytics environment. For any changes to this dialog box to take effect, you must restart the **opsa-task-manager** and **opsa-server** processes.

### Email

In order to send an email as an alert action, you must set up an SMTP server to send the emails. To do this, select Settings  from the main menu on the left and select **Alerts Settings** and complete the SMTP section. In the Allowed Domains field, enter the email domains that are valid email alert

recipients separated by commas. If this field is empty, all domains are allowed.

Restart the **opsa-task-manager** and **opsa-server processes** for the changes to take effect.

If you are working in a hardened environment, see "Configuring SSL for the SMTP Server Used for Operations Bridge Analytics Alerts" in the HPE Operations Bridge Analytics Hardening Guide for details about how to configure the SMTP server to work with SSL.


### Script

In order to select a script as an alert action, you must have a script in the following directory on every server appliance server:

```
/opt/HP/opsa/inventory/lib/user/alerts/scripts/<tenant_name>/
```

- Only shell scripts (.sh) are supported.
- The script must have permissions of exactly 0700 and the file owner must be "opsa".

### SNMP

1. To configure default SNMP settings, To do this, select Settings  from the main menu on the left and select **Alerts Settings**

Here you define the default SNMP settings that can be used by all SNMP alerts. If default settings are defined in the Alerts Settings user interface, and are selected for a given alert, the values in the Alerts Settings are always used for that alert. If you later modify the values in the Alerts Settings, they are dynamically modified in all alerts set to use the default settings.

**Note:** Although Operations Bridge Analytics supports SNMP versions 1 and 3, when using the default settings only version 3 is supported.

2. To configure your SNMP server to better read the SNMP traps from Operations Bridge Analytics, we recommend uploading the following file to your SNMP manager:

```
/opt/HP/opsa/inventory/lib/user/alerts/OpsAAlerts.mib
```

The contents of the SNMP trap can be deciphered by opening the MIB file.

3. Restart the **opsa-task-manager** and **opsa-server** processes for your changes to take effect.

### OMi Event

You can configure an OMi Agent to retrieve alerts from Operations Bridge Analytics and create events from the alerts. For details, see "[Sending Events to HPE Operations Manager i \(OMi\)](#)" on page 157

## How to Run Alert Scripts Using a Specific Operating System User

You can configure OBA to run alert scripts using only one specified operating system user for security purposes. This allows you to prevent the alert scripts from accessing specific directories by controlling the permissions assigned to the user.

1. Create an operating system user with the desired permissions and restrictions.
2. Enable the JMX console by changing the suffix of the following file on the server appliance from **.tx** to **.txt**:

**/opt/HP/opsa/conf/jmxNotHardened.tx**

3. Wait five minutes before attempting to log in to the JMX console.
4. Log in to the JMX console using the following syntax:

**http://<server\_URL>:8081**

The default user name and password is **opsadmin**

5. Go to **OPSA-Infrastructure:service=Settings** and locate the function **setGlobalSettingValue**.
6. Enter the following values:

Field	Value
contextName	opsa-alerts-engine-settings
settingName	opsa.alerts.script.user
newValue	<operating system user name of your choice>

7. Select **Invoke** to complete the procedure.

## How to Manage Alert Resources on Vertica

Operations Bridge Analytics alerts use the same Vertica database resource pool as Operations Bridge Analytics panes. If alerts are consuming too many resources, this may result in performance issues for panes.

To resolve this issue, you can configure Operations Bridge Analytics alerts to use a designated resource pool in Vertica. For details about Vertica resource pools, refer to the Vertica documentation.

To use this feature, create a resource pool in Vertica for this use and specify it by name in **Settings**



**> Alerts Settings > Vertica Settings.**

Example resource pool using Vertica Vsql database utility that can be used by Operations Bridge Analytics:

```
dbadmin=> CREATE RESOURCE POOL ALERTS_POOL EXECUTIONPARALLELISM
4;
```

## Example AQL Queries

### Examples

The following are examples of possible AQL queries that could be used to create an alert.

1. BPM transactions that took longer than 4 seconds.

```
from i in (bpm_application_performance) where (i.transaction_response_time>"4000") let
analytic_interval=between($starttime, $endtime) let interval=$interval group by i.application select
i.transaction_response_time
```

2. Host in which a jdbcException occurs within a time window.

```
"xql: JdbcException hostname=*.hp.com | between $STARTTIME $ENDTIME"]
```

3. Host in which a system metric (sitescope\_cup\_metrics) has crossed a specific value (moving\_avg(i.utilization)).

```
[metricQuery({sitescope_cpu_metrics}, {(i.target_name ilike "<my host FQDN>")}), { i.target_
name}, {moving_avg(i.utilization)}]]
```

4. One of three specified hosts exceeded 90% CPU usage.

```
from i in (oa_sysperf_global) let analytic_interval=between($starttime,$endtime) let
interval=$interval let aggregate_playback=$aggregate_playback_flag where (((i.host_name like
"<my host FQDN 1>") || (i.host_name like "<my host FQDN 2>")) || (i.host_name like "<my host
FQDN 3>")) && (i.cpu_util>40)) group by i.host_name select i.cpu_util
```

5. Free disk space of a specified host has gone below 2GB

```
from i in (nmmispi_netcomponent_component) where ((i.disk_space_free_mb < 2000) && (i.host_
name like ""*)) let analytic_interval=between($starttime,$endtime) let interval=$interval let
aggregate_playback=$aggregate_playback_flag group by i.host_name select i.disk_space_free_
mb
```

# Chapter 7: Correlate Metrics

It can be useful to understand which metrics have similar data patterns. You can compare metrics to each other by using the correlation function.

## Learn About

### About Correlation

The correlation feature takes all metrics in a pane and runs a correlation ( $r$ ) function on each unique pair of metrics. The results are displayed in a pane that show the results of the correlation for each pair and a visualization of the metric pair over time.

The correlation feature can be run in out-of-the-box dashboards, but they cannot be saved with the correlation pane as they are not editable.

Metric data taken every 300 seconds is used to calculate the correlation and display the correlation graph. This value cannot be changed and does not vary regardless of the granularity of the pane the correlation was opened from. This may result in the correlation graph appearing differently from other panes displaying the same metrics with different granularity.

### Correlation Values ( $r$ )

The correlation values vary from -1 to 1. The higher the absolute value of the correlation, the closer the relationship. For example, a correlation of 0.99 indicates a very strong, direct correlation. A correlation of -0.99 indicates a very strong inverse correlation.

When you sort the correlation pane by correlation values, the absolute value is used to calculate the order.


### Limitation

- In some cases, the correlation cannot be calculated due a variety of reasons such as lack of historical data.
- The correlation feature is limited in the amount of data it can calculate in each pane. If the limit is

reached, only some of the correlations will be calculated.

## User Tasks

### How to Correlate Metrics

1. From any line chart, click **More Pane Actions**  and select **Correlate**.
2. You can filter the results by entities or metric names by entering strings in the column headers. The same string is entered in corresponding A and B columns. To use a different filter for columns A and B, use the syntax `string1::string2` where `string1` filters column A and `string2` filters column B.
3. You can sort the results by clicking the column header names.

## UI Description

### Correlation Pane

User interface elements are described below.

#### To Access

From any query pane, click **More Pane Actions**  and select **Correlate**.

UI Element	Description
<b>Metric A Entity, Metric B Entity</b>	<p>The entity of the metric in the metric A or B name column.</p> <p>You can filter this column by entering a string in the header. The same string is entered in both Metric A and B entity names. To use a different filter for columns A and B, use the syntax <code>string1::string2</code> where <code>string1</code> filters column A and <code>string2</code> filters column B.</p> <p>You can drill down to open a dashboard focusing on the entity by selecting an entity in this column.</p>



UI Element	Description
	<p><b>Note:</b> There is no significant difference between columns A and B. They are just identifiers. Each metric is compared to every other metric exactly once.</p>
<p><b>Metric A Name, Metric B Name</b></p>	<p>The name of the metric.</p> <p>You can sort the column by clicking the column header.</p> <p>You can filter the column by entering a string in the header of this column. The same string is entered in both Metric A and B names. To use a different filter for columns A and B, use the syntax string1::string2 where string1 filters column A and string2 filters column B.</p> <p><b>Note:</b> There is no significant difference between columns A and B. They are just identifiers. Each metric is compared to every other metric exactly once.</p>
<p><b>Correlation (r)</b></p>	<p>The correlation value indicating how closely correlated Metric A and B are to each other. For more details, see <a href="#">"Correlation Values (r)" on page 71</a></p>

# Chapter 8: Topology Manager

The Topology Manager enables you define a logical hierarchy for monitored hosts. You can group hosts together based on their function, their location, or any other grouping that is meaningful to you when organizing your services.

## Learn About


### Services, Groups, and Hosts

Hosts are organized into **groups** and **services**. A **service** is a collection of **groups**, and a **group** is a collection of **hosts**.

For example, you might create a service that includes web servers, applications servers, and database servers. In order to easily reference all these hosts and get a holistic view of the service, you would create groups for web servers and so on. The groups will correspond to the groups you want to look at in Operations Bridge Analytics. A subsequent search for this service will return results for all the underlying hosts, providing a single pane of glass for all hosts that make up the service.

## Tasks

How to define a service:

1. Click  **Settings** and select **Topology Manager**.
2. Select **New**, and enter a name for your service.
3. Enter a group name and a host, then click **Add**.

**Tip:** You can define a dynamic set of hosts by using the \* symbol. For example, if you enter **dbhost\*** as your host name, Operations Bridge Analytics will add all hosts that begin with the string **dbhost** to the specified group. The group definition will be updated automatically if additional hosts are defined with the string **dbhost**.

You can select the host from a list; as you type the first letters of the host, the list filters automatically. When adding a host, you can add it to an existing group or to a new one.

- Continue defining groups and their hosts until you are done, and then click **Save**.

As a simple example, you can define a service called MyService, as follows:

- This service is made up of the groups **MyWebServers**, **MyAppServers**, and **MyDBServers**.
- These groups are made up of **WebHost1-3**, **AppHost1-3**, and **DBHost1-3** respectively.

The screenshot shows the 'Topology Manager' window. On the left, there is a form for defining a service. The 'Service Name' is 'MyService'. Below it is a table with columns 'Group Name' and 'Host Name'. The table contains the following entries:

Group Name	Host Name	Action
MyDBServers	DBHost3	Delete
MyWebServers	WebHost1	Delete
MyWebServers	WebHost2	Delete
MyWebServers	WebHost3	Delete
MyAppServers	AppHost1	Delete
MyAppServers	AppHost2	Delete
MyAppServers	AppHost3	Delete
MyDBServers	DBHost1	Delete
MyDBServers	DBHost2	Delete

On the right side of the window, there is a circular topology diagram. The diagram shows a central circle labeled 'MyService'. Surrounding it are three concentric rings representing groups: 'MyDBServers' (outermost, dark red), 'MyAppServers' (middle, orange), and 'MyWebServers' (innermost, yellow). Each group contains three host nodes: 'DBHost1-3', 'AppHost1-3', and 'WebHost1-3' respectively.

After you define a service, you can then search for it and view metrics, events and logs that are relevant to all the hosts in that service.

#### Searching for a Service Defined in Topology Manager

After you have defined a service, it can be referenced in searches and resulting dashboards.

For example, suppose you have defined a service called MyService, as follows:

- This service is made up of the groups **MyWebServers**, **MyAppServers**, and **MyDBServers**.
- These groups are made up of **WebHost1-3**, **AppHost1-3**, and **DBHost1-3** respectively.

You can now run the following searches:

- Service: "MyService". This search returns a dashboard with information regarding the different hosts in all the groups that are part of the **MyService** service, with their events and logs.
- Service: "MyService" Drill To: "MyWebServers" - This search returns a dashboard with data on all the hosts that belong to the **MyWebServers** group in the service, including metrics, events and logs.

When you search for a service, the sunburst chart only displays metrics that have the tag "toposunburst". Collections are configured with some metrics tagged by default, but you can add tags to additional metrics if required.

**Note:** You can also use a host-based search (for example Host: "WebHost1") to then focus on a specific host that seems to have issues.

These different searches provide you with a drill-down capability. When you look at the service, you can pinpoint the group or in some cases the specific host that may be causing the issue. When you look at a group you can quickly focus on a specific host that exhibits problems. The final drill-down to a specific host helps you pinpoint the root cause of the problem.

For more details, see ["Search Tool" on page 32](#).

## Chapter 9: About the Analytics Query Language (AQL)

Use the Analytics Query Language (AQL) when the Phrased Query Language (PQL) syntax is not specific enough to return the data you need. When using AQL you can be more specific about the data collected. You can also filter, group, and order the collected data in a single query.

AQL queries use a syntax similar to the ANSI Standard SQL. When using AQL, it is helpful if you have minimal knowledge of databases as well as scripting or programming skills. However, it is not mandatory to have this knowledge to get started using AQL queries.

**Tip:** Before you begin writing AQL queries, view the collection information that is stored in Operations Bridge Analytics to determine the kinds of data available in your environment. You will use this information as part of your AQL syntax. For details, see ["How to View Collection Information" on page 90](#).

Note the following:

- When building AQL queries, you can also define AQL functions or expressions.
- AQL functions are a convenient way of defining and naming frequently used AQL queries for reuse. When you define the function, you define the associated AQL query as well as the argument values to pass to that AQL query. See the [AQL Developer Guide](#) for more information.

## Chapter 10: Anomaly Detection

Anomalies are major changes in the amount or value of collected data. Operations Bridge Analytics automatically searches for, detects, and displays anomalies. You can send an event to OMi when an anomaly is detected.

### Learn About

#### What is an Anomaly?

Operations Bridge Analytics automatically calculates a normal range for each item of collected data. This range is called the **Baseline**.



A **Breach** is defined as any major change from a baseline in the amount or value of collected data.

Operations Bridge Analytics uses your settings and an internal algorithm to determine when one or more breaches should be defined as an **Anomaly**. When this occurs, the anomaly is comprised of all the data in a given time range from one or more logs and/or metrics. To put it simply, when it is determined that the incoming data is highly unusual, it is defined as an anomaly.

All data types are used when calculating an anomaly. Anomalies can be triggered on hosts, entities, or services. The algorithm for recognizing an anomaly depends on many different items, each potentially increasing the chance that an anomaly will be triggered. Some of the items that contribute to this chance are:

- Value and frequency of breaches. The more breaches and the farther they are from the baseline, the higher the chance of an anomaly.
- Tags can be manually specified to increase the change for an anomaly.
- The number of logs and events per cluster as well as message significance.
- Whether there has been a recent major change to the host or entity.
- User defined settings such as specific tags or metrics.

## How to Configure Anomaly Settings

1. Click Settings  and select **Anomalies Settings**.
2. Click , and modify the settings in the **Triggers** tab as desired.

UI Element	Description
<b>Chance to trigger anomaly (sensitivity level)</b>	Adjusts the overall chance of triggering an anomaly.
<b>Increase chance to trigger anomaly</b>	You can increase the chance to trigger an anomaly based on each factor listed here.
<b>Minimum number of breached metrics/message groups</b>	In general, anomalies are triggered when more than one metric /message group is breached multiple times. This setting allows you to define a minimum number of metrics that must be breached to trigger an anomaly.
<b>Tags that influence the chance to trigger an anomaly</b>	You can define tags that will affect the anomaly calculation. For this to be effective, you must make sure that these tags are used on incoming data appropriately.

3. Click **Next** to move on to the **Preview** tab.
4. Click **Next** to move on to the **Actions** tab. Here you can configure a setting which will create an event in OMi when an anomaly is triggered. You can specify whether this action will occur for each anomaly or limit the action to occur no more than once over a specified amount of time.

This action will not occur until you complete the procedure: "[Sending Events to HPE Operations Manager i \(OMi\)](#)" on page 157.

## How to Send an Event to OMi upon Anomaly Detection

You can configure a setting which will create an event in OMi when an anomaly is triggered. You can specify whether this action will occur for each anomaly or limit the action to occur no more than once over a specified amount of time.

1. Go to **Settings > Anomalies Settings**.
2. Click **Next** until you get to the Actions tab.

3. Check the **Send to OMi** checkbox and configure the settings.
4. Perform the procedure in the section "[Sending Events to HPE Operations Manager i \(OMi\)](#)" on [page 157](#) to enable OMi to retrieve the events.



# Collections

This section contains the following topics:

["Installing and Configuring a Third-Party Agent" on page 91](#)

["Troubleshooting Source Type Manager Error Messages" on page 126](#)

["Managing the Content for Data Source Types" on page 133](#)

["General Collection Information" on page 82](#)

["Using Tags for Source Types" on page 136](#)

[" Communicating Collection Names and Meta Data Information to your Users " on page 147](#)

# Chapter 11: General Collection Information

This topic describes the terms and procedures related to data collection sources.

## Learn About

### About Keys and Link Tags

Keys identify a column in a collection that you want Operations Bridge Analytics to use to do either of the following:

- Narrow a search within a single collection
- Match metrics for one entity (collection row) to the same or related entity (collection row) across collections

Typically, key columns uniquely identify an entity instance.

When using a key column to narrow a search within only one collection, Operations Bridge Analytics returns only those metrics for the specified key column value. For example, if the **host\_name** column is defined as a key in a cpu metrics collection, the host\_name key column enables you to search for cpu metrics for a specific host name.

When using keys to identify a column in a collection that you want Operations Bridge Analytics to use to match metrics for a specific entity across collections make sure the required column is configured in each collection. For example, you might find that host\_name is an attribute that identifies the host in most of your collections. However, perhaps in one or two collections, server\_name is the attribute used to identify the host. In this scenario, you specify **host\_name** as a key column in the collections that include the host\_name attribute and **server\_name** as a key column in the collections that include server\_name. When a user enters a host\_name value in a PQL search query, Operations Bridge Analytics looks for that value in all key columns across collections.

Note the following:

- When you define a service using the Topology Manager, Operations Bridge Analytics configures the link tags to establish the relationships between the collections for your service. You can then

search for information using these relationships. See ["Topology Manager" on page 74](#) for more information.

## About Tags

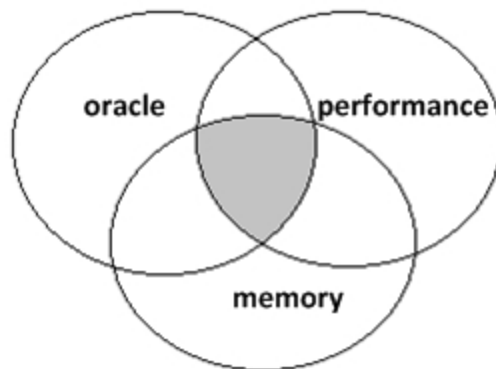
A tag is a word that is associated with a collection or with a metric or attribute that is stored as part of a collection.

Tags are used in the Operations Bridge Analytics Phrased Query Language (PQL) to create an Operations Bridge Analytics dashboard. They help to define the following:

**Note:** Tags are not limited to these example uses.

- Entities for which you want information, such as **host**, **database**, and **application**
- Hardware and software components, such as **cpu**, **memory**, **disk**, **interface**, **tablespace**, **process**, and **threads**
- Metrics or problem areas, such as **utilization**, **availability**, **performance**, and **change**

Operations Bridge Analytics returns results based on an intersection of the tags used in the search query. For example, the query **oracle memory performance** returns only the metrics that are associated with all three tags (**oracle memory performance**) as represented in the following diagram:



**Note:** If you include a hostname in your query, Operations Bridge Analytics refines the search to include only those metrics associated with the host name you specify.

As an Operations Bridge Analytics administrator, you might want to add, edit, or remove tags after they are initially configured. See `opsa-tag-manager.sh` (available from `help > reference pages`) and ["Using Tags for Source Types" on page 136](#) for more information.

To view the tags available for a collection, see ["How to View Collection Information" on page 90](#) or use the `opsa-tag-manager.sh` (available from `help > reference pages`) command.

### Uses for Tags

Use	Example	Result
Represent the data for an entire collection	If you have configured an HPE NNM iSPI Performance for Metrics collection, the tag <b>performance</b> might be used for that collection.	When you type <b>performance</b> in your phrased search query, the value for all attributes in the NNM iSPI Performance for Metrics collection are considered for use in the metrics displayed.
Provide one or more synonyms for an attribute stored in a collection	The tag <b>host</b> might be used as a synonym for the attribute <b>host_name</b>	When you type <b>host</b> in your search query, Operations Bridge Analytics uses the value stored for <b>host_name</b> in each collection table for which the tag is defined.
Group attributes that provide similar information	The tag <b>cpu utilization</b> might be used to represent the following CPU attributes: <ul style="list-style-type: none"> <li>• <code>cpu_idle_time</code></li> <li>• <code>cpu_sys_mode</code></li> <li>• <code>cpu_util_time</code></li> <li>• <code>cpu_util</code></li> <li>• <code>cpu_user_mode</code></li> <li>• <code>cpu_context_switch_rate</code></li> <li>• <code>cpu_run_queue</code></li> </ul>	When you type <b>cpu utilization</b> in your search query, Operations Bridge Analytics uses the values stored for the CPU attributes in each collection in which the tag <b>cpu utilization</b> is defined.
Focus on attributes that are prototypical	The tag <b>primary</b> might be used to tag the most important metric attributes for a specific area, such as <code>cpu</code> ). This means that when the user enters <b>cpu primary</b> in the search query, the results focus on only a few important metrics, which are tagged as <b>primary</b> .	When you type <b>&lt;hostname&gt;cpu</b> in your search query, Operations Bridge Analytics uses the following metrics in its results. <ul style="list-style-type: none"> <li>• <code>cpu_idle_time</code></li> <li>• <code>cpu_sys_mode</code></li> <li>• <code>cpu_util_time</code></li> <li>• <code>cpu_util</code></li> <li>• <code>cpu_user_mode</code></li> <li>• <code>cpu_context_switch_rate</code></li> <li>• <code>cpu_run_queue</code></li> </ul>

## Uses for Tags, continued

Use	Example	Result
		<p>When you type <code>&lt;hostname&gt;cpu primary</code> in your search query, Operations Bridge Analytics might use only the following metrics in its results.</p> <ul style="list-style-type: none"> <li>• <code>cpu_util</code></li> <li>• <code>cpu_user_mode</code></li> </ul>
Group attributes across collections	<p>The tags <b>performance primary</b> could be used for the attributes that assist with identifying performance problems across collections.</p> <p>As another example, you might tag all metrics that are useful for identifying status or health information across collections.</p>	<p>When you type <b>performance primary</b>, Operations Bridge Analytics returns performance metrics from both the HPE Operations Smart Plug-in for Oracle and HPE Operations Agent collections.</p>
Dynamically extend your collections	<p>Use the same tag name for more than one collection. For example, you might use the tag name <b>event</b> and <b>events</b> for the following collections:</p> <ul style="list-style-type: none"> <li>• HPE Operations Manager (OM)</li> <li>• HPE Operations Manager i (OMi)</li> </ul>	<p>When you type <code>&lt;host name&gt; events</code> in your search query, both the Operations Manager i events and Operations Manager events data is used to return your results.</p>

## About Meta Data

Operations Bridge Analytics stores collections information as meta data (descriptors). Example meta data information includes:

- Collection table names.

**Note:** Operations Bridge Analytics stores metrics, topology, inventory, log file, and event information in the form of collection tables. These collection tables are also known as property groups. The columns that represent the metrics collected and that store values within these tables are also known as properties. A property can be either an attribute or a metric.

- Metrics, attributes, and tags per collection.
- The length of time the data is retained per collection.
- Data type information per collection.

## About Collectors

A Collector is responsible for collecting data from one or more data Source Types. The data collected is organized by collections.

Each collector is configured to run in an Operations Bridge Analytics Collector Agent.

Each server that is running the Operations Bridge Analytics Collector agent is configured as a Operations Analytics Collector host. See Adding or Connecting Source Types for more information.

## About Collections

Operations Bridge Analytics stores metrics, topology, inventory, log file, and event information in the form of collections. Each collection is associated with a database table in which an Operations Bridge Analytics Collector stores the data collected.

**Note:** These collection tables are identified in the Operations Bridge Analytics database as **property\_group\_uid**. The columns that represent the metrics collected and that store values within these tables are stored in the database as **property\_uid**. This is important to know when using the SystemMetaInfo dashboard to identify text strings to include in your search queries.

As the Operations Bridge Analytics administrator, you configure one or more data Source Types per Operations Bridge Analytics collection. See Configuring Collections for more information.

## Collection Data Sources

Operations Bridge Analytics gathers metrics, topology, inventory, event, and log file data from a diverse set of possible data Source Types. The table below describes the details of these Source Types.

- The Operations Bridge Analytics administrator configures the data Source Types.
- Operations Bridge Analytics data Source Types marked with an asterisk (\*) indicate the data sources for which Operations Bridge Analytics provides configuration templates.

## Business Process Monitor (BPM)

**Description:** Collects metric data from HPE Business Process Monitor.

**Required Software:** HPE Business Process Monitor (BPM).

**Configuration template provided by Operations Bridge Analytics:** yes.

### Custom CSV files

**Description:** Collects metric, inventory, topology, log, and event data that resides in a CSV file.

**Required Software:** No requirements. Many applications export data, such as topology and metrics information, into CSV files. In addition, your network administrator might have written customized scripts to export data to CSV files.

**Configuration template provided by Operations Bridge Analytics:** no.

### HPE Operations Agent

**Description:** Collects global system information in the form of metrics. Examples of the type of metric collected by default include host name, time stamp, and global metrics such as CPU total utilization, and disk input and output rate.

**Required Software:** HPE Operations Manager

**Configuration template provided by Operations Bridge Analytics:** yes.

See the *HPE Operations Agent User's Guide* for information about attributes that can be collected as metrics.

### HPE Operations MPs

**Description:** Collects global system information in the form of metrics. Examples of the type of metric collected by default include host name, time stamp, and global metrics such as CPU total utilization, and disk input and output rate.

**Required Software:** HPE Operations Manager

**Configuration template provided by Operations Bridge Analytics:** yes.

See the HPE Operations Manager management pack documentation for information about attributes that can be collected as metrics.

### HPE Operations Smart Plug-in for Oracle

**Description:** Collects global Oracle database information in the form of metrics.

**Required Software:** HPE Operations Manager

**Configuration template provided by Operations Bridge Analytics:** yes.

See the *HPE Operations Smart Plug-in for Oracle Reference Guide* for information about attributes that can be collected as metrics.

## HPE Network Node Manager i Software (NNMi) Custom Poller

**Description:** Collects numeric metrics from any NNMi Custom Poller MIB expression.

**Required Software:** HPE Network Node Manager i Software (NNMi)

**Configuration template provided by Operations Bridge Analytics:** yes.

**Examples of Metrics Collected by Default:** Node Name, Time Stamp (ms), SOURCE, Node UUID, IP Address, MIB Expression, Poll Interval (ms), MIB Instance, Metric Value, Display Attribute, Filter Value.

See the *NNMi Help for Operators* for more information about each of these attributes.

## HPE Network Node Manager iSPI Performance for Metrics

**Description:** Collects interface and node component metrics from HPE NNM iSPI Performance for Metrics. Examples of collected information:

- Interface health extension pack metrics
- Component health extension pack metrics

**Required Software:** HPE Network Node Manager iSPI Performance for Metrics.

**Configuration template provided by Operations Bridge Analytics:** yes.

See the HPE Network Node Manager iSPI Performance for Metrics online help for more information about attributes that can be collected as metrics.

## HPE Operations Manager (OM) events

**Description:** Collects events generated by HPE Operations Manager (OM).

**Required Software:** HPE Operations Manager.

**Configuration template provided by Operations Bridge Analytics:** yes.

**Examples of Event Metrics Collected by Default:** EventID, TimeReceivedTimeStamp, TimeCreatedTimeStamp, Severity, NodeName, State, EventText, MessageGroup, EventObject, MsgSource, Application, AutoState, AutoAcknowledge, OperatorAcknowledgeFlag, Service.



## HPE Operations Manager i (OMi) events

**Description:** Collects events generated by HPE Operations Manager i Software.

**Required Software:** HPE Business Service Management (BSM)

**Configuration template provided by Operations Bridge Analytics:** yes.

**Examples of Event Information Collected by Default:** EVENT, ID, DATE\_CREATED, DATE\_RECEIVED, TIME\_STATE\_CHANGED, TITLE, DESCRIPTION, PRIORITY, STATE, SEVERITY, TYPE, CATEGORY, SUBCATEGORY, APPLICATION, ASSIGNED\_GROUP, ASSIGNED\_USER, CIREF\_ID, HOSTREF\_ID, HOSTINFO\_IPADDRESS, HOSTINFO\_DNSNAME, ORIGINATING\_IPADDRESS, ORIGINATING\_DNSNAME, SENDER\_IPADDRESS, SENDER\_DNSNAME, PARENT\_ID, RC\_FLAG, POLICY\_TYPE, POLICY\_NAME, CORRELATION\_TYPE, CORRELATION\_RULE\_ID, LOG\_ONLY

See the *HPE Operations Manager Administrator's Reference* for more information about each of these attributes.

## HPE Run-Time Service Model (RTSM)

**Description:** Collects Configuration Item (CI) inventory information that is stored in BSM.

**Required Software:** HPE Business Service Management (BSM)

**Configuration template provided by Operations Bridge Analytics:** yes.

**Examples of Inventory Collected by Default:** Cild, CiType, display\_label, name, description.

## HPE SiteScope

**Description:** Collects metrics such as CPU utilization, memory utilization, pages per second, and memory pool size. This list varies depending on your collection.

See the *HPE SiteScope Monitor Reference* for more information about available monitoring attributes.

**Required Software:** HPE SiteScope.

**Configuration template provided by Operations Bridge Analytics:** no.

# Tasks

## How to View Collection Information

Go to the **SystemMetalInfo** dashboard to view:

- Collections and any tags for each collection
- Columns per collection and tag names per column
- Columns defined as keys as well as whether the data stored in the column is a metric or attribute

## How to Register an Operations Bridge Analytics Collector Host

You must register at least one Operations Bridge Analytics Collector Host to create a collection. For details, see ["Registering Operations Bridge Analytics Collector Hosts" on page 235](#)

## Chapter 12: Installing and Configuring a Third-Party Agent

Operations Bridge Analytics supports data collections using third-party agents, like BSM Connector. To set up data collections using a third-party agent, you must install that agent and configure it to send data to an Operations Analytics Collector host. One extra approach you can use is to install Operations Analytics Data Pipe, which is Logstash software included with Operations Bridge Analytics, on servers from which you want to collect data.

**Note:** If you plan to install and use your own version of Logstash instead of the Operations Analytics Data Pipe, install and configure it using the reference material at [Logstash Reference](#).

Do the following to install and configure Operations Analytics Data Pipe (or other third-party agents):

1. Install the third-party agent on the server or servers from which you want to collect data.

**Note:** This agent can be the Operations Analytics Data Pipe agent (Logstash), but can also be something else, such as BSMC, an unmodified Logstash, or a custom-developed script.

To install the Operations Analytics Data Pipe agent, run the following command: `opsa_outpost-<version-information>.rpm`

2. Configure the third-party agent to send data to the Operations Analytics Collector host. The third-party agent sends its data to the Kafka topic of the source type in JSON format. For example, you might use a Logstash JSON output CODEC (`logstash-codec-json`). The JSON events must all contain configured collection properties as fields.


**Note:** Supports the Kafka approach supported by Operations Bridge Analytics.

**Note:** You can view the required endpoint information by reviewing the defined collection.

3. An OBA whitelist is a list of IP addresses permitted to access Operations Bridge Analytics.

You do not normally add an Operations Analytics Data Pipe server to the whitelist. Only complete this step if you are not using the Operations Bridge Analytics console to configure the Operations Analytics Data Pipe. Adding an Operations Analytics Data Pipe server to the whitelist assumes that you are using some kind of cloning technology to copy an already configured Operations Analytics Data Pipe to another server.

This whitelist is not enabled by default, so you must complete these steps if you want to set up an OBA whitelist. To add an Operations Analytics Data Pipe server to this list, do the following:

- a. From the Operations Bridge Analytics console, open the Operations Bridge Analytics tuning page using **Control > Alt > Click** the  **Settings** menu item.
- b. Click **OpsA Tuning Page**.

**Caution:** The **OpsA Tuning Page** is for use by HPE Operations Bridge Analytics customer support personnel only. Some settings cannot be undone and may be harmful to your system.

- c. Locate the **Externally configured LogStash hosts IPs** name. Enter the IP address of the Operations Analytics Data Pipe server you are adding to the comma-separated list of the IP addresses of Operations Analytics Data Pipe servers.
- d. From the Operations Analytics Collector host, run the following command as the `opsa` user to commit your changes:

```
/opt/HP/opsa/bin/opsa-kafka restart
```

**Note:** Using wildcard characters in the whitelist feature is not recommended. If you must use wildcard characters, make sure to keep the IP address list as limited as possible to improve Operations Bridge Analytics security.

4. As the Source Type Manager does not know about these remote data channels, they are not listed in the Operations Bridge Analytics console. Add the channel type for the collection you are configuring using **Add Channel** when configuring the collection for this remote data channel.

**Note:** These data channels are configured, started, stopped, and removed outside of Operations Bridge Analytics.

## Chapter 13: Adding a New Source Type — Command Line Method

Use the instructions in this section to configure Custom Collections or SiteScope Collections using command lines.

It is recommended you use the Source Type Manager to add Source Types (Custom Collections). See [Adding or Connecting Source Types](#) for more information.

In special circumstances, you can use the instructions in this section to configure a Custom collection using the `opsa-collection-config.sh` script.

To collect data from sources that do not use predefined collection templates, you can use the `opsa-collection-config.sh` script to configure a Custom CSV collection. Use the following list to determine if this method might work for you:

- The data source must provide Comma-separated values (CSV) data. CSV data is the only method that Operations Bridge Analytics provides to collect data when using a command line.
- The data source must collect CSV data based on time. There has to be a time and date column for each row in the CSV file. Both the time and date must be in that same column.

**Note:** If this requirement is not met, you must merge these columns before creating the collection.

- The data source cannot exceed 200 data columns. If you try to create a Custom CSV collection containing more than 200 data columns, the collection creation fails.
- The maximum supported CSV file size is 500 MB.
- Data from the CSV data source must be accessible to the Operations Analytics Collector host.
- The CSV file can be local or remote to the collector and is assumed to be available in the source directory at regular intervals.
- Each column must have a header.
- Column names must not contain any spaces.
- Operations Bridge Analytics uses the CSV file to create a table in Vertica. Vertica objects include tables, views, and columns. Your CSV file must use the following naming conventions:

- A column name must be from 1 to 128 characters long.
- A column name must begin with a letter (A — Z), diacritic marks, or non-Latin characters (200–377 octal).
- A name cannot begin with an underscore (\_). Leading underscores are reserved for system objects.
- Names are not case-sensitive. For example, CUSTOMER and Customer represent the same names. However, if you enclose a name in quotation marks, it is case-sensitive.

**Note:** Object names are converted to lowercase when they are stored in the Vertica database.

- A name cannot match a Vertica reserved word such as WHERE, VIEW, Table, ID, User, or Query.
- A name cannot match another Vertica object that has the same type.
- The Maximum number of columns cannot exceed 1549 in a CSV file as that value is a Vertica limitation when creating a table.
- The CSV file format has to be uniform for a single collection. For example, if you create a collection with 10 columns, the subsequent files that are provided for import within Operations Bridge Analytics must have same format. This format includes column names and data types.

For an example of data you might choose to collect using a Custom CSV collection, see the *Creating a Content Pack for Operations Analytics* White Paper at [HPE Live Network](#).

**Note:** Do the following to locate the *Creating a Content Pack for Operations Analytics* White Paper:

1. Select **Products**.
2. Navigate to the **Operations Intelligence (Operations Bridge Analytics)** product, then click **Operations Intelligence**.
3. Click **Resources**, then locate the *Creating a Content Pack for Operations Analytics* White Paper.

## Important Prerequisite Steps

Complete the following prerequisite work before configuring your Custom CSV Collection using the steps in "[Configuration Steps](#)" on [page 97](#):

1. Tenants enable you to separate information from these data sources into groups, such as collections, user accounts, and user groups. When running the commands in this section, the tenant model you select affects which Tenant Admin user you will use. Use one of the following tenant models:
  - **Default Tenant:** If you plan to use the default tenant, `opsa_default`, use `opsatenantadmin` as the tenant admin user and `opsatenantadmin` as the default tenant admin when running the commands in this chapter.
  - **Use your own Tenant:** If you plan to configure a new tenant or use an existing tenant (other than the Default Tenant), see ["Manage Users and Tenants" on page 219](#). If you use this option, you will need to use the tenant admin user and password you created when running the commands in this section.
2. For the Custom CSV Collection, your data must be available in CSV format. If your data is not available in CSV format, you must find a way to convert the data, or the Custom CSV Collection will not work for you.
3. Choose the `<filename>.csv` file you want to load into the Operations Bridge Analytics database. For Operations Bridge Analytics, consider that most `<filename>.csv` files for a CSV collection will have a CSV file with a header and at least two rows of data. For this example, assuming this sample file name is `your_file.csv`, copy the `your_file.csv` file to the `/tmp` directory.

For Operations Bridge Analytics, consider that most `<filename>.csv` files for a CSV collection will have a CSV file with a header and at least two rows of data. For example, the header could include three columns: two with data and one with the time and date.

**Note:** The `your_file.csv` sample file contains a good sample of data. OBA uses this sample data to determine the data types and meta data to place in the `<your_template_name>.xml` sample file used in these instructions.

Do not include any of the values from the following table in the header, as Vertica does not permit these values to be used as header names

**Reserved Words for Vertica (do not use these values in the header name)**

Index Letter	Value
A	ALL, ANALYSE, ANALYZE, AND, ANY, ARRAY, AS, ASC
B	BINARY, BOTH

**Reserved Words for Vertica (do not use these values in the header name), continued**

<b>Index Letter</b>	<b>Value</b>
C	CASE, CAST, CHECK, COLUMN, CONSTRAINT, CORRELATION, CREATE, CURRENT_DATABASE, CURRENT_DATE, CURRENT_SCHEMA, CURRENT_TIME, CURRENT_TIMESTAMP, CURRENT_USER
D	DEFAULT, DEFERRABLE, DESC, DISTINCT, DO
E	ELSE, ENCODED, END, EXCEPT
F	FALSE, FOR, FOREIGN, FROM
G	GRANT, GROUP, GROUPED
H	HAVING
I	IN, INITIALLY, INTERSECT, INTERVAL, INTERVALYM, INTO
J	JOIN
K	KSAFE
L	LEADING, LIMIT, LOCALTIME, LOCALTIMESTAMP
M	MATCH
N	NEW, NOT, NULL, NULLSEQUAL
O	OFF, OFFSET, OLD, ON, ONLY, OR, ORDER
P	PINNED, PLACING, PRIMARY, PROJECTION
R	REFERENCES
S	SCHEMA, SEGMENTED, SELECT, SESSION_USER, SOME, SYSDATE
T	TABLE, THEN, TIMESERIES, TO, TRAILING, TRUE
U	UNBOUNDED, UNION, UNIQUE, UNSEGMENTED, USER, USING
W	WHEN, WHERE, WINDOW, WITH, WITHIN

Choose the following parameter values to use when running the `opsa-csv-template-gen.sh` script:

4.
  - name: Choose a name that accurately describes the data you plan to collect. For example, you might choose the name `mycsv` for the source.
  - domain: Choose a domain that accurately describes a domain in which the data you plan to



collect resides. For example, you might choose the domain `birds`, to support the example in this section.

- **group:** Choose a group that accurately describes the group for which you plan to collect data. For example, you might choose the domain `eagle`, to support the example in this section.

See the `opsa-csv-template-gen.sh` reference page (or the Linux man page) for more information.

5. Choose the following parameter values you plan to use when running the `opsa-collection-config.sh` script:

- **source:** For the custom CSV collections, always use `custom` for the source.
- **domain:** Use the domain that you selected in the previous step.
- **group:** Use the group that you selected in the previous step.

See the `opsa-collection-config.sh` reference page (or the Linux man page) for more information.

## Configuration Steps

After you complete the steps in this section, the Custom CSV Collection reads data from the CSV files within 60 seconds of the file being placed in the source directory.

For several examples of data you might choose to collect using a Custom CSV collection, see the *Creating a Content Pack for Operations Analytics* White Paper at [HPE Live Network](#).

**Note:** Do the following to locate the *Creating a Content Pack for Operations Analytics* White Paper:

1. Select **Products**.
2. Navigate to the **Operations Intelligence (OpsA)** product, then click **Operations Intelligence**.
3. Click **Resources**, then locate the *Creating a Content Pack for Operations Analytics* White Paper.

1. Do the following from the Operations Analytics Server
  - a. Run the following command to create a template for this new collection based on the sample data in the `your_file.csv` file:
 

```
$OPSA_HOME/bin/opsa-csv-template-gen.sh -inputfile /tmp/your_file.csv -name mycsv -domain birds -group eagle -sourcedir /opt/HP/opsa/data/<mydata> -datecolumn Time -dateformat MM/dd/yyyy
```

```
hh:mm:ss -timezone GMT+0 -filepattern '*.csv' -grouptype metrics -
key String, Usage in MHz
```

See the *opsa-csv-template-gen.sh* reference page (or the Linux man page) for more information.

**Note:** To specify a time zone that supports Daylight Savings Time, use the desired daylight savings time value you need as the `timezone` attribute. See ["Daylight Savings Time Codes" on page 199](#) for a list of valid timezone attributes.

**Note:** You must define at least one property as a key column using the `-key` option. Do not specify a timestamp or metric as a key column with the `-key` option.

After this command completes, it creates the `<your_template_name>.xml` file and shows the path to this file. The `<your_template_name>.xml` file is a collection template created from the `your_file.csv` file. Look for a message similar to the following:

```
Generated the Custom CSV collection template
/opt/HP/opsa/conf/collection/server/config.templates/custom/1.0/bi
rds/eagle/mycsv.xml
```

- b. Create the following directory on the Operations Analytics Collector host:
 

```
/opt/HP/opsa/data/<mydata>
```
- c. Run the following command from the Operations Analytics Collector host to set the correct file ownership:
 

```
chown opsa /opt/HP/opsa/data/<mydata>
```

The purpose of the `-datecolumn`, `-dateformat`, and `-timezone` options are to identify one column from the `your_file.csv` file as the `timestamp` column for the database table. This column selection is mandatory for Operations Bridge Analytics collections using metric tables. These options are provided to help you, as the Operations Bridge Analytics administrator, identify the correct column.

**Note:** When creating a custom CSV template, do not use a column named `timestamp_utc`, as doing so causes an error when you attempt to publish the collection. If you already registered a collection, see ["Removing a Collection Registration for a Tenant" on page 236](#) for instructions about removing the registration for this collection.

**Note:** As an example, suppose you plan to use `your_file.csv` as your CSV file, and that

it contains the following information:

- a. Using this information in an example, you would use the following command to create your custom CSV template:

```
$OPSA_HOME/bin/opsa-csv-template-gen.sh -inputfile /tmp/your_
file.csv -name mycsv -domain birds -group eagle -sourcedir
/opt/HP/opsa/data/mydata -datecolumn Time -dateformat
MM/dd/yyyy hh:mm:ss -timezone GMT-7 -filepattern *.csv -
grouptype metrics -key String
```

After this command completes, look for a message similar to the following:

```
Generated the Custom CSV collection template
/opt/HP/opsa/conf/collection/server/config.templates/custom/1.0
/birds
/eagle/mycsv.xml
```

- b. Create the following directory on the Operations Analytics Collector host:
- ```
/opt/HP/opsa/data/mydata
```
- c. Run the following command from the Operations Analytics Collector host: to set the correct file ownership:
- ```
chown opsa /opt/HP/opsa/data/mydata
```

**Note:** As an example, suppose you plan to use `your_file.csv` as your CSV file, and that it contains the following information:

```
Time,Value1,String1
02/23/2014 23:42:00,6.543,eagle
02/23/2014 23:52:00,7.543,eagle
02/23/2014 23:62:00,8.543,eagle
```

Use the following pattern letters when configuring the date format to use when parsing date strings:

Letter	Date or Time Component	Presentation	Examples
G	Era designator	Text	AD
Y	Year	Year	1996; 96
M	Month in Year	Month	July; Jul; 07

Letter	Date or Time Component	Presentation	Examples
w	Week in Year	Number	27
W	Week in month	Number	2
D	Day in year	Number	189
d	Day in month	Number	10
F	Day of week in month	Number	2
E	Day in week	Text	Tuesday; Tue
a	Am/Pm marker	Text	PM
H	Hour in day (0-23)	Number	0
k	Hour in day (1-24)	Number	24
K	Hour in am/pm (0-11)	Number	0
h	Hour in am/pm (1-12)	Number	12
m	Minute in hour	Number	30
s	Second in minute	Number	55
S	Millisecond	Number	978
z	Time zone	General time zone	Pacific Standard Time; PST; GMT-08:00
Z	Time zone	RFC 822 time zone	-0800

The following examples show how to interpret date and time patterns in the U.S. locale. The given date and time are 2001-07-04 12:08:56 local time in the U.S. Pacific Time time zone.

Date and Time Pattern	Result
"yyyy.MM.dd G 'at' HH:mm:ss z"	2001.07.04 AD at 12:08:56 PDT
"EEE, MMM d, 'yy"	Wed, Jul 4, '01
"h:mm a"	12:08 PM
"hh 'o'clock' a, zzzz"	12 o'clock PM, Pacific Daylight Time

Date and Time Pattern	Result
"K:mm a, z"	0:08 PM, PDT
"yyyyy.MMMMM.dd GGG hh:mm aaa"	02001.July.04 AD 12:08 PM
"EEE, d MMM yyyy HH:mm:ss Z"	Wed, 4 Jul 2001 12:08:56 -0700
"yyMMddHHmmssZ"	010704120856-0700
"yyyy-MM-dd'T'HH:mm:ss.SSSZ"	2001-07-04T12:08:56.235-0700
"MM/dd/yyyy hh:mm:ss"	10/04/2001 12:08:56
To use epoch time, substitute <code>-dateformat s</code> for the <code>-dateformat MM/dd/yyyy hh:mm:ss</code> option as shown in following example: <code>-dateformat s 1002197336</code> Look at the resulting epoch time shown in the next column:	1002197336 (the epoch equivalent of 10/04/2001 12:08:56)

- You must have registered an Operations Bridge Analytics for the Custom CSV collections you plan to configure.

To check the registration status of your Operations Analytics Collector host, do the following:

- Run the following command: `$OPSA_HOME/bin/opsa-collection-config.sh -list -collectorhosts -allversions -username opsatenantadmin`
- Review the list of registered Operations Analytics Collector hosts. If the Operations Analytics Collector host you plan to register is not on the list, you must register it using the instructions in this section.

See ["Registering Operations Bridge Analytics Collector Hosts"](#) for more information.

- Using this example as a guideline, review the collection properties in the `/opt/HP/opsa/conf/collection/server/config.templates/custom/1.0/birds/eagle/mycsv.xml` file:

- Change the property type (`type="attribute"` or `type="metric"`).

**Note:** A collection property can be either an attribute (a descriptor for an entity, such as `host_name`) or a metric (typically a measurement), such as `CPU utilization`.

- Review the attributes and decide which of them are key attributes. Set up two three key attributes by setting `key="yes"` for the desired key attribute.

**Note:** You can use keys to uniquely identify an entity instance so users can narrow a search within a single collection or match metrics for one entity (a collection row) to the

same metric or a related entity across collections.

**Note:** When using PQL and the `withkey` command, **you can use no more than three key column values for a single query**. See *About the Phrase Query Language* in the *Operations Bridge Analytics Help* for more information.

c. Save your work.

**Optional Step:** You might have a need to transform data before it is stored in the Operations Bridge Analytics database. You can do this by editing the `<your_template_name>.xml` file and adding transform methods.

4. Operations Bridge Analytics provides the following methods for transforming data:

- o `add(x)`
- o `subtract(x)`
- o `multiply(x)`
- o `divide(x)`
- o `replace(x)`  
where `x` is a float data type.
- o `concat(str)`
- o `replace(str)`
- o `replace with(currentStr, newStr)`  
where `Str` represents string for a string data type

For example, consider the following column description:

```
<column name="CPU Utilization" position="9" datatype="float"
label="CPU Utilization" columnname="cpu_util" length="0" key="no"
type="metric" tags="utilization,performance,primary" mapsto=""
unit="%" value="" />
```

In this example, you want the column description to read as follows:

```
<column name="CPU Utilization" position="9" datatype="float"
label="CPU Utilization" columnname="cpu_util" length="0" key="no"
type="metric" tags="utilization,performance,primary" mapsto=""
unit="%" value="multiply(100)" />
```

To add the transform, edit the `<your_template_name>.xml` file, add `value-multiply(100)` to the column for CPU Utilization, then save your work.

**Valid values for unit**

You can use any of the following entries for the unit field:

```
"%"  
"bytes"  
"mbps"  
"kbps"  
"gbps"  
"kb"  
"mb"  
"gb"  
"hz"  
"khz"  
"mhz"  
"ghz"  
"BIT"  
"PB"  
"EB"  
"W"  
"V"  
"A"  
"secs"  
"millisecs"  
"ms"  
"pages/sec"  
"per second"  
"switches/sec"  
"bytes/sec"  
"KB/sec"  
"interrupts/sec"  
"pages/sec"  
"errors/sec"  
"reads/sec"  
"bps"  
"per hour"  
"per min"
```

5. For this *birds* example, run the following command from the Operations Analytics Server to create the collector configuration:

```
$OPSA_HOME/bin/opsa-collection-config.sh -create -collectorhost
```

```
<fully-qualified domain name of the collector host> -source custom -
domain birds -group eagle -username opsatenantadmin
```

**Note:** The `opsa-collection-config.sh` script prompts you for the Tenant Admin password for the username you use in the `opsa-collection-config.sh` command.

**Note:** When you run the command in this step, always use the `-source custom` argument when creating a custom CSV collector configuration.

To create and publish collections supported by Operations Bridge Analytics, you normally provide source, domain, and group options to the `opsa-collection-config.sh` script. The definition for each of these options is as follows:

- **source:** Specifies the name of the source collector.
- **domain:** Specifies the domain name to which the collected data belongs.
- **group:** Specifies the group name to which the collected data belongs.

**Note:** The `opsa-collection-config.sh` script uses the values of source, domain, and group to select the right collection template and create the desired collection configuration.

To see the predefined values for these options, see the *opsa-collection-config.sh* reference page (or the Linux man page).

**Note:** Although the *opsa-collection-config.sh* reference page provides you with the predefined values for these options, use the `custom` source option along with options that differ from the predefined values for the `domain` and `group` options when creating Custom CSV Collections.

6. Run the following command from the Operations Analytics Server to publish this collection configuration to the Operations Analytics Collector host:

```
$OPSA_HOME/bin/opsa-collection-config.sh -publish -collectorhost
<fully-qualified domain name of the collector host> -username
opsatenantadmin
```

The `-publish` option uploads the collection configuration you created to the Operations Analytics Collector host. To verify that the collection configuration published successfully, look for a message stating the following:

- The publish was successful.
- A table was successfully created.



- o The collection was restarted.

7. Run the following command from the Operations Analytics Server to validate the collection configuration you created:

```
$OPSA_HOME/bin/opsa-collection-config.sh -list -allversions -
collectorhosts -username opsatenantadmin
```

To verify a successful collection configuration creation, look for a message showing the expected collector host name, tenant name, and tenant version. The message should also include the source template details such as its version, domain, and group.

8. You must copy the data files (or set up some way of automatically copying the data files) from the data source to the Operations Analytics Collector host and set the correct file ownership. Do the following for the collection you plan to configure:

- a. Copy the files to the following directory on the Operations Analytics Collector host: `$OPSA_HOME/data/mydata` (or to the directory that relates to the custom collection you created).
- b. Run the following command from the Operations Analytics Collector host to set the correct file ownership:

```
chown opsa $OPSA_HOME/data/mydata
```

After completing this step, you should see data in the `$OPSA_HOME/data/mydata_processed` folder within a few minutes.

**Note:** After Operations Bridge Analytics processes data in the `yourfile.csv` file, it removes the `yourfile.csv` file from the `$OPSA_HOME/data/mydata` directory and creates the `$OPSA_HOME/data/mydata_processed` folder and its contents.

9. From the Operations Bridge Analytics console, view the **OpsA Meta Info** dashboard. Look for the **property group uid** for the collection you created and published.

**Note:** The property group uid consists of a combination of the `source`, `domain`, and `group` parameters you used to create the collection. For this example, you would have used a name of `custom`, a domain of `birds`, and a group of `eagle` when creating the collection. The resulting property group uid would be `custom_birds_eagle`.

- a. Type the property group uid (`custom_birds_eagle`) for this collection in the **Collection Columns > property group uid** Filter.
- b. After typing property group uid (`custom_birds_eagle`) for this collection in the **Collection Columns > property group uid** Filter, you should see information in the resulting table.

10. Create dashboards and query panes for the data you are now collecting. Follow the instructions shown in the *Dashboards and Query Panes* section of the *Operations Bridge Analytics Help* for information about creating dashboards and query panes.
11. Create AQL functions for the data you are now collecting. See the instructions shown in the *Define Analytic Query Language (AQL) Functions* section of the *Operations Bridge Analytics Help* for information about creating AQL functions.
12. If you want to add tags to a Custom CSV Collection, use the `opsa-tag-manager.sh` command. See ["Using Tags for Source Types" on page 136](#) and the `opsa-tag-manager.sh` reference page (or the Linux man page) for more information.

## Troubleshooting the Custom CSV Collection

If you suspect problems with your Custom CSV Collection, do the following:

1. To check the registration status of your Operations Analytics Collector host, do the following:
  - a. Run the following command: `$OPSA_HOME/bin/opsa-collection-config.sh -list -collectorhosts -allversions -username opsatenantadmin`
  - b. Review the list of registered Operations Analytics Collector hosts. If the Operations Analytics Collector host you plan to register is not on the list, you must register it using the instructions in this section.
2. View the collected data to make sure it is what you expect. If it is not, continue checking the remaining items in this list.
3. Review the content of the `your_file.csv` file and the associated `<your_template_name>.xml` file to make sure it is configured to collect the right data.
4. Use a CSV file for the Custom CSV Collection. Check the `<filename>.csv` file you loaded into the Operations Bridge Analytics database. For Operations Bridge Analytics, consider that most `<filename>.csv` files for a CSV collection will have a CSV file with a header and at least two rows of data.
5. Check the quality of the data you are collecting. If it is not what you expected, review the content of the `<filename>.csv` file you loaded into the Operations Bridge Analytics database, as it might not be collecting the right data for you.

## Removing the Registration and Data for a Custom CSV Collection

To remove the registration for a Custom CSV Collection, do the following:

1. Run the following command:

```
$OPSA_HOME/bin/opsa-collection-config.sh -unregister -source custom -group group -domain domain -collectorhost <fully-qualified domain name of collector host>
```

**Note:** If you remove the registration for this CSV collection, and do not complete the remaining steps, remember the following important information:

- The collected data remains intact and is not removed.
- If you decide to register this collection again, you must not reuse the `your_file.csv` file, (or whatever csv file name you used to create the collection template), as you run the risk of duplicating the original collection data.
- It is a best practice to complete all of these removal steps to avoid collecting duplicate data.

2. After unregistering this Custom CSV Collection, remove the collection from the database using the following command:

```
$OPSA_HOME/bin/opsa-collection-config.sh -purgecollection -source custom -domain domain -group group -collectorhost <fully-qualified domain name of collector host> -username opsatenantadmin
```

See the `opsa-collection-config.sh` reference page (or the Linux man page) for more information.

**Note:** The command in this step also removes all Custom CSV Collection data for the specified tenant from the Operations Bridge Analytics database.

**Note:** After unregistering a Custom CSV Collection, the data remains intact. This intact data means that you can register a Custom CSV Collection that you removed and resume that Custom CSV Collection.

3. Remove the data. For example, for the NOAA example, you would remove the `$OPSA_HOME/data/noaaCustom_processed` directory.

See the `opsa-collection-config.sh` reference page (or the Linux man page) and ["Removing a Collection Registration for a Tenant" on page 236](#) for more information.

## SiteScope - Command Line Method

After you complete the steps in this section, SiteScope starts sending data to the Custom SiteScope Collection. The Custom SiteScope Collection collects data as it arrives from SiteScope.

**Note:** If you are using SiteScope in an application failover configuration, only configure the Custom SiteScope collection with the primary SiteScope server.

**Note:** Operations Bridge Analytics does not support any SiteScope version that uses a freemium license.

The following table shows the monitor types currently supported by the Custom SiteScope Collection:

**Note:** If a SiteScope monitor type has only unsupported counters configured, Operations Bridge Analytics ignores that monitor type when creating the collection. Operations Bridge Analytics does not support monitor counter names longer than 128 characters. If a supported monitor's counter name is longer than 128 characters, Operations Bridge Analytics ignores that counter.

Operations Bridge Analytics supports the default counters of the supported monitors listed in ["Supported Monitor Types" on the next page](#). If a monitor is configured in SiteScope with custom counters or metrics, such as calculated metrics or custom counters of **Script**, **JMXMonitor**, or **XMLMetrics** monitors, follow the instructions shown in ["SiteScope Monitors and Their Counters" on the next page](#) before creating this collection.

**Supported Monitor Types**

Apache	Memory	URLContent
BACIntegrationConfiguration	MicrosoftWindowsEventLog	URLMonitor
BACIntegrationStatistics	MQStatusMonitor	URLSequenceMonitor
Composite	MSActiveServerPages	VMware
ConnectionStatisticsMonitor	MSIIServer	VMwareHostCPUMonitor
CPU	MSSQLServer	VMwareHostMemoryMonitor
DatabaseCounter	MSWindowsMediaServer	VMwareHostStateMonitor
DHCP	NetworkBandwidthMonitor	VMwareHostStorageMonitor
Directory	Oracle	WebServer
DiskSpace	Ping	WebService
DNS	Port	WebSphere
DynamicDiskSpace	SAPPerformance	WindowsPerformance
File	Script	WindowsResources
FTPMonitor	Service	WindowsServicesState
HealthServerLoadMonitor	SiebelApplicationServer	XMLMetrics
HyperVMonitor	SolarisZones	
JMXMonitor	SQLQuery	
LDAPMonitor	SSLCertificatesStatus	
LogEventHealthMonitor	Sybase	
LogMonitor	UnixResources	

**SiteScope Monitors and Their Counters**

A SiteScope collection consists of several collections, one for each monitor type, when each collection has metrics and attributes corresponding to a monitor's counters. A collection is mapped to a database table while metrics and attributes are stored in this table's columns.

An Operations Bridge Analytics SiteScope collection's configuration framework creates collections with metrics and attributes according to the monitor types and counters configured in the SiteScope server from which Operations Bridge Analytics is collecting data. The created configuration is based on

UOM files obtained from the SiteScope server. These files contain a list of monitors and their counters as they are configured on that SiteScope server.

In addition to the list of monitors and their counters, Operations Bridge Analytics must determine the data type used for each counter. This data type can be either float (for metric data) or string (for attribute data). This information is not available directly from SiteScope and is configured locally on the Operations Analytics Server file system in the `/opt/HP/opsa/conf/collection/sitescope_metadata_patterns/` directory in files named `<monitor name>_datatypes`. These files have predefined configurations suitable for the default counters of common SiteScope monitor types. As mentioned earlier, the list of supported monitor types is shown in ["Supported Monitor Types" on the previous page](#).

Monitor types that have user-defined counters, such as **Script**, **JMXMonitor**, or **XMLMetrics**, usually require that you manually add these custom-counters' names to the corresponding `<monitor name>_datatypes` files before creating the collections. This requirement also applies to any SiteScope monitor if it has **Calculated Metrics** defined in at least one instance of its type.

**Note:** If Operations Bridge Analytics cannot define a data type for a monitor's counter, its values will not be collected. If Operations Bridge Analytics defines a wrong data type for a monitor's counter, Operations Bridge Analytics might omit any data received from that monitor.

### Modifying Data Types Configurations

To prevent a problem with SiteScope data collections due to the above requirements, you can modify the data types configuration. Detailed instructions about modifying the SiteScope metadata configuration files, including the data types configuration files, can be found in the following text file on the Operations Analytics Server's file system: `/opt/HP/opsa/conf/collection/sitescope_metadata_patterns/custom/README_BEFORE_CREATING_PATTERNS.txt`

Each `<monitor name>_datatypes` file contains lines in the following format: regular expression, comma, data type (float or string). Each regular expression is expected to match one or more counter names as they appear in the UOM file. Specific regular expressions should appear before more general expressions.

For example, to define all counters starting with `size` as data type float and all the other counters as data type string, use the following:

```
size.*,float
.*,string
```

It is also possible to define the data type for exact counter names through escaping regular expressions by surrounding the name with `"\\Q` and `\\E"`.

For example, for a counter named `%cpu` that should be of data type float use the following:

```
"\Q%cpu\E",float
```

### Modifying Units and Tags

Similar to configuring data types, you can optionally configure units and tags for counters of a monitor by modifying the `<monitor name>_units` and `<monitor name>_tags` files respectively.

The tags file can contain a comma separated list of tags after a regular expression. The line that begins with `global_tags` defines collection-level tags. See ["Using Tags for Source Types" on page 136](#) for more information.

**Note:** The units you can specify in the `<monitor name>_units` files can only be from the following list:

%, mbps, kbps, gbps, kb, mb, gb, hz, khz, mhz, ghz, bytes, BIT, PB, EB, W, V, A, secs, millisecs, ms, pages/sec, per second, switches/sec, bytes/sec, KB/sec, interrupts/sec, packets/sec, pages/sec, errors/sec, reads/sec, bps, per hour, per min, Celsius.

After modifying the configuration files within the `/opt/HP/opsa/conf/collection/sitescope_metadata_patterns/` directory, you can run the `/opt/HP/opsa/scripts/opsa-sis-regex-matches.sh <path to uom file name>` command to see how Operations Bridge Analytics processes the counters from the UOM file.

If you plan to connect more than one SiteScope server to Operations Bridge Analytics, and you do not plan to connect them all at once (for example, if you use the Source Type Manager instead of a command line collection configuration), you must do the following:

1. Export the UOM files from all of these SiteScope servers to a single common folder on the Operations Analytics Server (rename the files if needed).
2. Supply the path to the folder to which you exported the UOM files using the `-uomfiles` option (using a command line) or in the UOM folder path (using the Source Type Manager) when adding each SiteScope collection.

## Detailed Configuration Steps

Configuring a SiteScope Collection by creating custom collector templates is a two-step process:

1. ["Generating and Configuring Templates \(Custom SiteScope Collection\)" on the next page](#)
2. Continue with ["Configuring SiteScope for Integrating Data with Operations Bridge Analytics \(Automated Method\)" on page 115](#)

If you prefer using a manual method to configure SiteScope for Integrating data with Operations Bridge Analytics see ["Adding a New Source Type — Command Line Method" on page 93](#).

## Generating and Configuring Templates (Custom SiteScope Collection)

To configure a Custom SiteScope Collection, you must use SiteScope Unit Of Measurement (UOM) files as an input for the `opsa-sis-collector-auto-conf.sh` script.

To use metrics that are not supported by the default UOM file complete the steps shown below.

1. Complete these substeps for each SiteScope server from which you plan to collect data.
  - a. Using the SiteScope UI, navigate to the **Diagnostics Integration Preferences** page (**Using SiteScope > Preferences > Integration Preferences > Diagnostics Integration Preferences**)
  - b. Click **Generate UOM XML**. Doing so creates the UOM XML file on the HPE SiteScope server in the following location: `%SITESCOPE_HOME%\conf\integration\data_integration_uom.xml`.
2. Create an empty directory on the Operations Analytics Server; then copy the generated UOM files to this newly created directory.

**Note:** Rename the UOM files before you copy them to the newly created directory, as many of the generated UOM files might have the same name (`data_integration_uom.xml`).

**Note:** When creating SiteScope collection templates, only place valid UOM files in the directory. Do not place any other files in that directory.

3. Optional: You can use the `opsa-sis-collector-auto-conf` script to create complete collection templates for most of the monitor types shown in ["Adding a New Source Type — Command Line Method" on page 93](#). However, there are a few created templates you might need to customize after you create them. For example, you might need to customize the template contents of the following SiteScope monitor types, as you should vary the template content to match the data you configure the monitor to collect:
  - Script
  - XMLMetrics
  - JMXMonitor



There are two tasks you might need to complete when customizing the creation of a SiteScope collection template for a particular monitor type:

a. **Parsing the counter names to separate out metric names from instance**

**attributes:** Create a regular expression definition in the

`/opt/HP/opsa/conf/collection/sitescope_measure_regex_patterns/custom` directory. See the

`/opt/HP/opsa/conf/collection/sitescope_measure_regex_patterns/custom/README_BEFORE_CREATING_PATTERNS.txt` file for specific instructions about creating regular expressions to parse the counter names for a SiteScope monitor type.

b. **Defining the data type, tags and units for a parsed metric:** Create a regular expression

definition in the `/opt/HP/opsa/conf/collection/sitescope_metadata_patterns/custom` directory. See the

`/opt/HP/opsa/conf/collection/sitescope_measure_regex_patterns/custom/README_BEFORE_CREATING_PATTERNS.txt` file for specific instructions about creating regular expression definitions for assigning data types, tags, and units to metrics for a SiteScope monitor type.

After you finish these steps, use the `-uomfiles` option in the next set of steps to define a UOM folder path containing UOM files you manually extracted:

1. If you are using Operations Bridge Analytics for SiteScope version 11.22IP or newer, skip this step (proceed to "[Configuring SiteScope for Integrating Data with Operations Bridge Analytics \(Automated Method\)](#)" on page 115). If you are using an earlier version of SiteScope (earlier than SiteScope version 11.22IP), complete one of the following options:
  - **Option 1:** Use the `opsa-sis-collector-auto-conf.sh` script with the default UOM file. The default UOM file is located at `$OPSA_HOME/conf/collection/sitescope_configuration/uom/data_integration_uom.xml`. Using the default UOM file, proceed to step 2.
 

**Note:** Operations Bridge Analytics includes a default UOM file, `$OPSA_HOME/conf/collection/sitescope_configuration/uom/data_integration_uom.xml`, which supports many of the metrics supported by Operations Bridge Analytics. Use the `-uomfiles` option to optionally define a UOM folder path containing UOM files you manually extracted.
  - **Option 2:** To use metrics that are not supported by the default UOM file complete the steps shown below.

- i. Complete these substeps for each SiteScope server from which you plan to collect data.
  - A. Using the SiteScope UI, navigate to the **Diagnostics Integration Preferences** page (**Using SiteScope > Preferences > Integration Preferences > Diagnostics Integration Preferences**)
  - B. Click **Generate UOM XML**. Doing so creates the UOM XML file on the HPE SiteScope server in the following location: %SITESCOPE\_HOME%\conf\integration\data\_integration\_uom.xml.

- ii. Create an empty directory on the Operations Analytics Server; then copy the generated UOM files to this newly created directory.

**Note:** Rename the UOM files before you copy them to the newly created directory, as many of the generated UOM files might have the same name (data\_integration\_uom.xml).

**Note:** When creating SiteScope collection templates, only place valid UOM files in the directory. Do not place any other files in that directory.

- iii. Optional: You can use the `opsa-sis-collector-auto-conf` script to create complete collection templates for most of the monitor types shown in ["Adding a New Source Type — Command Line Method" on page 93](#). However, there are a few created templates you might need to customize after you create them. For example, you might need to customize the template contents of the following SiteScope monitor types, as you should vary the template content to match the data you configure the monitor to collect:

- Script
- XMLMetrics
- JMXMonitor

There are two tasks you might need to complete when customizing the creation of a SiteScope collection template for a particular monitor type:

- A. **Parsing the counter names to separate out metric names from instance attributes:** Create a regular expression definition in the `/opt/HP/opsa/conf/collection/sitescope_measure_regex_patterns/custom` directory. See the `/opt/HP/opsa/conf/collection/sitescope_measure_regex_patterns/custom/README_BEFORE_CREATING_PATTERNS.txt` file for specific instructions about creating regular expressions to parse the counter names

for a SiteScope monitor type.

- B. Defining the data type, tags and units for a parsed metric:** Create a regular expression definition in the `/opt/HP/opsa/conf/collection/sitescope_metadata_patterns/custom` directory. See the `/opt/HP/opsa/conf/collection/sitescope_measure_regex_patterns/custom/README_BEFORE_CREATING_PATTERNS.txt` file for specific instructions about creating regular expression definitions for assigning data types, tags, and units to metrics for a SiteScope monitor type.

After you finish these steps, use the `-uomfiles` option in the next set of steps to define a UOM folder path containing UOM files you manually extracted:

## 2. Configuring SiteScope for Integrating Data with Operations Bridge Analytics (Automated Method)

Complete the following tasks to configure HPE SiteScope to forward data to an Operations Analytics Collector host.

- a. A node list file contains details about the sources from which you plan to collect information. The node list file for the Custom SiteScope Collections must include the information shown in the following table.

**Note:** Each of the following settings could be configured for a specific SiteScope server, such as `server1`. If the SiteScope server value is missing, the default setting is used. For example, if the "`<server1>.port =` " string does not exist in the node list file, Operations Bridge Analytics uses the value of the "`default.port =` " setting for `server1`.

### Node List Fields and Values

Field	Value
<code>server.names</code>	The aliases of the SiteScope server names, delimited by commas. These are the servers from which you plan to collect SiteScope information.
<code>&lt;server&gt;.hostdnsname</code>	IP Address or fully-qualified domain name of the SiteScope servers for which you are configuring collections. If you want to support failover for the SiteScope servers, specify all the SiteScope servers included in the failover configuration.
<code>.port</code>	The port used to connect to the SiteScope server. Set this if a server does not use the <code>default.port</code> value.  The <code>server.port</code> setting could be configured for a specific server, such

**Node List Fields and Values, continued**

Field	Value
	as <code>server1</code> . If the server value is missing, the default setting is used. For example if the " <code>&lt;server1&gt;.port =</code> " string does not exist in the node list file, Operations Bridge Analytics uses the value of the " <code>default.port =</code> " setting for <code>server1</code> .
<code>.username</code>	The default user name used to connect to the SiteScope server. This is typically <code>admin</code> . This field might be set to empty (no value), as it is possible to configure SiteScope not to ask for a username and password to log on.
<code>.initString</code>	<p>The default value of the <code>initString</code> used for SSL communication with the SiteScope server. <b>You can obtain this <code>initString</code> from the SiteScope screen shown below this table.</b></p> <p><b>Note:</b> If you cannot find this <b>SiteScope LWSSO <code>initString</code></b> in the user interface for the version of SiteScope you are using, you can find the string in the SiteScope file system at <code>&lt;SiteScope installation directory&gt;\conf\lwssolwssofmconf.xml</code>.</p>
<code>.use_ssl</code>	<p>Set this field to <code>true</code> to enable SSL communication with the SiteScope server. The default setting is <code>false</code>.</p> <p>If you set this field to <code>true</code>, you must perform the following procedure before continuing with the SiteScope collection configuration:</p> <ol style="list-style-type: none"> <li>i. Copy the root CA certificate from the SiteScope server to the Operations Analytics Server. <ul style="list-style-type: none"> <li><b>Note:</b> Ask the SiteScope Administrator where this certificate is located on the SiteScope server.</li> <li><b>Note:</b> You must use a <code>.crt</code> file as shown in the example in the next step. If you must generate a <code>.crt</code> file from a <code>.cer</code> file, look in <i>Configuring SiteScope to Use SSL</i> in the <i>HPE SiteScope Deployment Guide</i> for an explanation about how to generate the <code>.crt</code> file from the SiteScope server using the <code>.cer</code> file. Look for something like the following: <pre>keytool.exe -importcert -alias &lt;certificate alias&gt; -file c:\SSL\certnew.cer -keystore C:\SiteScope\java\lib\security\cacerts</pre> </li> </ul> </li> <li>ii. After copying the root CA certificate to the Operations Analytics Server, set the CA certificate file for full permissions (<code>rwx rwx rwx</code>).</li> <li>iii. Import the root CA certificate into the SiteScope truststore: in the SiteScope UI, access <b>Preferences &gt; Certificate Management</b></li> </ol>

## Node List Fields and Values, continued

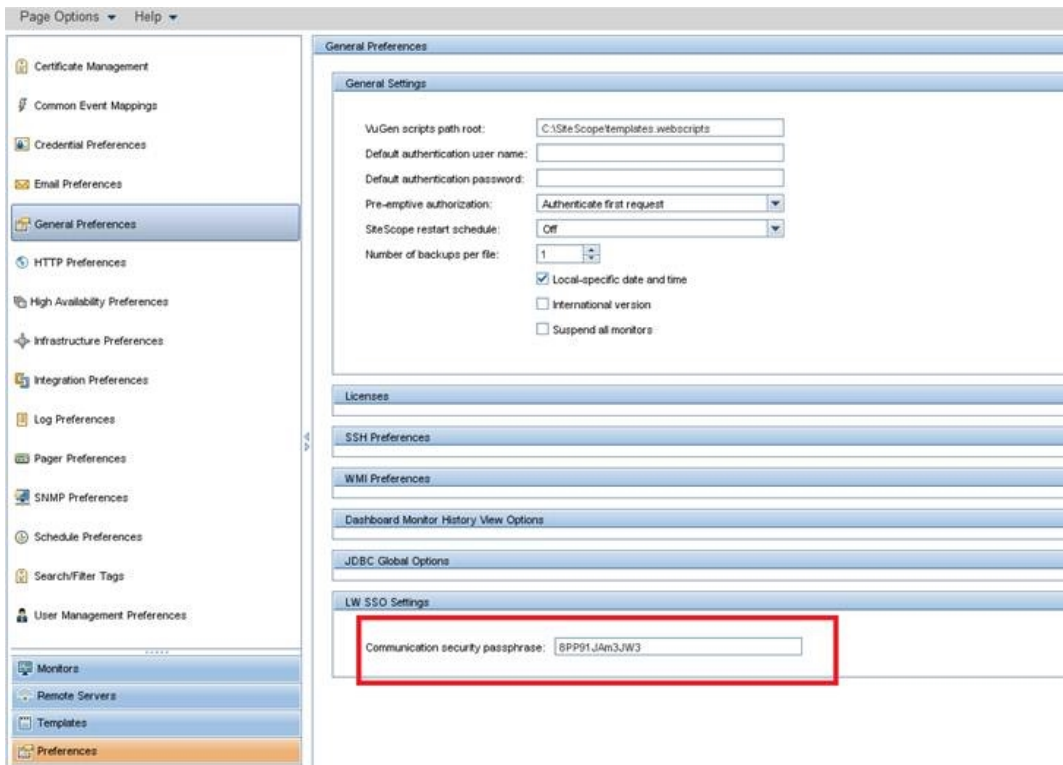
Field	Value
	<p>&gt; <b>New file</b> &gt; <b>Select</b> &gt; <b>Import</b>. If required, you can change the alias.</p> <p>iv. Run the <code>opsa-server-manager.sh</code> script as the root user.</p> <p><b>Note:</b> Running the <code>opsa-server-manager.sh</code> script could result in a message similar to the following:</p> <pre>Run wizard as root or com.hp.opsa.server.admin.ssl.config.OPSCertStoreException: please run this procedure manually with root credentials:</pre> <p><b>If you see this message, there will be no residual effect. The remedy is to complete only one of the following actions:</b></p> <ul style="list-style-type: none"> <li>• Run the <code>opsa-server-manager.sh</code> script as root and complete the steps shown below.</li> <li>• Do not run the <code>opsa-server-manager.sh</code> script. Instead, run the following command manually using root credentials: <pre>sudo keytool -import -trustcacerts -alias CN=HPQ Issuing Certification Authority 2016-1, DC=americas, DC=cpqcorp, DC=net -keystore /opt/HP/opsa/jdk/jre/lib/security/cacerts -file /home/opsa/HPQ Issuing Certification Authority 2016-1.pem -storepass changeit</pre> </li> </ul> <p>A. Log on as the <code>opsaadmin</code> user.</p> <p>B. Choose <b>Option 2</b> to configure SSL.</p> <p>C. Choose <b>Option 4</b> to import the trusted certificate into the OpsA truststore.</p> <p>D. Enter the file name of the certificate you want to import; then press <b>Enter</b>.</p> <p>E. Repeat the prior steps for additional certificate files you want to import.</p> <p>F. Exit the <code>opsa-server-manager.sh</code> script.</p> <p>See the <i>opsa-server-manager.sh</i> reference page (or the Linux manpage) for more information.</p>
.opsa_collector	The fully-qualified domain name or the IP address of the common collector that collects data from the SiteScope servers. Do not use <code>localhost</code> or <code>127.0.0.1</code> .

**Node List Fields and Values, continued**

Field	Value
	<b>Note:</b> This IP address must be accessible from the SiteScope server.

**Finding the initstring in SiteScope**

**Note:** For the integration with Operations Bridge Analytics to work correctly, you must enter the communication security passphrase (LWSSO initString) as shown in the example in following graphic. If this field is empty, see the SiteScope documentation for the instructions to set a value in this field.



View the sample node list file shown below:

```
server.names=sis01313, sis01388
#properties for sis01313 servers
sis01313.hostdnsname=sis1.somedomain.com
#properties for sis01388 server
sis01388.hostdnsname=sis2.somedomain.com
sis01388.port=18080
#common properties for sis servers
```

```
default.port=8080
default.username=admin
default.initString=8PP91JAm3JW3
default.use_ssl=false
default.opsa_collector=opsac
```

To edit the node list file, do the following from the Operations Analytics Server:

Edit the `$OPSA_HOME/conf/collection/sitescope_configuration/sample_SiteScope_node.properties` file, adding the appropriate information from the examples shown above, then save your work.

**Note:** The sample file mentioned in this step does not contain a password property. When using the `opsa-collection-config.sh` script (in a later step) to encrypt the password, this script prompts you for the password, encrypts it, and inserts it into the sample file.

- b. Run the following command from the Operations Analytics Server to encrypt the password:
- ```
$OPSA_HOME/bin/opsa-collection-config.sh -encrypt $OPSA_HOME/conf/collection/sitescope_configuration/sample_SiteScope_node.properties
```

**Note:** If the SiteScope password is empty, edit the nodelist file and remove the value from the appropriate `<server>.password` setting. For example, you might change the value to `sis01.password =`

**Note:** You will be prompted to enter the password after running this command.

- c. Run the following command from the Operations Analytics Server to create the collector configuration.
- ```
$OPSA_HOME/bin/opsa-sis-collector-auto-conf.sh -nodelist $OPSA_HOME/conf/collection/sitescope_configuration/sample_SiteScope_node.properties -username opsatenantadmin -password <password>[-ignoretag] [-forceupdate] [-forcedelete] [-skipcontent] [-uomfiles] <path to directory containing UOM files>]
```

**Note:** When running the `opsa-sis-collector-auto-conf.sh` script, you might see an error similar to the following :

```
No implementation defined for
org.apache.commons.logging.LogFactory.
```

If this error occurs, run the command in this step from the `/opt/HP/opsa/bin/support/` directory.

Use the following option definitions for this command:

- The `-nodelist` option points to the node list file created earlier.
- `opsatenantadmin` is the default predefined Tenant Admin user for the predefined `opsa_default` tenant. If you are not using the default tenant, use the Tenant Admin user and password for the tenant you defined for your collections.
- `opsatenantadmin` is the password for the default predefined Tenant Admin user (for the predefined `opsa_default` tenant). If you are not using the default tenant, use the Tenant Admin user and password for the tenant you defined for your collections.
- Use the `-ignoretag` option to ignore the step of tagging the monitors within SiteScope. The `opsa-sis-collector-auto-conf.sh` script creates a tag named `opsa_<tenant-name>` and associates it with the root SiteScope group, which means that all monitors will be recursively tagged automatically and dynamically. In some cases, you might want to configure only a subset of the monitors. In those situations, use the `ignoretag` option to manually handle the tagging.
- Use the `-forceupdate` option if you did not make any changes since the last time you ran the `opsa-sis-collector-auto-conf.sh` script, and still want to **force** the script to make changes in already saved SiteScope profiles. If you use the `-forceupdate` option when running the `opsa-sis-collector-auto-conf.sh` script, it deletes the old integration configuration and replaces it with the new configuration. For example, if you made some manual changes on the SiteScope profile side and want to return to the original configuration, use the `-forceupdate` option.
- Use the `-forcedelete` option if you want to remove SiteScope configurations made since you last ran the `$OPSA_HOME/bin/opsa-sis-collector-auto-conf.sh` script. To do this, remove the corresponding alias from the `server.names=` setting in the `nodelist` file, then run the `$OPSA_HOME/bin/opsa-sis-collector-auto-conf.sh` script using the `-forcedelete` option.
- As mentioned earlier, Operations Bridge Analytics includes a default UOM file, `$OPSA_HOME/conf/collection/sitescope_configuration/uom/data_integration_uom.xml`, which supports many of the metrics supported by Operations Bridge Analytics. Use the `-uomfiles` option to optionally define a UOM folder path containing UOM files you manually extracted.

After completing the configuration steps in this section, SiteScope begins forwarding data to the Operations Analytics Collector host based on the configuration choices you made.



## Configuring SiteScope for Integrating Data with Operations Bridge Analytics(Manual Method)

Complete the steps using this option if you prefer using a manual method to configure SiteScope for Integrating data with Operations Bridge Analytics.

The following tasks, showing steps and diagrams, explain an example of configuring HPE SiteScope to forward data to an Operations Analytics Collector host.

**Note:** You must complete the step in ["Adding a New Source Type — Command Line Method"](#) before completing the configuration steps in this section.

To configure SiteScope to send data to Operations Bridge Analytics, you must complete the following tasks:

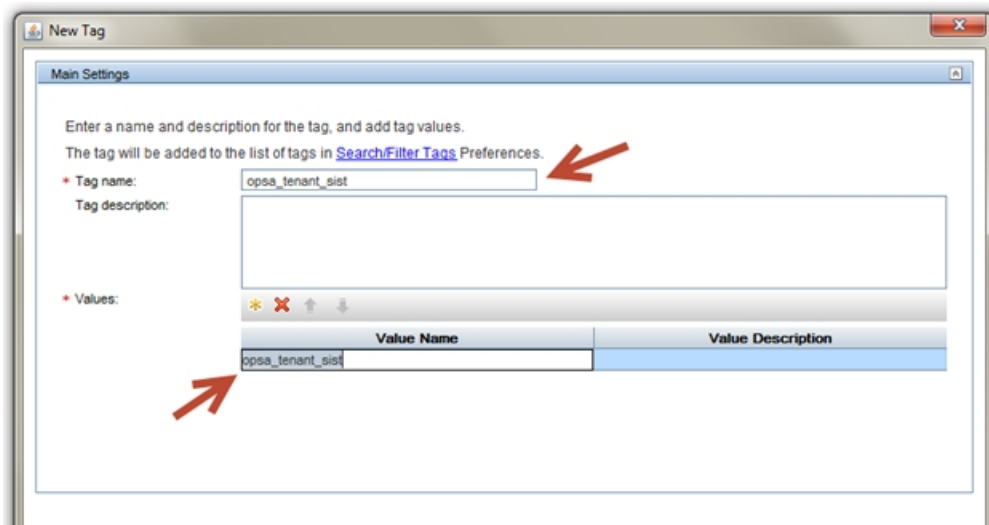
- ["Task 1: Creating a SiteScope Tag" below](#)
- ["Task 2: Using the New SiteScope Tag to Mark the Monitor or Monitor Groups" on the next page](#)
- ["Task 3: Creating a New Data Integration Preference" on page 123](#)

### **Task 1: Creating a SiteScope Tag**

To create a SiteScope tag, do the following:

1. Log on to SiteScope as an **Admin** user.
2. Navigate to **Preferences > Search/Filter Tags**
3. Click the **New Tag icon** (the gold-colored star) to create a new tag.

The following shows the window that should open:



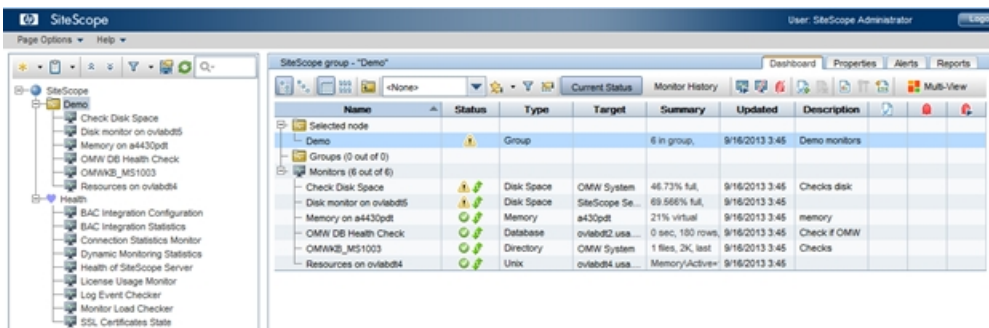
For the **Tag Name** value, enter the name of your choice. For example, you might enter `opsa_tenant_sist`. Click the gold-colored star in the **Values** area, then enter a **Value Name** using the identical string that you used for the **Tag Name** value (`opsa_tenant_sist` for this example).

4. Click **OK** to save the tag definition.

## Task 2: Using the New SiteScope Tag to Mark the Monitor or Monitor Groups

To use the tag you just created to mark the Monitor Groups, individual Monitors, or both, from which you want metrics sent to Operations Bridge Analytics, do the following:

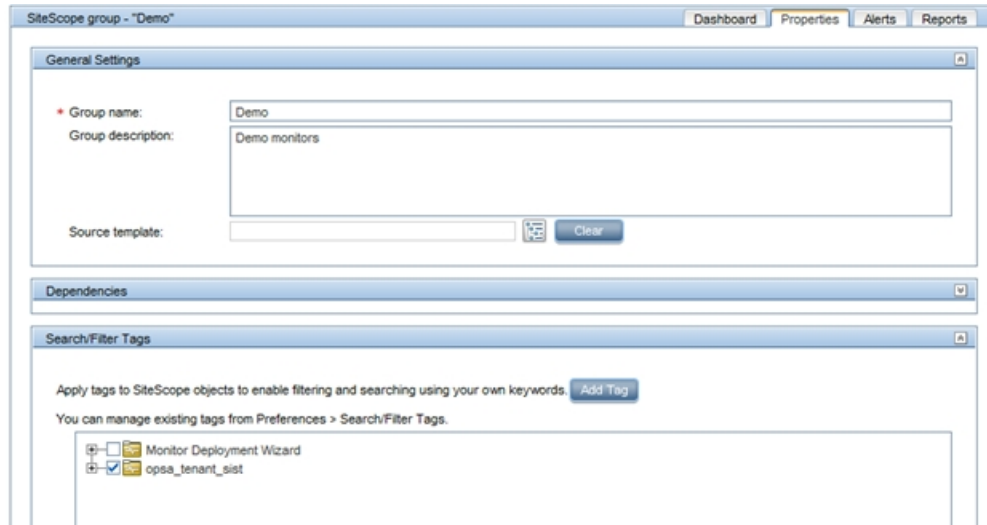
1. Navigate to the Monitors panel in SiteScope. This is normally the main screen you see when you first log on to SiteScope. The following shows an example system:



2. For each Monitor Group or individual Monitor from which you want metrics sent to Operations Bridge Analytics, mark the Group or Monitor with the tag you created in "[Task 1: Creating a SiteScope Tag](#)" on the previous page. For example, to mark the entire **Demo** Monitor Group (as in

sending metrics from all of the monitors in the group), follow these steps:

- a. Select the **Monitor Group** name in the hierarchy list on the left of the screen.
- b. Click the **Properties** tab. For a Monitor Group, the following window opens:



- c. In the **Search/Filter Tags** configuration panel, select the checkbox for the tag you created in ["Task 1: Creating a SiteScope Tag" on page 121](#).
- d. Click **Save** to save your changes to the Monitor Group configuration.

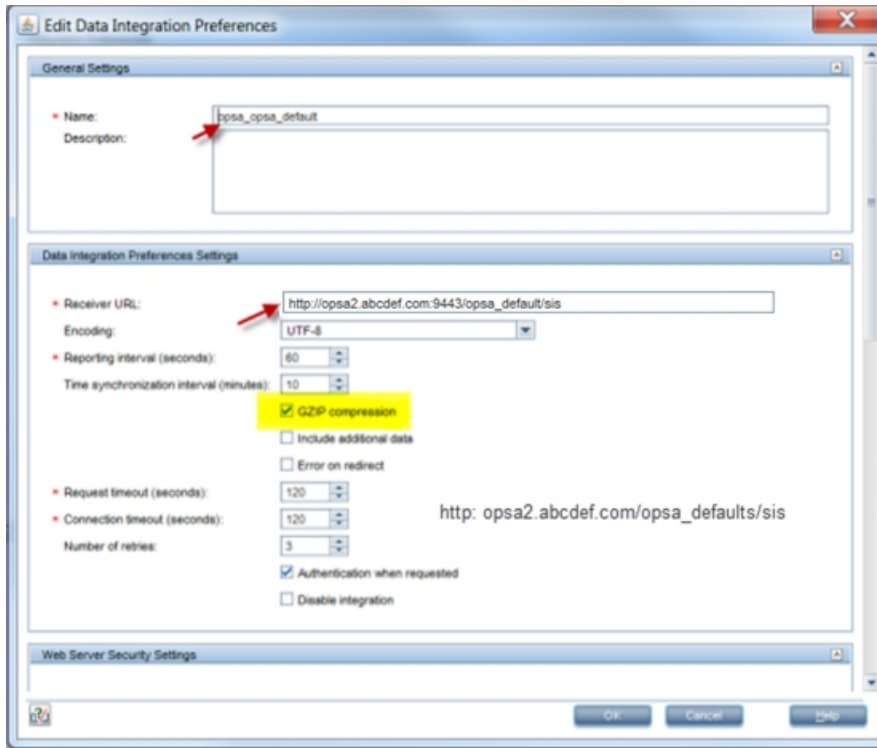
**Note:** If you do not want to send metrics **from all of the monitors within a group**, you must mark each desired monitor individually. The steps are the same as:

- i. Select the **Monitor Group** name in the hierarchy list on the left of the screen.
- ii. Click the **Properties** tab and a window opens.
- iii. Navigate to the **Search/Filter Tags** panel.
- iv. Select the checkbox for the tag you created in ["Task 1: Creating a SiteScope Tag" on page 121](#).
- v. Click **Save** to save your changes to the Monitor Group configuration.

### Task 3: Creating a New *Data Integration* Preference

In this final task, configure a new `Data Integration` preference that tells SiteScope where to send the marked data metrics:

1. From SiteScope, Navigate to **Preferences > Integration Preferences**.
2. Click the gold-colored star (the New Integration icon), then select the **Data Integration** link in the pop-up window. The following configuration window should appear:



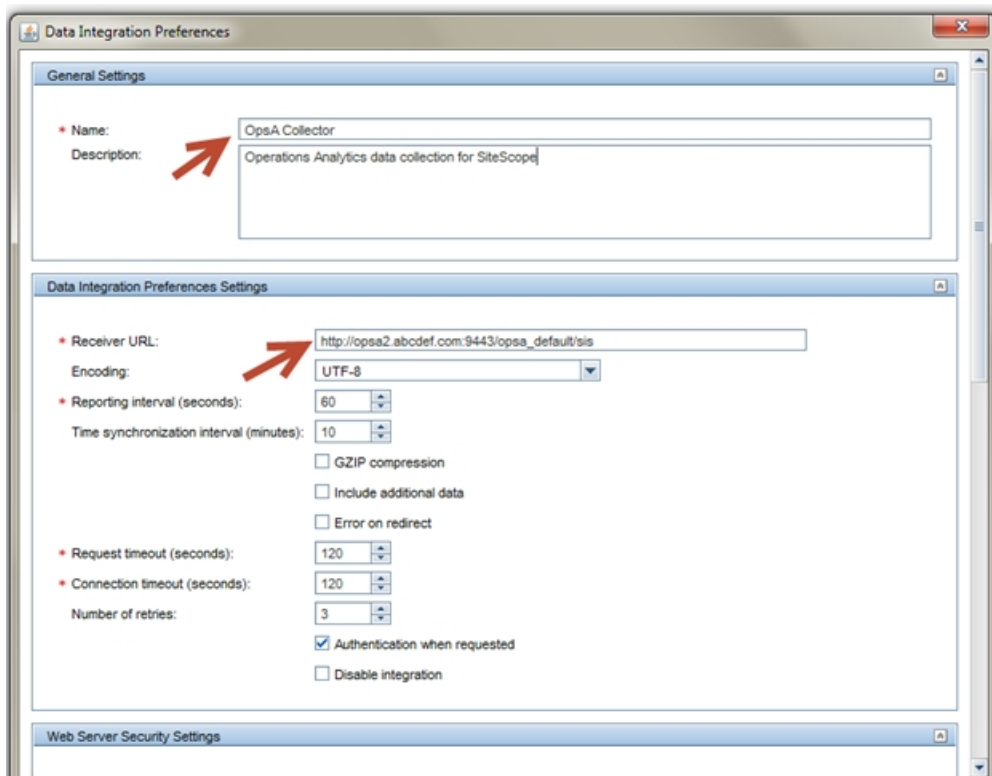
Provide a Name for this Data Integration, then provide the Receiver URL using the following format: `http://<fully-qualified domain name or ip address of the Operations Analytics Collector host>:9443/<tenant_name>/sis`

Select the **GZIP compression** option.

In this example, the target Operations Analytics Collector host is `opsa2.abcdef.com` and the target OBA tenant is `opsa_default` (the default tenant). You do not need to change any other settings, as shown in the configuration window above.

3. Scroll down in the configuration window. In the **Web Server Security Settings** panel, authenticate using the credentials for the tenant being configured, which is `opsa` in this example.

**Note:** These credentials are the same as those you would use to log on to the Operations Bridge Analytics console for a given tenant. For the example, the credentials are `opsa` (user name) and the associated password you set for this user during installation.



4. Finally, check the box for the tag that you created earlier in "[Task 1: Creating a SiteScope Tag](#)" on [page 121](#). Selecting this tag is the most important setting, as it connects the previously marked **Monitor Groups** and **Monitors** to the Data Integration being configured.
5. Click **OK** to create the new SiteScope Data Integration.

After completing the configuration steps in this section, SiteScope begins forwarding data to the Operations Analytics Collector host based on the configuration choices you made.

## Chapter 14: Troubleshooting Source Type Manager Error Messages

The information in this section helps you troubleshoot messages you might receive when configuring collections when using the Source Type Manager.

**Question:** When configuring a Custom Collection, I receive an error message that the data contains multiple time formats and an invalid CSV file. What should I do?

**Answer:** The file or files you provide in the `/opt/HP/opsa/data/<directory name>` folder must contain one timestamp format in the Timestamp format column. If your data contains multiple timestamp formats, you must correct that problem before configuring a custom collection.

**Note:** Operations Bridge Analytics only supports timezones with whole hour offsets.

**Question:** When configuring a Custom Collection, I receive an error message that Operations Bridge Analytics failed to parse the data with the selected data format. What should I do?

**Answer:** The file or files you provide in the `/opt/HP/opsa/data/<directory name>` folder must use the following guidelines when creating the CSV file:

- Custom collections support the UTF-8 character set.
- Files for use by a custom collection should contain a header and at least three rows of data.
- Operations Bridge Analytics does not support CSV file headers that contain the following special characters: \ (backslash), " (double quote), , (comma), < (less than), and > (greater than). Several other special characters are also supported, but not recommended. Examples of these are %, &, and @.
- The data source must collect CSV data based on time. There has to be a time and date column for each row in the CSV file. Both the time and date must be in

that same column.

**Note:** If this is not true, you must merge these columns before creating the collection.

- A minimum of one column needs to be designated as a key column. You can designate no more than three columns as key columns.
- The data source must provide Comma-separated values (CSV) data. CSV data is the only method that Operations Bridge Analytics provides to collect data (instead of those predefined or custom collection methods described in [Configuring Collections - Workflow](#)).
- The data source cannot exceed 200 data columns by default. If you must increase the number of columns, see the instructions explaining how to adjust the `maxcolumns.collection` parameter towards the end of this section.

**Note:** If you try to create a Custom collection containing more than 1549 data columns, the collection creation will fail. That value is a Vertica limitation when creating a table.

- See [Vertica Documentation](#) to understand any Vertica system limitations you might encounter.

**Note:** To navigate to the Vertica System Limits section for Vertica 7.1x, do the following:

- a. Click **Documentation**.
  - b. Click **HPE Vertica 7.2x**.
  - c. Click **Complete Documentation:HTML**.
  - d. Click **SQL Reference Manual**.
  - e. Click **System Limits**.
- Data from the CSV data source must be accessible to the Operations Analytics Collector host.

- The CSV file can be local or remote to the collector and is assumed to be available in the source directory at regular intervals.
- Column names should not contain any spaces.
- `/n` is considered an end of line.
- The CSV file can contain empty or blank lines, as they are ignored. However, the file contents must end with `/n`.
- When quoting characters, use standard rules for CSV files. For example, if a string contains a comma, you must add quotation marks around the comma.

**Note:** Do not use line breaks within quoted fields, as doing so is an exception to this rule.

- Decimal representations have a dependency on Vertica. We are current using `en_US@collation=binary (LEN_KBINARY)`.
- The CSV file will be used to create a table in Vertica. Vertica objects include tables, views, and columns. Your CSV file must use the following naming conventions:
  - A column name must be from 1 to 128 characters long.
  - A column name must be unique, and not match any other column names.
  - A column name must begin with a letter (A through Z), diacritic marks, or non-Latin characters (200-377 octal).
  - Column Names are not case sensitive. For example, `CUSTOMER` and `Customer` represent the same names. However, if you enclose a column name in quotation marks, it is case sensitive.

**Note:** Object names are converted to lowercase when they are stored in the Vertica database.

- A column name must not match another Vertica object that has the same type,
- A name cannot match a Vertica reserved word such as `WHERE`, `VIEW`, `Table`,



ID, User, or Query.

- A name cannot match the another Vertica object that has the same type.
- The CSV file format has to be uniform for a single collection. For example, if you create a collection with 10 columns, the subsequent files that are provided for import within Operations Bridge Analytics must have same format, including column names and data types.

**Question:** When configuring a Custom Collection, I receive an error message that the data has more columns than the maximum configured limit. What should I do?

**Answer:** Do the following:

1. As the opsa user, edit the `/opt/HP/opsa/conf/collection/framework.properties` file.
2. Change the `maxcolumns.collection` parameter to a value that supports the number of columns you include in your data.
3. Save your work.
4. From the Operations Bridge Analytics console, use the Configuration Manager to configure the collection.

**Note:** Increasing the `maxcolumns.collection` parameter results in Operations Bridge Analytics reduced browser performance. Use practical numbers when increasing this value.

**Question:** When creating a Custom Collection (JDBC), I received an error message similar to the following: `Unsupported frontend protocol <version>: server supports <lower version> to <upper version>`. What should I do?

**Answer:** The JDBC library you provided is incompatible with the database (Vertica, MSSQL, or Oracle). You must provide a JDBC library that is supported

and works with your database version. Review the database documentation to determine which JDBC libraries work with the database version you are using.

**Question:** When configuring a Custom Collection (JDBC), I created an SQL statement that used a column name that included the name of a disallowed command (update).

For example, suppose I created the following SQL statement:

```
select update , insert , delete , creat e, into , drop , truncate
, grant , revoke from myd_vm06628_evt.dbo.shimi2
```

When I tried to create the collection, I received an error message similar to the following:

```
This operation failed due to an incorrect entry in SQL Statement
field. The UPDATE SQL command is not a read-only command. Only
read-only SQL commands are permitted.
```

What should I do?

**Answer:** Change the SQL statement to read as follows:

```
select [update] , [insert] , [delete] , [create] , [into] ,
[drop] , [truncate] , [grant] , [revoke] from myd_vm06628_
evt.dbo.shimi2
```

When you create the collection now using the SQL statement in this new form, you will be able to successfully create the collection.

**Question:** When configuring a Custom Collection (JDBC) that collects CLOB objects (character large objects) in MSSQL, I receive an error message that OBA failed to parse the data. Verify the data and try again. I need to configure similar collections for Vertica and Oracle. What should I do?

**Answer:** You cannot set up this collection using CLOB objects in either an MSSQL, Vertica, or Oracle collection. There is no workaround for this limitation. You must exclude any columns containing CLOB or binary data from your select statement.

**Question:** When configuring a Custom Collection (JDBC) for MSSQL that collects the timestamp data type for the SQL Timestamp Column, I receive an error message about converting a timestamp. What should I do?

**Answer:** When configuring a Custom Collection (JDBC) for MSSQL collection, the collection only supports the datetime data type for the SQL Timestamp Column. It does not support the timestamp data type.

**Question:** After configuring a Custom Collection for a File, JDBC, TCP, or UDP channel, I expected to receive approximately 1000 data records for this collection during the first hour. I only received 800 data records and I am concerned. What should I do?

**Answer:** Check that your data source is providing the data you expect according to the data format chosen during collection configuration as shown in the **Preview** step. Any deviations from the original data format you chose causes data parsing errors and dropped data. If the data source is providing the expected data, then contact HP Software Support for more assistance.

**Question:** When configuring a Custom Collection (JDBC) for MSSQL collection, the collection does not include data inserted in to the database table with a timestamp value that is out-of-order in the SQL timestamp column. What should I do?

**Answer:** The JDBC channel uses the SQL Timestamp column to track the position in the table where it read the last row during the last collection interval. This SQL timestamp column must be a linearly increasing timestamp column. Since the JDBC channel remembers the last row's SQL timestamp column value, the JDBC channel will not read any rows inserted in to the table with an older timestamp than the last cursor (tracked position). To summarize, the records inserted in to the table must have a linearly increasing timestamp value in the SQL timestamp column.

**Question:** I used the `opsa-collection-config.sh` script to create and publish an initial version of a Custom Collection. After Trying to use the Source Type Manager to publish an edit I made to this Custom Collection, the page cleared and the edit shows a continuous `Loading Data...` message. What should I do?

**Answer:** Click **Back** to exit the continuous Loading Data... message. Rename the

`/opt/hp/opsa/conf/collection/server/config.templates/custom/1.0/<domain>/<group>/<oldname>.xml` file located on the Operations Analytics Collector host to `custom_collection.xml`. Continue with your plans to edit this collection.

## Chapter 15: Managing the Content for Data Source Types

Data source type content files define the data that Operations Bridge Analytics can parse and extract for analysis experts, partners, and customers. You create this content manually or by exporting a published source. You deploy this content by importing this published source. To complete either one of these actions, run the `opsa-di-source-manager.sh` script from a command line from the Operations Analytics Server. A data source type content file includes the following configuration information:

- The parser configuration (the parameters used for selecting data fields).
- The line breaking configuration (the configuration for where to break the log entry lines).
- The supported channel types (the channel types supported by this source type).
- The collection template (definitions of column metadata, keys, and tags).

Use the `opsa-di-source-manager.sh` script to import or export the content for a data source type configuration file for the following purposes:

- Import content developed by HPE for Operations Bridge Analytics.
- Import content developed by Operations Bridge Analytics customers.
- Export or import a source type configuration that was created by using the Operations Bridge Analytics console.

To be able to export a source, either use an already published source type or create a new one by doing the following:

1. From the Operations Bridge Analytics console, connect to a Source Type.
2. Define a channel for this source type.
3. During the Fields step, create and edit all the fields you want. At a minimum, define the field you want to use as the timestamp field as data type `datetime`.
4. During the Common Metadata step, select the field you defined as the timestamp field in the previous step as the timestamp field for this step.

**Note:** Decide if you want Operations Bridge Analytics to use the the timezone from the collected data or from the channel. Set the correct format if Operations Bridge Analytics

processed it incorrectly.

5. During the Common Metadata step, navigate to **Text Search and significant analytics > Analytics Type** and select the analytics check box related to this Source Type. Make the three mandatory field selections, including the severity mapping if Operations Bridge Analytics did not properly process this setting.

6. Complete the Preview & Publish step.

7. Run the following command to export this data source type configuration file:

```
/opt/HP/opsa/scripts/opsa-di-source-manager.sh -export -user opsatenantadmin -
password opsatenantadmin -sourceName <source name> -zipFile <source zip file
name>
```

To use the `opsa-di-source-manager.sh` script to import the data source type configuration files you just created, do the following:

1. Create a zip file of the files created in the above example and copy it to a location on the Operations Analytics Server.

**Note:** Write down the location to which you copy the zip file. You will need to use this zip file location with `opsa-di-source-manager.sh` script and the `fullPathZipFile` option when you import the data source type configuration file.

2. Run the following command to import this data source type configuration file:

```
/opt/HP/opsa/scripts/opsa-di-source-manager.sh -import -user opsatenantadmin -
password opsatenantadmin -sourceName <source name> -fullPathZipFile
<path/source zip file name>.
```

3. Your imported source will appear in the Operations Bridge Analytics console on the Source Type Manager page with the status template. To use this source to collect data, connect to it and publish this new source type. See [Adding or Connecting Source Types](#) for more information.

As discussed earlier, you can create your own data source configuration files. You can also use new source configuration files developed for Operations Bridge Analytics by HPE or by third-party developers. You can enhance your existing content by exporting this source content manually or by exporting a published source.

Operations Bridge Analytics also provides syslog Smart Connectors. See the *Smart Connector Guide* for more information. In certain cases you might want to enrich or alter the Smart Connector content. To enhance existing Smart Connectors, use the `opsa-di-source-manager.sh` script with the `enhance` option as explained below.

There are two files to consider when enhancing your existing content:

- The `order.order` file: OBA uses the contents in this file to parse data fields in the order shown within the file.

Edit this file and organize the contents, adjusting the order in which Operations Bridge Analytics uses the listed vendors to parse syslog files.

- The `<vendor>.properties` files: Each set of content configuration files includes a new `<vendor>.properties` file that must be added to the zip file before using the `opsa-di-source-manager.sh` script to enhance the data source type configuration files.

To use the `opsa-di-source-manager.sh` script to enhance the data source type configuration files, do the following:

1. Locate the `order.order` file and do one of the following:
  - Edit the current `order.order` file, adding the contents of the new `order.order` file to the current file. Save your changes.
  - Save a copy of the current `order.order` file, then overwrite it with the new `order.order` file.
2. Copy the new `vendor.properties` file into the location of the unzipped files.
3. Add the new `vendor.properties` and `order.order` file into the original zip file.
4. Run the following command to enhance this data source type configuration file:

```
/opt/HP/opsa/scripts/opsa-di-source-manager.sh -enhance -fullPathZipFile  
<path/source zip file name> -sourceName <source name> -user opsatenantadmin -  
password opsatenantadmin.
```

See the `opsa-di-source-manager.sh` reference page (or the Linux manpage) for more information.

## Chapter 16: Using Tags for Source Types

The Phrased Query Language (PQL) is a proprietary search tool provided with Operations Bridge Analytics that uses tags and keys to narrow the data for which you are searching. After you start typing, suggestions appear automatically based on the tags and keys defined in predefined Source Types. For custom Source Types, you must configure keys and tags to match the search needs for the data you plan to collect.

### Learn About

OBA stores collected data in the form of Source Type tables located in a Vertica database. When configuring a Source Type using the Source Type Manager, you define the keys and tags during the Fields and Common Metadata steps.

#### Available PQL Searches using Tags

All PQL searches are primarily based on tags. PQL searches use tags to narrow your search results. Before deciding which keys and tags to use, you must research how you want PQL to narrow the searches for the data you are collecting. The information in this section discusses PQL searches using the following syntax:

- PQL searches use a `<tagname> withkey <key attribute value>` translation when performing the search.
- By using the `Host: keyword` in a PQL search, it automatically creates a `host withkey <example.servername.com>` command that, when searched on, generates a host dashboard for the query.

**Note:** Keys and tags are defined when you create Source Types. When configuring a Source Type using the Source Type Manager, the Source Type's host field is set to be a key so that Operations Bridge Analytics can make host suggestions when you use the `Host: keyword`. You can edit tags and keys using the Source Type Manager or you can make tag changes from the Operations Analytics Server using the `opsa-tag-manager.sh` script.

Using the `withkey` keyword in a search adds a filter for data from any key attribute field that you configured before registering a Source Type.

**Note:** When using Splunk as the log data source, you must directly type the hostname or



IP address in the search bar. Do not use the Host: `<hostname>` or Host: `<IP Address>` for a Splunk PQL search.

- By using the Host: keyword in a PQL search in combination with a Focus On keyword, Operations Bridge Analytics suggests both key values and tag names.
- Start-typing, Application, Service, or Host keywords: Using these keywords in a PQL search brings up the default dashboard for the tags and keys you provide in a search. The default dashboard shows the following information (if available) from a host or service search:
  - metric data
  - significant messages (Log Analytics)
  - log messages
  - anomalies

The default dashboard shows the following information (if available) from an application search:

- metric data
- log messages

A key designation in a column is set by configuring **no more than three key attributes** from the Operations Bridge Analytics console during the Common Metadata step when adding a new Source Type or by setting a `key="yes"` entry in a Source Type's `<collection>.xml` file before publishing a Source Type. Setting this value tells PQL that this entire column is a key search field. When using a key column to narrow a search within a Source Type, Operations Bridge Analytics returns only those metrics for the specified key column value. For example, if the `host_name` column is defined as a key attribute in a `cpu metrics` Source Type, the `host_name` key column enables you to search for `cpu metrics` for a specific host name.

Complete the Type selection (to attribute or metric) for columns during the **Fields** step or by setting a `type="attribute"` or `type="metric"` in the `<collection>.xml` file before publishing a new channel for a Source Type.

Use the primary tag to tag the most important metrics or attributes for a specific area, such as `cpu`. If you enter `cpu primary` in the search query, the results focus on only a few important metrics, which are tagged as `primary`. The primary tag is good for configuring the specific data you want to show up in a dashboard.

Operations Bridge Analytics supports the following searches:

- Using the Start Typing: keyword: You type in tags and keys to narrow a data search.
- Using the Host: keyword: By using the Host: keyword in a PQL search, it automatically invokes

`host withkey <example.servername.com>` and generates a host dashboard for the query.

- Using the `withkey` keyword: You can easily do PQL searches using data from a key attribute field to which you assigned a tag during the **Fields** step in a Source Type template file. When typing a tag in a PQL search, the search field includes suggestions as to which tags are available for searching. When typing a PQL search, you must have configured at least one key in the Source Type on which you are searching for your PQL search to work. You can also provide no more than three keys as long as these keys have been configured in the Source Type on which you are searching. The ordering of the keys you add is important, as Operations Bridge Analytics processes the keys you added by the assigned priority. An example of a PQL search using three tags and one key is as follows: `host_name cpu system performance withkey <server.mydomain.com>`

**Note:** The `withkey` command filters according to key values.

So you can see that creating the right tags and keys is important for being able to search a Source Type's data. When configuring an XML template file for a custom Source Type, consider the following:

- You can assign a key to a data field as long as it is an attribute (for example, it cannot be metric data).
- Any key you add into a Source Type's XML template file is static, and cannot be modified within a registered Source Type.
- You must configure a `Host` field as a key ("key=yes") to get host suggestions when running a PQL search.

There are two types of tags, property tags and property group tags:

- **Property tags:** These tags are set for data columns. See the following example for syntax.  
Example : `tags="process,performance,primary"`
- **Property group tags:** These tags are set at the Source Type level. Examples are `host` and `system`. You can do PQL searches using property group tags to see data for an entire Source Type.

When configuring an XML template file for a custom Source Type, you can add a tag for either attribute or metric data fields. Consider the following when creating tags:

- The tags you add into a Source Type's XML template file configure the initial tags for a Source Type. You can update a Source Type's tags using the `opsa-tag-manager.sh` script. See the `opsa-tag-manager.sh` reference page (or the UNIX man page) for more information.
- It is important to add a tag for at least one metric field for suggestions to appear during a PQL search.

- For PQL searches to work correctly, you must configure at least one key and one tag for a Source Type.
- Add a `host` tag to every metric field that you want to view in the host dashboards (by doing a `Host:<my host>` search).
- Add a `host_name` tag to every key attribute field that you want to view.
- Add a `primary` tag to every metric field that you want included in a host dashboard as a result of a guided search.
- Tag a `Host` field with a `host_name` tag. Doing so permits you to use a `Drill-to` keyword in a PQL search.

## User Tasks

Use the **Tags** fields during the Fields Source Type configuration step and the **Source Type Tags** fields during the Common Metadata configuration step to configure your desired tags.

## Command Line Usage Examples for Creating Tags

It is recommended that you use the **Tags** fields during the Fields Source Type configuration step and the **Source Type Tags** fields during the Common Metadata configuration step to configure your desired tags.

Another alternative for you is to use the interactive `opsa-collection-config.sh` script to set up tags for a Source Type. As an example of setting up tags for a custom Source Type (before creating and publishing a Source Type), edit the XML template file for the custom Source Type and do the following :

1. Locate the field that shows the server name and add both a `host` and `host_name` tag to this field.
2. Locate the metric field or fields that you want to tag and add both a `host` and `primary` tag to these fields.
3. Publish the Source Type using the interactive `opsa-collection-config.sh` script shown in Adding or Connecting Source Types or by using the **Custom Source Type** registration instance in the **Source Type Manager**. See ["Registering Operations Bridge Analytics Collector Hosts" on page 235](#) for more information.

4. After the data for your Source Type is being collected, wait 30 minutes or more, then make use of a Source Type's keys and tags to view data using Operations Bridge Analytics Phrase Query Language (PQL). For example, after 30 minutes or more, you can have suggestions such as `Host:my host` from a guided search.

Below are some examples of using the `opsa-tag-manager.sh` to adjust the tags for your custom collection:

- A property tag is associated with a data column within a collection. By creating one or more property tags, you can use a PQL search that narrows the displayed data to one or more data columns within a collection.
- A property group tag is associated with a specific collection. By creating a property group tag, you can use a PQL search that narrows the displayed data to a specific collection.

### Creating Property Tags

Use the following tasks as an example when creating tags for a collection:

1. ["Define the PQL and tag names you want to use" below.](#)
2. ["Configure the tags" on page 142.](#)

### Define the PQL and tag names you want to use

Suppose you are collecting data in a collection called `custom_sysperf_global` and you already marked key attributes for this collection. For this example, this collection includes the metrics property UIDs shown in ["Property UIDs for the custom\\_sysperf\\_global Collection Example" below](#):

#### Property UIDs for the custom\_sysperf\_global Collection Example

Collection property group uid	Property UID
custom_sysperf_global	mem_free
custom_sysperf_global	mem_pageout_byte_rate
custom_sysperf_global	mem_pageout_rate
custom_sysperf_global	mem_swap_util
custom_sysperf_global	mem_util
custom_sysperf_global	cpu_user_mode_util
custom_sysperf_global	cpu_util

**Property UIDs for the custom\_sysperf\_global Collection Example, continued**

Collection property group uid	Property UID
custom_sysperf_global	disk_util_peak
custom_sysperf_global	fs_space_util_peak
custom_sysperf_global	mem_swap_util
custom_sysperf_global	mem_util

Looking at this information, you decide to create tags so that you can use the following PQL searches to view this collected data:

- Memory search: Start Typing: memory
- Utilization search: Start Typing: utilization

To do this, you decide to add the memory and utilization tag names to the Property UIDs as shown in "[Property UIDs and Tags for the custom\\_sysperf\\_global Collection Example](#)" below.

**Note:** As mentioned earlier, If you prefer to have metrics from this collection displayed in an OBA host dashboard you would need to consider the following actions:

- Add a host tag to every metric field that you want to view.
- Add a host\_name tag to every key attribute field that you want to view.
- Add a primary tag to every metric field that you want included in a host dashboard as a result of a guided search.
- Tag a Host field with a host\_name tag. Doing so permits you to use a Drill-to keyword in a PQL search.

**Property UIDs and Tags for the custom\_sysperf\_global Collection Example**

Collection property group UID	Property UID	Tag Name
custom_sysperf_global	mem_free	memory
custom_sysperf_global	mem_pageout_byte_rate	memory
custom_sysperf_global	mem_pageout_rate	memory
custom_sysperf_global	mem_swap_util	memory
custom_sysperf_global	mem_util	memory

### Property UIDs and Tags for the custom\_sysperf\_global Collection Example, continued

Collection property group UID	Property UID	Tag Name
custom_sysperf_global	cpu_user_mode_util	utilization
custom_sysperf_global	cpu_util	utilization
custom_sysperf_global	disk_util_peak	utilization
custom_sysperf_global	fs_space_util_peak	utilization
custom_sysperf_global	mem_swap_util	utilization
custom_sysperf_global	mem_util	utilization

### Configure the tags

To configure tags that enable you to search on both memory and utilization, do the following:

1. Create a `/tmp/mytag.csv` file.
2. Add the following content to the file:

```
custom_sysperf_global,mem_free,memory
custom_sysperf_global,mem_pageout_byte_rate,memory
custom_sysperf_global,mem_pageout_rate,memory
custom_sysperf_global,mem_swap_util,memory
custom_sysperf_global,mem_util,memory
custom_sysperf_global,cpu_user_mode_util,utilization
custom_sysperf_global,cpu_util,utilization
custom_sysperf_global,disk_util_peak,utilization
custom_sysperf_global,fs_space_util_peak,host,utilizatio
custom_sysperf_global,mem_swap_util,utilization
custom_sysperf_global,mem_util,utilization
```

3. Save your work.
4. Run the following command to create these new property tags:  

```
opsa-tag-manager.sh -username opsatenantadmin -password opsatenantadmin -add_
tags -type property -file /tmp/mytag.csv
```

After you finish the above tasks, wait 15 minutes or more, then use variations of the following PQL searches to test the property tags you configured:

- Memory search: Start Typing: `memory`
- Utilization search: Start Typing: `utilization`

## Creating Property Group Tags

Reviewing "[Property UIDs for the custom\\_sysperf\\_global Collection Example](#)" on page 140, you might decide that you also want to create tags so that you can use the following PQL search, viewing the data from the entire collection instead of creating tags for individual Property UIDs:

All metrics from this custom collection search: Start Typing: `my_system_performance`

For this approach, do the following:

1. Create a `/tmp/mytag.csv` file.
2. Add the following content to the file:  
`custom_sysperf_global,my_system_performance`
3. Save your work.
4. Run the following command to create these new property group tags:  
`opsa-tag-manager.sh -username opsatenantadmin -password opsatenantadmin -add_tags -type property_group -file /tmp/mytag.csv`

After you finish the above tasks, wait 15 minutes or more, then use the following search to view all metrics from you custom collection to test the property group tag you configured:

All metrics from this custom collection search: Start Typing: `my_system_performance`

As discussed earlier, Operations Bridge Analytics supports the following types of tags:

- **Property Group Tags:** Operations Bridge Analytics administrators add these tags to an entire collection.
- **Property Tags:** Operations Bridge Analytics administrators add these link tags to one or more properties (or database columns) for a specific collection.

To manage tags, use the `opsa-tag-manager.sh` script. See the *opsa-tag-manager.sh* reference page (or the Linux man page) for more information.

**Note:** Tags, property uids, and property group uids are not case sensitive. They are always converted into lowercase.

## Syntax Summary

To summarize the syntax of the `opsa-tag-manager.sh` script discussed earlier in this section, use the following command to add tags:

## Adding Tags

- **Property Tags:** `$OPSA_HOME/bin/opsa-tag-manager.sh -add_tags -type property -file /opt/HP/opsa/tmp/property_tags.csv -username opsatenantadmin`
- **Property Group Tags:** `$OPSA_HOME/bin/opsa-tag-manager.sh -add_tags -type property_group -file /opt/HP/opsa/tmp/property_group_tags.csv -username opsatenantadmin`

### Listing Tags

Use the following command to list tags:

- **Property Tags:** `$OPSA_HOME/bin/opsa-tag-manager.sh -list_tags -type property [-propertygroup_id ID] [-property_id ID] -username opsatenantadmin`
- **Property Group Tags:** `$OPSA_HOME/bin/opsa-tag-manager.sh -list_tags -type property_group [-propertygroup_id ID] -username opsatenantadmin`

### Deleting Tags

Do not delete any pre-existing tags used for pre-defined collection templates, as that might disrupt these collections.

Use the following command to delete tags:

- **Property Tags:** `$OPSA_HOME/bin/opsa-tag-manager.sh -delete_tags -type property -propertygroup_id <property group id> -tag_name <list of comma-separated tags> -username opsatenantadmin`
- **Property Group Tags:** `$OPSA_HOME/bin/opsa-tag-manager.sh -delete_tags -type property_group -propertygroup_id <property group id> -tag_name <list of comma-separated tags> -username opsatenantadmin`

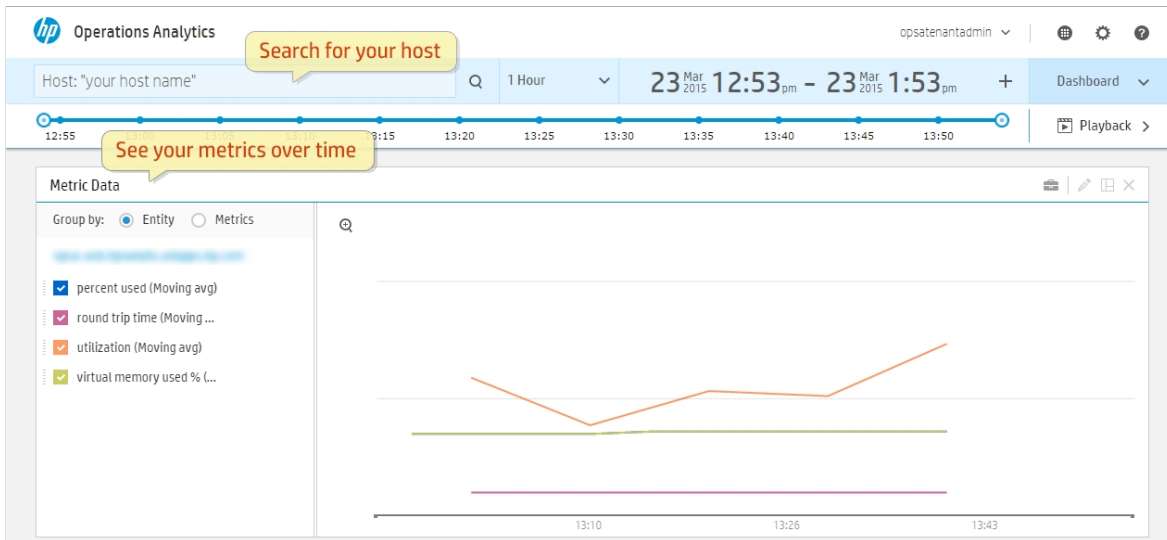
## Tagging Collection Best Practice

To make your data easier to search, add your desired tags to both the collection and to each preferred data column.



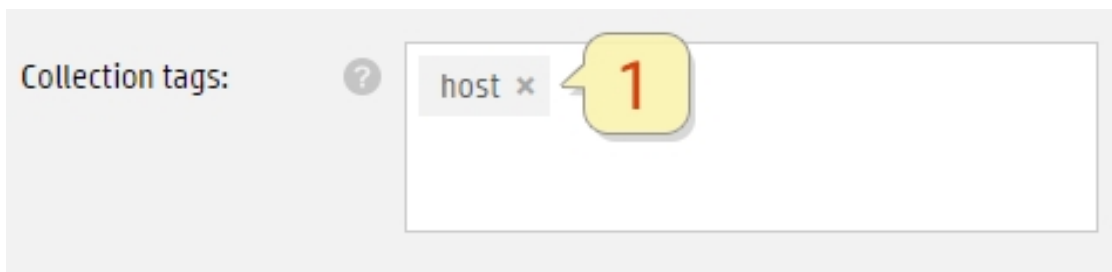
## Tagging a Collection For Searching by Host

If your data contains a host, you might prefer to search the data by host name as shown in the following image.



To configure this host name search, complete the following steps.

1. Add a **Host** tag to the **Collection tags** field.



2. Add a **Host\_Name** tag to the column you want tagged as a host. Your data might include several columns that contain host information. If that is the case, you must choose one column as the main host column and add the **Host\_Name** tag to this column.
3. Set this column as a key.

**Note:** When selecting data columns to be **Key** fields, set no more than three columns to a Key value of **true**.

Label:	?	hostname		s
Type:	?	attribute		a
Tags:	?	host_name		
Key:	?	true		n
Data type:	?	string		ti
Units:	?	n/a		n

4. Add a **primary** tag to each metric that you want to appear in a host search. You can tag all of your metrics as **primary**, however a best practice is to select no more than 20 primary metrics.

Label:	?	hostname		stamp	value	tenantId	region
Type:	?	attribute		attribute	metric	metric	attribute
Tags:	?	host_name			primary	primary	
Key:	?	true		n/a	n/a	n/a	false
Data type:	?	string		timestamp	float	string	string
Units:	?	n/a		n/a			n/a

If you followed these steps, you will be able to search by specific host names.

## Chapter 17: Communicating Collection Names and Meta Data Information to your Users

One way for operators to view the tags and property groups available to them is to View the **OpsA Meta Info** dashboard, which displays all of the active collections and the tags being used. The information in this dashboard provides operators with a lot of the information they need for more effective queries. See [Dashboards and Query Panes](#) for more information.

The following example uses the `$OPSA_HOME/bin/opsa-tenant-manager.sh` script. This example uses a predefined Super Admin user (opsadmin) and the password for this user that you set during installation. You can also use the Operations Bridge Analytics console to manage users and tenants. See "[Manage Users and Tenants](#)" on page 219 for more information.

To create a list of the collections and tags your users will be interested in, you can also do the following:

1. To list all of the tenants configured for an Operations Analytics Server, run the `$OPSA_HOME/bin/opsa-tenant-manager.sh -list -loginUser opsadmin -loginPassword <password>` command from the Operations Analytics Server. Make a list of the tenants shown in the command output for your users. See the `opsa-tenant-manager.sh` reference page (or the Linux man page) for more information.
2. To list all of the published collectors and collections for a tenant, run the `$OPSA_HOME/bin/opsa-tenant-manager.sh -list -collectorhosts -username opsatenantadmin` command from the Operations Analytics Server. Make a list of the published collectors and collections shown in the command output for your users. See the `opsa-collection-config.sh` reference page (or the Linux man page) for more information.
3. Use the `$OPSA_HOME/bin/opsa-tag-manager.sh` script from the Operations Analytics Server to view and identify the tags in which your users are interested. Experiment with the options available with the `opsa-tag-manager.sh` script to identify the tags you must communicate to your users. See the `opsa-tag-manager` reference page (or the Linux man page) for more information. Make a list of these tags.
4. Combine the information from these steps and distribute this information to your Operations Bridge Analytics users.

# Integrations

This section contains the following topics:

["BSM and OMi Integrations" on page 149](#)

["Configure Log Integrations" on page 159](#)

# Chapter 18: BSM and OMi Integrations

Operations Bridge Analytics can be integrated with Business Service Management (BSM) and Operations Manager i (OMi).

For information on the OBA integration with BSM, see the *Operations Analytics Integration with BSM* guide.

For information about the OBA integration with OMi, see the *OMi Integrations Guide*.

## Learn About

### About the BSM and OMi Integrations

This section describes the details of the types of integrations between HPE Business Service Management (BSM), Operations Manager i (OMi), and HPE Operations Bridge Analytics.

This integration can enable the following features:

- **Cross-Launch Integration:** Drill down from BSM to Operations Bridge Analytics in the context of a specific CI, event, or SHA anomaly.

**Deprecated:** The SHA anomaly detection functionality is now natively part of Operations Bridge Analytics 3.00. The SHA cross-launch integration will be deprecated in subsequent releases.

- **Dashboard Integration:** Display the Operations Bridge Analytics user interface inside a dashboard in MyBSM or OMi.

Both these integrations allow you to use the forensic root cause analysis tools in Operations Bridge Analytics in conjunction with BSM and OMi monitoring tools.

### Prerequisites

The integration between BSM and Operations Bridge Analytics can only be performed on the following versions:

- BSM 9.23 or later
- Operations Bridge Analytics 2.10 or later. The integration with OMi is only supported starting from

version 2.30.

- OMi 10 or later

When using Single Sign-on, consider the following:

- Both systems must be configured for http or both systems must be configured for https. A mixture of these two protocols is not supported.
- Single Sign-on does not work if you use the Operations Analytics Server's IP address or short hostname. When using Single Sign-on, you must use the fully-qualified domain name of the Operations Analytics Server in the URL.

See *Single Sign-on* in the [Operations Bridge Analytics Hardening Guide](#) for more information.

## Tasks

### Cross Launch Integrations

You can configure an integration that allows you to open Operations Bridge Analytics directly from BSM in the context of a specific event or host. This allows you to open analysis tools from Operations Bridge Analytics such as log analytics and predictive analytics quickly and easily in the appropriate context.

#### How to Set Up a Cross Launch Integration for OMi Events

**Note:** This procedure is the same for OMi whether it is a part of BSM or a standalone product. The screen shots have been taken for OMi as a part of BSM.

You can configure a cross launch for individual CI types from the Operations Management Administration console. This is done using OMi's **User Tools** feature.

1. From the BSM or OMi user interface, go to **Admin > Operations Management** .
2. Go to the **Operations Console** Tab and select **Tools**.



3. Select the CI type for which you want to enable the cross launch.
4. Select **New Item**.



5. Complete the **General** Page. Specify the default category.
6. On the **Type** page, select **URL**.
7. Specify a URL as seen in the following examples:

To query a single specified host over the last day:

```
http://<opsa_server>:8080/opsa/#/logsearchhpql?search=host%20withkey%20%22${event.node.dnsName}%22&selectedTimeRange=ONE_DAY
```

To query all hosts over the last hour:

```
http://<opsa_server>:8080/opsa/#/logsearchhpql?search=host%20withkey%20%20*&selectedTimeRange=ONE_HOUR
```

#### How to Use a Cross Launch Integration from OMi

1. Go to **Applications > Operations Management > Events Perspective** and right-click the desired event.

**Note:** The cross launch functionality is defined as a tool and must be defined for each CI type.

2. Select **Launch > Tools**

3. Select the name of the URL you would like to launch.

#### How to Set Up a Cross Launch Integration for Anomalies in SHA

**Deprecated:** The SHA anomaly detection functionality is now natively part of Operations Bridge Analytics 3.00. The SHA cross-launch integration will be depreciated in subsequent releases.

1. In **Platform Administration > Setup and Maintenance > Infrastructure Settings**, select **Service Health Analyzer** in the **Applications** context.
2. In the **Service Health Analyzer - User Interface** table, locate the **Operations Bridge Analytics URL** setting.
3. Specify the Operations Bridge Analytics server in the URL as follows:  
**http://<your opsa server>:8080/opsa**
4. Click **Save** to enable the integration.

#### How to Use the Cross-Launch Integration from SHA

1. Go to **Applications > Service Health Analyzer > CI Analytics Data** tab.
2. Select the relevant Business Service and click **topology view**. Right-click any node that is a host.
3. Select **drilldown** and Operations Bridge Analytics.

An Operations Bridge Analytics dashboard focusing on the host opens in a new window.

#### Dashboard Integrations

You can display the Operations Bridge Analytics user interface within the user interface of a dashboard in OMi or MyBSM.

Prerequisite: You must configure LWSSO on the Operations Bridge Analytics environment. This procedure can be found in the [HPE Operations Analytics Hardening Guide](#).

#### How to Configure a BSM MyBSM Integration

This procedure explains how to configure a MyBSM page that displays the event browser and the Operations Bridge Analytics user interface.

1. Set up an Operations Bridge Analytics user that has the same user name and password as an administrative user in BSM.
2. In Operations Bridge Analytics, locate **/opt/HP/opsa/jboss/standalone/deployments/opsa-ui-web.war/WEB-INF/web.xml**.



Modify the following section from:

```
<init-param>  
<param-name>X-Frame-Options</param-name>  
<param-value>SAMEORIGIN</param-value>  
</init-param>
```

to:

```
<init-param>  
<param-name>X-Frame-Options</param-name>  
<param-value>Allow-From http://<BSM URL>/topaz</param-value>
```

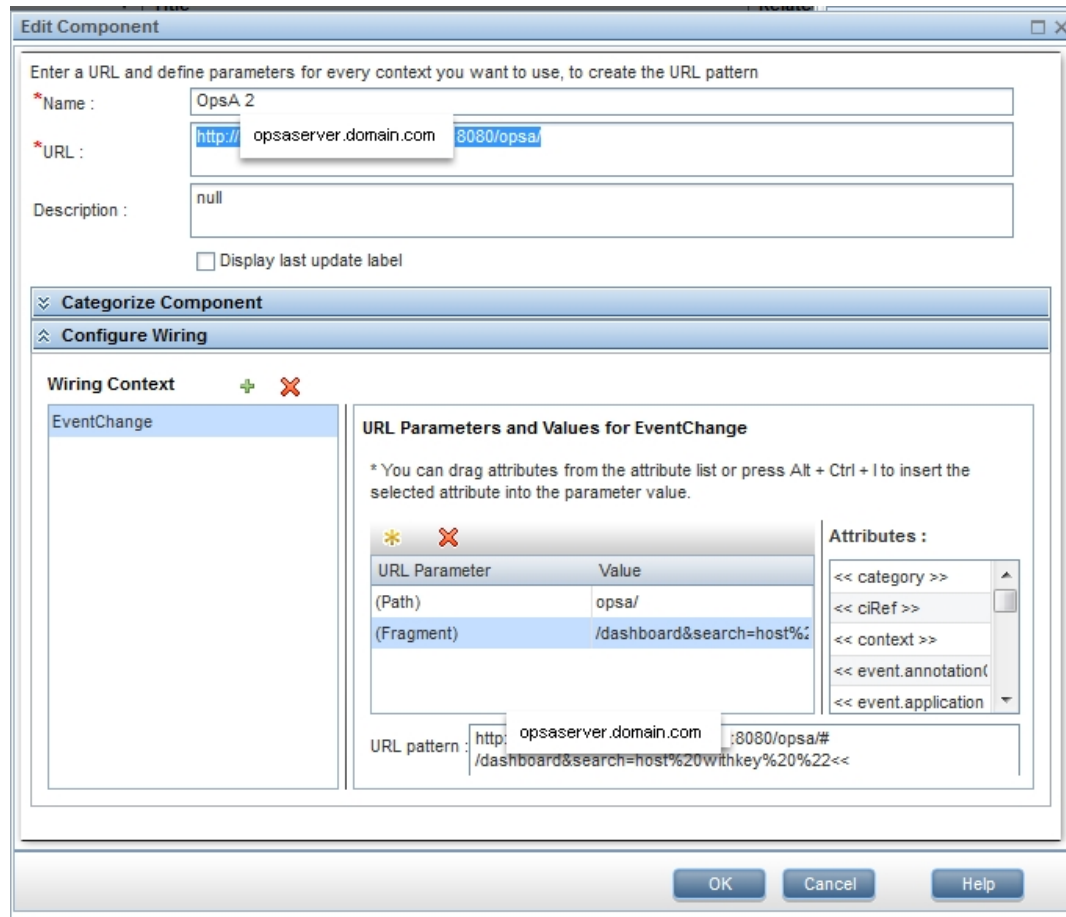
3. Restart Operations Bridge Analytics by running the command **opsa-server restart**.
4. We recommend adding a mapping of the Operations Bridge Analytics IP and the Operations Bridge Analytics FQDN in the windows host file in every client machine that will be used to access Operations Bridge Analytics.
5. Delete the cookies of all browsers used to access BSM.
6. Log in to BSM with a user that exists in both BSM and Operations Bridge Analytics.
7. Add Operations Bridge Analytics to the list of trusted hosts:
  - a. In the BSM JMX console, locate the **Topaz** section and select **service=LW-SSO Configuration**.
  - b. Locate the **addDNSDomainToTrustedHosts** element.
  - c. Add the Operations Bridge Analytics domain and select **Invoke** .
  - d. Verify that the domain has been added by going to **Administration > Platform > Users and Permissions > Authentication Management**. In the **Single Sign-On Configuration** table, verify that the domain you just added is visible under **Trusted Hosts/Domains**.
8. In BSM, go to **Applications > MyBSM**.
  - a. Create a new page.
  - b. Add a new component, specify a name and the Operations Bridge Analytics URL.  

**Example:** http://<OpsaURL>:8080/opsa
  - c. In the **Configure Wiring** section, specify the **EventChange** context and add a Path and

Fragment parameter as seen below. Specify the value as desired.

**For Example:** /dashboard&search=host%20withkey%20%22<<  
event.node.dnsName >>

For additional example URLs, see ["URL Syntax and Examples" on page 1.](#)



9. After you have saved your component you can add it to any page that contains an event browser.

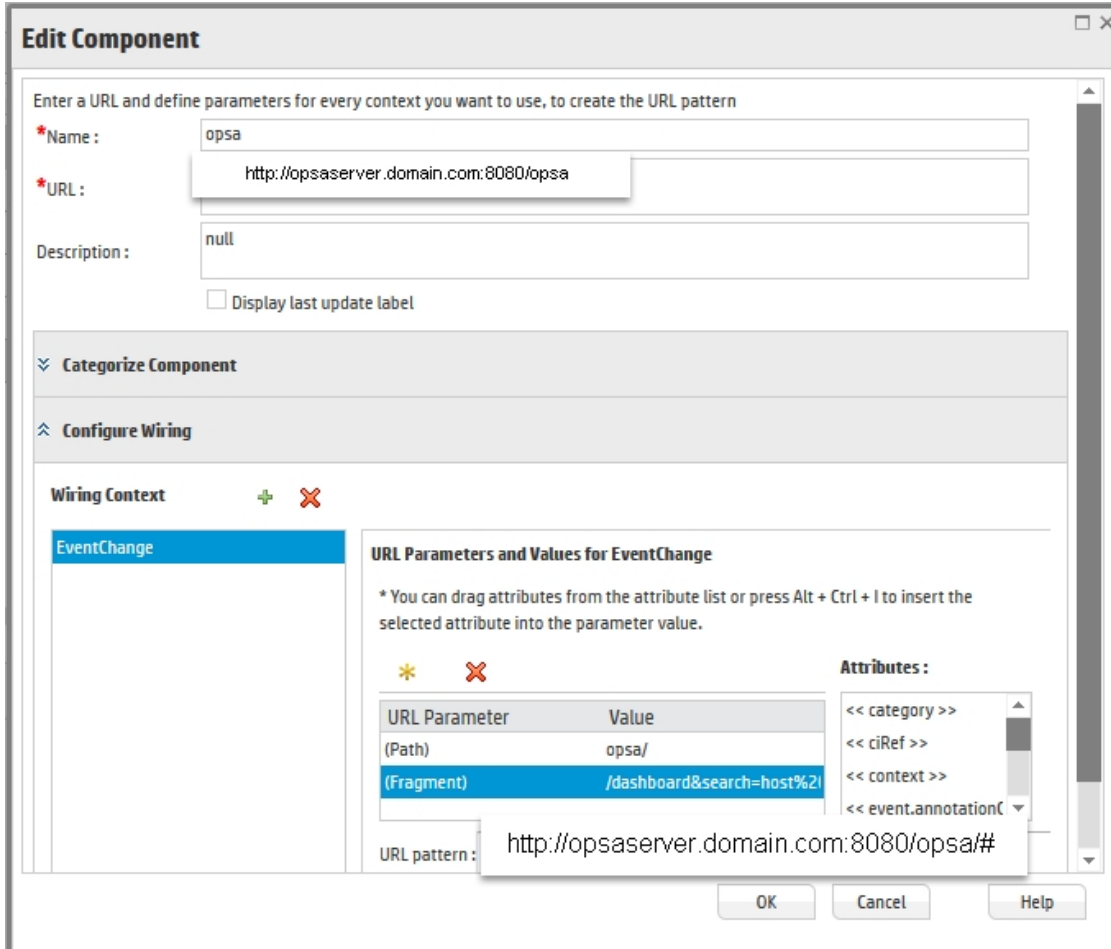
For instructions on configuring the dashboard integration between OBA and OMi, and on sending anomalies and alerts as events to OMi, see the *OMi Integrations Guide*.

To Configure an OMi Dashboard Integration

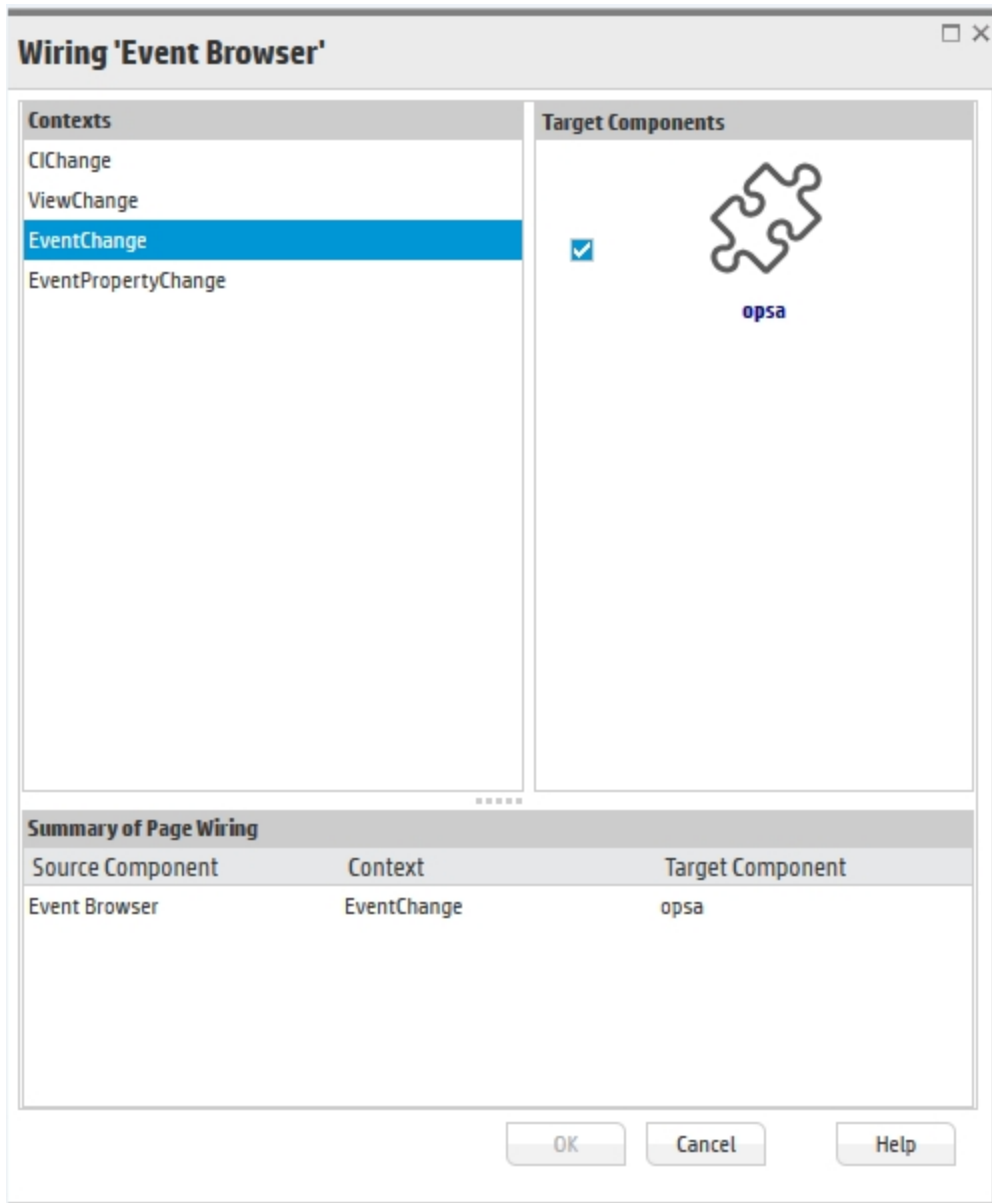
This procedure explains how to configure a dashboard that displays the event browser and the Operations Bridge Analytics user interface.

1. In OMi, create a new component with the name **opsa** and the url **opsa server FQDN:8080/opsa**.

Use the Configure Wiring section to append the URL you want to use when opening Operations Bridge Analytics. For example, the fragment `/dashboard&search=host%20withkey%20%22<<relatedCi.name >>%22` opens a dashboard focusing on a CI.



2. Create a new page, and add the component you just created, as well as the Event Browser component to the page.
3. Verify the wiring configuration for the page are as follows:



4. Save the page.
5. In Operations Bridge Analytics, locate `/opt/HP/opsa/jboss/standalone/deployments/opsa-ui-web.war/WEB-INF/web.xml`.

Modify the following section from:

```
<init-param>  
<param-name>X-Frame-Options</param-name>  
<param-value>SAMEORIGIN</param-value>  
</init-param>
```

to:

```
<init-param>  
<param-name>X-Frame-Options</param-name>  
<param-value>Allow-From http://<OMi URL>/opr-web</param-value>
```

6. Restart Operations Bridge Analytics by running the command **opsa-server restart**.
7. We recommend adding a mapping of the Operations Bridge Analytics IP and the Operations Bridge Analytics FQDN in the windows host file in every client machine that will be used to access Operations Bridge Analytics.
8. Delete the cookies of all browsers used to access OMi.
9. Add the FQDN of the Operations Bridge Analytics environment to the list of trusted hosts in OMi from the **Authentication Management** section.

#### Sending Events to HPE Operations Manager i (OMi)

You can configure an OMi Agent to retrieve alerts and anomalies from Operations Bridge Analytics and create events from them. This allows you to use the power of Operations Bridge Analytics to identify events using analytic tools while benefiting from OMi's advanced event management capabilities.

**Note:** For OMi to retrieve alerts and anomalies from Operations Bridge Analytics, you must be using OMi with Monitoring Automation (MA) capabilities and have the corresponding license installed in OMi.

**Note:** Details about procedures below that are performed in OMi and Operations Agent can be found in the OMi and Operations Agent documentation.

1. Connect the Operations Agent to your OMi server.

**Note:** The Operations Agent on all servers must be connected to OMi.

2. Import the content pack from the following location on the Operations Analytics server to OMi:

- **For OMi 9.2x**

`/opt/HP/opsa/content-packs/omi_content_pack/omi_092x_content_pack-3.00.zip`

- **For OMi 10**

`/opt/HP/opsa/content-packs/omi_content_pack/omi_100x_content_pack-3.00.zip`

This makes the management templates and aspect area available in the OMi user interface.

3. From OMi, assign and deploy the management templates and aspects to the Operations Analytics Server and Collector hosts.

All Operations Bridge Analytics alerts will now be retrieved by OMi.

# Chapter 19: Configure Log Integrations

We recommend using Operations Bridge Analytics to import logs directly from your source environment. However, we also support integrating with HPE ArcSight Logger or Splunk.

Log data can be imported from HPE ArcSight Logger or Splunk by configuring a Log Integration.

## Learn About

### About Importing Log Data

In order for Operations Bridge Analytics to import log data from Splunk or Logger, you must specify the hosts of the data sources and create mapping files. Mapping files specify how Operations Bridge Analytics should interpret the log data. For Splunk, these files are stored on the Operations Analytics Server. For Logger, these files must be manually copied to the Logger environment.

### Supported Configurations

Instances of Logger and Splunk are connected to Operations Analytics Collector hosts. The following limitations apply to combinations of instances:

- You can configure each instance of Logger on no more than one Operations Analytics Collector host.

## User Tasks

### How to Define your Log Data Source

The first step in importing log data is to define the data host or hosts.

1. Select **Data Manager**; then specify whether you will import data from **Logger Instances** or **Splunk Instances**.
2. Specify the details of one Logger or Splunk host.

3. Define additional sources as desired at any time by **Data Manager > Logger Instances** or **Data Manager > Splunk Instances**. If you are using Logger instances and want to improve collection performance in this area, follow the instructions in [Configuring Logger to Forward CEF Messages to Operations Analytics](#) to configure the **TCP Forwarding** feature on Logger.
4. Continue with the appropriate mapping procedure depending on your data source.
  - ["Map Arcsight Logger Data" below](#)
  - ["Map Splunk Data" on page 167](#)

## Map Arcsight Logger Data

If you are using an integration between Operations Bridge Analytics and HPE ArcSight Logger, have not configured a Connector for HPE ArcSight Logger, and want to configure a FlexConnector, you can use this section to create a flex configuration file. Flex configuration files are required when configuring FlexConnectors.


You can share the flex configuration files you create with the Operations Bridge Analytics Community and download files that have been shared by others.

**Note:** The flex configuration files that are created are only valid for FlexConnector types **Regex Log File** and **Regex Folder File**. To use this feature with other types of FlexConnectors, you can take the file created here and manually edit it as desired.

The processes in this section assume that you have installed Logger and FlexConnector, but have not yet configured the FlexConnector.

## User Tasks

### How to Create a FlexConnector Configuration File

1. Go to **Data Manager**; then select **Flex Configuration**.
2. Go to the **My Configuration Files** tab; then select .
3. Complete the Flex Configuration File Wizard:



### Select Sample File

**Sample log file.** Select a representative sample file that contains at least 1000 log messages and is less than 5 MB. It should contain a variety of log messages.

**Product name.** The name of the product that created the sample log file. It is used to help you identify which product is associated with this flex configuration file and this information helps log analytics to provide fine-tuned results per product.

### Line Parsing

In general, the individual log messages are automatically detected. The results are displayed in a table. If the results are accurate, click Next. Otherwise, specify a different method of line parsing by selecting **Adjust message breaking rule**.

- **Break on new line.** Uses line breaks to identify different log entries.
- **Break suggested by algorithm.** This is the default algorithm.
- **Log message starts with a pattern.** Use this to define a specific pattern that occurs at the beginning of each log entry.

### Mandatory Fields

Logger requires you to define a few fields such as Date and Time and Severity.

#### Define field by

For each of the four mandatory fields, you can define the field based on the following options:

#### By column selection

Specify a field by selecting the check box at the top of one or more columns from the table at the bottom of the user interface. Use this option if the field can be defined completely by one or more columns.

#### By text extraction

Specify a text selection from the table below. Use this option if the field can be defined by a part of one of the columns, but not a full column.

#### As fixed value


Specify a static value that will be used to define this field for every log entry.

#### By message arrival time

This option is only available for date and time field. It takes the date and time value from the time that log messages arrive in Logger.

By connector agent properties

This option is only available for the host field. It indicates the host of the smart connector should be used as the host of the log message.

Define the following four fields. When you are done completing each field click .

To modify a field that is already defined, click .

### Date and Time

UI Element	Description
Define field	See above
Example	Displays an example value for the field as you defined it.
Date & Time format	Enter the order and format of the date and time elements. For details about the meanings of date and time symbols, see <a href="#">"Date and Time Symbols" on page 166</a> .
Advanced definition	<p>You can see the field definition in HPE Logger syntax and manually edit it if required. The syntax is described in the Logger documentation about FlexConnector files.</p> <p><b>Note:</b> If you edit the expression, make sure that there is at least one set of parentheses and that the expression does not exceed 100 characters.</p>

### Severity

UI Element	Description
Define field	See above
Example	Displays an example value for the field as you defined it.
Advanced definition	You can see the field definition in HPE Logger syntax and manually edit it if required. The syntax is described in the Logger documentation about FlexConnector files.
Severity mapping	<p>Map at least two levels of severity. Fill in the fields with the text that is found in the log file that represents the severity and enter it in the appropriate column.</p> <p>Notes:</p>

, continued

UI Element	Description
	<ul style="list-style-type: none"> <li>○ Values are case sensitive, and spaces are considered part of the strings. Adding spaces before or after numbers may result in the numbers being misread as strings.</li> <li>○ You can specify a range of numbers only by specifying the lower number first as seen in the following example: 300..400</li> <li>○ Make sure that the different mapping values are unique and not overlapping. For example, if the value of one field is 300, and the value of a different field is 200..400, you will receive an error.</li> <li>○ Values that are unmapped will be mapped to severity "unknown".</li> <li>○ At least one value from the sample data must be mapped successfully to complete the wizard.</li> </ul>

Host

UI Element	Description
Define field	See above
Example	Displays an example value for the field as you defined it.
Advanced definition	You can see the field definition in HPE Logger syntax and manually edit it if required. The syntax is described in the Logger documentation about FlexConnector files.

Message Text

UI Element	Description
Define field	See above
Example	Displays an example value for the field as you defined it.
Advanced definition	You can see the field definition in HPE Logger syntax and manually edit it if required. The syntax is described in the Logger documentation about FlexConnector files.

Additional Fields

You can also define additional fields from the sample log file. The procedure is very similar to defining mandatory fields.

- a. Click  to define a new field.
- b. Select the desired field.
- c. Define the field by column selection, text extraction, etc. the same way that you defined the mandatory fields.

#### Preview and Save

This pane displays your sample log parsed according to the rules specified in the new Flex

Configuration file. Select  to create the file, or  to edit the file before publishing.

The file is created and can be downloaded to your local environment from the Flex Connector Utility. To use the file to configure a FlexConnector, see "[How to Configure FlexConnectors using FlexConnector Configuration Files](#)" below.

## How to Download a Flex Configuration File from the Operations Bridge Analytics Community

1. Go to **Data Manager**, then select **Flex Configuration**.
2. Select the **Community Configuration Files** tab and select any file.
3. To test whether a file will work on your data, select , and specify a sample log file. If you are satisfied with the results, **Download** the file at the end of the wizard. If you need to modify the file, select **Edit** and make any necessary modifications in the wizard before selecting **Download**.
4. To save a file from the community locally and make it accessible permanently in the **My Configuration Files** tab, select .

## How to Configure FlexConnectors using FlexConnector Configuration Files

This procedure assumes that you have installed Logger and FlexConnector, but have not yet configured the FlexConnector.

**Note:** The flex configuration files that are created by OBA are only valid for FlexConnector types **Regex Log File** and **Regex Folder File**.

1. Go to **Data Manager**, then select **Flex Configuration**.
2. Select a desired file from the **My Configuration Files** tab or from **Community Configuration**

**Files** tab and click .

3. Copy the file to the following directory on the machine where Flex Connector is installed:  
**<arcsight\_home>\current\user\agent\flexagent**
4. Run the HP ArcSight Connector Setup Wizard from the following location:

Windows:

**<arcsight\_home>\current\bin\runagentsetup.bat**

Linux:

**cd <arcsight\_home>/current/bin**

**./runagentsetup.sh**

5. Complete the wizard as appropriate for your FlexConnector configuration file. When specifying the Configuration Type, select **sdkfilereader**.

Once complete, data should start to flow to Logger.

For more details, see the *ArcSight FlexConnector Developer's Guide* and the *ArcSight SmartConnectors User's Guide*.

## How to Edit, Download, or Delete a Flex Configuration File

1. Go to **Data Manager**, then select **Flex Configuration**.
2. Select a desired file from the **My Configuration Files** tab or from **Community Configuration Files** tab.
3. Use the **Edit**, **Download**, and **Delete** buttons.

## How to Share your Flex Configuration Files to the Operations Bridge Analytics Community

1. Go to **Data Manager**, then select **Flex Configuration**.

2. From the **My Configuration Files** tab, select the file you want to share and click **Share**. You will see a message with instructions. After you click **OK**, a prepared email will open from your default email client.
3. Download the file to your local environment.
4. Attach the file to the email and add a description. If desired, you can also attach the sample log file you used to create the configuration file to the email as well.

## Reference

### Date and Time Symbols

The following symbols should be used when specifying the date and time format in the Flex Configuration File Wizard.

Symbol	Meaning	Presentation	Examples
G	Era designator	(Text)	AD
y	Year	(Number)	1996 or 96
M	Month in year	(Text & Number)	July or Jul or 07
w	Week in year	(Number)	27
W	Week in month	(Number)	2
D	Day in year	(Number)	129
d	Day in month	(Number)	10
F	Day of week in month	(Number)	2 (indicating 2nd Wed. July)
E	Day in week	(Text)	Tuesday or Tue
a	Am/pm marker	(Text)	AM or PM
H	Hour in day (0~23)	(Number)	0
k	Hour in day (1~24)	(Number)	24
K	Hour in am/pm (0~11)	(Number)	0
h	Hour in am/pm (1~12)	(Number)	12

, continued

Symbol	Meaning	Presentation	Examples
m	Minute in hour	(Number)	30
s	Second in minute	(Number)	55
S	Millisecond	(Number)	978
z	Time zone	(Text)	Pacific Standard Time or PST or GMT-08:00
Z	Time zone	RFC 822	-800 (indicating PST)

## Map Splunk Data

When using an integration between OBA and Splunk, log data is imported from Splunk, and Operations Bridge Analytics must map specific key columns to integrate the information. Each type of data can only be mapped once. You can add, delete, edit, and manage these mappings at any time. Data coming from Splunk is scanned, and unmapped source types are displayed here.

Activated mapping files map data coming from **all** configured Splunk instances in the **Splunk Instances** user interface. The files cannot be limited to specific Splunk instances.

**Note:** Logs originating from the OBA servers are not processed and sent to OBA when using Splunk. This is not the case for Logger.

**Note:** Unmapped source types are taken from a random sample of a few minutes of Splunk data. There may be other source types of data coming from Splunk that are not listed here.

## User Tasks

### How to Map a Source Type

1. Select **Data Manager**; then select **Splunk Source Type Mapping Wizard** and make changes in one of the following ways:

- o Select a line in the table whose Status is **Not Mapped** and click

Map

- o Select

New Source Type

- o Select a line whose Status is **Activated** and click Edit.

## 2. Complete the Source Type Mapping Wizard using the following guidelines

### Source Type Tab

**Source type.** If this is editable, specify the Splunk source type for the data you will map.

**Source.** Use this field if the specified source type has data coming in from multiple sources with different formats.

### Data Tab


This tab displays the latest data of the specified source type that was imported from Splunk.

If all the data is parsed without errors, you can continue to the next tab.

If you receive errors and lines are highlighted, it means that those lines could not be parsed. If you continue, data from those lines will not be imported to Operations Bridge Analytics. To resolve unparsed data, try one of the following strategies:

- o Go back and modify the source value in the previous tab.
- o Refine the sourcetype definitions in Splunk.

### Mandatory Fields Tab

You must define a few key fields by mapping them to portions of the incoming data or as fixed values. Specify any information required until there is a check  next to each mandatory field.

**Note:** We recommend not using data from the **Date and Time by Splunk** column to define part or all of the message text field.

Each field requires different information from the following list:

- o **Define field by:** For each of the mandatory fields, you can define the field based on the following options:

#### By column selection

Specify a field by selecting the check box at the top of one or more columns from the table at the bottom of the user interface. Use this option if the field can be defined completely by one or more columns.



#### By text extraction

Highlight a text selection from the table below. Use this option if the field can be defined by a part of one of the columns, but not a full column.

#### As fixed value

Specify a static value that will be used to define this field for every log entry.

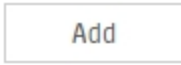
- **Example:** This displays an example of how the data would be mapped based on your definition.
- **Advanced definition.** You can see the field definition in Splunk syntax and manually edit it if required. The syntax is described in the Splunk.
- **Severity mapping.** Map at least two levels of severity. Fill in the fields with the text that is found in the log file that represents the severity and enter it in the appropriate column.

#### Notes:

- Values are case sensitive, and spaces are considered part of the strings. Adding spaces before or after numbers may result in the numbers being misread as strings.
- You can specify a range of numbers only by specifying the lower number first as seen in the following example: 300..400
- Make sure that the different mapping values are unique and not overlapping. For example, if the value of one field is 300, and the value of a different field is 200..400, you will receive an error.
- Values that are unmapped will be mapped to severity "unknown".
- At least one value from the sample data must be mapped successfully to complete the wizard.


#### Additional Fields

You can also define additional fields from the sample log file. The procedure is very similar to defining mandatory fields.

- a. Click  to define a new field.
- b. Select the desired field.
- c. Define the field by column selection, text extraction, etc. the same way that you defined the mandatory fields.

### Preview and Save

This pane displays your sample data mapped according to the rules you specified.

Select  to validate your settings, create and enable the mapping.

**Note:** Settings configured in all other tabs are verified at this stage.

3. If the messages coming from one Splunk source type have different formats and require multiple regular expressions, you can define additional regular expressions in the **conf/splunk/<tenant name>/sourcetype-<<splunk source type>>.properties** file, using the following example as a guide:


```
messageRegex=<Text>(P<messageText>.+)</Text>
messageRegex.2=<Summary>(P<messageSummary>.+)</Summary>
# first match wins
message=<<messageText>>|<<messageSummary>>
```

## How to Manually Add a Mapping File

You can take a mapping file that was manually created and add it to Operations Bridge Analytics.

1. Place the mapping file in the following directory:

```
<Opsa_HOME>\conf\splunk\<your_tenant_name>
```

2. Go to Log Integration  and select **Splunk Configuration**. You should see a line corresponding to the mapping file you added with a status of **Activated Manually**.

**Note:** You cannot edit mapping files with the status Activated Manually using the user interface.

## How to Edit a Mapping File

To edit mapping files that were not created manually, select **Data Manager**; select **Splunk Instances**; then click **Edit**.

**Note:** When editing, the wizard opens in the Mandatory Fields tab using the original data that was used to create the mapping file. If you want to use more up to date data, go back to the first tab of the wizard and start from there.

# Administration

This section contains the following topics:

["Administering Operations Bridge Analytics Performance" on page 172](#)

["Adding More Operations Bridge Analytics Servers" on page 187](#)

["Changing the Password of an Operations Bridge Analytics Collector Host" on page 188](#)

["Checking the Status of Operations And Operations Bridge Analytics Servers" on page 189](#)

["Configuring LDAP Server Authentication for Operations Bridge Analytics" on page 193](#)

["Content Packs " on page 197](#)

["Daylight Savings Time Codes" on page 199](#)

["Log Files in Operations Bridge Analytics" on page 211](#)

["Maintaining the Operations Bridge Analytics Database" on page 214](#)

["Manage Users and Tenants" on page 219](#)

["Modifying Unit Scaling on Collected Data" on page 233](#)

["Registering Operations Bridge Analytics Collector Hosts" on page 235](#)

["Resolve Host Aliases" on page 239](#)

["Troubleshooting" on page 249](#)

["Using Parametric Dashboards" on page 242](#)

## Chapter 20: Administering Operations Bridge Analytics Performance

Use the information in this section to adjust and maintain Operations Bridge Analytics performance.

### Improving Log Analytics Collection Performance

To improve Log Analytics Collection performance, you can choose to configure dedicated Operations Analytics Collector hosts for the data streaming component (Apache Storm).

To do this, disable Apache Storm on the Operations Analytics Collector hosts that have existing Log Analytics Collections configured.

1. On each Operations Analytics Collector host that has Log Analytics Collections configured, do the following:
  - a. Edit the following file: `/opt/HP/opsa/conf/deployment/opsa-deployment.xml`
  - b. Locate a line that looks similar to the following: `<process id="storm-supervisor" active="true" runsOnAppliance="Processing">`
  - c. Change **true** to **false** on that line as shown in the following bold text: `<process id="storm-supervisor" active="false" runsOnAppliance="Processing">`
  - d. Save your work.
2. On each Operations Analytics Collector host that has Log Analytics Collections configured, do the following to load the configuration change you just made:
  - a. Run the following command: `/opt/HP/opsa/scripts/opsa-deployment-manager.sh`
  - b. Run the following command: `/opt/HP/opsa/scripts/opsa-deployment-loader.sh`
3. On the Operations Analytics Server, do the following to resubmit the Storm topology:
  - a. Run the following command: `/opt/HP/ops/scripts/opsa-storm-kill-topology.sh`
  - b. Run the following command: `/opt/HP/ops/scripts/opsa-storm-submit-topology.sh`

After completing the above steps, you should see performance improvement in the Log Analytics Collections in which you made these changes.

# Increasing JVM Memory to Improve Collection Performance

Operations Analytics Collector hosts use more memory resource if they contain large numbers of collections or if the collections they contain are configured to frequently collect data. In Operations Analytics Collector hosts in either of these configurations, you might need to increase its JVM memory allocation.

To adjust the JVM memory allocation for an Operations Analytics Collector host, do the following:

1. As a root user, edit the `/opt/HP/opsa/conf/opsa-collector-env` file.
2. Change the `Xmx` value to 4096 or 8196, depending on how much resource your Operations Analytics Collector host is using.
3. Save your work.
4. As a root user, run the following command from the Operations Analytics Collector host:

```
$OPSA_HOME/bin/opsa-collector restart
```

Now the changes you made to the JVM memory allocation on the Operations Analytics Collector host are in place.

## Increasing the Index Entity Cache Size

Operations Bridge Analytics uses a repository for storing various configuration data. Operations Bridge Analytics tracks the usage of this memory and notifies you when it needs to increase in size.

The creation of keys and tags is important to keep the entity index size lower than the threshold. The entity index table is supposed to remain relatively small, and just contains keys for common data such as hostname, application, location, and other items. Creating wrong or incorrect keys and tags can cause the entity index key become too large. See ["Using Tags for Source Types" on page 136](#) for more information about correctly configuring keys and tags.

If Operations Bridge Analytics notifies you that you must increase the entity index size, do the following:

1. Run the following command:

```
select count(*) as count ,property_group_uid from opsa_default.entity_index
group by property_group_uid order by count desc
```

**Note:** The first rows show you which collection has been incorrectly defined.

2. Fix the keys used in the collection by using the instructions shown in ["Using Tags for Source Types" on page 136](#).

You need to register the collection with the right keys as follows:

**Note:** The entity\_index could be just truncated and the instructions in this step provide an option to run the job to remedy the issue.

3.
  - a. Access `http://<OpsaServer>:29902/mbean?objectname=OPSA-Infrastructure%3Aservice%3DSchedulerTaskManager`
  - b. displayJobsInfo
  - c. Entity Instance Loader Job
  - d. Execute Job now

The above steps, result in the recreation of the entity index table with the correct data (after you recreate one or more problem collections with the correct keys).

## Managing Collected Data File Usage with Existing Delete Policies

Operations Analytics Collector hosts store collected data on their file systems. Each Operations Analytics Collector host periodically runs a process controlled by **delete policies** to reduce the amount of stored data. You can adjust the parameters associated with these delete policies to better manage the data retained by each Operations Analytics Collector host.

To configure the parameters associated with these delete policies, do the following from each Operations Analytics Collector host you want to control:

1. Edit the `/opt/HP/opsa/conf/opsa-collector.properties` file.
2. Using the helpful comments that reside in the `opsa-collector.properties` file, remove the #

characters and set the desired parameters in the following lines:

```
#com.hp.opsa.collector.file.garbage.schedule.interval_min = 15
#com.hp.opsa.collector.file.garbage.diskfreepct.start = 30
#com.hp.opsa.collector.file.garbage.diskfreepct.stop = 50
#com.hp.opsa.collector.file.garbage.max.daysold = 5
#com.hp.opsa.collector.file.garbage.enabled = true
```

3. Save your work.
4. Run the following command from the Operations Analytics Collector host

```
$OPSA_HOME/bin/opsa-collector restart
```

Now the collected data on the Operations Analytics Collector hosts on which you made these changes are being managed by the newly adjusted parameters for these delete policies.

Although you can adjust parameters for the existing delete policies, you cannot add new delete policies or modify the functionality of the existing delete policies. The remainder of this section explains the static behavior of the existing delete policies.

Each Operations Analytics Collector host contains the following delete policies.

- DELETE\_ALWAYS : Delete the files if it exists.
- DELETE\_LOW\_FREE : Delete the files if the free disk space is low.
- DELETE\_WHEN\_OLD: Delete the file if it is old.

Each Operations Analytics Collector host is configured as shown in ["Delete Policies by Folder" below](#).

#### Delete Policies by Folder

Folder	Delete Policy
/opt/HP/opsa/data/archive	DELETE_WHEN_OLD & DELETE_LOW_FREE
/opt/HP/opsa/data/failed_to_load	DELETE_LOW_FREE
/opt/HP/opsa/data/load	DELETE_WHEN_OLD
/opt/HP/BSM/PMDB/extract	DELETE_ALWAYS

## Monitoring Operations Bridge Analytics Processes

Operations Bridge Analytics provides the `opsa` script to check status or control Operations Bridge Analytics services. See the `opsa` reference page (or the Linux man page) for more information.

Operations Bridge Analytics depends on several different services to be active on the deployed Operations Analytics Server and Collector hosts. These services start automatically when booting up your Operations Analytics Server and Collector hosts (you do not need to specifically configure these services).

You can use the `opsa` script to do several things:

- Run the `$OPSA_HOME/bin/opsa status` command script to check the status of all of these services at once.
- When necessary, you can control all of the Operations Bridge Analytics-related services on any Operations Analytics Server and Collector hosts (for example, in preparation for installing a software patch):
  - Start Operations Bridge Analytics services: `$OPSA_HOME/bin/opsa start`
  - Stop Operations Bridge Analytics services: `$OPSA_HOME/bin/opsa stop`

**Note:** A network disruption can cause Operations Bridge Analytics services to stop functioning. If you suspect that the Operations Analytics Server and Collector hosts lost connectivity to the network, you might restart them using `$OPSA_HOME/bin/opsa restart` command.

Operations Bridge Analytics also provides the `opsa-process-manager.sh` script to stop and start the Operations Bridge Analytics Process Manager service on a single Operations Analytics Server or Operations Analytics Collector host. You can also use the `opsa-process-manager.sh` script to monitor Operations Bridge Analytics processes. See the `opsa-process-manager.sh` reference page (or the Linux man page) for more information.

**Note:** It is common for users to manually manage all the Operations Bridge Analytics processes together by using the `opsa` script. It is also possible for users to stop and start individual components using commands such as `opsa-server` or `opsa-collector`. The `opsa-process-manager.sh` script recognizes the processes that users manually stop and does not attempt to restart these processes.

**Note:** A network disruption can cause this process management feature to stop functioning. If you suspect that the Operations Analytics Server and Collector hosts lost connectivity to the network, restart them as detailed in ["Restarting the Operations Bridge Analytics Server and Operations Bridge Analytics Collector Host"](#) on page 180 after the network connectivity is restored.

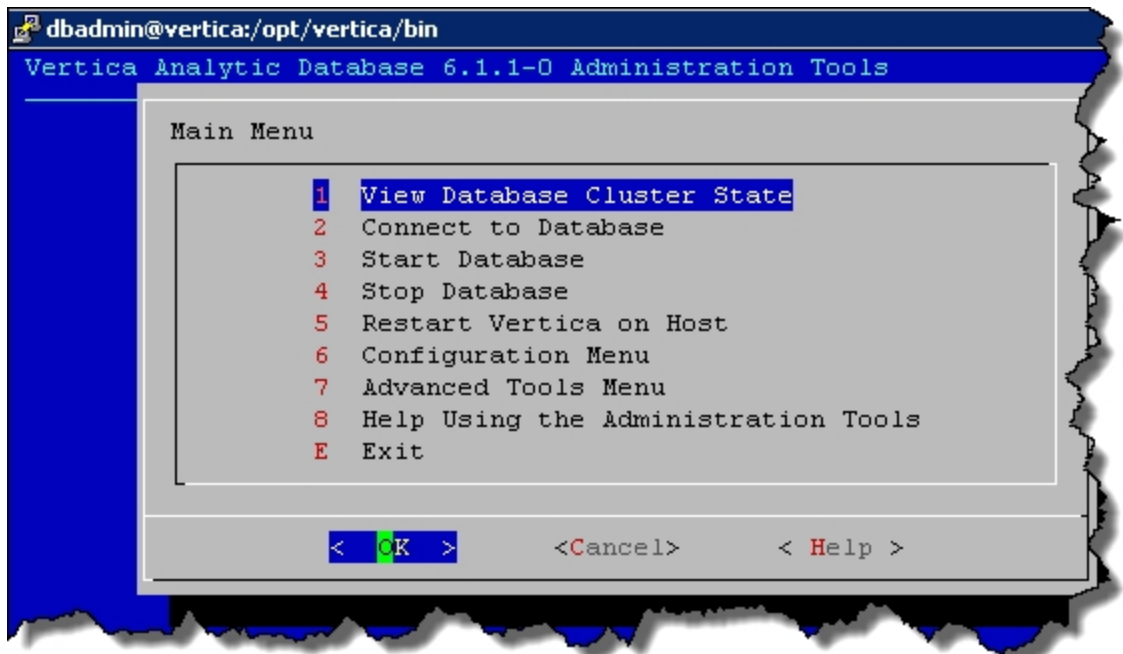


## Restarting Operations Bridge Analytics Processes

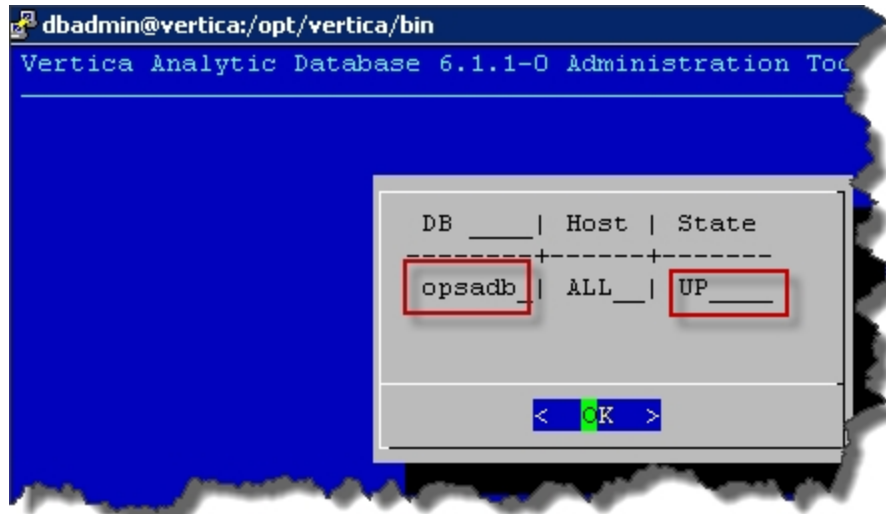
There are times when the Operations Bridge Analytics might abruptly shut down, as in during a power outage, network issue, or other unintended shutdown. For the Operations Bridge Analytics processes to function correctly, the Vertica database must completely start up before restarting the Operations Bridge Analytics processes. If the Vertica database is not available when the Operations Bridge Analytics processes start up, these processes might not function correctly.

To make sure the Operations Bridge Analytics processes start up correctly, do the following:

1. Do the following on the Vertica server to check the database:
  - a. Run the `su -dbadmin` command.
  - b. Run the `/opt/vertica/bin/adminTools` command. You should see a screen similar to the following:



- c. Enter 1 to view the state of the database; then click **OK**. You should see a screen similar to the following if the opsadb database is running:



- d. Click **OK** twice to exit the adminTools interactive command.
- e. If the database is not up, wait a few minutes, then rerun the previous steps to recheck the database.

**Note:** Do not start the Operations Bridge Analytics processes until the Vertica database is running.

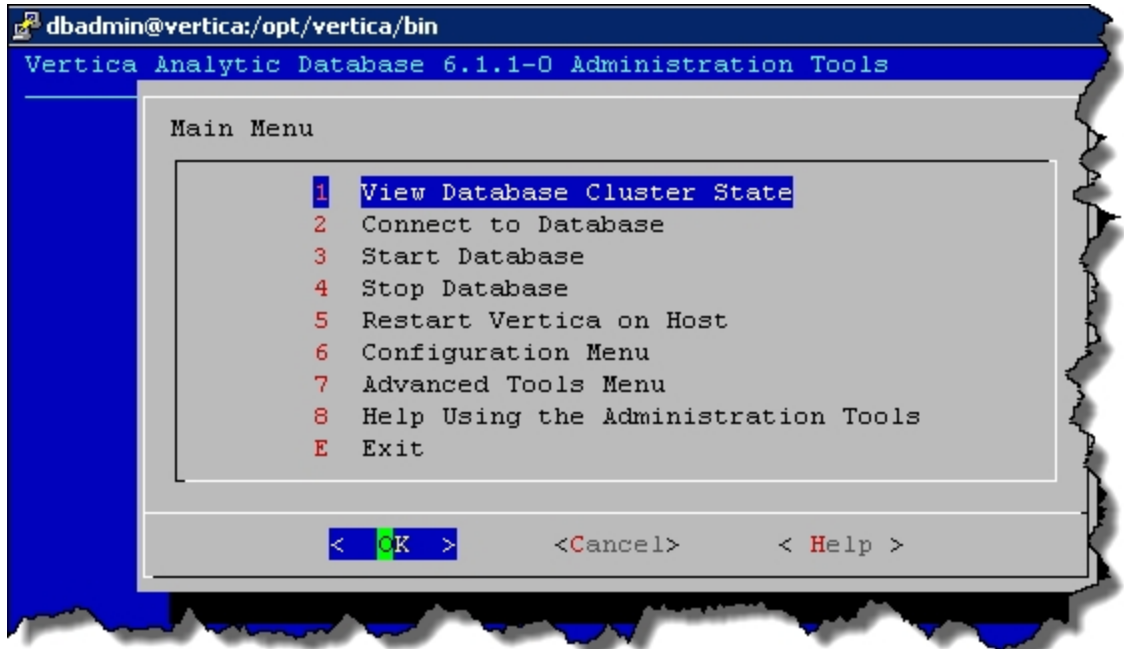
- Run the `opsa status` command on the Operations Analytics Servers and all of the Operations Analytics Collector hosts. For each server that does not have processes running, run the `opsa start` command.
- After five minutes, check to see that you can open the Operations Bridge Analytics console.

## Restarting Operations Bridge Analytics Processes after a Vertica Shutdown

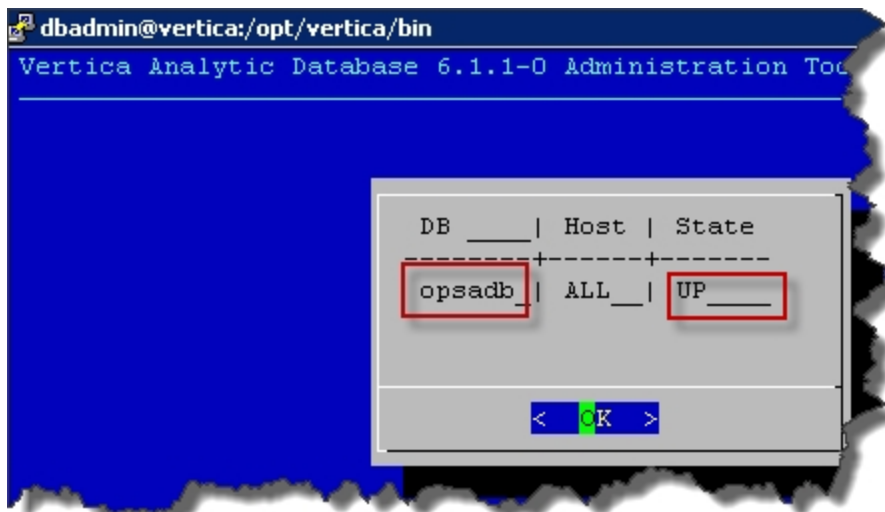
There are times when the Operations Bridge Analytics might abruptly shut down, as in during a power outage, network issue, or other unintended shutdown. For the Operations Bridge Analytics processes to function correctly, the Vertica database must completely start up before restarting the Operations Bridge Analytics processes. If the Vertica database is not available when the Operations Bridge Analytics processes start up, Operations Bridge Analytics might not function correctly.

To make sure the Operations Bridge Analytics processes start up correctly, do the following:

1. Do the following on the Vertica server to check the database:
  - a. Run the `su -dbadmin` command.
  - b. Run the `/opt/vertica/bin/adminTools` command. You should see a screen similar to the following:



- c. Enter 1 to view the state of the database; then click **OK**. You should see a screen similar to the following if the opsadb database is running:



- d. Click **OK** twice to exit the adminTools interactive command.
- e. If the database is not up, wait a few minutes, then rerun the previous steps to recheck the database.

**Note:** Do not start the Operations Bridge Analytics processes until the Vertica database is running.

2. Run the `opsa status` command on all of the Operations Analytics Server and Collector hosts. For each server that does not have processes running, run the `opsa start` command.
3. After five minutes, check to see that you can open the Operations Bridge Analytics console.

## Restarting the Operations Bridge Analytics Server and Operations Bridge Analytics Collector Host

**Restarting the Operations Analytics Server and the Operations Analytics Collector Host:** If you suspect that Vertica has stopped functioning (such as during a power outage, network outage, or other software disruption), you can restart the Operations Bridge Analytics services on the Operations Analytics Server and Collector hosts. The symptom you might see is that new data is no longer being collected with old data still available for viewing.

To restart the Operations Analytics Server and Collector hosts, do the following on each server:

```
$OPSA_HOME/bin/opsa restart
```

See the `opsa` reference page (or the Linux man page) for more information.

## Throttling Operations Bridge Analytics Network Traffic

The logs and events Operations Bridge Analytics collects results in an increase in network traffic. The Operations Analytics Data Pipe uses an open source data collection engine, Elastic Logstash (Logstash), to collect these logs and events. To help you manage this increase in network bandwidth usage, Operations Bridge Analytics provides a throttling mechanism that limits the maximum count of events that the Operations Analytics Data Pipe sends each second.

**Caution:** Only configure and use throttling to limit data spikes. If you configure throttling so that the outgoing event rate is lower than the average incoming event rate, doing so leads to data loss. For example, log files could be overwritten or rotated out before Operations Bridge Analytics fully processes them.

To configure the network traffic throttling mechanism, do the following:

1. Edit one of the following files on the server housing the Operations Analytics Data Pipe. Edit this file as the Administrator user on Windows or the root user on Linux:

**Windows:** %installdir%\outpost\conf\outpostconfig.properties

**Linux:** /opt/HP/opsa/outpost/conf/outpostconfig.properties

2. Using the example shown in this step, change the following properties:
  - Set the `logstash.properties.throttleEnabled` property value to `true` to enable throttling. While this property is set to `false`, Operations Analytics Data Pipe sends data as fast as it can.
  - Set the `logstash.properties.eventRate` property value to the number of events per second that you want the throttle to permit. For this example, this property value is set to 100,000 events per second. If throttling is disabled (`logstash.properties.throttleEnabled` property value is set to `false`), the `logstash.properties.eventRate` property is ignored.

**Example:**

```
# output throttling configuration. Event rate is measured in events per second.
logstash.properties.throttleEnabled=false
logstash.properties.eventRate=100000
```

3. Restart the `opsa-outpost` service as the Administrator user on Windows or the root user on Linux:
  - **Windows:** Do one of the following:
    - Restart the `opsa-outpost` Service:
      - A. Open the Services program (**Task Manager > Services tab > Services**)
      - B. Locate the **Operations Analytics Data Pipe** Service
      - C. Right-click the **Operations Analytics Data Pipe** Service
      - D. Select **Restart**
    - Restart the `opsa-outpost` service using a command line:
      - A. Open a command window.
      - B. Run the following command to stop the service:
 

```
net stop "Operations Analytics Logstash Service"
```

C. Run the following command to start the service:

```
net start "Operations Analytics Logstash Service"
```

- **Linux:** Run the following command:

```
service opsa-outpost restart
```

After completing the steps shown earlier, the throttling mechanism limits the maximum count of events that Logstash sends each second.

## Tuning Apache Kafka Processes

Apache Kafka is the messaging system that Operations Bridge Analytics uses for its collection processes. If you hover your mouse over or click a red alarm bell at the top right in the Operations Bridge Analytics console and see a message stating that the Kafka processes are not balanced, you must tune and maintain Apache Kafka configurations as explained below.

**Note:** After you complete the appropriate action as shown below and refresh the Operations Bridge Analytics console (or restart Operations Bridge Analytics), the notification is cleared.

## Expanding the Apache Kafka Cluster in Operations Bridge Analytics

To add a server to a Kafka cluster, assign it a unique broker id and start up Kafka on the new servers. These new servers will not automatically be assigned any data partitions, so unless you move partitions to them, they will not do any work until new topics are created. After you add one or more servers to the Kafka cluster, you might want to migrate some existing data to these servers.

To migrate data to one or more newly added Kafka cluster servers, you manually initiate a fully automated process that does the following:

- Kafka adds the new server as a follower of the partition it is migrating.
- Kafka permits the new server to fully replicate the existing data in that partition.
- After the new server has fully replicated the contents of this partition and joined the in-sync replica, one of the existing replicas will delete their partition's data.

You can use the `opsa-kafka-partition-reassignment-tool.sh` script to move partitions across brokers. An ideal partition distribution would ensure that an even data load and partition sizes exist across all brokers. The `opsa-kafka-partition-reassignment-tool.sh` script does not have the capability to automatically evaluate the data distribution in a Kafka cluster and move partitions around to attain an even load distribution. As such, the Kafka administrator must figure out which topics or partitions should be moved around.

You can run the `opsa-kafka-partition-reassignment-tool.sh` script in six mutually exclusive modes:

- `-auto-execute`: In this mode, the tool initiates the reassignment automatically and exits after it is finished.
- Use the following modes when you would like more control on the reassignment:
  - `-auto-verify`: In this mode, the `opsa-kafka-partition-reassignment-tool.sh` script verifies the status of the reassignment for all partitions listed during the last `-execute`. The `opsa-kafka-partition-reassignment-tool.sh` script monitors the progress contiguously until the reassignment is complete.
  - `-execute`: In this mode, the `opsa-kafka-partition-reassignment-tool.sh` script initiates the reassignment of partitions based on the user provided reassignment plan.
  - `-generate`: In this mode, given a list of topics and a list of brokers, the `opsa-kafka-partition-reassignment-tool.sh` script generates a candidate reassignment to move all partitions of the specified topics to the new brokers. This option provides a convenient way to generate a partition reassignment plan given a list of topics and target brokers.
  - `-rollback`: In this mode, the `opsa-kafka-partition-reassignment-tool.sh` script initiates the rollback of the reassignment of partitions based on the user provided reassignment plan.
  - `-verify`: In this mode, the `opsa-kafka-partition-reassignment-tool.sh` script verifies the status of the reassignment for all partitions listed during the last `-execute`. The status can be either of successfully completed, failed, or in progress.

See the *opsa-kafka-partition-reassignment-tool.sh* reference page (or the Linux man page) for more information.

### **Automatically migrating data to new machines**

Use the `opsa-kafka-partition-reassignment-tool.sh` script to move some topics off of the current set of brokers to the newly added brokers. This approach is more useful when you expand an existing cluster than when you move one partition at a time, since it is easier to move entire topics to the new set of brokers.

For a more automated approach to do this, use the `-auto-execute` option when using the `opsa-kafka-partition-reassignment-tool.sh` script. For example, run the following command to automatically reassign all partitions for all kafka topics between all the brokers:

```
$ $OPSA_HOME/bin/opsa-kafka-partition-reassignment-tool.sh -auto-execute -username
opsatenantadmin -password opsatenantadmin
```

After the above command completes, all partitions for all topics will be balanced on all the brokers.

There is also a more detailed approach. When using the `opsa-kafka-partition-reassignment-tool.sh` script to move some topics off of the current set of brokers to the newly added brokers, provide a list of topics that should be moved to the new set of brokers and a target list of new brokers. The `opsa-kafka-partition-reassignment-tool.sh` script evenly distributes all partitions for the given list of topics across the new set of brokers. During this move, the replication factor of the topic is kept constant. Effectively the replicas for all partitions for the input list of topics are moved from the old set of brokers to the newly added brokers.

For example, the following example moves all partitions for topics `foo1` and `foo2` to the new set of brokers 5 and 6. At the end of this move, all partitions for topics `foo1` and `foo2` will only exist on brokers 5 and 6.

1. Run the following command:

```
$ $OPSA_HOME/bin/opsa-kafka-partition-reassignment-tool.sh -generate -username
opsatenantadmin -password opsatenantadmin
```

2. Look for results similar to the following:

```
OPSA_HOME is set to /opt/HP/opsa
Kafka partition reassignment generate started...
Kafka partition reassignment generate finished successfully
```

3. Review the following three files in the `/opsa/kafka/bin` directory. These files are created when using the `-generate` option with the `opsa-kafka-partition-reassignment-tool.sh` script:
  - `topics-to-move.json`: This file contains a list of all of the topics that should be moved.
  - `expand-cluster-reassignment-rollback.json`: - This file contains the current partition reassignment configuration to be used in the case of a rollback.
  - `expand-cluster-reassignment.json`: This file contains the proposed partition reassignment configuration.

Example:

Current partition replica assignment

```
{"version":1,
"partitions":[{"topic":"foo1","partition":2,"replicas":[1,2]},
```



```
{
  "topic": "foo1", "partition": 0, "replicas": [3,4]},
  {"topic": "foo2", "partition": 2, "replicas": [1,2]},
  {"topic": "foo2", "partition": 0, "replicas": [3,4]},
  {"topic": "foo1", "partition": 1, "replicas": [2,3]},
  {"topic": "foo2", "partition": 1, "replicas": [2,3]}
}
```

#### Proposed partition reassignment configuration

```
{
  "version": 1,
  "partitions": [
    {"topic": "foo1", "partition": 2, "replicas": [5,6]},
    {"topic": "foo1", "partition": 0, "replicas": [5,6]},
    {"topic": "foo2", "partition": 2, "replicas": [5,6]},
    {"topic": "foo2", "partition": 0, "replicas": [5,6]},
    {"topic": "foo1", "partition": 1, "replicas": [5,6]},
    {"topic": "foo2", "partition": 1, "replicas": [5,6]}
  ]
}
```

4. Run the following command to initiate the reassignment of partitions based on the user provided reassignment plan:

```
$OPSA_HOME/bin/opsa-kafka-partition-reassignment-tool.sh -execute -username
opsatenantadmin -password opsatenantadmin
```

5. Look for results similar to the following:

```
Kafka partition reassignment execute started...
Kafka partition reassignment execute finished successfully
```

6. Run the following command to verify the status of the reassignment:

```
$OPSA_HOME/bin/opsa-kafka-partition-reassignment-tool.sh -verify -username
opsatenantadmin -password opsatenantadmin
```

7. Considering the example being followed, the result would look similar to the following:

```
Kafka partition reassignment verify started...
Status of partition reassignment:
Reassignment of partition [foo1,0] completed successfully
Reassignment of partition [foo1,1] is in progress
Reassignment of partition [foo1,2] is in progress
Reassignment of partition [foo2,0] completed successfully
Reassignment of partition [foo2,1] completed successfully
```

```
Reassignment of partition [foo2,2] completed successfully
Kafka partition reassignment verify finished successfully
```

See the *opsa-kafka-partition-reassignment-tool.sh* reference page (or the Linux man page) for more information.

## Tuning Apache Kafka Disk Partition Capacity

Apache Kafka is the messaging system that Operations Bridge Analytics uses for its collection processes. As you add more collections to Operations Bridge Analytics, the utilization of the Kafka repository at `opt/HP/opsa/data/kafka` increases. If the `/opt/HP/opsa/data/kafka` partition approaches 100% utilization you must adjust the number of days that data is being retained. An optimal value of data to retain should be 80% or less of the disk capacity.

To define the retention policy so that disk capacity doesn't exceed 80%, do the following:

1. Edit the `/opt/HP/opsa/conf/deployment/opsa-deployment.xml` file.
2. Complete only one of the following actions to set the retention policy to meet your needs:
  - **Base the retention policy on time:** Set the `log.retention.hours` parameter to a value less than the default of 168. This value is in hours.
  - **Base the retention policy on size:** Set the `log.retention.bytes` and `log.segment.bytes` parameters to identical values. These values reflect the size per topic, and the default value is 2 GB per topic.
3. Save your changes.
4. Run the following commands to restart the kafka process and commit your changes:
  - a. `/opt/HP/opsa/scripts/opsa-deployment-manager.sh`
  - b. `/opt/HP/opsa/scripts/opsa-deployment-loader.sh`
  - c. `/opt/HP/opsa/bin/opsa-kafka restart`

Continue to monitor the `/opt/HP/opsa/data/kafka` partition and make additional changes if it begins to exceed 80% disk capacity.

## Chapter 21: Adding More Operations Bridge Analytics Servers

As your Operations Bridge Analytics environment expands, you might need to add more Operations Analytics Servers. Operations Bridge Analytics supports a maximum of three Operations Analytics Servers. To add another Operations Analytics Server, do the following:

1. Install a new Operations Analytics Server as shown in the *HPE Operations Bridge Analytics Installation Guide*.
2. Run the `$OPSA_HOME/bin/opsa-server-postinstall.sh -scaleout` command to add the new Operations Analytics Server. See the *opsa-server-postinstall.sh* reference page (or the Linux man page) for more information.

**Note:** After the `opsa-server-postinstall.sh` command completes, the passwords for the `opsa`, `opsatenantadmin`, and `opsaadmin` users (on the added servers) match the passwords you set when you installed the original Operations Analytics Server.

3. Reboot all of the Operations Analytics Servers.
4. After all of the Operations Analytics Servers finish rebooting, you must reboot all of the Operations Analytics Collector hosts so they can identify the newly added Operations Analytics Server.

After completing the above steps, the newly added Operations Analytics Server should be ready to use.

## Chapter 22: Changing the Password of an Operations Bridge Analytics Collector Host

After registering an Operations Analytics Collector host you might need to change its password because of your security policy or for other reasons. You might have Source Data from Source Types that you do not want to lose.

To safely change the password of a registered Operations Analytics Collector host, do the following:

1. Open the RTSM JMX console using the following URL:

```
http://<fully-qualified domain name of the Collector Host>:29900/mbean?objectname=com.hp.opsa.collector.http.server%3Aname%3DCollectorRestServer
```

2. From the `CollectorRestServer` interface invoke `changeCollectorPassword`.
3. Type the new password twice in the parameter form fields.

## Chapter 23: Checking the Status of Operations And Operations Bridge Analytics Servers

### Configuring Operations Analytics Health

To configure Operations Bridge Analytics to monitor its own active components, do the following:

1. Make sure the Operations Bridge Analytics software is installed and configured as shown in the *HPE Operations Bridge Analytics Installation Guide*:
  - a. Vertica: See *Task 2: Installing and Configuring the Vertica Software* in the *HPE Operations Bridge Analytics Installation Guide*.
  - b. Operations Analytics Server: See *Task 3: Installing and Licensing the Operations Bridge Analytics Server using the VMware vSphere Client* in the *HPE Operations Bridge Analytics Installation Guide*.
  - c. Operations Analytics Collector Host: See *Task 4: Installing and Configuring the Operations Bridge Analytics Collector Host using the VMware vSphere Client* in the *HPE Operations Bridge Analytics Installation Guide*.

2. Edit the `/etc/yum.conf` file and add the proxy information for your network. Your entry should look similar to the following:

```
# The proxy server - proxy server:port number
proxy=http://mycache.mydomain.com:3128
# The account details for yum connections
proxy_username=yum-user
proxy_password=qwerty
```

Save your work.

3. Install Operations Agent on the Vertica database server using the information shown in the [Operations Agent and Infrastructure SPIs Installation Guide](#).
4. Configure the syslogs from the Vertica database server, the Operations Analytics Collector host, and the Operations Analytics Server to forward to the Operations Analytics Data Pipe server by appending `"*.* @<logger_hostname>:515"` to the `/etc/rsyslog.conf` file.)
5. Run the following command to restart the `rsyslog` service:

```
service rsyslog restart
```

Operations Bridge Analytics provides two methods for checking the status of servers running the Operations Bridge Analytics service:

## Command Line Interface

The table below describes the commands used to check the status of Operations Bridge Analytics:

Command	Description
<code>\$OPSA_HOME/bin/opsa-collection-config.sh -list -collectorhost &lt;collector hostname&gt; -username opsatenantadmin</code>	Run from an Operations Analytics Server to list the collections deployed to that Operations Analytics Collector host
<code>opsa-server status</code>	Check the status of the Operations Bridge Analytics service  <b>Note:</b> The <code>opsa-server</code> command must be run on the Operations Bridge Analytics server.
<code>opsa-collector status</code>	Checks the status of the collector service on the Collector Appliance.  <b>Note:</b> The <code>opsa-collector</code> command must be run on the Operations Bridge Analytics Collector Appliance.
<code>opsa-loader status</code>	Checks the status of the loader service on the Collector Appliance.  <b>Note:</b> The <code>opsa-loader</code> command must be run on the Operations Bridge Analytics Collector Appliance.

## OpsA Health Dashboard

Use the **OpsA Health** dashboard to investigate the health of the Operations Bridge Analytics servers. The table below describes the query panes available.

**Note:** If you view the message that no data is available, this might mean you do not have the required software to collect the expected data. See the **Required Software** column of the table below.

Query Pane	Description	Required Software
Host System Metrics over Time	<p>Use this visualization to determine server health for the Operations Bridge Analytics servers.</p> <p>Shows the average value over time for the following metrics for each server running the Operations Bridge Analytics service:</p> <ul style="list-style-type: none"> <li>• System up time</li> <li>• CPU utilization</li> </ul>	HP Operations Agent
Service Topology	<p>Use this visualization to determine the servers running Operations Bridge Analytics software.</p> <p>Shows topology information for the Operations Bridge Analytics service, including the following servers:</p> <ul style="list-style-type: none"> <li>• Operations Bridge Analytics server</li> <li>• Operations Bridge Analytics collector servers</li> <li>• HPE Operations Analytics Data Pipe servers</li> <li>• HPE Vertica database servers</li> </ul> <p>Also shows the CPU utilization and system up time for each of the Operations Bridge Analytics servers.</p>	Operations Bridge Analytics only
Collected Metric - Row Counts	Shows a row for the data being collected by each configured collection.	
Configured Collections Dictionary	Shows a table of information that includes collection property information for each collector host.	
Log Messages (100+)	<p>Use this visualization to troubleshoot any Operations Bridge Analytics log file error messages.</p> <p>Shows all log file messages for servers running the Operations Bridge Analytics service.</p> <p>Shows the results from the self-monitoring feature. It contains all log information from the Operations Analytics Server and Collector hosts that are running self-monitoring.</p>	Operations Bridge Analytics only

#### Additional Information About the OpsA Health Dashboard

The **OpsA Health** dashboard contains predefined panels to help you assess the health of your Operations Bridge Analytics servers and integrations. The top panels in the display show Operations Agent performance data from hosts that are in the Operations Bridge Analytics Service Topology definition. Nodes that are configured as part of the Operations Bridge Analytics Service Topology

include your Operations Analytics Servers, Operations Analytics Collector hosts, and Vertica database hosts.

The **Host System Metrics Over Time** pane shows metrics such as cpu and peak disk utilization from Operations Agent data being collected on hosts in the Operations Bridge Analytics Service Topology.

The **Service Topology** pane shows a pie-chart view of performance metrics from Operations Agent for the Operations Analytics Server and Collector hosts.

The **Row Count of Collected Metrics and Log** pane is useful for confirming that the collections are running as expected. As you configure additional Operations Bridge Analytics collections, the number of collections shown in this **Row Count of Collected Metrics and Log** pane increases.

For usability, augment the color coding by selecting the **Show Values** checkbox on the right. Hover over the left side collection labels to bring up a screen tip showing the full name of each collection. Without any configuration applied, you will see the following entries: "log\_group\_0\_metrics", "log\_group\_1\_metrics", and "log\_group\_2\_metrics". These entries are automatically generated collections related to the log file tracking facility.

An "opsa\_collection\_alerts" entry in the table tracks triggered alerts seen over time. If you configure Operations Agent collections, you will see "OA\_sysperf\_global" values coming in every 15 minutes, adding three rows for each Operations Agent node from which you collect data. Each additional collection adds more lines to this health display, although it may take up to 15 minutes after you configure a new collection for data to show up in this dashboard.

**Note:** A SiteScope collection may add up to 50 rows to this panel, which can make it more complicated to navigate. To make this easier, use the **Resize Pane > Increase Height** function in the upper right of the **Row Count of Collected Metrics and Log** pane to increase the pane height. Doing so reduces the number of pages you must navigate through using the page control on the lower right.

The next pane in the dashboard, **Configured Collections Dictionary**, shows a table of information that includes collection property information for each Operations Analytics Collector host.

The last pane, **Log Messages(100+)**, shows the results from the self-monitoring feature. It contains all log information from the Operations Analytics Server and Collector hosts that are running self-monitoring.



# Chapter 24: Configuring LDAP Server Authentication for Operations Bridge Analytics

The Operations Bridge Analytics console supports Lightweight Access Directory Protocol (LDAP) for user authentication. The instructions in this section explain how to configure Operations Bridge Analytics to connect to an LDAP server to validate Operations Bridge Analytics users.

**Important:** Only a Super Admin User, opsadmin by default, can configure Operations Bridge Analytics to authenticate users through an LDAP Server.

The instructions in this section assume the following:

- One or more LDAP servers are presently configured and successfully being used in your environment.


**Note:** Operations Bridge Analytics does the following to authenticate users when multiple LDAP servers exist:

- Operations Bridge Analytics does not contact LDAP servers in any specific order.
- Operations Bridge Analytics sequences through the LDAP servers until it successfully authenticates the user or it reaches the end of the list.

- You are able to log on to the Operations Analytics Server as a opsadmin user.
- You have information about the LDAP credentials and its internal hierarchy (group structure).

You can configure LDAP server authentication using one of two methods:

From the Operations Bridge Analytics console

1. Click  **Settings**, then select **LDAP Servers**.
2. Click **Add**, then enter information into the form.

**Note:** If you do not specify the optional LDAP integration username and LDAP integration user password during this LDAP configuration, anonymous binding must be enabled on the LDAP Servers.

**Tip:** For descriptions of the entry fields, hover over the  icons shown in the Operations


Bridge Analytics console.

If you select the **Use secure connection** option, complete the following steps before continuing.

To configure SSL for LDAP server authentication, do the following:

- a. Copy the LDAP's root server certificate to the Operations Bridge Analytics servers and give the file full permissions.
- b. Run the `opsa-server-manager.sh` script.
  - i. Log on as the `opsadmin` user.
  - ii. Choose **Option 2** to configure SSL.
  - iii. Choose **Option 4** to import the trusted certificate into the OpsA truststore.
  - iv. Enter the file name of the certificate you want to import; then press **Enter**.
  - v. Repeat the prior steps for additional certificate files you want to import.
  - vi. Choose **Option 6** from the main menu to restart the Operations Analytics Server.
  - vii. Exit the `opsa-server-manager.sh` script.
3. Although optional, it is a best practice to click **Validate** to test the connection to the LDAP server before adding the LDAP server in the next step.
4. After you are satisfied with your entries, click **Add** to finish the LDAP configuration.
5. Using the Users Manager in the Operations Bridge Analytics console, create an Operations Bridge Analytics user that uses an LDAP server for authentication. In this case you do not need to create a password when creating this user.

**Note:** You must belong to either the Super Admin or Tenant Admin user group to access the Users Manager.

6. Optional Step: Click  **Settings**, then select **LDAP Group Mapping** in the Operations Bridge Analytics console. Enter information into this form to provide mapping that enables automatic user profile creation in Operations Bridge Analytics after the LDAP Authentication during a user's first log on.

**Note:** You must belong to the Tenant Admin user group to access **LDAP Group Mapping**.

#### Using a Command Line

1. Run the following command to save the LDAP server configuration information to Operations Bridge Analytics:

```
$OPSA_HOME/bin/opsa-ldap-configuration-manager.sh add --username <opsa_
superadmin_username> --password <opsa_superadmin_password> --ldapusername
<ldap_username> --ldappassword <ldap_password> --ldaphostname <ldap_hostname>
--ldapbasedn <ldap_basedn> --ldapport <port> --userdn <userdn> --ssl [true
| false]
```

**Note:** The add option is used to add the LDAP server configuration information to Operations Bridge Analytics. All of the Operations Bridge Analytics users are authenticated by communicating to this LDAP server based on the additional configuration input. For example, notice the `ldap-basedn` and `userdn` attributes used in this example.

**Note:** If you do not specify the optional LDAP integration username and LDAP integration user password during this LDAP configuration, `anonymous` binding must be enabled on the LDAP Servers.

**Note:** User Naming attributes: `userPrincipalName` and `sAMAccountName` are supported for the `userdn` in the LDAP configuration.

**Tip:** If an SSL encrypted communication to LDAP server is required, the following default values are used: `--ldapport 636` and `--ssl true`. Otherwise the default values are `--ldapport 389` and `--ssl false`.

If you select the **Use secure connection** option, complete the following steps before continuing.

To configure SSL for LDAP server authentication, do the following:


- a. Copy the LDAP's root server certificate to the Operations Bridge Analytics servers and give the file full permissions.
- b. Run the `opsa-server-manager.sh` script.
  - i. Log on as the `opsaadmin` user.
  - ii. Choose **Option 2** to configure SSL.
  - iii. Choose **Option 4** to import the trusted certificate into the OpsA truststore.
  - iv. Enter the file name of the certificate you want to import; then press **Enter**.
  - v. Repeat the prior steps for additional certificate files you want to import.
  - vi. Choose **Option 6** from the main menu to restart the Operations Analytics Server.
  - vii. Exit the `opsa-server-manager.sh` script.

2. Run the following command to check that the LDAP information you added to Operations Bridge Analytics is accurate:

```
$OPSA_HOME/bin/opsa-ldap-configuration-manager.sh list --username <opsa_superadmin_username> --password <opsa_superadmin_password>
```

3. Using **Users Manager** in the Operations Bridge Analytics console, create an Operations Bridge Analytics user that uses an LDAP server for authentication. In this case you do not need to create a password when creating this user.

**Note:** You must belong to either the Super Admin or Tenant Admin user group to access the Users Manager.

4. Optional Step: Click  **Settings**, then select **LDAP Group Mapping** in the Operations Bridge Analytics console. Enter information into this form to provide mapping that enables automatic user profile creation in Operations Bridge Analytics after the LDAP Authentication during a user's first log on. This created user is assigned one role that corresponds to the mapping data.

**Note:** You must belong to the Tenant Admin user group to access **LDAP Group Mapping**.

See the *opsa-ldap-configuration-manager.sh* and *opsa-ldap-group-mapping-manager.sh* reference pages (or the Linux man pages) for more information.

## Maintenance Tasks

### Changing the IP Address or Host Name Used for the LDAP Authentication

To change the IP address or host name you used when you configured the LDAP authentication, use the *opsa-ldap-configuration-manager.sh* script and provide both the old and the new hostname.

Run the following command: *opsa-ldap-configuration-manager.sh* update -lh <oldname>.domain -nlh <newname>.domain

See the *opsa-ldap-configuration-manager.sh* reference page (or the Linux man pages) for more information.

## Chapter 25: Content Packs

You can combine additional information with the data collected by Operations Bridge Analytics by using the content packs shown in the following location: Operations Bridge Analytics [Content Packs](https://hpin.hp.com/node/19333/contentfiles) (<https://hpin.hp.com/node/19333/contentfiles>). It is recommended that you regularly check this link for new content packs, as new ones are frequently released.



## Chapter 26: Daylight Savings Time Codes

Use the following timezone attribute codes when setting a collection for Daylight Savings Time.

**Note:** See [http://en.wikipedia.org/wiki/List\\_of\\_tz\\_database\\_time\\_zones](http://en.wikipedia.org/wiki/List_of_tz_database_time_zones) for additional information about some of the time codes shown in the following table.

### Supported Daylight Savings Time Codes

Code	Code
ACT	Africa/Freetown
AET	Africa/Gaborone
AGT	Africa/Harare
ART	Africa/Johannesburg
AST	Africa/Juba
Africa/Abidjan	Africa/Kampala
Africa/Accra	Africa/Khartoum
Africa/Addis_Ababa	Africa/Kigali
Africa/Algiers	Africa/Kinshasa
Africa/Asmara	Africa/Lagos
Africa/Asmera	Africa/Libreville
Africa/Bamako	Africa/Lome
Africa/Bangui	Africa/Luanda
Africa/Banjul	Africa/Lubumbashi
Africa/Bissau	Africa/Lusaka
Africa/Blantyre	Africa/Malabo
Africa/Brazzaville	Africa/Maputo
Africa/Bujumbura	Africa/Maseru
Africa/Cairo	Africa/Mbabane
Africa/Casablanca	Africa/Mogadishu

**Supported Daylight Savings Time Codes, continued**

Code	Code
Africa/Ceuta	Africa/Monrovia
Africa/Conakry	Africa/Nairobi
Africa/Dakar	Africa/Ndjamena
Africa/Dar_es_Salaam	Africa/Niamey
Africa/Djibouti	Africa/Nouakchott
Africa/Douala	Africa/Ouagadougou
Africa/EI_Aaiun	Africa/Porto-Novo
Africa/Sao_Tome	America/Bahia
Africa/Timbuktu	America/Bahia_Banderas
Africa/Tripoli	America/Barbados
Africa/Tunis	America/Belem
Africa/Windhoek	America/Belize
America/Adak	America/Blanc-Sablon
America/Anchorage	America/Boa_Vista
America/Anguilla	America/Bogota
America/Antigua	America/Boise
America/Araguaina	America/Buenos_Aires
America/Argentina/Buenos_Aires	America/Cambridge_Bay
America/Argentina/Catamarca	America/Campo_Grande
America/Argentina/ComodRivadavia	America/Cancun
America/Argentina/Cordoba	America/Caracas
America/Argentina/Jujuy	America/Catamarca
America/Argentina/La_Rioja	America/Cayenne
America/Argentina/Mendoza	America/Cayman
America/Argentina/Rio_Gallegos	America/Chicago
America/Argentina/Salta	America/Chihuahua
America/Argentina/San_Juan	America/Coral_Harbour



**Supported Daylight Savings Time Codes, continued**

<b>Code</b>	<b>Code</b>
America/Argentina/San_Luis	America/Cordoba
America/Argentina/Tucuman	America/Costa_Rica
America/Argentina/Ushuaia	America/Creston
America/Aruba	America/Cuiaba
America/Asuncion	America/Curacao
America/Atikokan	America/Danmarkshavn
America/Atka	America/Dawson
America/Dawson_Creek	America/Indiana/Vevay
America/Denver	America/Indiana/Vincennes
America/Detroit	America/Indiana/Winamac
America/Dominica	America/Indianapolis
America/Edmonton	America/Inuvik
America/Eirunepe	America/Iqaluit
America/El_Salvador	America/Jamaica
America/Ensenada	America/Jujuy
America/Fort_Wayne	America/Juneau
America/Fortaleza	America/Kentucky/Louisville
America/Glace_Bay	America/Kentucky/Monticello
America/Godthab	America/Knox_IN
America/Goose_Bay	America/Kralendijk
America/Grand_Turk	America/La_Paz
America/Grenada	America/Lima
America/Guadeloupe	America/Los_Angeles
America/Guatemala	America/Louisville
America/Guayaquil	America/Lower_Princes
America/Guyana	America/Maceio
America/Halifax	America/Managua

**Supported Daylight Savings Time Codes, continued**

Code	Code
America/Havana	America/Manaus
America/Hermosillo	America/Marigot
America/Indiana/Indianapolis	America/Martinique
America/Indiana/Knox	America/Matamoros
America/Indiana/Marengo	America/Mazatlan
America/Indiana/Petersburg	America/Mendoza
America/Indiana/Tell_City	America/Menominee
America/Merida	America/Rainy_River
America/Metlakatla	America/Rankin_Inlet
America/Mexico_City	America/Recife
America/Miquelon	America/Regina
America/Moncton	America/Resolute
America/Monterrey	America/Rio_Branco
America/Montevideo	America/Rosario
America/Montreal	America/Santa_Isabel
America/Montserrat	America/Santarem
America/Nassau	America/Santiago
America/New_York	America/Santo_Domingo
America/Nipigon	America/Sao_Paulo
America/Nome	America/Scoresbysund
America/Noronha	America/Shiprock
America/North_Dakota/Beulah	America/Sitka
America/North_Dakota/Center	America/St_Barthlemy
America/North_Dakota/New_Salem	America/St_Johns
America/Ojinaga	America/St_Kitts
America/Panama	America/St_Lucia
America/Pangnirtung	America/St_Thomas

**Supported Daylight Savings Time Codes, continued**

<b>Code</b>	<b>Code</b>
America/Paramaribo	America/St_Vincent
America/Phoenix	America/Swift_Current
America/Port-au-Prince	America/Tegucigalpa
America/Port_of_Spain	America/Thule
America/Porto_Acre	America/Thunder_Bay
America/Porto_Velho	America/Tijuana
America/Puerto_Rico	America/Toronto
America/Tortola	Asia/Baghdad
America/Vancouver	Asia/Bahrain
America/Virgin	Asia/Baku
America/Whitehorse	Asia/Bangkok
America/Winnipeg	Asia/Beirut
America/Yakutat	Asia/Bishkek
America/Yellowknife	Asia/Brunei
Antarctica/Casey	Asia/Calcutta
Antarctica/Davis	Asia/Choibalsan
Antarctica/DumontDUrville	Asia/Chongqing
Antarctica/Macquarie	Asia/Chungking
Antarctica/Mawson	Asia/Colombo
Antarctica/McMurdo	Asia/Dacca
Antarctica/Palmer	Asia/Damascus
Antarctica/Rothera	Asia/Dhaka
Antarctica/South_Pole	Asia/Dili
Antarctica/Syowa	Asia/Dubai
Antarctica/Vostok	Asia/Dushanbe
Arctic/Longyearbyen	Asia/Gaza
Asia/Aden	Asia/Harbin

**Supported Daylight Savings Time Codes, continued**

<b>Code</b>	<b>Code</b>
Asia/Almaty	Asia/Hebron
Asia/Amman	Asia/Ho_Chi_Minh
Asia/Anadyr	Asia/Hong_Kong
Asia/Aqtau	Asia/Hovd
Asia/Aqtobe	Asia/Irkutsk
Asia/Ashgabat	Asia/Istanbul
Asia/Ashkhabad	Asia/Jakarta
Asia/Jayapura	Asia/Qatar
Asia/Jerusalem	Asia/Qyzylorda
Asia/Kabul	Asia/Rangoon
Asia/Kamchatka	Asia/Riyadh
Asia/Karachi	Asia/Riyadh87
Asia/Kashgar	Asia/Riyadh88
Asia/Kathmandu	Asia/Riyadh89
Asia/Katmandu	Asia/Saigon
Asia/Kolkata	Asia/Sakhalin
Asia/Krasnoyarsk	Asia/Samarkand
Asia/Kuala_Lumpur	Asia/Seoul
Asia/Kuching	Asia/Shanghai
Asia/Kuwait	Asia/Singapore
Asia/Macao	Asia/Taipei
Asia/Macau	Asia/Tashkent
Asia/Magadan	Asia/Tbilisi
Asia/Makassar	Asia/Tehran
Asia/Manila	Asia/Tel_Aviv
Asia/Muscat	Asia/Thimbu
Asia/Nicosia	Asia/Thimphu

**Supported Daylight Savings Time Codes, continued**

<b>Code</b>	<b>Code</b>
Asia/Novokuznetsk	Asia/Tokyo
Asia/Novosibirsk	Asia/Ujung_Pandang
Asia/Omsk	Asia/Ulaanbaatar
Asia/Oral	Asia/Ulan_Bator
Asia/Phnom_Penh	Asia/Urumqi
Asia/Pontianak	Asia/Vientiane
Asia/Pyongyang	Asia/Vladivostok
Asia/Yakutsk	Australia/Melbourne
Asia/Yekaterinburg	Australia/NSW
Asia/Yerevan	Australia/North
Atlantic/Azores	Australia/Perth
Atlantic/Bermuda	Australia/Queensland
Atlantic/Canary	Australia/South
Atlantic/Cape_Verde	Australia/Sydney
Atlantic/Faeroe	Australia/Tasmania
Atlantic/Faroe	Australia/Victoria
Atlantic/Jan_Mayen	Australia/West
Atlantic/Madeira	Australia/Yancowinna
Atlantic/Reykjavik	BET
Atlantic/South_Georgia	BST
Atlantic/St_Helena	Brazil/Acre
Atlantic/Stanley	Brazil/DeNoronha
Australia/ACT	Brazil/East
Australia/Adelaide	Brazil/West
Australia/Brisbane	CAT
Australia/Broken_Hill	CET
Australia/Canberra	CNT

**Supported Daylight Savings Time Codes, continued**

<b>Code</b>	<b>Code</b>
Australia/Currie	CST
Australia/Darwin	CST6CDT
Australia/Eucla	CTT
Australia/Hobart	Canada/Atlantic
Australia/LHI	Canada/Central
Australia/Lindeman	Canada/East-Saskatchewan
Australia/Lord_Howe	Canada/Eastern
Canada/Mountain	Europe/Berlin
Canada/Newfoundland	Europe/Bratislava
Canada/Pacific	Europe/Brussels
Canada/Saskatchewan	Europe/Bucharest
Canada/Yukon	Europe/Budapest
Chile/Continental	Europe/Chisinau
Chile/EasterIsland	Europe/Copenhagen
Cuba	Europe/Dublin
EAT	Europe/Gibraltar
ECT	Europe/Guernsey
EET	Europe/Helsinki
EST	Europe/Isle_of_Man
EST5EDT	Europe/Istanbul
Egypt	Europe/Jersey
Eire	Europe/Kaliningrad
Etc/GMT	Europe/Kiev
Etc/GMT0	Europe/Lisbon
Etc/Greenwich	Europe/Ljubljana
Etc/UCT	Europe/London
Etc/UTC	Europe/Luxembourg

**Supported Daylight Savings Time Codes, continued**

<b>Code</b>	<b>Code</b>
Etc/Universal	Europe/Madrid
Etc/Zulu	Europe/Malta
Europe/Amsterdam	Europe/Mariehamn
Europe/Andorra	Europe/Minsk
Europe/Athens	Europe/Monaco
Europe/Belfast	Europe/Moscow
Europe/Belgrade	Europe/Nicosia
Europe/Oslo	GB-Eire
Europe/Paris	GM
Europe/Podgorica	GMT0
Europe/Prague	Greenwich
Europe/Riga	HST
Europe/Rome	Hongkong
Europe/Samara	IET
Europe/San_Marino	IST
Europe/Sarajevo	Iceland
Europe/Simferopol	Indian/Antananarivo
Europe/Skopje	Indian/Chagos
Europe/Sofia	Indian/Christmas
Europe/Stockholm	Indian/Cocos
Europe/Tallinn	Indian/Comoro
Europe/Tirane	Indian/Kerguelen
Europe/Tiraspol	Indian/Mahe
Europe/Uzhgorod	Indian/Maldives
Europe/Vaduz	Indian/Mauritius
Europe/Vatican	Indian/Mayotte
Europe/Vienna	Indian/Reunion

**Supported Daylight Savings Time Codes, continued**

Code	Code
Europe/Vilnius	Iran
Europe/Volgograd	Israel
Europe/Warsaw	JST
Europe/Zagreb	Jamaica
Europe/Zaporozhye	Japan
Europe/Zurich	Kwajalein
GB	Libya
MET	Pacific/Enderbury
MIT	Pacific/Fakaofu
MST	Pacific/Fiji
MST7MDT	Pacific/Funafuti
Mexico/BajaNorte	Pacific/Galapagos
Mexico/BajaSur	Pacific/Gambier
Mexico/General	Pacific/Guadalcanal
Mideast/Riyadh87	Pacific/Guam
Mideast/Riyadh88	Pacific/Honolulu
Mideast/Riyadh89	Pacific/Johnston
NET	Pacific/Kiritimati
NST	Pacific/Kosrae
NZ	Pacific/Kwajalein
NZ-CHAT	Pacific/Majuro
Navajo	Pacific/Marquesas
PLT	Pacific/Midway
PNT	Pacific/Nauru
PRC	Pacific/Niue
PRT	Pacific/Norfolk
PST	Pacific/Noumea



**Supported Daylight Savings Time Codes, continued**

Code	Code
PST8PDT	Pacific/Pago_Pago
Pacific/Apia	Pacific/Palau
Pacific/Auckland	Pacific/Pitcairn
Pacific/Chatham	Pacific/Pohnpei
Pacific/Chuuk	Pacific/Ponape
Pacific/Easter	Pacific/Port_Moresby
Pacific/Efate	Pacific/Rarotonga
Pacific/Saipan	Turkey
Pacific/Samoa	UCT
Pacific/Tahiti	US/Alaska
Pacific/Tarawa	US/Aleutian
Pacific/Tongatapu	US/Arizona
Pacific/Truk	US/Central
Pacific/Wake	US/East-Indiana
Pacific/Wallis	US/Eastern
Pacific/Yap	US/Hawaii
Poland	US/Indiana-Starke
Portugal	US/Michigan
ROK	US/Mountain
SST	US/Pacific
Singapore	US/Pacific-New
SystemV/AST4	US/Samoa
SystemV/AST4ADT	UTC
SystemV/CST6	Universal
SystemV/CST6CDT	VST
SystemV/EST5	W-SU
SystemV/EST5EDT	WET

**Supported Daylight Savings Time Codes, continued**

<b>Code</b>	<b>Code</b>
SystemV/HST10	Zulu
SystemV/MST7	
SystemV/MST7MDT	
SystemV/PST8	
SystemV/PST8PDT	
SystemV/YST9	
SystemV/YST9YDT	

# Chapter 27: Log Files in Operations Bridge Analytics

This information in this section discusses the purpose and location of log files used in Operations Bridge Analytics.

## Using and Maintaining Audit Log Files

The information in this section discusses the log files Operations Bridge Analytics provides for auditing events associated with account and application activity. This audit activity does not include any information that might be considered sensitive in nature. Operations Bridge Analytics logs information related to the following topics:

- REST (Representational state transfer) calls
- Log on requests
- User setting changes
- Administrator setting changes
- Users attempting to log on without Operations Bridge Analytics roles
- Users attempting to use unauthorized resources
- Users accessing administrative consoles
- Create, delete, or disable user accounts
- Lock or release user accounts
- Password resets

Audit logs for the Operations Analytics Server reside in the following location:

```
$OPSA_HOME/log/audit/opsa-server-audit.log
```

These audit logs are configured for read and write permissions for the Operations Bridge Analytics Help user, and cannot be edited by other users.

There are several logging levels supported by the Operations Bridge Analytics audit logs. The following list is in order from the least severity to the most severity.

- INFO
- LOW
- MEDIUM
- HIGH
- CRITICAL

To change the level of logging of the Operations Analytics Server, edit the following file and follow the instructions shown in the file: **Operations Analytics Server:**

`$OSPA_HOME/jboss/standalone/configuration/standalone.xml`

**Note:** Back up the standalone.xml file before doing any editing. Carefully edit this file, keeping the xml well-formed and valid.

For example, to turn off logging, do the following.

1. Edit the following file on the Operations Analytics Server:

`$OSPA_HOME/jboss/standalone/configuration/standalone.xml`

2. Look for xml content that resembles the following:

```
<subsystem xmlns="urn:jboss:domain:logging:1.2">
  <periodic-rotating-file-handler name="AUDIT_FILE">
    <level name="INFO"/>
    <formatter>
      <pattern-formatter pattern="%d{yyyy-MM-dd HH:mm:ss,SSS} %s%E%n"/>
    </formatter>
    <file relative-to="jboss.server.log.dir" path="../../../../audit/opsa-
server-audit.log"/>
    <suffix value=".yyyy-MM-dd"/>
    <append value="true"/>
  </periodic-rotating-file-handler>
  <logger category="com.hp.opsa.common.audit" use-parent-
handlers="false">
    <handlers>
      <handler name="AUDIT_FILE"/>
    </handlers>
  </logger>
</subsystem>
```

3. Change the **INFO** text to **OFF**. Then save your changes.
4. Run the following command to apply your changes: `$OPSA_HOME/bin/opsa-server restart`

**Note:** After running an `opsa-server restart` command, information logged in the `/opt/HP/opsa/log/opsa-server.log` file is removed. To view the files that retain this information across restarts, see the log files located in the `/opt/HP/opsa/jboss/standalone/log` directory. Look for log file names that begin with `server.log`.

# Chapter 28: Maintaining the Operations Bridge Analytics Database

Use the instructions in this section to maintain the Operations Bridge Analytics databases.

## Backing up and Restoring Data

To back up or restore data for the Operations Analytics Server and Collector hosts, see the *Backing up and Restoring the Database* section of the [Vertica Administrator's Guide](#).

## Managing Vertica Data

By default, the Operations Bridge Analytics uses the Vertica Community Edition license, which is a non-expiring 1TB license. To avoid any disruptions in service, it is a good practice to monitor the size of the Operations Bridge Analytics database.

To check or verify the size of the Operations Bridge Analytics database, do the following:

1. Log on to the Vertica server as a root or dbadmin user.
2. Run the following command: `/opt/vertica/bin/vsql -U dbadmin -c 'select get_compliance_status();'`

**Note:** Only use the `-U dbadmin` option if you log on as a root user.

3. Review the compliance status. The message you see resembles the following example, which shows a 70 percent utilization percentage (70 percent of the 1TB that is available is currently in use):

```
-----  
get_compliance_status  
-----  
Raw Data Size: 0.00TB +/- 0.00TB  
License Size : 1.00TB  
Utilization : 70%  
Audit Time : 12-31 17:00:00-07  
Compliance Status : The database is in compliance with respect to raw data size.  
  
No expiration date for a Perpetual license  
(1 row)
```

If you have exceeded your licensed database size, do one or more of the following:

- **Shorten the data retention period:** See ["Setting Collection Retention Periods" on page 218](#) for more information.
- **Set a Purge Policy for the Vertica database:** See *Purging Deleted Data in Vertica Administrator's Guide*.
- **Manually purge data from the Vertica database:** See *Purging Deleted Data in the Vertica Administrator's Guide*.
- **Increase the Vertica license size:** See *Managing Licenses in the Vertica Administrator's Guide*.

See *Monitoring Database Size for License Compliance* in the *Vertica Administrator's Guide* for more information.

**Note:** Over time you might find that Operations Bridge Analytics collection data approaches or exceeds the storage space you configured in Vertica. To remedy this storage space issue, use the procedure shown in [Moving Data Storage Locations](#) to create a new storage location for select collection (tables) and move its existing content to the new location that you create.

## Resetting the Vertica Database Password

If you need to change the Vertica dbadmin password, use the instructions in this section. The steps shown in this section assume that Operations Bridge Analytics is already running.

1. The Vertica database admin user is dbadmin and its default password is dbadmin. Do the following to change the password:

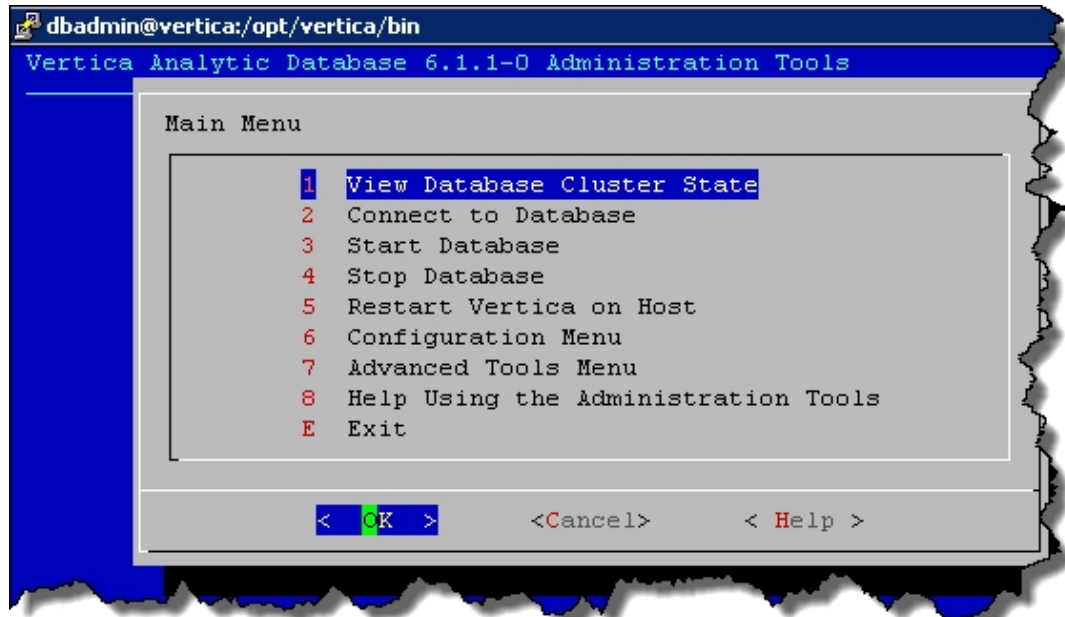
- a. Run the following command to log on to the `opsadb` database using the `vsq1` tool:  
`/opt/vertica/bin/vs1 -h hostname -p 5433 -U dbadmin -w dbadmin -d opsadb`

**Note:** `opsadb` is the Vertica database created during the Vertica installation.

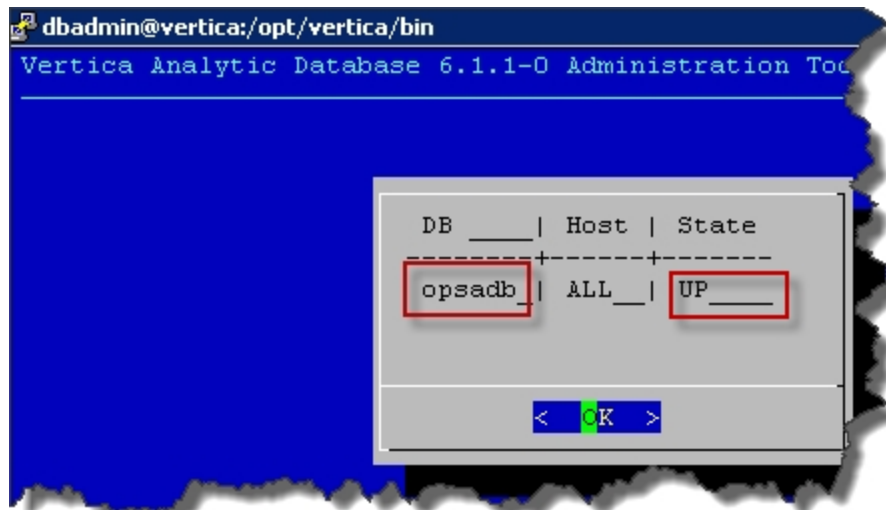
- b. Run the following command to change the password:  
`alter user dbadmin identified by '<new password>';`
  - c. Enter `\q` to quit the `vsq1` tool.
2. After completing the previous step, complete the following sub-steps.
    - a. Log on to the Operations Analytics Server and run the `opsa-server-postinstall.sh` script using the `scaleout` flag: `opsa-server-postinstall.sh -scaleout`. After you run this script, you will be asked to provide the database connect strings. During this step, provide the new password of the Vertica `dbadmin` user. Here is an example of the command sequence to use:
      - i. `[opsa@ACEVM145563026 opsa]$ cd /opt/HP/opsa/bin/`
      - ii. `[opsa@ACEVM145563026 bin]$ ./opsa-server-postinstall.sh -scaleout`
    - b. Log on to the to each Operations Analytics Collector host and run the following script: `opsa-collector-postinstall.sh`
  3. Do the following to check the database:



- a. Run the `su -dbadmin` command.
- b. Run the `/opt/vertica/bin/adminTools` command. You should see a screen similar to the following:



- c. The `opsadb` database should have been created when you first installed Operations Bridge Analytics. Enter 1 to view the state of the database; then click **OK**. You should see a screen similar to the following if the `opsadb` database is running:



- d. Click **OK** twice to exit the `adminTools` interactive command.

**Note:** If you must stop or restart the database, you can always do it from the first screen

shown in this step. You can also (carefully) complete other administrative operations using this tool.

## Setting Collection Retention Periods

By default, Operations Bridge Analytics's distributed version includes a three month data retention period. After purchasing and applying a production license, you can modify the data retention period as follows:

You can set the amount of time that Operations Bridge Analytics retains the data it is collecting. You can set the retention period for a collection or for all of the collections belonging to a tenant or a data source.

To set the amount of time to retain the data for a collection, use the following command:

```
$OPSA_HOME/bin/opsa-collection-config.sh -setretention <retention period in months> -source <source name> -domain <domain name> -group <group name> -username opsatenantadmin
```

See the *opsa-collection-config.sh* reference page (or the Linux man page) for more information.

The following shows several examples of setting collection retention periods:

- To set the retention period for a specific source, domain, and group, use the following command:  

```
/opt/HP/opsa/bin/opsa-collection-config.sh -setretention <retention period in months> -source <source> -domain <domain> -group <group> -username <username> [-force]
```
- To set the retention period for a specific source, use the following command:  

```
/opt/HP/opsa/bin/opsa-collection-config.sh -setretention <retention period in months> -source <source> -username <username> [-force]
```
- To set the overall retention period, use the following command: 

```
/opt/HP/opsa/bin/opsa-collection-config.sh -setretention <retention period in months> -username <username> [-force]
```


**Note:** When setting retention period for multiple collection policies, you can use the `-force` option to forcefully set the retention name and to avoid responding with `yes` for each collection.

After setting the retention period for specific collections belonging to a tenant, Operations Bridge Analytics removes any data record with a time stamp older than the listed retention period for those collections.

# Chapter 29: Manage Users and Tenants

This topic defines user accounts, user groups, and tenants and contains the procedures required to work with them.

To access

Click  **Settings** and select **User Manager**.

## Learn About

### About User Accounts

As an Operations Bridge Analytics administrator, you must configure a User Account for each user who needs to access the Operations Bridge Analytics graphical user interface.

Note the following:

- User Accounts must be unique across all Tenants.

**Tip:** To ensure the user name is globally unique, enter a user's email address as the user name.

- Each User Account must be assigned to a User Group.

To create a user account, see ["Add a User Account" on page 224](#), `opsa-tenant-manager.sh` (available from help > reference pages), and ["Creating Tenants Using a Script " on page 228](#).

The first time you log on, you will need to change the default password. Follow the password guidelines shown in the **Change Password** dialog box.

After ten failed attempts to access Operations Bridge Analytics from a specific user account, Operations Bridge Analytics denies access to users attempting access with this user account. This account restriction lasts for ten minutes. If you have any Operations Bridge Analytics access problems, discuss them with your Operations Bridge Analytics administrator.

By default, new passwords must be selected for every user every 182 days. This time can be modified by an administrator. For details, see "Resetting User Passwords" in the *Operations Bridge Analytics Hardening Guide*.

## About User Groups

User Groups are pre-defined in Operations Bridge Analytics and determine which tasks each User Account that is assigned to the User Group can perform.

### Note:

- User Accounts must be unique across all tenants.
- All User Groups have access to the Operations Bridge Analytics graphical user interface.
- You cannot add a new User Group to Operations Bridge Analytics.
- A User Account was assigned to the **Super Admin** User Group when Operations Bridge Analytics was installed.
- See **opsa-tenant-manager.sh** (available from help > reference pages) and "[Creating Tenants Using a Script](#)" on [page 228](#) for information about assigning a user to a User Group.

### Pre-defined User Groups

User Group	Description	Supported Tasks
Super Admin	<p><b>Note:</b> Operations Bridge Analytics permits only one Super Admin user.</p> <p>The user account assigned to this user group has access to the following information for each tenant defined:</p> <ul style="list-style-type: none"> <li>• User Accounts</li> <li>• User Groups</li> </ul>	<p>Add, modify, and delete tenants.</p> <p>Add, modify, and delete user accounts assigned to the Tenant Admin user group.</p>
Tenant Admin	<p>User accounts assigned to this User Group have access to the following information only for the tenant to which they are assigned:</p> <ul style="list-style-type: none"> <li>• Collectors</li> <li>• Collections</li> <li>• Meta Data</li> </ul>	<p>Add, modify, and delete user accounts.</p> <p>Manage the collectors, collections, meta data, and tags for a specified tenant.</p>

**Pre-defined User Groups, continued**

User Group	Description	Supported Tasks
	<ul style="list-style-type: none"> <li>• Tags</li> <li>• User Accounts</li> <li>• User Groups</li> </ul>	
User	User accounts assigned to this User Group have access to the Operations Bridge Analytics graphical user interface and to only the meta data and data for the tenant to which they are assigned.	<p>Access and perform tasks using the Operations Bridge Analytics Dashboards.</p> <p><b>Note:</b> Users assigned to this user group can also add and delete tags from a collection. See <a href="#">opsa-tag-manager.sh</a> (available from help &gt; reference pages) and <a href="#">"Creating Tenants Using a Script"</a> on <a href="#">page 228</a> for more information.</p>

New users are automatically assigned to a predefined user group. The user group to which a new user is assigned depends on the user group to which you are assigned when adding a new user.

**User Groups Assigned to New Users**

Your User Group	User Group Automatically Assigned to the New User
Super Admin	Tenant Admin
Tenant Admin	User

**About Tenants**

Operations Bridge Analytics supports multi-tenancy. This means one instance of Operations Bridge Analytics can serve multiple customers. Tenants ensure isolation of meta data and data across customers. The meta data includes the following:

- Collections
- Database schema
- Tags
- Dashboards
- User Accounts

For example, if you are a Manage Service Provider or Software as a Service Provider with multiple customers, tenants enable you to ensure that each customer accesses only the data for its data center or network.

When you install Operations Bridge Analytics, by default Operations Bridge Analytics creates the **opsa\_default** tenant.

To create one or more tenants, see **opsa-tenant-manager.sh** (available from help > reference pages) and ["Creating Tenants Using a Script" on page 228](#) for more information.

#### Important Tenant Information

A collection is automatically associated with a tenant depending on the Tenant Admin user that the Operations Bridge Analytics administrator provides as input when running the `$OPSA_HOME/bin/opsa-collection-config.sh` script.

Before creating collections using the **Source Type Manager** or the `$OPSA_HOME/bin/opsa-collection-config.sh` script, **you must decide on one of the following options** before proceeding with any collection configuration:

- Use the default Tenant, `opsa_default`, its corresponding default tenant username (`opsatenantadmin`), and the password for this user that you selected during installation. If you choose this option, skip directly to ["Registering Operations Bridge Analytics Collector Hosts" on page 235](#).
- Decide on which existing tenant to use.
- Create a new tenant and its corresponding Tenant Admin.

**Note:** Any user that is associated with a new tenant created by a member of the Super Admin user group cannot see collected information (in any dashboard) from any of the existing predefined collections (for any of the existing tenants, including the `opsa_default` tenant). After a member of the Super Admin user group creates a new tenant, the tenant admin user associated with that tenant needs to create collections for this new tenant.

When using the `$OPSA_HOME/bin/opsa-collection-config.sh` script, some examples use a predefined Tenant Admin user, `opsatenantadmin`, for the predefined `opsa_default` tenant. When defining collections, replace the `opsatenantadmin` shown in the example with the Tenant Admin user for the collection you are creating.

**Note:** You can configure a collector to collect data from a data source for only one tenant. So a single collector cannot be used to collect data from a single data source for multiple tenants.

**Note:** There might be tenant limitations when configuring collections for products that support multiple tenants. Each collector you configure for a collection supports a single tenant, so the data source from which it is collecting must also be for a single tenant.

Operations Bridge Analytics provides the following predefined User Groups:

- **Super Admin:** During installation, the `opsadmin` user gets created, and assigned to the Super Admin user group. You set the password for this user during installation. The primary responsibility of users assigned to the Super Admin user group is to add, modify, and delete tenants and users assigned to the Tenant Admin user group. See ["Manage Users and Tenants" on page 219](#) for more information. See the `opsa-tenant-manager.sh` reference page (or the Linux man page) for information about creating and managing tenants.
- **Tenant Admin:** During installation, the `opsatenantadmin` user gets created, and assigned to the Tenant Admin user group. You set the password for this user during installation. Only a user assigned to the Super admin user group is permitted to create a user assigned to the Tenant Admin user group. The primary responsibility of the Tenant Admin user is to add, modify, and delete users for a specific tenant. See ["Manage Users and Tenants" on page 219](#) for more information. See the `opsa-tenant-manager.sh` reference page (or the Linux man page) for information about creating and managing users for a tenant.
- **User:** During installation, the `opsa_default` user gets created, and assigned a normal user role. You set the password for this user during installation. Only a user assigned to the Tenant admin user group is permitted to create a user having a normal user role. This role is for the normal user who can use the Operations Bridge Analytics console and has access to data for the user group to which it is assigned. This user account must be unique across all tenants. See ["Manage Users and Tenants" on page 219](#) for more information.

If you plan to use a tenant model, you can create additional tenants from the Operations Bridge Analytics console or by using the `$OPSA_HOME/bin/opsa-tenant-manager.sh` script. See ["Manage Users and Tenants" on page 219](#) for more information about creating a tenant using the Operations Bridge Analytics console. To create a tenant and a Tenant admin user for a collection by using the `opsa-tenant-manager.sh` script, do the following:

1. Run the `$OPSA_HOME/bin/opsa-tenant-manager.sh` command from the Operations Analytics Server as a user assigned to the Super Admin User Group. See *Managing Users and Tenants* in the *Operation Analytics Help* for information about managing users and tenants. See the `opsa-tenant-manager.sh` reference page (or the Linux man page) for information about managing tenants.
2. Enter **Add a new tenant** and follow the interactive commands to add the new tenant.
3. Run the `$OPSA_HOME/bin/opsa-tenant-manager.sh` command as a user assigned to the Super Admin User Group.
4. Enter **Add a new user** and follow the interactive commands to add a user assigned to the Tenant Admin user group for the newly created tenant.

See the *opsa-tenant-manager.sh* reference page (or the Linux man page) or *Manage Users* in the *OBA Help* for information about managing users.


If you do not create a Tenant Admin user while adding a new tenant (as shown above in steps 3 and 4), add the Tenant Admin user for the new tenant later using the `$OPSA_HOME/bin/opsa-tenant-manager.sh` script. Do the following:

1. Run the `$OPSA_HOME/bin/opsa-tenant-manager.sh` command.
2. Enter **Add a new user** option.
3. Enter the Super Admin username and password.
4. Enter the Tenant Name for which you must add the Tenant Admin user.
5. Enter the new Tenant Admin user name.
6. Enter the new password for the new Tenant Admin user name.
7. Confirm the password.

The newly added Tenant Admin user is now available to add, modify, and delete users for its specified tenant. See the *opsa-user-manager.sh* reference page (or the Linux man page) for more information.

## Tasks

### Add a User Account

1. Click  **Settings** and select **Users Manager**.

Operations Bridge Analytics shows the **Users Manager** form.

**Note:** You must belong to either the Super Admin or Tenant Admin User Group to access the **Users Manager** option.

2. Click  **Add User**.

Operations Bridge Analytics shows the **Add User** form. Follow the password guidelines shown in the **Add User** dialog box.

3. In the **User Name** attribute, enter the user account name.



- Local Authentication
  - Enter the user account name into the **User Name** field
  - Enter the **Password** following the password guidelines.
- LDAP Authentication

Enter the user account name into the **User Name** field.

**Note:** The user account you created will be automatically assigned to the current tenant.

**Tip:** If the User Naming Attribute in the LDAP Configuration is `userdn=userPrincipalName`, the user name must be an email address.

**Note:** When adding an LDAP authenticated user, Operations Bridge Analytics searches for the user being added in the configured LDAP server or servers. Operations Bridge Analytics adds the user only if it can find the user in one of the configured LDAP servers. If the user cannot be found in one of the configured LDAP servers, no user is added.

4. Finish entering your passwords for a locally authentication user, then click **Add**.

Operations Bridge Analytics lists the new user account in the **Users Manager** table with its associated user group and tenant.

See the `opsa-user-manager.sh` reference page (or the Linux manpage) for more information.

5. Do the following:
  - a. If you are using LDAP authentication, select the **LDAP Authenticated User** checkbox.

**Note:** If you are using LDAP authenticated users, you must follow the instructions shown in "[Configuring LDAP Server Authentication for Operations Bridge Analytics](#)" on [page 193](#) for the **LDAP Authenticated User** checkbox to appear.

- b. Finish entering your passwords, then click **Save**.

Operations Bridge Analytics lists the new user account in the **Users Manager** table with its associated user group and tenant.

See the `opsa-user-manager.sh` reference page (or the Linux man page) for more information.

You can also add a user account using the `opsa-user-manager.sh` script. Run the following command:

```
$OPSA_HOME/bin/opsa-user-manager.sh -add -loginUser <Super Admin or Tenant Admin User Name> -loginPassword <password> -newUser <new username> -newUserPassword <new user password>
```

**Note:** See the `opsa-user-manager.sh` reference page (or the Linux man page) for more information.

After creating a new user use the `opsa-user-manager.sh` script, to show a list of users run the commands shown in the following examples:

- **To list Tenant Admin users:** `$OPSA_HOME/bin/opsa-user-manager.sh -list -loginUser opsaadmin -loginPassword <opsaadmin password>`
- **To list users by Tenant:** `$OPSA_HOME/bin/opsa-user-manager.sh -list -loginUser <Tenant Admin User> -loginPassword <Tenant Admin Password>`

You can delete a user account using the `opsa-user-manager.sh` script. Run the following command:  
`$OPSA_HOME/bin/opsa-user-manager.sh -delete -loginUser <Tenant Admin User> -loginPassword <Tenant Admin Password> -user <username>`

## Change Your User Account Password

You can change your user local account password at any time. The password for an LDAP authenticated account can only be changed on the LDAP server.

### To change your user local account password:

1. In the upper right corner of the Operations Bridge Analytics console, click your user account name.
2. Select **Change Password**.

The **Change Password** dialog box appears (only for users that are using a local account). Follow the password guidelines shown in the **Change Password** dialog box and change your password.

3. Click **Update** after you finish to save your changes.

You can also modify the password for a user account using the `opsa-user-manager.sh` script. Run the following command:

```
$OPSA_HOME/bin/opsa-user-manager.sh -modify -loginUser <username> -loginPassword <password> -newUserPassword <new user password>
```

### Note:

- Run the `opsa-user-manager.sh` command as an `opsa` user, not as a root user. Running `opsa-user-manager.sh` as a root user is not supported.
- See the `opsa-user-manager.sh` reference page (or the Linux man page) for more information.

## Change the Account Locking Threshold

If the number of times you fail to successfully log on to the Operations Bridge Analytics console

exceeds the default locking threshold, you will be locked out of Operations Bridge Analytics. Do the following to change the default locking threshold:

1. As an opsa user, edit the `/opt/HP/opsa/conf/opsa-config.properties` file on the Operations Analytics Server.
2. Change the `failed.counter.threshold` value to the value you desire for the number of failed log ons.
3. Change the `user.account.lockout.timeout`, value to the value you desire of the amount of time to wait before the user account lock expires.
4. Save your work.
5. Run the following command from the Operations Analytics Server to implement these property changes:

```
$OPSA_HOME/bin/opsa-server restart
```

See the opsa-server reference page (or the Linux man page) for more information.


## Add a Tenant

As an Operations Bridge Analytics administrator, if you belong to the **Super Admin** User Group, you can add one or more tenants.

### Note:

- You can also use **opsa-tenant-manager.sh** (available from help > reference pages) to add tenants to Operations Bridge Analytics.
- If you do not configure one or more tenants, Operations Bridge Analytics stores all of the meta data, collection and query information in the **opsa\_default** tenant.
- User account names must be unique across all tenants.

**To add a tenant adn a tenant admin:**

1. Click  **Settings** and select **Users Manager**.

Operations Bridge Analytics shows the **Users Manager** form.

**Note:** You must belong to either the Super Admin or Tenant Admin User Group to access the **User Management** option.

2. Click  **Add User**.

Operations Bridge Analytics shows the **Add User** form.

3. If you belong to the Super Admin User Group, in the **Tenant** attribute, enter the name of a tenant you want to create. Tenant names cannot begin with a number. The initial alpha character can be followed by alphanumeric characters (including an underscore).

**Note:** OBA converts all tenant names to lowercase.

4. Click **No matches found - Click to Add**.
5. In the **Add Tenant** dialog, click **OK**.
6. Add a Tenant Admin to the current Tenant.

For the **User Name** attribute, enter the user account name. Select one of following options for authentication:

- o Local Authentication
  - Enter the user account name into the **User Name** field.
  - Enter the **Password** following the password guidelines.
- o LDAP Authentication

Enter the user account name into the **User Name** field.

7. Click **OK** to add the Tenant Admin.

### Creating Tenants Using a Script

Operations Bridge Analytics gathers metrics, topology, event, and log file data from a diverse set of possible data sources. Tenants enable you to separate information from these data sources into groups, such as collections, user accounts, and user groups.

For each collection you define for the data sources supported by Operations Bridge Analytics, you must define a corresponding Tenant Admin or use the default Tenant, `opsa_default`, and the associated Tenant Admin user, `opsatenantadmin`, if you choose to not use a tenant model to separate information.

## Important Tenant Information

A collection is automatically associated with a tenant depending on the Tenant Admin user that the Operations Bridge Analytics administrator provides as input when running the `$OPSA_HOME/bin/opsa-collection-config.sh` script.

Before creating collections using the **Source Type Manager** or the `$OPSA_HOME/bin/opsa-collection-config.sh` script, **you must decide on one of the following options** before proceeding with any collection configuration:

- Use the default Tenant, `opsa_default`, its corresponding default tenant username (`opsatenantadmin`), and the password for this user that you selected during installation. If you choose this option, skip directly to ["Registering Operations Bridge Analytics Collector Hosts" on page 235](#).
- Decide on which existing tenant to use.
- Create a new tenant and its corresponding Tenant Admin.

**Note:** Any user that is associated with a new tenant created by a member of the Super Admin user group cannot see collected information (in any dashboard) from any of the existing predefined collections (for any of the existing tenants, including the `opsa_default` tenant). After a member of the Super Admin user group creates a new tenant, the tenant admin user associated with that tenant needs to create collections for this new tenant.

When using the `$OPSA_HOME/bin/opsa-collection-config.sh` script, some examples use a predefined Tenant Admin user, `opsatenantadmin`, for the predefined `opsa_default` tenant. When defining collections, replace the `opsatenantadmin` shown in the example with the Tenant Admin user for the collection you are creating.

**Note:** You can configure a collector to collect data from a data source for only one tenant. So a single collector cannot be used to collect data from a single data source for multiple tenants.

**Note:** There might be tenant limitations when configuring collections for products that support multiple tenants. Each collector you configure for a collection supports a single tenant, so the data source from which it is collecting must also be for a single tenant.

Operations Bridge Analytics provides the following predefined User Groups:

- **Super Admin:** During installation, the `opsaadmin` user gets created, and assigned to the Super Admin user group. You set the password for this user during installation. The primary responsibility of users assigned to the Super Admin user group is to add, modify, and delete tenants and users assigned to the Tenant Admin user group. See ["Manage Users and Tenants" on page 219](#) for more information. See the `opsa-tenant-manager.sh` reference page (or the Linux man page) for information about creating and managing tenants.
- **Tenant Admin:** During installation, the `opsatenantadmin` user gets created, and assigned to the Tenant Admin user group. You set the password for this user during installation. Only a user assigned to the Super admin user group is permitted to create a user assigned to the Tenant Admin

user group. The primary responsibility of the Tenant Admin user is to add, modify, and delete users for a specific tenant. See ["Manage Users and Tenants" on page 219](#) for more information. See the *opsa-tenant-manager.sh* reference page (or the Linux man page) for information about creating and managing users for a tenant.

- **User:** During installation, the `opsa_default` user gets created, and assigned a normal user role. You set the password for this user during installation. Only a user assigned to the Tenant admin user group is permitted to create a user having a normal user role. This role is for the normal user who can use the Operations Bridge Analytics console and has access to data for the user group to which it is assigned. This user account must be unique across all tenants. See ["Manage Users and Tenants" on page 219](#) for more information.

If you plan to use a tenant model, you can create additional tenants from the Operations Bridge Analytics console or by using the `$OPSA_HOME/bin/opsa-tenant-manager.sh` script. See ["Manage Users and Tenants" on page 219](#) for more information about creating a tenant using the Operations Bridge Analytics console. To create a tenant and a Tenant admin user for a collection by using the `opsa-tenant-manager.sh` script, do the following:

1. Run the `$OPSA_HOME/bin/opsa-tenant-manager.sh` command from the Operations Analytics Server as a user assigned to the Super Admin User Group. See *Managing Users and Tenants* in the *Operation Analytics Help* for information about managing users and tenants. See the *opsa-tenant-manager.sh* reference page (or the Linux man page) for information about managing tenants.
2. Enter **Add a new tenant** and follow the interactive commands to add the new tenant.
3. Run the `$OPSA_HOME/bin/opsa-tenant-manager.sh` command as a user assigned to the Super Admin User Group.
4. Enter **Add a new user** and follow the interactive commands to add a user assigned to the Tenant Admin user group for the newly created tenant.

See the *opsa-tenant-manager.sh* reference page (or the Linux man page) or *Manage Users* in the *OBA Help* for information about managing users.

If you do not create a Tenant Admin user while adding a new tenant (as shown above in steps 3 and 4), add the Tenant Admin user for the new tenant later using the `$OPSA_HOME/bin/opsa-tenant-manager.sh` script. Do the following:

1. Run the `$OPSA_HOME/bin/opsa-tenant-manager.sh` command.
2. Enter **Add a new user** option.
3. Enter the Super Admin username and password.

4. Enter the Tenant Name for which you must add the Tenant Admin user.
5. Enter the new Tenant Admin user name.
6. Enter the new password for the new Tenant Admin user name.
7. Confirm the password.

The newly added Tenant Admin user is now available to add, modify, and delete users for its specified tenant. See the *opsa-user-manager.sh* reference page (or the Linux man page) for more information.

#### Delete a Tenant

To delete a tenant from Operations Bridge Analytics, you must delete the tenant, then remove files from the Operations Analytics Collector host being used by the tenant you delete.

1. Remove all of the collection registrations for a tenant before deleting the tenant. See "[Removing a Collection Registration for a Tenant](#)" on page 236 for more information.
2. There are two methods to use to delete a tenant from Operations Bridge Analytics. To delete a tenant from Operations Bridge Analytics, **use only one of the following methods**:

**Note:** There are additional steps you must complete to remove files from your configured collectors after deleting a tenant.

- **Method 1:** Run the `$OPSA_HOME/bin/opsa-tenant-manager.sh` command as a user assigned to the Super Admin User Group. `opsaadmin` is a Super Admin user created during installation. You reset the password for this user during installation. Then follow the interactive commands to remove the tenant.
- **Method 2:** Run the `$OPSA_HOME/bin/opsa-tenant-manager.sh -delete -loginUser opsaadmin -loginPassword opsaadmin -tenant <tenant name>`

See the *opsa-tenant-manager.sh* reference page (or the Linux man page) for information about creating and managing tenants.

3. To remove files from your configured collectors, do the following:
  - a. From each Operations Analytics Collector host that contains collectors for the tenant being removed, run only one of the following commands to remove the tenant collection configuration:
    - If the Operations Analytics Collector host is only collecting data for the tenant being removed:
 

```
rm -rf /opt/HP/opsa/conf/collection/config.files/<collector host>
```
    - If the Operations Analytics Collector host is collecting data for multiple tenants:

```
rm -rf /opt/HP/opsa/conf/collection/config.files/<collector  
host>/<tenant>
```

- b. *Only complete this step if an Operations Analytics Collector host currently collects data for tenants other than the one being deleted.* Run the following command from the Operations Analytics Server to publish this collection configuration to the Operations Analytics Collector host. Use a Tenant Admin user for one of the other active tenants for which that this Operations Analytics Collector host is collecting.

```
$OPSA_HOME/bin/opsa-collection-config.sh -publish -collectorhost  
<fully-qualified domain name of the collector host> -username  
<tenant admin user>
```

The `-publish` option uploads the collection configuration you created to the Operations Analytics Collector host. To verify that the collector configuration published successfully, look for a message stating that the publish was successful, a table was successfully created, and the collection was restarted.

- c. From the Operations Analytics Collector host, run the following commands to remove specific files from the Operations Analytics Collector host associated with the tenant being removed :

- `rm -rf /opt/HP/opsa/data/load/<tenant name>`
- `rm -rf /opt/HP/opsa/data/failed_to_load/<tenant name>`



# Chapter 30: Modifying Unit Scaling on Collected Data

Data can be displayed in different scales, for example 1000 bytes may be displayed as 1 kilobyte or 1000 bytes. This procedure shows you how to modify the way data is displayed in query panes.

1. Open the configuration file of the collection from which the data originates. The files are found in the **/opt/HP/opsa/conf/collection/server/config.templates** directory.

**Example:**

```
/opt/HP/opsa/conf/collection/server/config.templates/bpm/1.0/application/performance/bpm_collection.xml
```

2. Locate the name of the metric you want to modify. In the example below, this is **Transaction\_Response\_Time**. Add a `scaling_unit` element using the following options:

%,mbps,kbps,gbps,kb,mb,gb,hz,khz,mhz,ghz,bytes,BIT,PB,EB,W,V,A,secs,millisecs,ms,page  
s/sec,per  
second,switches/sec,bytes/sec,KB/sec,interrupts/sec,packets/sec,errors/sec,reads/sec,bps,pe  
r hour,per min

then specify the factor that you want to multiply the incoming data by.

**Example:** This example takes incoming milliseconds and displays them as seconds.

```
<collection sourcegroup="performance" .....  
  
<column name="Transaction_Response_Time" position="9" datatype="float" length="0"  
key="no" value="" mapsto="" label="Transaction Response Time" columnname=""  
unit="ms" scaling_unit="secs" factor="0.001" type="metric"/> </collection>
```

3. Run the create and publish commands on the collection.

**Example:**

```
opt/HP/opsa/bin/opsa-collection-config.sh -create -nodelist  
/opt/HP/opsa/conf/collection/sample/bpm_nodelist -collectorhost 1.2.3.4 -source bpm -  
domain application -group performance -username <admin username> -password <admin  
password>  
  
/opt/HP/opsa/bin/opsa-collection-config.sh -publish -collectorhost 1.2.3.4 -username  
<admin username>-password <admin password>
```

# Chapter 31: Registering Operations Bridge Analytics Collector Hosts

Register the Operations Analytics Collector host you plan to use with the Operations Analytics Server. If you plan to use a tenant model, using tenants other than `opsa_default` (the default tenant), you must use the `-tenant` option with the `opsa-collection-config.sh` command. See the `opsa-collection-config.sh` reference page (or the Linux man page) for more information.

**Note:** Before completing the steps in this section, it is recommended that you add an entry to the `/etc/hosts` file for the Operations Analytics Collector host you plan to register.

## Automatically Creating Alert Collections

All of the alerts generated by Operations Bridge Analytics are stored as collections. This collected information is used to show dashboards for these alerts generated over time. Unlike all of the other collections, there is no manual configuration or registration required for the Alerts Collections. A new Alerts Collection gets created with each newly created Operations Bridge Analytics tenant.

See *Alerts* in the *Operations Bridge Analytics Help* for more details about the Alerts feature.

An Alerts Collection gets created each time an Operations Analytics Collector host is registered to an Operations Analytics Server. When adding Operations Analytics Servers, as described in ["Adding More Operations Bridge Analytics Servers" on page 187](#), do the following:

Run the following command from each newly added Operations Analytics Server to create the alerts collection:

```
$OPSA_HOME/bin/opsa-collection-config.sh -create -collectorhost <collector IP address> -source opsa -domain collection -group alerts -username <tenant admin user> -password <tenant admin password>
```

## Checking the Registration Status of a Operations Analytics Collector Host

To check the registration status of your Operations Analytics Collector host, do the following:

1. Run the following command: `$OPSA_HOME/bin/opsa-collection-config.sh -list -collectorhosts -allversions -username opsatenantadmin`
2. Review the list of registered Operations Analytics Collector hosts. If the Operations Analytics Collector host you plan to register is not on the list, you must register it using the instructions in this section.

## Registering an Operations Analytics Collector Host

To register an Operations Analytics Collector host with an Operations Analytics Server, do the following:

1. Run the following command on the Operations Analytics Collector host to make sure the `opsa-collector` process is running:

```
$OPSA_HOME/bin/opsa-collector status
```

Look for a message stating the `opsa-collector` process is running. If the message states that the `opsa-collector` process is stopped, restart the process using the following

command: `$OPSA_HOME/bin/opsa-collector start`

2. Run the following command from the Operations Analytics Server:

```
$OPSA_HOME/bin/opsa-collection-config.sh -register -collectorhost  
<fully-qualified domain name of the collector host> -port 9443 -  
username opsatenantadmin
```

**Note:** If you have the Operations Analytics Collector host configured to use SSL for data communications, use the `-ssl` option in this command. If you have changed the HTTP user name or password on the Operations Analytics Collector host, use the `-coluser` and `-colpass` option in this command. You must also use the fully-qualified domain name of the Operations Analytics Collector host when using this command. See the *opsa-collection-config.sh* reference page (or the Linux man page) for more information.

**Note:** The `opsa-collection-config.sh` script prompts you for the Tenant Admin password for the username you use in the `opsa-collection-config.sh` command.

**Note:** The default port to which OBA listens is 9443. You can modify this port in cases of port conflicts. See *Configuring the HTTPS and HTTPS Port for the Operations Bridge Analytics Collector Appliance* in the [Operations Analytics Hardening Guide](#) for more information.

If the script communicates successfully with the Operations Analytics Collector host, it registers it in the Operations Analytics Server database and displays a success message.

## Removing a Collection Registration for a Tenant

If you no longer want to analyze data for a collection, you must remove the collection registration and the stored data for that collection.

**Note: Important:** Just unregistering a collection does not drop the tables from the Operations Bridge Analytics database. If you do not complete all of the following steps, try to register the

collection again using the original name. Operations Bridge Analytics does not create the database table. By completing all of the following steps, you run the `opsa-collection-config.sh` script with the `-purgecollection` option. Doing so drops the database table and removes any references to the table.

To remove the collection registration and the stored data for that collection, do the following:

1. Run the following command to list all of the collectors for the tenant:

```
$OPSA_HOME/bin/opsa-collection-config.sh -list -collectorhosts -allversions -username opsatenantadmin
```

See the `opsa-collection-config.sh` reference page (or the Linux man page) for more information.

2. Unregister the collections you no longer want to analyze for a tenant using the following command:

```
$OPSA_HOME/bin/opsa-collection-config.sh -unregister -source <collection source> -domain <collection domain> -group <collection group> -collectorhost <collector host> -username opsatenantadmin
```

**Note:** The `unregister` option is the opposite of the `create` option. The `unregister` option removes a collection from being collected on an Operations Analytics Collector host where the `create` option was used to create that collection.

**Note:** The command in this step also removes any Custom Collection entries for the specified tenant.

3. Repeat the previous two steps until there are no collectors listed when running the command shown in step 1. If the command in step 1 lists no collectors, it means none of the original collectors for the tenant are collecting data for the collection you plan to remove.
4. After unregistering all of the collections you no longer want to analyze for a tenant (from all the tenant's collectors), remove the collection from the database using the following command:

```
$OPSA_HOME/bin/opsa-collection-config.sh -purgecollection -source <collection source> -domain <collection domain> -group <collection group> -collectorhost <collector host> -username <Tenant Admin User>
```

See the `opsa-collection-config.sh` reference page (or the Linux man page) for more information.

**Note:** The command in this step also removes all Custom Collection data for the specified tenant from the Operations Bridge Analytics database.

**Note:** After unregistering a Custom Collection, the data remains intact. Having this data still

intact means you can register a Custom Collection that you removed and resume that Custom Collection.

5. View the dashboards associated with the collections you purged. The data from these purged collections are no longer present in their associated dashboards.

## Chapter 32: Resolve Host Aliases

If you have multiple collections importing data from the same source, the source may have multiple aliases. For example, in one collection it may be identified by the IP address and in another collection it may be identified by the FQDN. Operations Bridge Analytics automatically detects host aliases and incorporates the data into your dashboards and search results.

To access

Click **Data Manager** on the left side of the Operations Bridge Analytics console; then click **Host Aliases Settings**.

### Learn About

#### About Host Aliases

If you have multiple collections importing data from the same source, the source may have multiple aliases. For example, in one collection it may be identified by the IP address and in another collection it may be identified by the FQDN. Operations Bridge Analytics automatically detects host aliases and incorporates the data into your dashboards and search results.

Host alias data is used when displaying search results for a specific host, or in dashboards when a host is specified in an AQL. When metric data is displayed as a search result, data for each alias is displayed separately.

In an AQL query, data for all aliases is returned unless you use a double equals symbol == in place of a single one. In such a case, only the results exactly matching the specified host identifier will be displayed.

In the topology manager, if you add a host that has aliases the aliases will be added as well.

# Tasks

## How to Configure Host Alias Settings

1. Click **Data Manager** on the left side of the Operations Bridge Analytics console; then select **Host Aliases Settings**.
2. By default, host aliases are enabled and function automatically, using DNS resolving to identify host aliases.

Hosts Aliases Back

Enabling Identification of Host aliases allows Operations Analytics to automatically discover and use host aliases.  
DNS resolving is used in this process, or you can manually import a host file.

Enable Identification of Host aliases

Use DNS resolving to identify Host aliases


To manually add Host Aliases, upload a host file:

Remove manually imported aliases if DNS resolving detects a mismatch

3. If DNS resolving cannot function in your environment, you can manually add a list of hosts and their aliases in the form of a host or .csv file.  
  
Disable the **DNS resolving** checkbox and use the **Upload** button to upload a file. Each line in the file should represent one host and its aliases.
4. Periodically, the list of host aliases is verified to make sure nothing in your environment has changed. In version 3.0, this process occurs once per week. If a change is detected, and you want the mismatches to be removed even though the data was uploaded manually as a file, select the **Remove manually imported aliases...** checkbox.
5. To download the current list of aliases in the form of a .csv file, select **Download All Saved Aliases**. Each line in the file represents one host and its aliases.



## How to See if Data is Coming from a Host Alias

1. In any query pane, select **More Pane Actions**  and click **View Data Origins**.
2. The original host identifier is specified in the **Original Name** column.

If the data displayed has been modified because of a detected host alias, the **Displayed Name** will be different from the **Original Name**.

## Reloading Host Aliases After Deletions

If Operations Bridge Analytics shows any inaccurate or incorrect aliases you might want to delete the current aliases. Use the information in this section to clean up the current aliases and restart the alias resolving.

**Note:** For the steps in this section to be successful, you must have configured collections and they must be actively collecting data. After you delete any host aliases, Operations Bridge Analytics does not retrieve new aliases for hosts that are already known.

If you want to Operations Bridge Analytics to start over and resolve the aliases again, do the following:

1. Run the following commands from the Vertica server to delete the content from the `host_lookup_aliases` and `host_lookup_unique_hosts` tables from the Vertica database.
  - a. `TRUNCATE TABLE <tenant> host_lookup_aliases;`
  - b. `TRUNCATE TABLE <tenant> host_lookup_unique_hosts;`
2. Run the following command from the Operations Analytics Server to restart the `opsa-server` processe: `$OPSA_HOME/bin/opsa-server restart`
3. Run the following command from the Operations Analytics Server to restart the `opsa-task-manager` processe: `$OPSA_HOME/bin/opsa-task-manager restart`
4. Run the following commands from the Operations Analytics Collector host to resubmit the aliases resolving processing:
  - a. `$OPSA_HOME/scripts/opsa-post-persist-processing-kill-topology.sh`
  - b. `$OPSA_HOME/scripts/opsa-post-persist-processing-submit-topology.sh`

## Chapter 33: Using Parametric Dashboards

Operations Bridge Analytics provides you with the ability to use dashboards as launching points for parametric dashboards. For example, assume you have an existing dashboard, called *MyDashboard*. From *MyDashboard*, assume you want to navigate to launch a parametric dashboard, called *MyParametricDashboard*.

**Note:** This section discusses using an existing dashboard to implement a navigation (drill) to a parametric dashboard. The use of parametric dashboards is only one form of drill. There is a PQL drill as well, and that drill is not covered in this section.

To configure this drill point, do the following:

1. Using the *MyDashboard* dashboard, click **Parameters** in the panel and scroll down. To determine the parameters you want to enter, do the following:
  - a. **Drill Destination:** Decide what name you want to use for the dashboard to which you want to drill (*MyParametricDashboard*).
  - b. **Drill Label Field, Drill Value Field,** and the optional **Drill Type Field:** Identify the parameter names for these panels. To obtain these values, do the following:
    - i. Navigate to the *MyParametricDashboard* dashboard.
    - ii. Click **Edit Pane Settings**.
    - iii. Scroll down; then click **Show Properties**.
    - iv. If necessary, enter a filter to limit the number of entries you want to review.
    - v. Write down the following values for the **Drill Label Field, Drill Value Field** and the optional **Drill Type Field**:
      - **Drill Label Field:** Use a combination of the property `group_id` and property `uid` (concatenated by an underscore (`_`) for the value in this field).

**Note:** In your AQL statement for the pane, if you use an alias for the property selector designated to be used in the **Drill Label Field**, append `aliased <alias>` to the value you enter in the **Drill Label Field**. For example, you would enter `property_group_uid_property_uid aliased <alias>` in the **Drill Label Field** parameter value. See the [AQL Developer Guide](#) for details about specifying aliases for selectors in AQL statements.

- **Drill Value Field:** Use a combination of the `property_group_id` and `property_uid` (concatenated by an underscore (`_`) for the value in this field).

**Note:** In your AQL statement for the pane, if you use an alias for the property selector designated to be used in the **Drill Value Field**, append `aliased <alias>` to the value you enter in the **Drill Value Field**. For example, you would enter `property_group_uid_property_uid aliased <alias>` in the **Drill Value Field** parameter value. See the [AQL Developer Guide](#) for details about specifying aliases for selectors in AQL statements.

- **Drill Type Field** (optional): Use a combination of the `property_group_id` and `property_uid` (concatenated by an underscore (`_`) for the value in this field).

**Note:** In your AQL statement for the pane, if you use an alias for the property selector designated to be used in the **Drill Type Field**, append `aliased <alias>` to the value you enter in the **Drill Type Field**. For example, you would enter `property_group_uid_property_uid aliased <alias>` in the **Drill Type Field** parameter value. See the [AQL Developer Guide](#) for details about specifying aliases for selectors in AQL statements.

- Open the *MyDashboard* dashboard, click **Parameters** in the pane, then scroll down. Note the highlighted fields shown below.

Query	Visualization	Parameters	
	Interval:	300	Seconds
	Offset:	0	
	Limit:	500	
	N:	5	
	Percentile:	10	Percentile
	Outlier Upper Limit:	95	Percentile
	Outlier Lower Limit:	1	Percentile
	Time Offset:	0	Seconds
	Start Time Offset:	0	Seconds
	End Time Offset:	0	Seconds
	TimeOut:	0	Seconds
	Drill Destination:		
	Drill Label Field:		
	Drill Value Field:		
	Drill Type Field:		

- Enter the values you identified for the **Drill Destination**, **Drill Label Field**, **Drill Value Field**, and **Drill Type Field**.
- Save** your work.
- Open the *MyParametricDashboard* dashboard for editing.
- In the AQL, use the following as an example to edit the AQL: Change *<the observed string or ID string>* to read as param1.

**Note:** The *<the observed string or ID string>* represents the parameter you are passing into the *MyParametricDashboard* dashboard. You are limited to passing one parameter.

**Note:** After you replace the ID string with param1, the dashboard is now a "template" dashboard. Any instantiation of this dashboard will not be editable.

After completing the above steps, you can drill to the *MyParametricDashboard* dashboard from a link within the *MyDashboard* dashboard.

Below is a simple example, using a dashboard you created, *MyAlertsDashboard*, and configuring it to drill to a parametric dashboard, *MyAlertsInstance*, which you created.

1. Using the *MyAlertsDashboard* dashboard, click **Parameters** in the panel, and scroll down. Note the highlighted fields shown below.

Query	Visualization	Parameters	
Interval:	300	Seconds	
Offset:	0		
Limit:	500		
N:	5		
Percentile:	10	Percentile	
Outlier Upper Limit:	95	Percentile	
Outlier Lower Limit:	1	Percentile	
Time Offset:	0	Seconds	
Start Time Offset:	0	Seconds	
End Time Offset:	0	Seconds	
TimeOut:	0	Seconds	
Drill Destination:			
Drill Label Field:			
Drill Value Field:			
Drill Type Field:			

To determine the parameters you want to enter, do the following:

- a. **Drill Destination:** Decide what name you want to use for the dashboard to which you want to drill. For this example, you are using *MyAlertsInstance*.
  - b. **Drill Label Field, Drill Value Field, and Drill Type Field:** Identify the parameter names for these panels. To obtain these values, do the following:
    - i. Navigate to the dashboard to which you want to drill. For this example, you are using *MyAlertsInstance*.
    - ii. Click **Edit Pane Settings**.
    - iii. Scroll down; then click **Show Properties**.
    - iv. If necessary, enter a filter to limit the number of entries you want to review. For this example you can enter `alerts` in the filter to limit the entries.
    - v. Write down the following values for the **Drill Label Field, Drill Value Field, and Drill Type Field**:
      - **Drill Label Field:** For this example, you want to use a time stamp for this field. Use a combination of the `property_group_id` and `property_uid` (concatenated by an underscore (`_`) for the value in this field). For this example, you decide to use `opsa_collection_alerts_timestamp` as a value for this field.
      - **Drill Value Field:** For this example, you want to use an identifier for the instance for this field. Use a combination of the `property_group_id` and `property_uid` (concatenated by an underscore (`_`) for the value in this field). For this example, you decide to use `opsa_collection_alerts_alert_instance_id` as a value for this field.
      - **Drill Type Field:** For this example, you want to use an identifier for the instance for this field. Use a combination of the `property_group_id` and `property_uid` (concatenated by an underscore (`_`) for the value in this field). For this example, you decide to use `opsa_collection_alerts_alert_instance_id` as a value for this field.
2. Open the *MyAlertsDashboard* dashboard, click **Parameters** in the pane, and scroll down.

- Enter the values you identified for the **Drill Destination** (*MyAlertsInstance* for this example), **Drill Label Field** (*opsa\_collection\_alerts\_timestamp* for this example), **Drill Value Field** (*opsa\_collection\_alerts\_alert\_instance\_id* for this example) and **Drill Type Field**. Note the highlighted fields shown below.

Query	Visualization	Parameters	
Interval:	300		Seconds
Offset:	0		
Limit:	500		
N:	5		
Percentile:	10		Percentile
Outlier Upper Limit:	95		Percentile
Outlier Lower Limit:	1		Percentile
Time Offset:	0		Seconds
Start Time Offset:	0		Seconds
End Time Offset:	0		Seconds
TimeOut:	0		Seconds
Drill Destination:	MyAlertsInstance		
Drill Label Field:	opsa_collection_alerts_tir		
Drill Value Field:	opsa_collection_alerts_al		
Drill Type Field:			

- Save** your work.
- Open the *MyAlertsInstance* dashboard for editing.
- In the AQL, use the following as an example to edit the AQL: Change *<the observed string or ID string>* to read as *param1*. For this example, change `{{(i.alert_instance_id ilike "902496")}}` to `{{(i.alert_instance_id ilike param1)}}`

**Note:** The *<the observed string or ID string>* represents the parameter you are passing into the *MyAlertsInstance* dashboard. You are limited to passing one parameter.

**Note:** After you replace the ID string with `param1`, the dashboard is now a "template" dashboard. Any instantiation of this dashboard will not be editable.

After completing the above steps, you can drill to the *MyAlertsInstance* dashboard from a link within the *MyAlertsDashboard* dashboard.



# Troubleshooting

This section contains the following topics:

"Collection Troubleshooting Topics" below

"General Troubleshooting Tips" on page 253

"Integration Troubleshooting Topics" on page 255

## Chapter 34: Collection Troubleshooting Topics

### Checking a Collector's Status

To check a collector's status, do the following:

- Run the following command from an Operations Analytics Server to list the collections deployed to that Operations Analytics Collector host:

```
$OPSA_HOME/bin/opsa-collection-config.sh -list -collectorhost  
<collector hostname> -username opsatenantadmin
```

- Run the following commands from an Operations Analytics Collector host to check the status of collector sources and processes:

- `$OPSA_HOME/bin/opsa-collector status`
- `$OPSA_HOME/bin/opsa-loader status`

- Run the following command from an Operations Analytics Server to check the status of the collector sources and processes configured on an Operations Analytics Collector host:

```
$OPSA_HOME/bin/opsa-collection-config.sh -status -collectorhost  
<collector hostname> -username opsatenantadmin
```

### Troubleshooting the Absence of Collection Data

The information in this section helps you troubleshoot collections that have been published to an Operations Analytics Collector host, but are not collecting data. This troubleshooting takes place on the Operations Analytics Collector host.

After configuring a collection, open the **OpsA Health** Dashboard and check **MOVING\_TOTAL (collector\_rows)** to see if it contains a row for each newly configured collection. If any of your newly

configured collections are not present, you might need to restart the collector using the following command: `$OPSA_HOME/bin/opsa-collector start`

- Always run the following commands to check that the collector and data loader are functioning correctly.
  - `$OPSA_HOME/bin/opsa-collector status`
  - `$OPSA_HOME/bin/opsa-loader status`
- Look for any error messages in the `/opt/HP/opsa/log/opsa-collector.log` and `/opt/HP/opsa/log/loader.log` files.
- If you want to adjust the logging levels, edit the `/opt/HP/opsa/conf/opsa-collector-log.properties` file and set the following properties:
  - `log4j.logger.com.hp.opsa.collector = DEBUG`
  - `log4j.logger.com.hp.opsa.collector.common = DEBUG`
  - `log4j.logger.com.hp.opsa.collector.agent = DEBUG`
  - `log4j.logger.com.hp.opsa.collector.server = DEBUG`
- If your collection problem is with the following collections, look in the associated log files shown for the collection:
  - HP Operations Agent or HP Operations Smart Plug-in for Oracle Collections
    - `/opt/HP/BSM/PMDB/log/collections.log`
    - `/opt/HP/BSM/PMDB/log/hpacollector.log`
  - HP Operations Manager or HP Operations Manager i (HPOM or OMi) Collections
    - `/opt/HP/BSM/PMDB/log/collections.log`
    - `/opt/HP/BSM/PMDB/log/dbcollector.log`
  - Any of associated HP BSM RTSM Collections
    - `/opt/HP/BSM/PMDB/log/collections.log`
    - `/opt/HP/BSM/PMDB/log/topologycollector.log`
- Custom SiteScope Collection: If your collection problem is with the Custom SiteScope Collection, do the following:
  - Check the `%SITESCOPE_HOME%/log/error.log` and `%SITESCOPE_HOME%/log/data_integration.log` files on the SiteScope server for any error messages about not being able to push SiteScope data to an Operations Analytics Collector host.
  - Check the Operations Analytics Collector host data integration to make it is configured correctly on the SiteScope server. See [Configuring Collections](#) for more information.

- For the following collections, look in the specific processed folder to check that the collector is collecting data for that collection:

- HP Operations Agent Collection: `/opt/HP/opsa/data/pa_processed/<tenant>`
- HP Operations Smart Plug-in for Oracle Collection: `/opt/HP/opsa/data/ora_pa_processed/<tenant>`
- NNMi Custom Poller Collection: `/opt/HP/opsa/data/nnm_processed/<tenant>`

**Note:** The NNMi Custom Poller collector needs to have read/write access to the NNMi CSV files to move them to the processed directory. If the collector cannot move them, the NNMi Custom Poller CSV files will be reprocessed the next time the collector starts up. See Configuring Collections for more information.

- NNM ISPi Performance for Metrics Interface Health  
Collection: `/opt/HP/opsa/data/netinterface_processed/<tenant>`

**Note:** The NNM ISPi Performance for Metrics Interface Health collector needs to have read/write access to the NNM ISPi Performance for Metrics Interface Health CSV files to move them to the processed directory. If the collector cannot move them, the NNM ISPi Performance for Metrics Interface Health CSV files will be reprocessed the next time the collector starts up. See Configuring Collections for more information.

- NNM ISPi Performance for Metrics Component Health  
Collection: `/opt/HP/opsa/data/netcomponent_processed/<tenant>`

**Note:** The NNM ISPi Performance for Metrics Component Health collector needs to have read/write access to the NNM ISPi Performance for Metrics Component Health CSV files to move them to the processed directory. If the collector cannot move them, the NNM ISPi Performance for Metrics Component Health CSV files will be reprocessed the next time the collector starts up. See Configuring Collections for more information.

- HP Operations Manager (HPOM ) Collections: `/opt/HP/opsa/data/om_events_processed/<tenant>`
- HP Operations Manager i (OMi) Collections: `/opt/HP/opsa/data/omi_events_processed/<tenant>`
- Custom SiteScope Collection:  
`/opt/HP/opsa/data/sis_processed/<tenant>`  
Look for collected Customer SiteScope Collection data in `/opt/HP/opsa/data/SIS_GDI-API_DATA/<tenant>`.

- Custom Collection: `<custom source parent directory>_processed/<tenant>`

**Note:** The Custom CSV collector needs to have read/write access to the Custom CSV files to move them to the processed directory. If the collector cannot move them, the Custom CSV files will be reprocessed the next time the collector starts up. See [Configuring Collections](#) for more information.

- To check if data is being loaded into the Operations Bridge Analytics database, a user can look at the files in the `/opt/HP/opsa/data/load/<tenant>` directory. Files with a `.working` extension are files to which the collector is actively writing. Working files should never be older than 10 minutes. So any files with a `.csv` extension are ready to be loaded into the Operations Bridge Analytics database. If the system is functioning correctly, there should not be any `*.csv` files older than 10 minutes as well.
  - If you do not find any files with a `.csv` extension in the `/opt/HP/opsa/data/load/<tenant>` directory, do the following:
    - i. Check for any CSV files that were successfully loaded into the Operations Bridge Analytics database by looking in the `/opt/HP/opsa/data/archive/<tenant>` directory.
    - ii. If you do not see files for the collection in question, check to see if the data loader has rejected the load files by looking in the `/opt/HP/opsa/data/failed_to_load` directory.

#### Troubleshooting Configurations from the Operations Bridge Analytics Server

To troubleshoot collector and collection configuration, do the following from the Operations Analytics Server:

- If you completed the instructions to set up Operations Bridge Analytics System Health in ["Checking the Status of Operations And Operations Bridge Analytics Servers"](#) and installed and configured the Operations Bridge Analytics Log File Connector on the Operations Analytics Collector hosts (to collect Operations Bridge Analytics log files), you can check the **OpsA Health** dashboard and look for `ERROR` and `WARN` severity log messages.
- Look in the `/opt/HP/opsa/log/collection_config.log` file for any errors and warnings.
- If you want to adjust the logging level, edit the `/opt/HP/opsa/bin/log4j.properties` file and set the following properties. Then reconfigure the collection and view the results.
  - `log4j.logger.com.hp.opsa.collection.config=DEBUG,coll_cfg`
  - `log4j.logger.com.hp.opsa.collector=DEBUG,coll_cfg`

### Messages Appear as Unparsed Messages without Appearing in Collections

**Problem:** You configure a new source type using the Source Type Manager and you define one or more fields calculated as arithmetic functions of other fields. You notice that some events do not enter the expected Operations Bridge Analytics collections, but do appear as unparsed messages.

**Note:** To view unparsed messages, open the **OpsA Health** dashboard and view the messages shown in the **Unparsed Messages** section.

**Note:** If Operations Bridge Analytics receives an event or message that has null as a value for one or more of the fields used in the arithmetic function you are using, it will not parse the entire event or message.

Here are some ways to notice this issue:

- You know how many log messages and events the source emits per time period and you notice that this number is larger than the entries that appear in the collection.
- You create an AQL query for the `opsa_unparsed_messages` collection and see all the messages and events that were not parsed. If you see messages in this collection it means that these messages and events are absent from the expected collection.

**Workaround:** Do not use arithmetic functions when working with fields that you expect will contain a null value part of the time. Instead, the calculated fields should be created during an earlier stage of the data flow. For example do the calculation in the SQL query of a JDBC source.

## Chapter 34: General Troubleshooting Tips

This section includes some general troubleshooting tips and techniques for resolving Operations Bridge Analytics issues.

**Question:** When I log on to an Operations Analytics Server or Operations Analytics Collector host as an `opsa` user, I receive an `Account locked due to <n> failed logins` message, yet I know the password I supplied is correct.

**Answer:** This message seems to indicate that I need to wait some period of time after the last failed attempt to try to log on again. However, for the this `opsa` user, this message means you are really supplying the wrong password. Obtain the correct password for the `opsa` user and try again. You will be able to log on immediately by using the correct password.

**Question:** I am using an integration between Operations Bridge Analytics and Logger and suspect that my Logger collection is missing some log data.

**Answer:** Configuring Logger to use the **TCP Forwarding** feature, also known as CEF forwarding, is more reliable. Use the instructions shown in [Configuring Logger to Forward CEF Messages to Operations Analytics](#) to resolve this issue.

**Question:** I use the `logrotate` Linux command with the `copytruncate` feature to rotate the logs for a product that has its logs collected by Operations Bridge Analytics. Are there any `logrotate` command limitations I should be aware of?

**Answer:** Using the `logrotate` command's `copytruncate` feature is strongly discouraged:

- In high load scenarios, lines were missed in the short time frame right before the rotation.
- When using a pattern for the logfile name, every line is sent twice to the Operations Analytics Server.

**Question:** I installed Operations Bridge Analytics, which installed Operations Agent over the top of an existing Operations Agent installation, without error. The Operations Bridge Analytics issue is that I cannot set up any Operations Agent or OMi collections.

**Answer:** The only known remedy is to complete a new Operations Bridge Analytics installation on a server that has a fresh operating system installed with no other software applications installed, such as HPE Operations Agent.

**Question:** How can I verify that a Source Type published successfully?

**Answer:** Do the following:

1. From the Operations Bridge Analytics console, view the **OpsA Meta Info** dashboard:
2. Enter the property group uid for this Source Type in the **Collection Columns** Filter. The property group uid is the name of the string (in the form of `<source type name>_logstash_metrics`).
3. If the resulting table shows data, then the Source Type published successfully.

**Question:** How do I enable the topology feature to recognize hosts coming from a Source Type?

**Answer:** To enable the topology feature to recognize hosts coming from a Source Type, do the following:

1. Enable the JMX console by changing the suffix of the following file on the server appliance from `.tx` to `.txt`:  
**`/opt/HP/opsa/conf/jmxNotHardened.tx`**
2. Wait five minutes before attempting to log on to the JMX console.
3. Log in to the JMX console using the following syntax:

**http://<server\_URL>:8081**

The default user name and password is **opsadmin**

4. Locate the OpsA Infrastructure Settings area.
5. Locate the **java.lang.String get GLOBALSettingDefaultValue** item.
  - a. Set the value to **opsa-customtopology-settings**.
  - b. Invoke the function and copy the list of values in the results to a text file
  - c. Add a line to represent the custom collection using the following syntax:  
`<collection_name>, <field from collection tagged as host>`
6. Locate the **java.lang.String set GLOBALSettingDefaultValue** item
  - a. Set the value of **contextName** to **opsa-customtopology-settings**.
  - b. Set the value of **settingName** to **opsa.customtopology.nodegroup.link\_tags**.
  - c. Copy the list of values from the text file you saved to the **newValue** field.

The topology feature now recognizes hosts coming from this Source Type.

## Chapter 34: Integration Troubleshooting Topics

The OMi DashBoard Integration Results in a Certificate Error

For the information in this section, consider the following:

- You completed the instructions shown in "[Integration Troubleshooting Topics](#)" above.
- You configured Single Sign-on as shown in *Single Sign On* in the *HPE Operations Bridge Analytics Hardening Guide*.

When using a browser, you might see a certificate error when navigating from OMi to an Operations Bridge Analytics dashboard from outside the virtual environment. To remedy this problem, use the following remedies:

Remedy for a Firefox Browser

1. Export the certificate from the browser.

- a. Open Operations Bridge Analytics in the browser.
  - b. Navigate from OMi to an Operations Bridge Analytics dashboard from outside the virtual environment to see the certificate error you have been experiencing.
  - c. Select **Certificate error > View certificates**.
  - d. Select the **Details** tab.
  - e. Select **Copy to File....**
  - f. Select the following format: **Base-64 encoded X.509 (.CER)**.
  - g. Select **Next**.
  - h. Enter *Filename*.
  - i. Select **Next/Finish**.
2. Import the Base-64 encoded X.509 (.CER) version of the certificate into the browser.
    - a. Click **Open menu** in the upper right of the browser.
    - b. Open **Options**; then select **Advanced**.
    - c. Click **View Certificates**.
    - d. Click **Servers**.
    - e. Click **Add Exception** and add the fully-qualified domain name of the Operations Analytics Server.
    - f. Navigate to **View Certificates > Servers** again.
    - g. Click **Import .....** and import the Base-64 encoded X.509 (.CER) version of the certificate that you exported earlier into the Firefox browser.

#### Remedy for an Internet Explorer Browser

1. Export the certificate from the browser.
  - a. Open Operations Bridge Analytics in the browser.
  - b. Navigate from OMi to an Operations Bridge Analytics dashboard from outside the virtual environment to see the certificate error you have been experiencing.
  - c. Select **Certificate error > View certificates**.
  - d. Select the **Details** tab.
  - e. Select **Copy to File....**



- f. Select the following format: **Base-64 encoded X.509 (.CER)**.
    - g. Select **Next**.
    - h. Enter *Filename*.
    - i. Select **Next/Finish**.
  2. Import the Base-64 encoded X.509 (.CER) version of the certificate into the browser.
    - a. Select **Start > Run** and run the **mmc.exe** command to open a **mmc console**.
    - b. Select **File > Add/remove Snap-in...**
    - c. After a new window opens, select **Certificates > Add**.
    - d. Select **Computer Account**; then click **Next**.
    - e. Select **Local Computer**; then click **Finish**.
    - f. Click **OK** to complete this task.
    - g. Select **Certificates (Local Computer)** to complete this task.
    - h. Right-click **Trusted Root Certification Authorities**; then select **All Tasks > Import** to open the **Certificate Import Wizard**.
    - i. Click **Next**.
    - j. Browse to the location to which you exported the certificate file during Step 1.
    - k. Follow the steps of the interactive wizard to complete the certificate import. For example, you might select **Next > Next > Finish** to complete the certificate import.
    - l. After the **Certificate Import Wizard** informs you that the import was successful, click **OK**.
    - m. You are finished. Close the **mmc console**.

Now you should no longer see a certificate error when navigating from OMi to an Operations Bridge Analytics dashboard from outside the virtual environment.

# Send documentation feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

**Feedback on Operations Bridge Analytics Help (Operations Bridge Analytics 3.00)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to [ovdoc-asm@hpe.com](mailto:ovdoc-asm@hpe.com).

We appreciate your feedback!