Hewlett Packard
Enterprise

# HPE Operations Analytics

Software Version: 2.32

## HPE Operations Analytics Help

Document Release Date: June 2016
Software Release Date: June 2016

# 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. HPE 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 HPE 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

## Trademark Notices

Microsoft, Windows, and Windows NT are U.S. registered trademarks of the Microsoft group of companies.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

# Documentation Updates

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

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hpe.com/group/softwaresupport/search-result?keyword=.

This site requires an HPE Passport account. If you do not have one, click the **Create an account** button on the HPE Passport Sign in page.

# Support

Visit the HPE Software Support website at: **https://softwaresupport.hpe.com**

This website provides contact information and details about the products, services, and support that HPE Software offers.

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

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

Most of the support areas require that you register as an HPE Passport user and sign in. Many also require a support contract. To register for an HPE Passport ID, go to **https://softwaresupport.hpe.com** and click **Register**.

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

## HPE Software Integrations, Solutions and Best Practices

Access the Hewlett Packard Enterprise Software Support site (**https://softwaresupport.hpe.com/manuals**) to search for a wide variety of best practice documents and materials.

# Contents

# Chapter 1: Getting Started with HPE Operations Analytics

## About

### What can Operations Analytics do for me?

Welcome to Operations Analytics, an analysis tool that provides a unified approach to proactively manage and solve simple and complex IT operations problems.

In today’s complex data center environments, the source of a problem is not always easy to detect using traditional management and troubleshooting tools that look only for pre-determined solutions to known potential problems. For example, many management and troubleshooting tools are designed to provide analytics for a specific problem context, such as root cause isolation, outlier detection, and service level agreement violation. They provide these services by using a specific data set and analytics technique.

With Operations Analytics you generate insights from the data in your IT environment that you choose to collect. And because identifying the most useful analytics to derive from the data generally depends on the problem context, with Operations Analytics you, the user, provide each data request in the form of a search query.

Operations Analytics enables you to use simple search queries using the Phrased Query Language (PQL) to view metric, topology, event, and log file information related to the context you specify. Operations Analytics also enables you to use its Analytics Query Language (AQL) for more precise searches; for example, when you know the exact log file message or combination of analytics required to troubleshoot a problem.

When entering a search query, Operations Analytics offers suggestions as you type. It then uses your query to analyze the information available and displays the most important and related metrics.

Operations Analytics processes data according to your search query. These results assist you with the following kinds of tasks:

- Identify and analyze the pattern of problems in your IT environment.
- Identify the cause of resource or application usage problems.
- Troubleshoot server and network performance problems.
- Identify configuration or inventory changes.

### What are the main features?

- **Dashboards.** Operations Analytics allows you to create your own dashboard or to use one of the out-of-the-box dashboards. Dashboards are collections of Query Panes, which display specific metrics in your choice of visual representations. The dashboards can also display the log viewer. For more details, see "Dashboards and Query Panes" on page 12.
- **Search.** To use Operations Analytics, you must first define the context of the problem or area for which you want information. To do so, use the Search Query field. Operations Analytics then uses the search query you specify to determine the related metrics, topology, inventory, event, and log file information to

display. For more details, see "Search Tool" on page 25.

- **Play Back History.** Play back your search query results using the Playback feature. For more details, see "Play Back History" on page 37.
- **Predictive Analytics.** Predictive analytics enables you to generate a prediction line for one or more metrics based on past behavior and seasonal trends. For more details, see "Predictive Analytics" on page 46.
- **Log and Event Analytics.**A forensic tool that helps you locate the most significant messages in a given time range. For more details, see "Log and Event Analytics" on page 39.
- **Topology Management.** 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. For more details, see "Topology Manager" on page 59.
- **User Management.** Operations Analytics allows you to create and manage user accounts. For more details, see "Manage Users and Tenants" on page 145.
- **Alerts.** You can configure Operations Analytics to send different types of alerts based on criteria you define. For details, see "Alerts" on page 48.
- **Track Logs and Events.** You can specify message groups or parameters to track and treat as metrics. This allows you to view data trends over time in a graphical format. Additionally, this enables analytic operations such as correlations, alerts, predictive analytics, etc. on specified texts in the tracked entities.
- **Correlation.** You can take a group of metrics and compare each metric to every other metric in the group with one click. This allows you to determine how closely related the data over time is for different metrics. With this feature, it is possible to identify connections and relationships between problematic metrics and tracked logs.

# Tasks

## How do I start using Operations Analytics?

We recommend starting with one of the following tasks:

- Use the OA Environment Overview dashboard to help determine, at a glance, problem areas to investigate more closely in your IT environment.

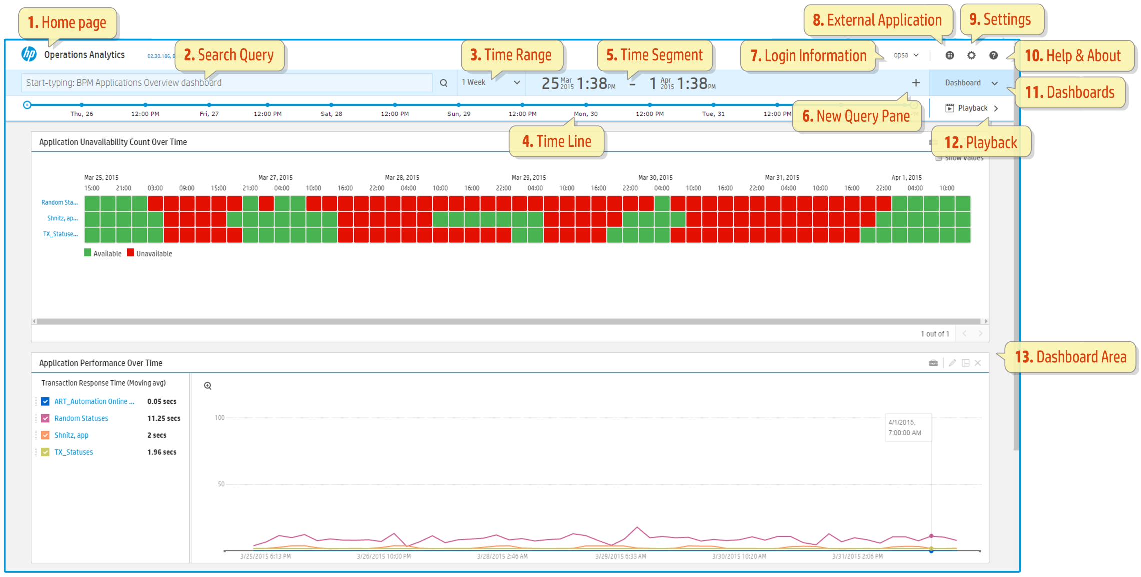
  Click Operations Analytics to navigate to the **OA Environment Overview** dashboard. See "Dashboards and Query Panes" on page 12 for more information.
- Enter a search query that defines the context of the problem you are trying to solve.

  For example, you might query for CPU utilization information for a specific host name or for memory utilization for all database instances for a specified application.

  As you type, Operations Analytics provides a list of suggestions to help define the context of the problem you are trying to get information about. See "Search Tool" on page 25 for more information.
- Select an existing dashboard from the **Dashboards** menu.
- Create a new dashboard by selecting **New** from the **Dashboards** menu.

# User Interface

## How does the Operations Analytics console work?



## 1 Home Page

The Operations Analytics logo opens the OA Environment Overview dashboard. This dashboard provides an overview of the following information for the hosts in your IT environment:

- Top five CPU utilization (cpu_util)
- Top five disk utilization (disk_io_rate)
- Top five memory utilization (mem_util)
- Top five network utilization (net_packet_rate)

Use this dashboard to help determine, at a glance, problem areas to investigate more closely in your network environment.

Note the following:

- Operations Analytics displays the LogsOverview dashboard when you initially log on to Operations Analytics.
- Each subsequent time you log on, Operations Analytics displays the last dashboard you accessed. In the **Dashboard** menu a check mark indicates the dashboard in use.
- 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.

To access the home page, click the Operations Analytics logo to return to the OAEnvironmentOverview dashboard.

See "Out-of-the-Box Dashboards Provided by Operations Analytics" on page 12 for more information.

## 2 Search Query

Defines the context for the data you want to examine.

Operations Analytics gathers and analyzes the data based on the search query you enter.

To perform a search, enter the string to search for. As you type, a list of suggestions are displayed to enhance the search query. This list is dynamically generated based on your data.

## 3 Time Range

Specifies the time frame within which Operations Analytics should obtain the data to display.

Use the Time Range menu to specify the time in hours, days, or months.

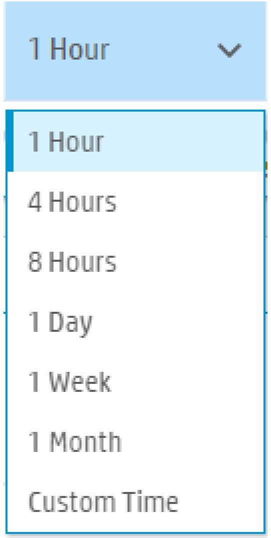
> **Note:** The time range is historical. It spans the selected time range ending at the current time.

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

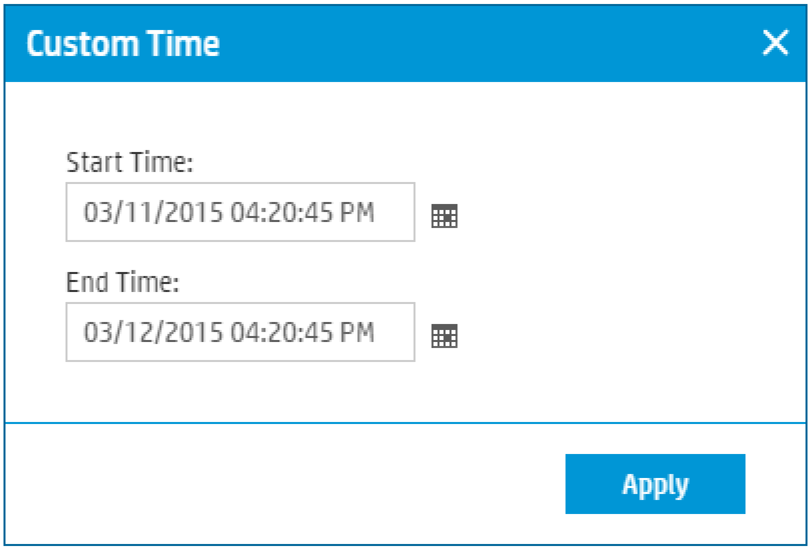
By default, Operations Analytics uses a time range of 1 Hour.

**To use the time range feature:**

1. In the Time Range menu, click ⌄ .
2. Select the time in hours, days, or months.



3. To specify a start and end date using the Operations Analytics calendar, select **Custom Time**.
4. Click the calendar icon to display the calendar for either **Start Time** or **End Time** as shown in the following example.



Start Time: 03/11/2015 04:20:45 PM

End Time: 03/12/2015 04:20:45 PM

5. After you have completed selecting your Start Time and End Time Dates, click **Apply**.

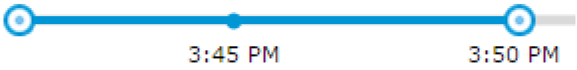
See "Filter Search Query Results " on page 35 for more information.

## 4 Time Line

Enables you to filter the time segment for which the data is displayed.

This feature is useful when you want to fine tune the Time Range selected.

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:



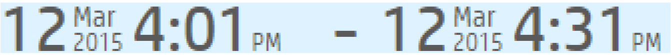
See "Filter Search Query Results " on page 35 for more information.

## 5 Time Segment

Displays the time segment you selected from the Time Line.

See "Filter Search Query Results " on page 35 for more information.

After you slide each end of the time line to the beginning and end point of the time you want to use, the From and To time changes to match the latest selection.



## 6 New Query Pane

Enables you to add one or more query panes using one of the following:

- Analytics Query Language (AQL) query
- AQL function
- AQL expression

  See the AQL Developer's Guide for Operations Analytics for more information.

To add a new query, see "Dashboards and Query Panes" on page 12.

## 7 Log In Information

Displays your user name. See "About User Accounts" on page 145 for more information.

Enables you to do the following:

- Access user settings
  - Change your password. See "Change Your User Account Password" on page 148 for more information.
  - Log out.

To log out, click your user account name and select **Logout**.

## 8 HP ArcSight Logger

To launch HP ArcSight Logger, click and select the HP ArcSight Logger IP address or host name to which you want to connect.

## 9 Settings

Access various settings for features such as Alerts, Collections, User Management, and Tracked Logs. Some items are only visible to administrative users.

## 10 Help, Reference Pages and About

Access the following information for Operations Analytics:

- Help
- Reference pages - descriptions of command line interface commands.
- License, database, and version information

## 11 Dashboards

Lists the following saved dashboards:

- Provided by Operations Analytics.
- Shared by the users in your user community (tenants).
- Saved by the current user.

You can select a dashboard from this list rather than using the search query to create your own.

For more details, see "Dashboards and Query Panes" on page 12.

## 12 Playback

Replay Operations Analytics results.

This option is useful to help you identify when a problem began to occur.

For more details, see "Play Back History" on page 37

## 13 Dashboard Area

An Operations Analytics dashboard is the graphical user interface for troubleshooting your IT operations problems.

For more details, see "Dashboards and Query Panes" on page 12.

**Note:** When you first access Operations Analytics, it displays the LogsOverview dashboard. Each subsequent time you log on, Operations Analytics displays the last saved dashboard you accessed. In the **Dashboards** menu a check mark indicates the dashboard in use.

# Chapter 2: Dashboards and Query Panes

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 layout and can be shared with other users.

### To access

- Enter a new search query in the Search Query field.
- Select an existing dashboard from the **Dashboards** menu.
- Create a new dashboard by selecting **New** from the **Dashboards** menu.

# Learn About

### 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 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.

### Out-of-the-Box Dashboards Provided by Operations Analytics

| Name | Description |
|---|---|
| BPM Applications Overview | **Note:** See "Configuring an HPE Business Process Monitor Collection" in the HPE Operations Analytics Configuration Guide for the configuration steps required to display this dashboard information.<br>Use the BPM Applications Overview to view the following:<br>• Application Availability Over Time<br>The heat map value in this dashboard is the number of failed transactions.<br>• Application Performance Over Time<br>• Application Layer Performance Over Time<br>• Top 10 Transactions Performance<br>• Top 10 Locations Performance |

| Name | Description |
|---|---|
| Logs Apache | **Note:** This dashboard is available only if you have installed the *Apache HTTP Server Access File* and *Apache HTTP Server Error File* SmartConnectors provided by HPE ArcSight Logger. SmartConnectors are not included as part of Operations Analytics.<br>Displays the following information. Information for access log and error log are displayed next to each other:<br>• Log messages count over time<br>• Log messages count by severity<br>• Top 10 hosts with failure messages<br>• Total errors per host<br>• Log messages.<br>**Note:** You can change the sort order of the message displayed in the log messages panes by modifying the AQL query. For details, see the AQL Developer Guide . |
| Logs Linux | **Note:** This dashboard is available only if you have installed the *Linux Audit File* and *Linux Syslog File* SmartConnectors provided by HPE ArcSight Logger. SmartConnectors are not included as part of Operations Analytics.<br>Displays the following information. Information is calculated per host.<br>• Log messages count over time<br>• Log messages count by severity<br>• Top 10 hosts with failure messages<br>• Top 10 log message categories<br>• Log messages<br>**Note:** You can change the sort order of the message displayed in the log messages panes by modifying the AQL query. For details, see the AQL Developer Guide . |
| Logs Search | **Note:** See "Installing and Configuring HPE ArcSight Logger" in the HPE Operations Analytics Installation Guide for the configuration steps required to display this dashboard information.<br>Displayed by default when you initially log on to Operations Analytics. This dashboard provides an overview of the following information for the log messages in your IT environment:<br>• Log Messages - All<br>• Log Messages - Syslog Only<br>**Note:** You can change the sort order of the message displayed in the log messages panes by modifying the AQL query. For details, see the AQL Developer Guide . |

| Name | Description |
|---|---|
| Logs Windows | **Note:** This dashboard is available only if you have installed the *Microsoft Windows Event Log - Local* SmartConnector provided by HPE ArcSight Logger. SmartConnectors are not included as part of Operations Analytics.<br>Displays the following information. Information is calculated per host.<br>• Log messages count over time<br>• Log messages count by severity<br>• Top 10 log message categories<br>• Top 10 hosts with failure messages<br>• Log messages<br>**Note:** You can change the sort order of the message displayed in the log messages panes by modifying the AQL query. For details, see the AQL Developer Guide . |
| NNMi Network SPI | Displays the following information:<br>• Top 10 Network Interfaces with Utilization In<br>• Top 10 Network Interfaces with Utilization Out<br>• Top 10 network interfaces based on highest error percentages<br>• Top 10 network interfaces based on highest discard percentages<br>• Top 10 network interfaces based on highest in and out throughput<br>• Top 10 network devices based on highest CPU utilization<br>• Top 10 network devices based on highest memory utilization<br>• Top 10 unavailable nodes<br>• Top 10 network devices based on highest SNMP response times |
| OA Environment Overview | **Note:** See "Configuring an HPE Operations Agent Collection" in the HPE Operations Analytics Configuration Guide for the configuration steps required to display this dashboard information.<br>This dashboard provides an overview of the following information for the hosts in your IT environment:<br>• Top 10 CPU utilization (cpu_util)<br>• Top 10 disk utilization (disk_io_rate)<br>• Top 10 memory utilization (mem_util)<br>• Top 10 network utilization (net_packet_rate)<br>Use this dashboard to help determine, at a glance, problem areas to investigate more closely in your network environment.<br>To return to this dashboard, click hp Operations Analytics . |

| Name | Description |
|---|---|
| OA Microsoft ActiveDirectory Server | This dashboard provides information from a selection of metrics taken from the Operations MP for MS ActiveDirectory Collection. |
| OA Microsoft Exchange Server | This dashboard provides information from a selection of metrics taken from the Operations MP for MS Exchange Collection. |
| OA Microsoft SQL Server | This dashboard provides information from a selection of metrics taken from the Operations MP for MS SQL Server Collection. |
| OA Oracle Database MP | This dashboard provides information from a selection of metrics taken from 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 | **Note:** See "Configuring an HPE Operations Manager (HPOM) Events Collection" in the HPE Operations Analytics Configuration Guide for the configuration steps required to display this dashboard information.<br>Use this dashboard to view the following information:<br>• Event Count Over Time<br>• Top 10 Hosts with Event Count Over Time<br>• Event Count by Host - Current Week<br>• Event Count by Host - Previous Week<br>• Event Count by Severity - Current Week<br>• Event Count by Severity - Previous Week<br>• Table of the first 500 OM events |

| Name | Description |
|---|---|
| OMi Events | **Note:** See "Configuring an HPE Operations Manager i (OMi) Events Collection" in the HPE Operations Analytics Configuration Guide for the configuration steps required to display this dashboard information.<br>Use this dashboard to view the following information:<br>• Total count of the OMi events over time<br>• Percentage of OMi events by host<br>• Total count of OMi events by State<br>• Top hosts that have highest number of OMi events<br>• Percentage of OMi events by application<br>• Event count by the host<br>• Event count by host from the previous week<br>• Event count by severity<br>• Event count by severity from the previous week<br>• Table of the first 500 OMi events |
| OneView Environment Overview | • OneView Topology with Health Status<br>• All Data Centers by Total Open Alerts<br>• All Data Centers by Alert Arrival Count<br>• Data Centers by Server Utilization and Power Consumption<br>• Distribution of Recent Inventory Changes<br>• All Racks across Data Centers by Health Status<br>• All Power Device across Data Centers by Health Status |
| OneView Interconnect 360 | • Top 10 Interconnects by Throughput<br>• Top 10 Busiest Interconnects<br>• Bottleneck Analysis (Layer 2)<br>• Bottleneck Analysis (Layer 3)<br>• Distribution of Ports in Full-Duplex Mode in Interconnects<br>• Distribution of Ports in Half-Duplex Mode in Interconnects<br>• Interconnects by Open Critical Alerts Count |
| OneView Inventory Changes | • Recent Inventory Changes<br>• Distribution of Inventory Changes by State and Category<br>• Number of Enclosures<br>• Number of Blade Servers<br>• Number of Physical Servers |

| Name | Description |
|---|---|
| OneView Power Device 360 | • All Power Devices<br>• Top 10 Power Devices by Open Alerts Count<br>• Power Devices Metrics |
| OneView Rack 360 | • All Racks with Health Status<br>• Top 10 Racks by Total Open Alerts<br>• All Racks by Alert Arrival Count<br>• All Racks by Critical Syslog Arrival Count |
| OpsA Alerts | Displays all instances of triggered alerts going back three months by default.<br>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. |
| Opsa Health | **Note:** See "Checking Operations Analytics System Health" in the HPE Operations Analytics Configuration Guide for the configuration steps required to display this dashboard information.<br>Displays the metrics, topology, and log information available for the following Operations Analytics servers and appliances:<br>• Operations Analytics Collector Appliance<br>• Operations Analytics Server Appliance<br>• List of configured collections that Operations Analytics is collecting data for.<br>This dashboard provides current details about Operations Analytics system health. See "Check the Health of Operations Analytics" on page 155 for more information. |
| OpsA Meta Info | Displays the following information for the collections in your IT environment:<br>• Collections and any tags for each collection<br>• Columns (metrics) per collection and tag names per column<br>• Columns defined as keys.<br>See "How to View Collection Information" on page 78 for more information. |
| SiteScope Environment Overview | Displays the following information monitored by SiteScope:<br>• Top CPU Utilization<br>• Top Disk Utilization<br>• Top Memory Utilization<br>• Top 10 Hosts with Ping Roundtrip Time<br>• Top 10 Hosts with URL Content Roundtrip Time<br>• Top 10 Hosts with JMX Physical Memory |
| Tracked Logs | Displays data collected from tracked logs and parameters.<br>Contains log and parameter count over time, and data distribution query panes. |

# 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 the procedure for copying 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 Analytics will overwrite the original dashboards as it automatically saves any changes you make.

## How to Copy a Dashboard

1. Navigate to the **Dashboard** menu.
2. Click **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** menu.
2. Click **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 **Dashboards** menu.
2. Click **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 **Dashboards** menu.
2. Click **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 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 Analytics dashboard, click **More Pane Actions** 🧰.
2. Click **Export to CSV** to export the pane results to a CSV file.

## 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 Analytics administrator can provide descriptions for the arguments required for each AQL Function provided. See "Add / Edit Query Pane - Query Tab" on page 22 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), columns (property uid), and whether the column contains **metric**[1] or **attribute**[2] values.

Also see "How to View Collection Information" on page 78 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.<br>See the AQL Developer Guide for more information. |
| collection | Specifies the name of the collection for which Operations Analytics should return search results. |
| custom | Indicates that Operations Analytics cannot identify the argument type.<br>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 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.<br>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 Analytics to use.<br>See the AQL Developer Guide for more information. |
| metric | Either of the following:<br>○ Name of the metric column.<br>○ Tag that represents the metric column. |
| ordering | Specifies an argument required for the `order by` clause. |

3. *Optional*. Use the **Visualization** tab to change the visualization that is displayed.
   a. Navigate to the **Visualizations** tab.
   b. Navigate to the Visualizations options:

[1] Typically a measurement stored in a collection. For example, CPU utilization.
[2] A descriptor stored in a collection for an entity, such as host_name.

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 Analytics displays the default visualization for the AQL query.

See "Working with Query Panes" on page 28 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 Analytics console. For example, if you specify a time interval using the $interval parameter, Operations 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**.

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" in the HPE Operations Analytics Configuration Guide .

### 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

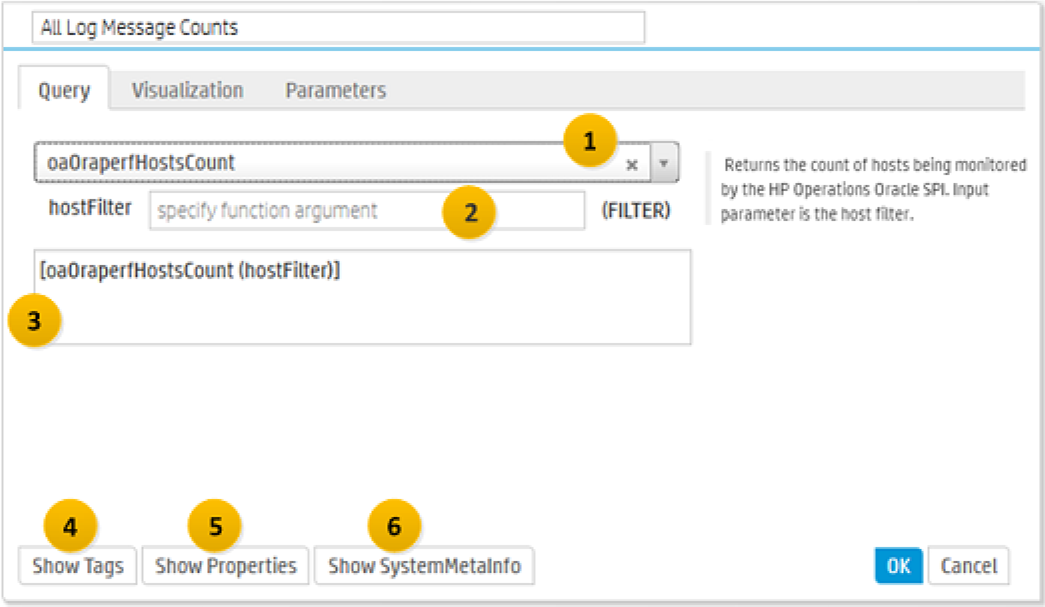
| Item | Description |
|---|---|
| Dashboard Name List | Operations Analytics lists all of the dashboards available for your use. These include:<br>• Dashboards created by the current user.<br>• Dashboards shared by other users in the same user community (tenant). |
| New | Creates a new dashboard. |
| Save As | If you are in an unsaved dashboard as a result of a search, Save As saves the search results as a dashboard.<br>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 **Dashboards** menu.<br>**Note:** 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.



All Log Message Counts

oaOraperfHostsCount

hostFilter: specify function argument (FILTER)

Returns the count of hosts being monitored by the HP Operations Oracle SPI. Input parameter is the host filter.

[oaOraperfHostsCount (hostFilter)]

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 Analytics and your Operations Analytics administrator.

   Your Operations 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 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 Analytics administrator.

   Argument values are usually stored as meta data for your Operations Analytics collection. Use the **Dashboards** menu to navigate to the **SystemMetaInfo** 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 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 Analytics server:

   - `$OPSA_HOME/inventory/lib/hp/aql`

   - `$OPSA_HOME/inventory/lib/user/aql`

   > **Tip:** Your Operations 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**[1] or **attribute**[2]) that is stored in the associated column.

6. **View the SystemMetaInfo Dashboard**

   Enables you to view the SystemMetaInfo 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**[3] or **attribute**[4]

   See "How to View Collection Information" on page 78 for more information.

[1] Typically a measurement stored in a collection. For example, CPU utilization.
[2] A descriptor stored in a collection for an entity, such as host_name.
[3] Typically a measurement stored in a collection. For example, CPU utilization.
[4] A descriptor stored in a collection for an entity, such as host_name.

# Chapter 3: Search Tool

The search tool allows you to create a dashboard by focusing on elements in your environment.

The search tool is located in the top right of the user interface. It searches for elements in your environment and creates a dashboard focusing on the specified item.

The search tool uses a proprietary query language called Phrased Query Language (PQL). This language is presented in a user friendly format and for the most part detailed syntax knowledge is not required. After you start typing, suggestions are automatically displayed. For more information about PQL syntax, see below.

# Learn About

### Example PQL queries

For the purposes of these example, the example host name is `myhost.enterprise.com` and the Los Angeles office domain is `la.enterprise.com`

| Query | Results |
|---|---|
| `oracle performance withkey *enterprise.com` | Display all metrics associated with the tags **oracle** and **performance** for all host names in the ***.enterprise.com** domain. |
| `cpu_util withkey *enterprise.com` | Display the values for the **cpu_util** metric for all host names in the ***enterprise.com** domain. |
| `Host: example.servername.hp.com` | 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.<br>**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. |
| `opsa withkey *enterprise.com,instance1` | Display the metrics associated with the tag **opsa** for the local host and for all hosts in the enterprise.com domain. |
| `service withkey MyService filtering groups withkey groupName1` | Used to filter the collection of database metrics for MyService. Displays only results for the database metrics for the group named **groupName1**. |
| log("`connection error\"`") | Displays log entries with the string "**connection error ""** |
| log("`severity AND critical`") | Displays log entries that include the strings "severity" AND "critical" |

| Query | Results |
|---|---|
| service withkey MyService1 | returns all information for MyService1 |
| service withkey MyService1 filtering groups | returns all information for the group configured for MyService1 |
| service withkey MyService1 filtering groups withkey groupName1 | returns the related groups information for only the instance named **groupName1** |
| Multiple Hosts ("host1", "host2", "host3*") dashboard | returns a dashboard focusing on the following hosts: 1, 2, and any host starting with the string "host3" (such as "host345") |

## Search Tool Syntax - Advanced

The search tool uses statements that conform to one of the following models:

- tag1 tag2 withkey key attribute1, key attribute2, key attribute3
- tag1
- metric1 withkey key attribute1, key attribute2, key attribute3
- metric1

- If a key attribute includes a space, it must be in quotes. For example "my item".
- Multiple tags can be used. When more than one tag is present, the results returned are only those in which both tags are present.
- Aterisks (*) can be used as wildcards throughout the query.
- The keyword **service** indicates you want the query to return only the data related to the topology service you specify.

  ```
  service withkey myservicename
  ```

  Returns a dashboard with information about the service myservicename

  ```
  service withkey service1 filtering groups withkey group1
  ```

  Returns a dashboard with information about group1 within the service myservicename.
- Use the following syntax to query log files:

  ```
  "<string>"
  ```

  ```
  log ("<string> AND|OR <string>")
  ```

  To include quotes within your search query, precede each quote with the backslash character.

  You can also include tags in your log queries. For example, `system log("severity AND critical")` finds all metrics tagged system and log file messages containing **severity** and **critical**.

**Tip:** To view the tags and column names defined in your environment, see the SystemMetaInfo dashboard.

# Tasks

### How to use the search tool

1. Click inside the Search tool and select the type of item you want to search for. You can select suggested items or manually type at any time.
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 Analytics uses its default dashboard layout and populates the dashboard with the data requested by your search.

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

# Chapter 4: Working with Query Panes

This section describes the different types of charts and visualizations used to display data in Query Panes.

# Learn About

## Data Types

### Moving Aggregate Data Visualizations

Operations Analytics presents moving aggregate (time series) data as line charts, heat maps, bar charts and pie charts. Moving aggregate (time series) data is data that is 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 hosts in a specified domain at 1 hour intervals for the last 24 hours.

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

### Overall Aggregate Data Visualizations

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

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

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

### Default Visualizations

If you select a visualization that is not supported by your Analytics Query Language (AQL) search query, Operations Analytics uses the default visualizations described in the following **Default Visualizations** tables. See "Dashboards and Query Panes" on page 12 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 Analytics displays a bar chart by default. You can also use topN and bottomN analytic functions to visualize pie charts and tables.

## 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 that are measured by your metrics. To do so, select **Group by Entity** or **Group by Metric**.
- Select the entities or metrics to display by using the drop down menu.
- Select the group to display by using the **Go To Page** menu or the arrows at the bottom of the pane.

## About Heat Maps

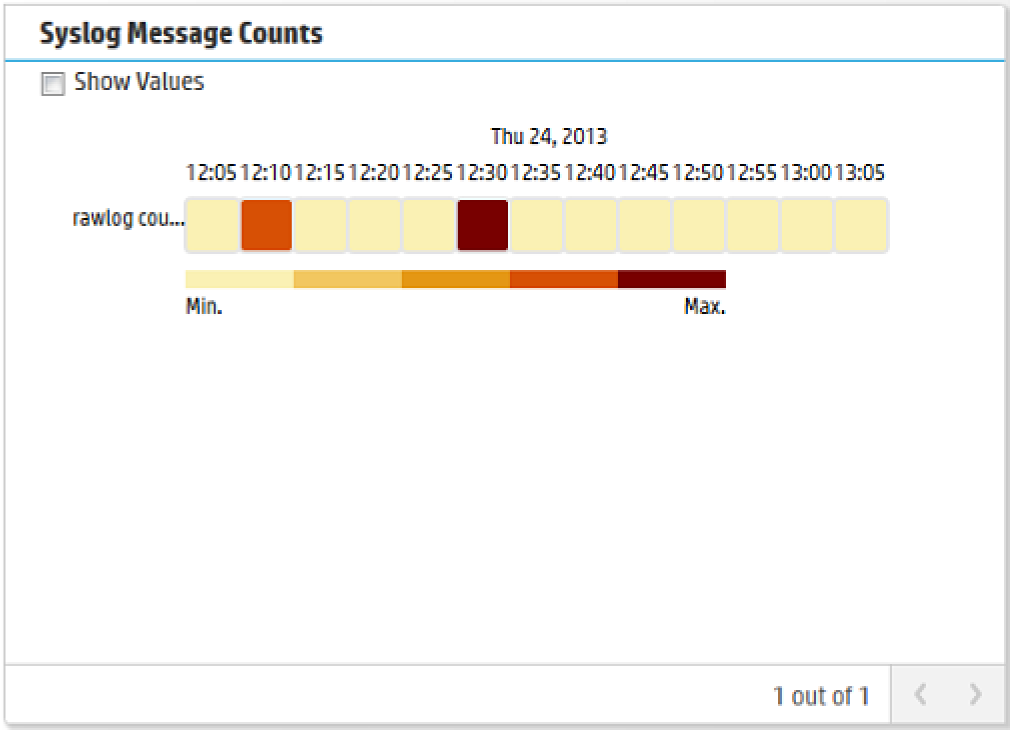
You can use moving aggregate (time series) analytic functions to display your results as a heat map.

Moving aggregate (time series) analytic functions display 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 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 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.

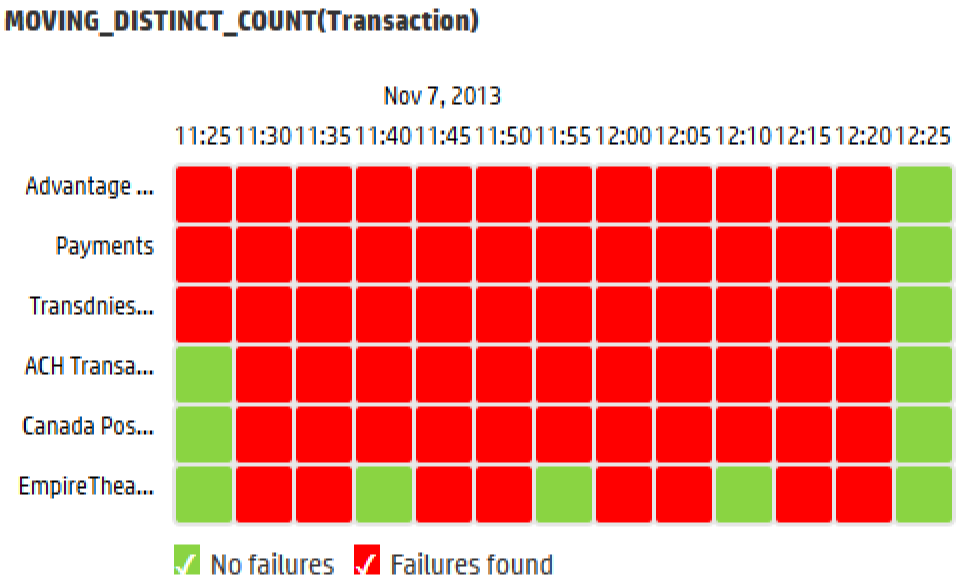
The following heat map example displays the number of syslog log file messages generated over a specified time period:



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 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 seconds will appear as 46m).
- Some dashboards provided by Operations Analytics use heat maps to display metrics that indicate some type of failure. Operations Analytics uses green to indicate **No failures** and red to indicate **Failures found**.

For example:



You can perform the following operations on heat maps:

## Display the value within each heat map cell

You can display the first few characters of the value that is represented within each heat map cell by clicking ✓**Show Values**.

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

**To re-calculate 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 Analytics recalculates the heat colors based on the new minimum and maximum values.

## View additional heat maps in a query pane

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

### Modify the color scheme

Operations 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 Analytics displays multiple line charts in a single query pane when the Analytic Query Language (AQL) search query requests in multiple line charts.
- Operations Analytics displays 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 are displayed in the list, select **Group by Entity** or **Group by Metric**.
- To display 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

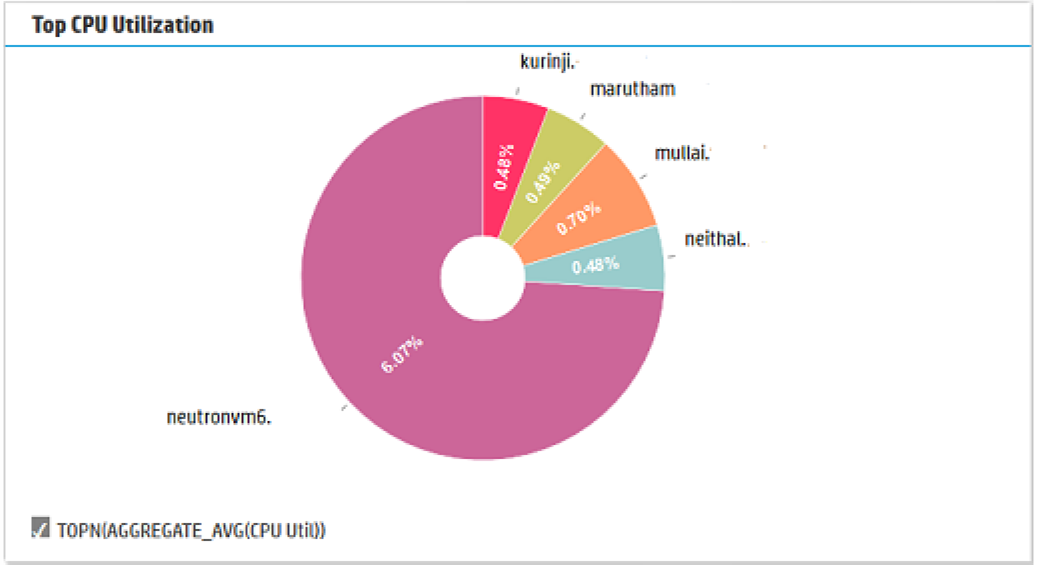
You can use both moving aggregate (time series) and overall aggregate (summary) analytic functions to display your results as a pie chart.

Moving aggregate (time series) analytic functions display 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 hosts in a specified domain at 1 hour intervals for the last 24 hours.

Each moving aggregate value displayed represents a re-computed value using each data points 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 Analytics displays each of these re-calculated values, one per pie chart segment.

Overall aggregate (summary) data is data that is 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 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 display 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 Analytics uses a darker color to indicate there is more of a particular value and a lighter shade of the same color to indicate there is less of a value.
- Gray indicates no values are available.
- Operations 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 display, use the dropdown menu.
- To return the sunburst chart to its orignial detail, click the center of the chart.
- To drill down 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 Analytics presents overall aggregate data as bar charts, pie charts, or tables. Overall aggregate data is data that is grouped by total, average, minimum, or maximum values within a specified time range.

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

> **Note:** Operations Analytics also displays 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 be displayed. Operations 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 Analytics initially displays a maximum of eight columns.
- If more than eight columns are returned from the search, Operations 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 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 display 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 39.

# Chapter 5: Filter Search Query Results

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

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

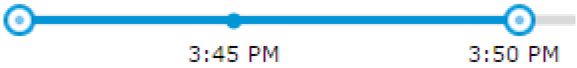
Operations Analytics enables you to focus on a specified time segment using the slide bar that appears above the metrics, log file and event data displayed. For example, you might want to focus on a particular day or a particular peak period.

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

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:

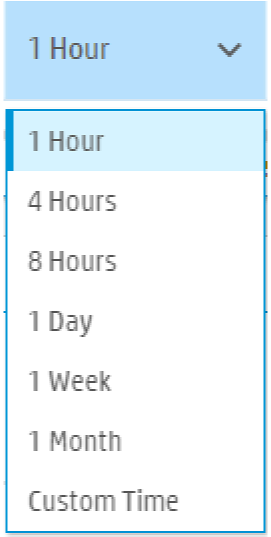


Operations Analytics filters the information available to focus only on the time segment you selected in each of the metric visualizations displayed. The log file and event information is also filtered based on the time segment you specify.

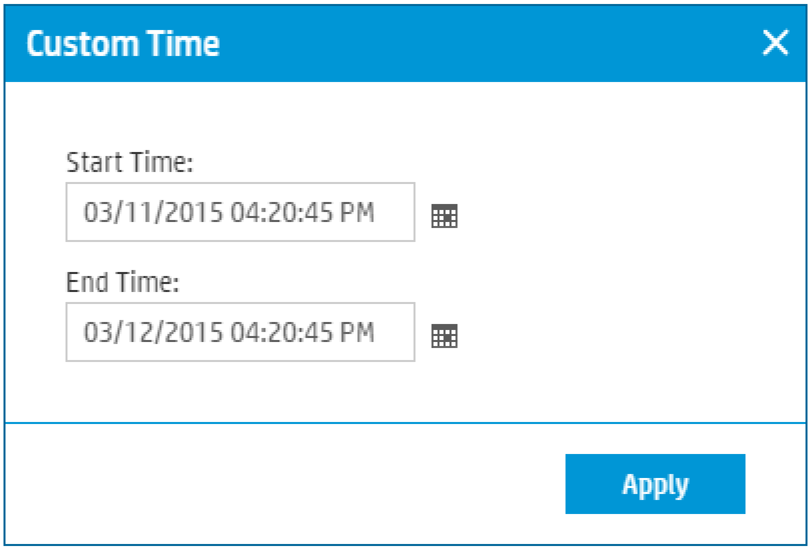
Use the Time Range option to filter the results by a specified time period.

**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 displayed:



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



Custom Time

Start Time: 03/11/2015 04:20:45 PM

End Time: 03/12/2015 04:20:45 PM

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

Filter result:

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 25 for more information.

# Chapter 6: Play Back History

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

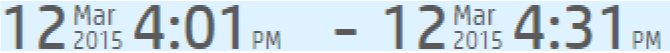
  **Note:** If you provide an $interval parameter value in a **query pane**[1], Operations Analytics uses the $interval value you specify for the time segment for only that query pane . See "Dashboards and Query Panes" on page 12 for more information.

**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 unpause 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 Analytics replays only the results for the current query pane.

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



12 Mar 2015 4:01 PM - 12 Mar 2015 4:31 PM

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

[1] Displays the results of an Analytic Query Language (AQL) query, AQL function, or AQL expression. If you use the Phrased Query Language (PQL) in your search, HP Operations Analytics converts the PQL query to one or more AQL queries and subsequent query panes.

To exit playback mode, click ✕.

# Chapter 7: 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.

# Learn About

### About Log and Event Analytics

Searching for the root cause of a problem can be daunting. Even using PQL searching technology, knowing where to start can be difficult. Operations Analytics has designed powerful Log and Event Analytics algorithms that create a lista of the top suspected log messages and events and display 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 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 Workflow

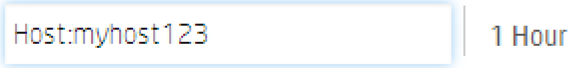
1. Make sure that Log and Event data is coming into Operations Analytics.
   - Log data can come from either Splunk or Logger. For details about how to configure this, see "Configure Log Integrations" on page 62.

   - Event data for Log and Event Analytics can only come from the following collections:

Custom, Operations Manager Events (Windows), Operations Manager i Events, and Operations SPI for Oracle.

For details about setting up these collections, see "Configuring Collections " on page 82

2. Search for a host, groups of hosts, or a service using the search tool.

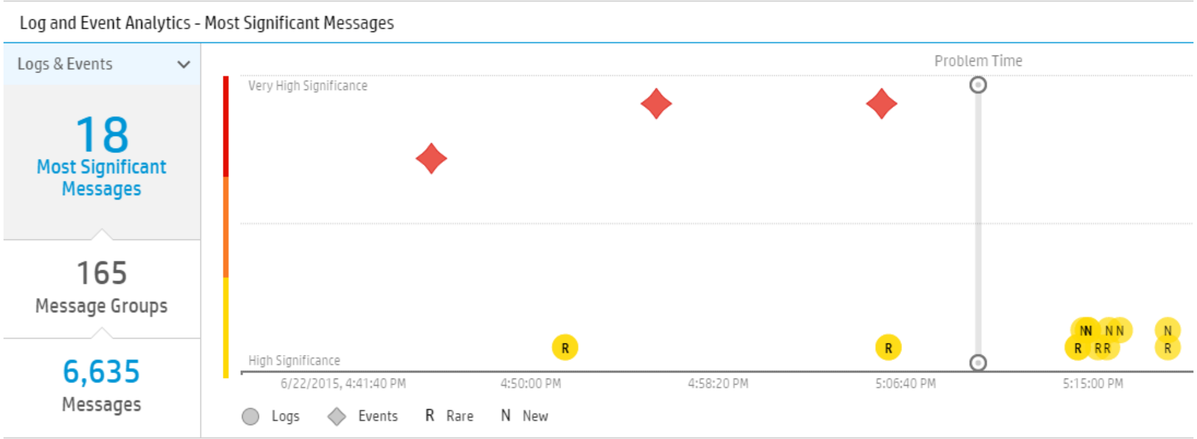


Host:myhost123

1 Hour

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

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 Analytics then recalculates the most significant messages based on the problem time you select.



4. Hover over the bubbles and diamonds in the graph to view the tooltips. At this point in the procedure, all additional steps are optional and you can stop as soon as you have located the root cause of your problem.

5. Click a circle or the area labeled **X Most Significant Messages** on the left to open the log viewer.

> **Note:** To open the log and event viewer in the general log messages tab, select the area labeled **X Messages.**

6. Use the filtering capabilities of the log and event viewer to locate the root of your problem.

   a. Use the fields at the top of each column to filter the results. For example, if you type "error" in the field at the top of the Message Text column, the results will be limited to items that have the string "error" in the message text. Alternatively, you can double-click a word in the message text column to filter the results by that word.

   > **Note:** You can use a variety of custom expressions in the Message Text field. For details, see below.

   b. Select **Show liked only** to display message groups that you have previously liked using the 👍 button.

   c. You can manually ignore individual message groups by using the ignore ⊖ button. You can later restore these items by using the **Ignored Messages** button.

7. You can view the distribution of all messages that are similar to a specific message by viewing the graphs on the bottom right of the log viewer. When you select a message, the distribution of messages with the same group ID is displayed. When you select underlined text in the message text field, the distribution of messages with different values for the underlined text is displayed.

   Select either Parameter Distribution or Parameter Over Time to display different graphs about the parameter. These selections affect what data is collected and displayed if you track this parameter.

   > **Example:** The message text is "Processing error on server 1234" You can click the string "1234" to view the distribution of server names for all messages that have the same text and the same group ID.

8. To track a message group or parameter and display it in a dashboard, Select ⌖ Track Message Group or ⌖ Track Parameter. For more details, see "Track Message Groups and Parameters" on page 44.
9. To view all messages, including non-significant messages, select the **All messages** tab.

## 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 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 log viewer, 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 log viewer, 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(<aqllit></aqllit>, $starttime, $endtime, $problemtime)**

For details about creating custom query panes, see "How to Add or Edit a Query Pane" on page 19.

## How to Search for Strings in Log and Event Analytics

You can improve your expressions when searching for strings by using the tips in this section. They are applicable in both the Text field of the Log Viewer and the *Expressions field of the Log and Event Analytics Settings user interface.

| Expression | Meaning |
|---|---|
| and | Search for both strings before and after the expression.<br>**For example:** *one and two* means search for the strings "one" and "two". |
| a space between strings | Spaces are interpretted as and expressions<br>**For example:** *one two* means search for the strings "one" and "two". |
| or | Search for either the string before or after the or expression.<br>**For example:** *one or two* means search for "one" or "two". |
| "expression" | Search for the exact expression (whole word only).<br>**For example:** *one and two* means search for the exact expression "one and two".<br>**Tip:** To search for a string that contains any of the other expressions described in this table such as ( ),? and, or, * put them in quotation marks " ".<br>**Limitation:** You cannot search for a string in which the string itself contains quotation marks " ". |
| ( ) | Groups expressions<br>**For example:** *(one or two) and three* means search for the string "three" and either "one" or "two". Parentheses can be used multiple times and can be stacked in expressions like *four and (three or (one and two))*. |
| * | The wildcard expression is intrepreted as any number of characters (including 0).<br>**For example:** *User*23* means search for the string "UserX23" where X is any string including empty.<br>**Exception:** If you use * at the end of a word and no other wildcard expressions are used, the results will only return strings that occur at the beginning of a message. |

| | |
|---|---|
| ? | The limited wildcard expression is interpreted as one unknown character.<br>**For example:** *User?23* means search for the string "UserX23" where X is any one character. |

## How to Modify the Color Scheme

Operations Analytics enables you to choose from a number of different color schemes for different visualization types. The top three colors in each scheme are used for Log and Event Analytics visualizations.

Click the Settings ⚙ button and select **Color Scheme**.

# Chapter 8: 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.

### To Access:

Navigate to Log and Event Analytics. For details, see "Log and Event Analytics" on page 39. Select Track Message Group or Track Parameter.

## 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 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.

Once 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.

> **Note:** This features is only available for the logs that are included in the Log and Event Analytics user interface.

## User Tasks

### How to Track a Message Group

1. Navigate to Log and Event Analytics. For details, see "Log and Event Analytics" on page 39.
2. Select a message group or parameter.
3. Select Track Message Group or Track Parameter

   > **Note:** If you are tracking a numeric parameter, the data that will be displayed depends on the view you have selected in Log and Event Analytics at the time you click the **Track Parameters** button. If you have selected **Parameter Over Time**, data over time will be collected. If you have selected **Parameter Distribution**, data will be collected about the various values of the parameter and their prevalence.

4. Complete the user interface:
   a. Specify a message group name if this group was not already named.
   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 in search results when searching for related hosts.
   d. You can add tags to the tracked message group or parameter in order 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.

# Chapter 9: 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 Analytics can predict the future behavior of some metrics and display this information in a query pane. The prediction line is displayed 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 displays 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 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.

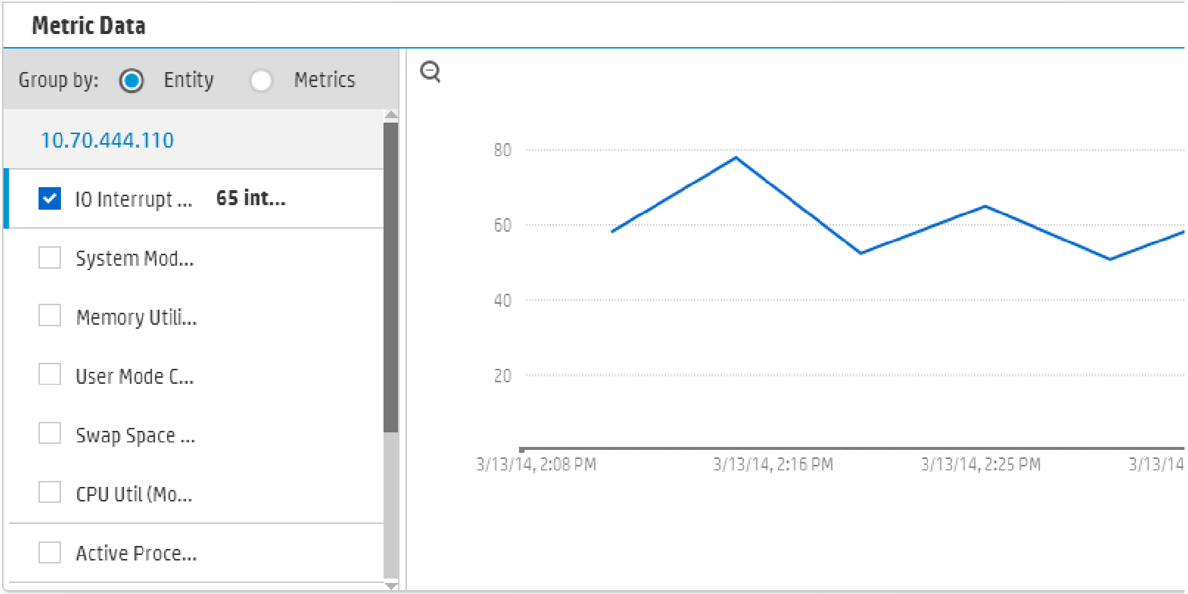
**Limitations:**

- 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 wish 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 displays the margin of error, click ↗.
5. To remove the prediction lines, click **Disable Predict** Predict.

# Chapter 10: Alerts

Alerts allow you to trigger different actions based on conditions and time intervals that you specify. This feature allows you to use Operations 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, or send an SNMP trap.

Alerts are created based on AQL queries. The query is taken from a pane, but can be modified in the alerts wizard. Once 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 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 configure an OMi Agent to retrieve alerts from Operations Analytics and create events from the alerts. For details, see the HPE Operations Analytics - BSM Integration Guide.

## About Alert Types

**Abnormality based Alerts.** Operations 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 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. Others 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 Analytics environment. For options about how to increase this maximum number, speak to HPE 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** 💼 and select **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 the previous page.
4. Complete the **Create Alerts Wizard**. Details of selected user interface elements are described below.

   First Page

| UI Element | Description |
|---|---|
| **Alert Type** | For details about the different alert types, see "About Alert Types" on the previous page.<br>• **Abnormality based alert on selected metrics.** Create an abnormality based alert. Select up to ten metrics to use.<br>• **Threshold based alert on selected metrics.** Create a threshold based alert. Select up to ten metrics to use.<br>• **Threshold based alert on all metrics.** Create a threshold based alert using all metrics. |
| **Select Metrics** | Select up to ten metrics. This option is only relevant for some alert types. |
| **Define Alert** | Once you click **Define Alert**, you will not be able to return to this page of the wizard. |

Details Page

| UI Element | Description |
|---|---|
| **Severity** | Select the severity you would like to associate with instances of this alert. |
| **AQL** | 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.<br>Once the alert is created, there is no connection between the query in the original 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. |
| **Check data in the last..** | When calculating whether or not to trigger an alert, the query is run over this time period. |
| **Test AQL** | 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 |
|---|---|
| **Run every**<br>**Run weekly**<br>**Run monthly** | Determines how often to check if an alert should be triggered.<br>**Note:** This schedule is determined by the client time zone, not the server time zone.<br>We recommend making sure this value is less than the value for the Check data in the last setting. For details, see "Best Practices - Defining Alert Schedules" on the previous page. |

| UI Element | Description |
|---|---|
| **Abnormal Results Definition** | 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.<br>You can see a graphic representation of the abnormal and normal ranges as you modify your selections.<br>• **Normal Range.** The size of the sleeve surrounding the dynamically generated threshold that defines a normal AQL results.<br>• **Value is** The location that results can be considered abnormal.<br>• **and also** 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).<br>**For example:** 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 “and also above 50”. In this case, the range must be more than 5 standard deviations away from the baseline average AND over 50% . |
| **Trigger if number of results** | 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 |
|---|---|
| **Send email** | Specify the email recipients and email subject. If there is more than one recipient, separate them using commas. For example:<br>email1@abc.com,email2@abc.com<br>You must specify which domains are permitted in the Alerts Settings. |

| UI Element | Description |
|---|---|
| **Run script** | This option is disabled if there are no scripts in the /opt/HP/opsa/inventory/lib/user/alerts/scripts/<tenant_name> directory.<br>Input script parameters separated by commas. You can use any script parameters, as well as the following Operations Analytics variables as parameters:<br>**<<AlertLink>>:** A link to an Operations Analytics dashboard focusing on the alert instance.<br>**<<AlertId>>** - The alert ID.<br>**<<AqlDefinition>>** - The alert AQL query.<br>**<<AlertName>>** - The alert name.<br>**<<AlertUserId>>** - The user ID of the alert owner.<br>**<<AlertTrigger>>** - The alert trigger condition.<br>**<<AlertTimeFrame>>** - The alert calculation time period.<br>**<<AlertSeverity>>** - The alert severity.<br>**<<AlertAqlResultCount>>** - The number of results of the alert query over the defined time period.<br>**<<AlertDescription>>** - The alert description.<br>**<<AlertID>>** - The ID of the alert.<br>**<<AlertType>** - The type of the alert.<br>**Note:** You can configure Operations Analytics to run alert scripts using only one specified operating system user for security purposes. For details, see "How to Run Alert Scripts Using a Specific Operating System User" on page 54. |
| **Encrypt** | Encrypts the script parameters. This is recommended when passwords are included in the parameters. |
| **SNMP** | 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. |
| **Perform action on every trigger** | Perform the alert action every time an alert is triggered. |
| **Perform action at most once every** | This prevents the alert action from happening too frequently.<br>**Note:** You can use this action to prevent notifications from redundant alerts, for details, see "Best Practices - Defining Alert Schedules" on page 49. |
| **Run Test Alert** | This triggers a test alert with the name **TestAlert<alertname>**. 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 via the **Alerts Manager** user interface.

- 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 dasboard provided by Operations 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 via the **Alerts Manager** user interface. If an alert is deactive, it is saved but no alerts are triggered and no actions are taken. Active alerts are fully functional. The Alerts Management user interface can be found by clicking the Settings ⚙ button.

### How to Edit an Alert

You can edit alert definitions via the **Alerts Manager** user interface. The Alerts Management user interface can be found by clicking the Settings ⚙ button.

# Administrator Tasks

### How to Set up Alert Action Capabilities

Before you can configure alerts to trigger an action, an Operations 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 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, go to the Settings ⚙ Menu 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 Analytics Alerts" in the HPE Operations Analytics Configuration 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, go to the Settings ⚙ Menu 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 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 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.

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

You can configure Operations Analytics 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 applicance 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 **opsaadmin**

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 Analytics alerts use the same Vertica database resource pool as Operations 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 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 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 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)})]
   ```

3. Log messages with the string "Collection configuration".

   ```
   aqlrawlog(<aqllit>(message CONTAINS "Collection configuration") </aqllit>,$starttime,$endtime,"",$limit)
   ```

4. Log messages with the strings "Collection" AND "configuration".

   ```
   aqlrawlog(<aqllit>(message CONTAINS "Collection" AND message CONTAINS "configuration") </aqllit>,$starttime,$endtime,"",$limit)
   ```

5. Log messages with the string "error".

```
aqlrawlog(<aqllit>(message CONTAINS "error")</aqllit>,$starttime,$endtime,"",$limit)
```

6. 404 error messages.

   ```
   aqlrawlog(<aqllit>(message CONTAINS "404") AND (sourceServiceName CONTAINS "OPSA")
   </aqllit>, $starttime, $endtime, "", $limit)
   ```

7. Log messages with critical severity.

   ```
   aqlrawlog(<aqllit>(sourceServiceName CONTAINS "OPSA") AND (agentSeverity CONTAINS
   "Critical")</aqllit>, $starttime, $endtime, "", $limit)
   ```

8. 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
   ```

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

   ```
   from i in (nnmispi_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 11: 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 |
|---|---|
| **Metric A Entity, Metric B Entity** | The entity of the metric in the metric A or B name column.<br>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 string1::string2 where string1 filters column A and string2 filters column B.<br>You can drill down to open a dashboard focusing on the entity by selecting an entity in this column.<br>**Note:** There is no significant difference between columns A and B. They are just identifiers. Each metric is compared to every other metric exactly once. |
| **Metric A Name, Metric B Name** | The name of the metric.<br>You can sort the column by clicking the column header.<br>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.<br>**Note:** There is no significant difference between columns A and B. They are just identifiers. Each metric is compared to every other metric exactly once. |
| **Correlation (r)** | The correlation value indicating how closely correlated Metric A and B are to each other. For more details, see "Correlation Values (r)" on the previous page |

# Chapter 12: 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 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

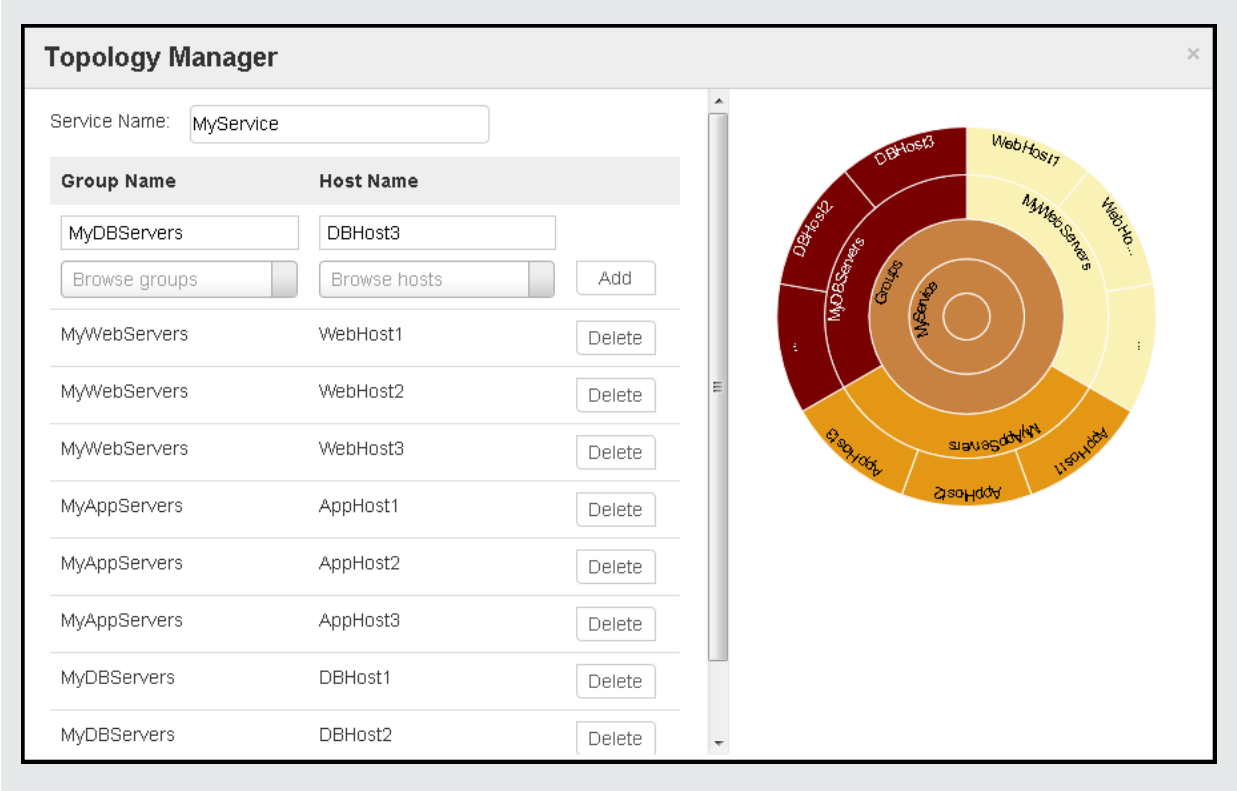
### How to define a service:

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 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.
4. 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.



Topology Manager

Service Name: MyService

| Group Name | Host Name | |
|---|---|---|
| MyDBServers | DBHost3 | |
| Browse groups | Browse hosts | Add |
| MyWebServers | WebHost1 | Delete |
| MyWebServers | WebHost2 | Delete |
| MyWebServers | WebHost3 | Delete |
| MyAppServers | AppHost1 | Delete |
| MyAppServers | AppHost2 | Delete |
| MyAppServers | AppHost3 | Delete |
| MyDBServers | DBHost1 | Delete |
| MyDBServers | DBHost2 | Delete |

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 execute 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 25.

# Chapter 13: Configure Log Integrations

Log data is imported from Arcsight Logger or Splunk by configuring a Log Integration.

# Learn About

### About Importing Log Data

In order for Operations Analytics to import log data from Splunk or Arcsight Logger, you must specify the hosts of the data sources and create mapping files. Mapping files specify how Operations Analytics should interpret the log data. For Splunk, these files are stored on the Operations Analytics Server. For Arcsight Logger, these files must be manually copied to the Arcsight Logger environment.

> **Note:** Operations Analytics server logs are imported automatically after you set up the first log integration with Arcsight Logger.
>
> To view Operations Analytics collector logs, you need to run opsa-flex-config.sh on each Operations Analytics Collector host and perform the following steps from the command line:
>
> 1. Review the list of Logger hosts already configured for the opsa_default tenant.
> 2. Enter the serial number of the Logger host for which you want to configure the Operations Analytics Log File Connector for HPE Arcsight Logger.

### Supported Configurations

Instances of Arcsight Logger and Splunk are connected to Operations Analytics Collector hosts. The following limitations apply to combinations of instances:

- You can only configure a Log Integration for either Arcsight Logger or Splunk, but not both.
- You can configure each instance of Arcsight 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(s).

1. Select the Log Integration ⊞ button and specifying whether you will import data from Arcsight Logger or Splunk.
2. Specify the details of one Arcsight Logger or Splunk host.
3. Define additional sources as desired at any time by ⊞ > **Logger Instances** or **Splunk Instances**.
4. Continue with the appropriate mapping procedure depending on your data source.

- "Map Arcsight Logger Data" below
- "Map Splunk Data" on page 68

# Map Arcsight Logger Data

If you have not configured a Connector for 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 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 Log Integration ⊞ and select **Flex Configuration**.
2. Go the **My Configuration Files** tab and select Create New.
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

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.

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 fo rthe 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 OK.

To modify a field that is already defined, click Edit ⌄.

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 "Date and Time Symbols" on page 68. |
| 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.<br>**Note:** 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. |

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 | 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.<br>Notes:<br>• 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.<br>• You can specify a range of numbers only by specifying the lower number first as seen in the following example: 300..400<br>• 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.<br>• Values that are unmapped will be mapped to severity "unknown".<br>• At least one value from the sample data must be mapped successfully to complete the wizard. |

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 Add 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 Publish to create the file, or Prev 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 Analytics Community

1. Go to Log Integration ⊞ and 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 Test, 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 Edit Locally.

## 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 Operations Analytics are only valid for FlexConnector types **Regex Log File** and **Regex Folder File**.

1. Go to Log Integration ⊞ and select **Flex Configuration**.
2. Select a desired file from the **My Configuration Files** tab or from **Community Configuration Files** tab and click Download.
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 HPE 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 **sdkrfilereader**.

   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 Log Integration ⊞ and 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 Analytics Community

1. Go to Log Integration ⊞ and 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 |
| 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 log data is imported from Splunk, Operations Analytics must map specific key columns in order 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 Operations Analytics servers are not processed and sent to Operations Analytics when using Splunk. This is not the case for Arcsight 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. Go to Log Integration ⊞ and select **Splunk Configuration**.
2. Open the **Source Type Mapping Wizard** in one of the following ways:
   - Select a line in the table whose Status is **Not Mapped** and click Map.
   - Select New Source Type
   - Select a line whose Status is **Activated** and click Edit.
3. 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 Analytics. To resolve unparsed data, try one of the following strategies:

   - Go back and modify the source value in the previous tab.
   - 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:

- **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 Add 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 **Activate** to validate your settings, create and enable the mapping.

> **Note:** Settings configured in all other tabs are verified at this stage.

4. 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 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

You can edit mapping files that were not created manually by going to Log Integration ⊞, selecting **Splunk Configuration**, and clicking **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.

# Chapter 14: About Collections

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 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 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 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 Analytics looks for that value in all key columns across collections.

Note the following:

- When you define a service using the Topology Manager, Operations 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 59 for more information.

### About Tags

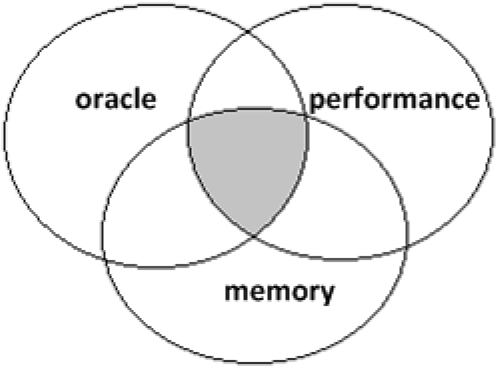
A tag is a word that is associated with a collection or with a metric or attribute that is stored as part of a collection.

Tags are used in the Operations Analytics Phrased Query Language (PQL) to create an Operations 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 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 Analytics refines the search to include only those metrics associated with the host name you specify.

As an Operations 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 "Configure Your Collections" in the HPE Operations Analytics Configuration Guide for more information.

To view the tags available for a collection, see "How to View Collection Information" on page 78 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 **performance** might be used for that collection. | When you type **performance** 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 **host** might be used as a synonym for the attribute **host_name** | When you type **host** in your search query, Operations Analytics uses the value stored for **host_name** in each collection table for which the tag is defined. |

### Uses for Tags, continued

| Use | Example | Result |
|---|---|---|
| Group attributes that provide similar information | The tag **cpu utilization** might be used to represent the following CPU attributes:<br>• cpu_idle_time<br>• cpu_sys_mode<br>• cpu_util_time<br>• cpu_util<br>• cpu_user_mode<br>• cpu_context_switch_rate<br>• cpu_run_queue | When you type **cpu utilization** in your search query, Operations Analytics uses the values stored for the CPU attributes in each collection in which the tag **cpu utilization** is defined. |
| Focus on attributes that are prototypical | The tag **primary** might be used to tag the most important metric attributes for a specific area, such as cpu). This means that when the user enters **cpu primary** in the search query, the results focus on only a few important metrics, which are tagged as **primary**. | When you type **<*hostname*>cpu** in your search query, Operations Analytics uses the following metrics in its results.<br>• cpu_idle_time<br>• cpu_sys_mode<br>• cpu_util_time<br>• cpu_util<br>• cpu_user_mode<br>• cpu_context_switch_rate<br>• cpu_run_queue<br>When you type <***hostname***>**cpu primary** in your search query, Operations Analytics might use only the following metrics in its results.<br>• cpu_util<br>• cpu_user_mode |
| Group attributes across collections | The tags **performance primary** could be used for the attributes that assist with identifying performance problems across collections.<br>As another example, you might tag all metrics that are useful for identifying status or health information across collections. | When you type **performance primary**, Operations Analytics returns performance metrics from both the HPE Operations Smart Plug-in for Oracle and HPE Operations Agent collections. |

### Uses for Tags, continued

| Use | Example | Result |
|---|---|---|
| Dynamically extend your collections | Use the same tag name for more than one collection. For example, you might use the tag name **event** and **events** for the following collections:<br>• HPE Operations Manager (OM)<br>• HPE Operations Manager i (OMi) | When you type <*host name*> **events** in your search query, both the Operations Manager i events and Operations Manager events data is used to return your results. |

## About Meta Data

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

- Collection table names.

  > **Note:** Operations 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**[1] or a **metric**[2].

- 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 sources. The data collected is organized by collections.

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

Each server that is running the Operations Analytics Collector agent is configured as a Collector Appliance.

See "Adding a New HPE Operations Analytics Collection" the HPE Operations Analytics Configuration Guide for more information.

## About Collections

Operations 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 Analytics Collector stores the data collected.

> **Note:** These collection tables are identified in the Operations 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.

[1] A descriptor stored in a collection for an entity, such as host_name.
[2] Typically a measurement stored in a collection. For example, CPU utilization.

As the Operations Analytics administrator, you configure one or more data sources per Operations Analytics collection.

See "Configure Collections" in the HPE Operations Analytics Configuration Guide for information about how to configure collections.

## Collection Data Sources

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

- The Operations Analytics administrator configures the collection data sources.
- Operations Analytics data sources marked with an asterisk (*) indicate the data sources for which Operations 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 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 Analytics:** no.

### Log files and Structured Log Files

**Description:** Collects raw log file information. These log files must be configured in HPE ArcSight Logger or Splunk. If you are an Operations Analytics administrator, see the HPE Operations Analytics Configuration Guide for more information.

**Required Software:**

- **Regular Log Files:** HPE ArcSight Logger
- **Structured Log Files:** HPE Operations Analytics or Splunk

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

**Examples of Types of Log Files Collected by Default:** syslog, database, applications, network device log files.

### 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 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 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 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 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 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 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 Manage i Software.

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

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

**Examples of Inventory Collected by Default:** CiId, 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 Analytics:** no.

# Tasks

### How to View Collection Information

Operations Analytics stores metrics, topology, inventory, log file, and event information in the form of collection tables. Becoming familiar with the data collected is useful to help determine the type of queries you might want to perform. For example, you can include the collection name or its associated tag name to return all data from a specified collection. Because each collection is stored as part of a database table, you might also specify a collection column name (for example, cpu_util) to return a subset of data across one or more collections. See "Search Tool" on page 25 for more information.

When viewing collection information, use the mapping described in the table below to determine the collection information to include in your queries.

> **Note:** As shown in the mapping table, 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**[1] or a **metric**[2]. The property groups are uniquely identified by **property group uid** and properties are uniquely identified within a property group by **property uid**. When specifying a collection name or column name in your search query, use the **property group uid** and **property uid** values.

### Column Descriptions for Meta Data Tables

| Information | Table Column Name Displayed in the Dashboard |
|---|---|
| Collection names | property group uid |
| Columns (metrics or attributes) per collection | property uid |
| Tag names, if any, per collection or column | tag name |
| Columns defined as keys. | Look for rows in which the iskey value is true |

> **Note:** You can also use opsa-tag-manager.sh (available from help > reference pages) to view tag information.

**To view collection information**:

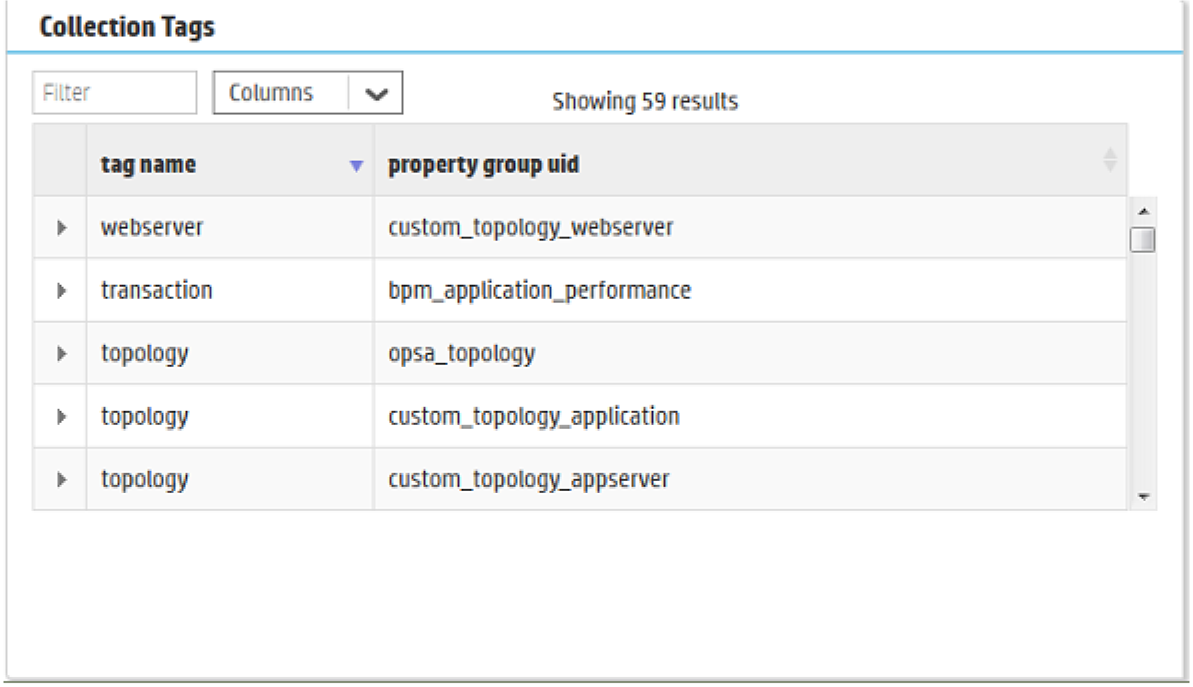
1. Navigate to the **Dashboards** menu.
2. Select **SystemMetaInfo**.

   > **Tip:** You can also access this dashboard using the **Show SystemMetaInfo** option when adding or editing a query pane.

   Operations Analytics displays tables that include the following information:

[1] A descriptor stored in a collection for an entity, such as host_name.
[2] Typically a measurement stored in a collection. For example, CPU utilization.

- Tags, if any, assigned to each collection (property group uid):

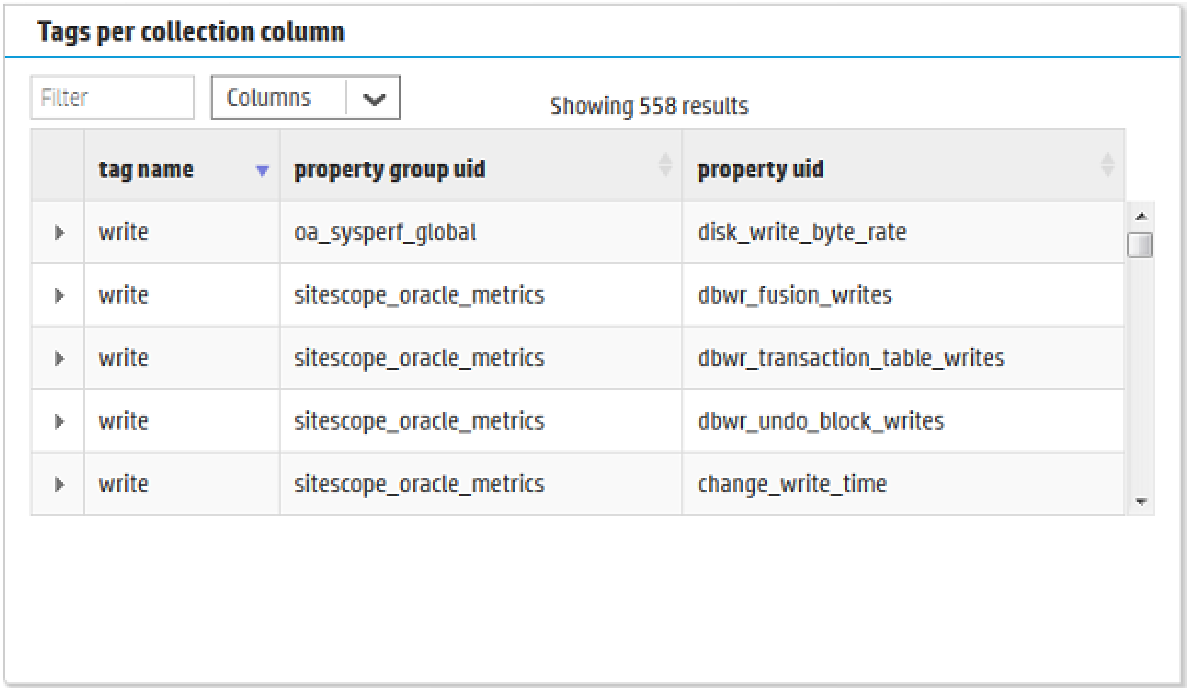


**Collection Tags**

Showing 59 results

| | tag name | property group uid |
|---|---|---|
| ▸ | webserver | custom_topology_webserver |
| ▸ | transaction | bpm_application_performance |
| ▸ | topology | opsa_topology |
| ▸ | topology | custom_topology_application |
| ▸ | topology | custom_topology_appserver |

- Tags associated with columns (property uid) within each collection.

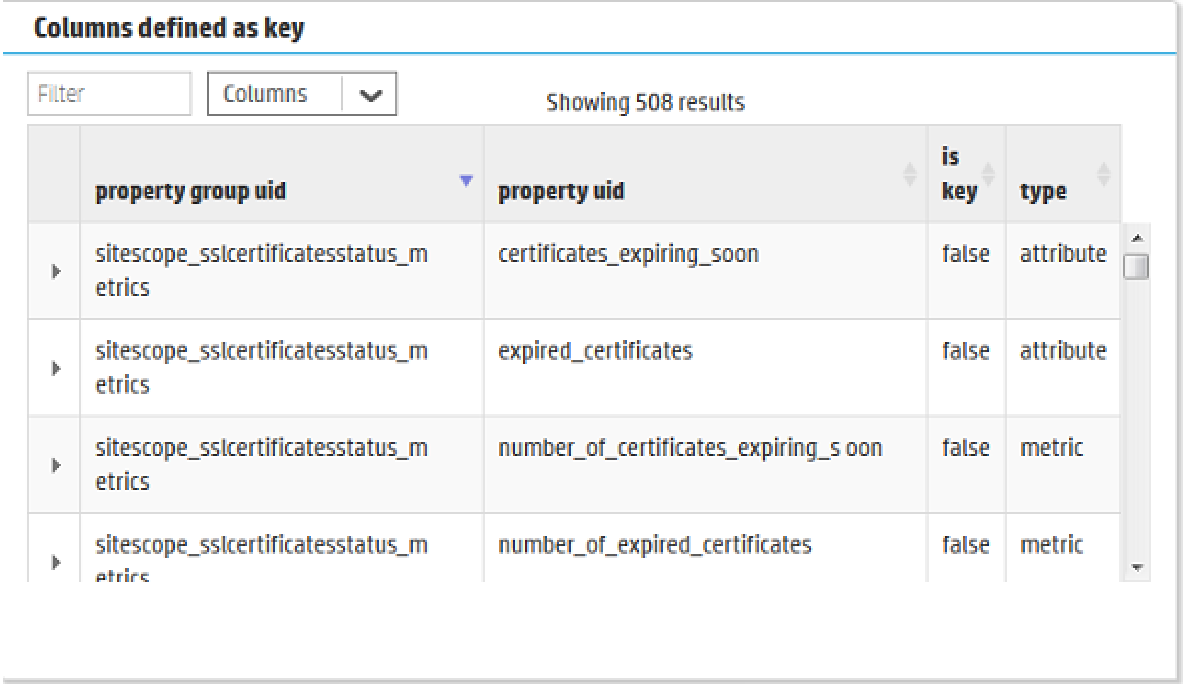


**Tags per collection column**

Showing 558 results

| | tag name | property group uid | property uid |
|---|---|---|---|
| ▸ | write | oa_sysperf_global | disk_write_byte_rate |
| ▸ | write | sitescope_oracle_metrics | dbwr_fusion_writes |
| ▸ | write | sitescope_oracle_metrics | dbwr_transaction_table_writes |
| ▸ | write | sitescope_oracle_metrics | dbwr_undo_block_writes |
| ▸ | write | sitescope_oracle_metrics | change_write_time |

- Columns that are configured as key columns (iskey) in each collection. Key columns are used to filter metrics across collections.



Columns defined as key

Showing 508 results

| | property group uid | property uid | is key | type |
|---|---|---|---|---|
| ▸ | sitescope_sslcertificatesstatus_metrics | certificates_expiring_soon | false | attribute |
| ▸ | sitescope_sslcertificatesstatus_metrics | expired_certificates | false | attribute |
| ▸ | sitescope_sslcertificatesstatus_metrics | number_of_certificates_expiring_s oon | false | metric |
| ▸ | sitescope_sslcertificatesstatus_metrics | number_of_expired_certificates | false | metric |

See "About Table Data" on page 33 for more information about working with tables.

# Chapter 15: Configuring Collections

To configure Operations Analytics to collect data from the supported data sources you plan to use, you must configure collections.

This topic focuses on the preferred method of configuring collections: using the Collections Manager user interface.

**Caution:** If you use the Collections Manager to edit and publish an existing collection, all of the previously collected data will be lost.

You can also configure collections by running the opsa-collection-config.sh script. See the Operations Analytics Configuration Guide for more information.

**Note:** The collection configuration instructions shown in this section do not include configuring collections for the Operations Analytics - HPE OneView integration. Operations Analytics configures those collections when you enable the integration. See the Operations Analytics - HPE OneView Integration Guide for more information.

# General Tasks

### How to Access the Collections Manager

1. Log on to the Operations Analytics console with the tenant administrator credentials for your tenant. This would be the **opsatenantadmin** user when using the default tenant.
2. Click the **Settings** menu in the upper right.
3. Click **Collections Manager** to open the Collections Manager.
4. Click **Add Collection Instance** to pull down a list of potential collections and select the collection you want to configure.

   **Note:** You must register each Operations Analytics Collector Appliance you plan to use with the Operations Analytics Server Appliance. If this pull-down list is disabled, there is no Operations Analytics Collector Appliance registered for your tenant. See *Registering Each Collector Appliance* in the *HPE Operations Analytics Configuration Guide* for more information.

### How to Delete a Collection

When viewing the **Collections Manager** screen, notice the **Stop Collecting** and **Delete** buttons in the upper right. If you no longer want to analyze data for a collection, do the following:

**Note:** For SiteScope collections, the Collections Manager does not permit you to delete only one instance, rather it deletes all instances of the this type that are connected to the same Operations Analytics collector. To delete one instance, use the **opsa-collection-setup.sh** script to delete a connection to the SiteScope server. For details, see the Operations Analytics Configuration Guide .

1. In the **Collections Manager**, select the collection you want to remove.
2. **Do only one of the following**:
   - To stop collecting data for the selected collection click the **Stop Collecting** button.

     **Note:** Selecting this button stops the collection of more data, but does not drop the database tables for the selected collection.

   - To stop collecting data for the selected collection and purge the existing collected data, click the **Delete** button.

     **Note:** Selecting this button stops the collection of more data, and drops the database tables for the selected collection.

     **Note:** Clicking the **Delete** button does not remove any dashboards related to the deleted collection.

**Note:** To view information about an existing collection, select one of the existing collections from the **Collections Manager**, then click **View** in the upper right.

# Collection Specific Tasks

## BSM RTSM CIs

1. Specify Collection Details

| Name | Description |
|---|---|
| **Collector Host** | Select the fully-qualified domain name or IP address of the common collector that will collect data for this collection. |
| **RTSM Host Name** | Determine the fully-qualified domain name of the RTSM DPS server. |
| **RTSM User Name** | Determine the user name to use for connecting to the RTSM DPS server. This value is typically `admin`. |
| **RTSM Password** | Determine the password for the RTSM user name to use for connecting to the RTSM DPS Server. |
| **RTSM Port** | 21212 |

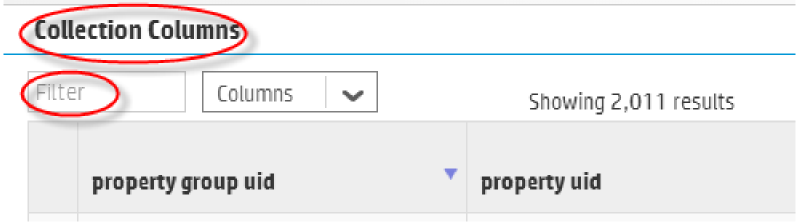
| Name | Description |
|---|---|
| **Create collection without correctness validation** | Select this check box if you want to create a collection without validating that it can connect to the data source. This is useful for creating a collection with a non-existing data source, then manually copying data to data input folders on the Operations Analytics collector. |

2. Click **Create Collection** to create and publish a new collection or **Override Collection** to modify an existing collection.
3. Validate the Collection Results

   Let the collection run for five minutes or longer. From the Operations Analytics Console, view the **OpsA Meta Info** dashboard. Look for the **property group uid** for the collection you just created and published.

   After typing the property group uid (`rtsm_ci_inventory`) for this collection in the **Collection Columns Filter**, you should see information for this collection.

   a. Type the property group uid (`rtsm_ci_inventory`) for this collection in the **Collection Columns Filter**:



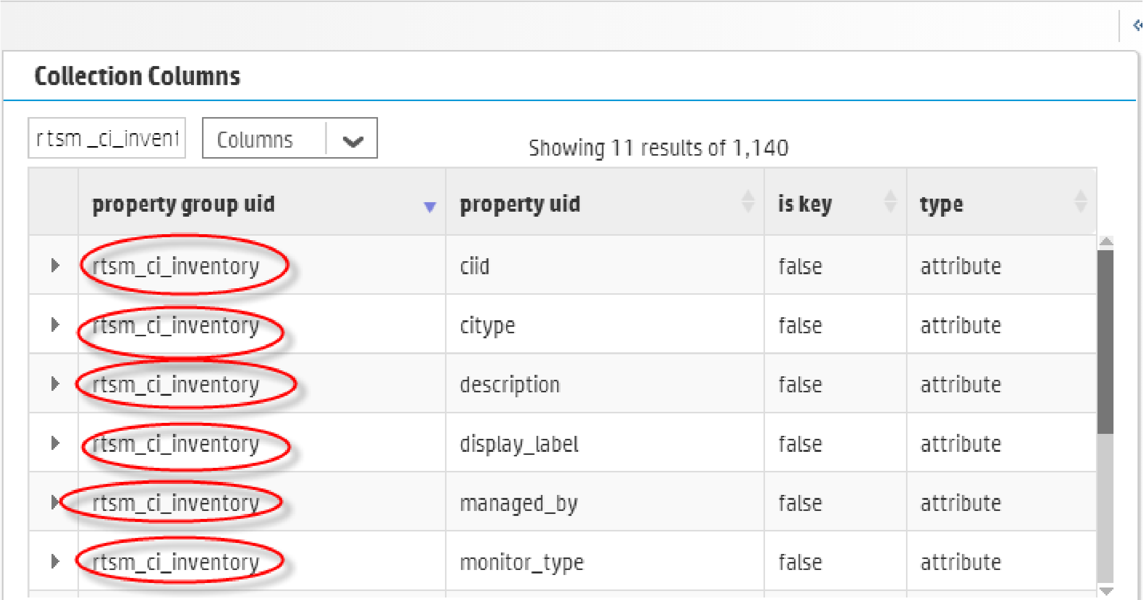
Collection Columns

Filter | Columns

Showing 2,011 results

| property group uid | property uid |
|---|---|

   b. After typing the property group uid (`rtsm_ci_inventory`) for this collection in the **Collection Columns Filter**, you should see information for this collection.



Collection Columns

rtsm_ci_invent | Columns

Showing 11 results of 1,140

| property group uid | property uid | is key | type |
|---|---|---|---|
| rtsm_ci_inventory | ciid | false | attribute |
| rtsm_ci_inventory | citype | false | attribute |
| rtsm_ci_inventory | description | false | attribute |
| rtsm_ci_inventory | display_label | false | attribute |
| rtsm_ci_inventory | managed_by | false | attribute |
| rtsm_ci_inventory | monitor_type | false | attribute |

4. Next Steps

a. Create dashboards and query panes for the data you are now collecting. See "Dashboards and Query Panes" on page 12 for more information.

b. 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 AQL Developer Guide for more information.

c. If you want to add tags to an BSM RTSM CIs Collection, use the opsa-tag-manager.sh command. See *Creating, Applying, and Maintaining Tags for Custom Collections* in the Operations Analytics Configuration Guide and the *opsa-tag-manager.sh* reference page (or the Linux manpage) for more information.

## Business Process Monitor

1. Specify Collection Details

| Name | Description |
|---|---|
| **Collector Host** | Select the fully-qualified domain name or IP address of the common collector that will collect data for this collection. |
| **BSM DPS Host Name** | Determine the host name of the active BSM DPS Server. |
| **RTSM Integration User Name** | Determine the RTSM Admin user name. |
| **RTSM Integration Password** | Determine the RTSM Admin password. |
| **RTSM Port** | 21212. Other ports required to be required open for the Operations Analytics cluster are 80, 1098, 1099, 2506, 2507, and 29602. |
| **Create collection without correctness validation** | Select this check box if you want to create a collection without validating that it can connect to the data source. This is useful for creating a collection with a non-existing data source, then manually copying data to data input folders on the Operations Analytics collector. |

- **RTSM Port**: 21212. Other ports required to be required open for the Operations Analytics cluster are 80, 1098, 1099, 2506, 2507, and 29602.

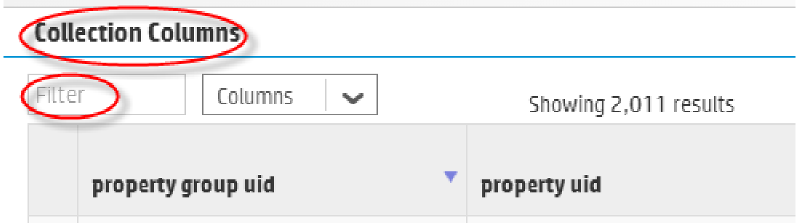
- **Create collection without correctness validation**: Select this check box if you want to create a collection without validating that it can actually connect to the data source. This is useful for creating a collection with a non-existing data source, then manually copying data to data input folders on the Operations Analytics collector.

2. Click **Create Collection** to create and publish a new collection or **Override Collection** to modify an existing collection.

3. Validate the Collection Results

   Let the collection run for five minutes or longer. From the Operations Analytics console, view the **OpsA Meta Info** dashboard. Look for the **property group uid** for the collection you just created and published.

   a. Type the property group uid (`bpm_application_performance`) for this collection in the **Collection Columns Filter:**

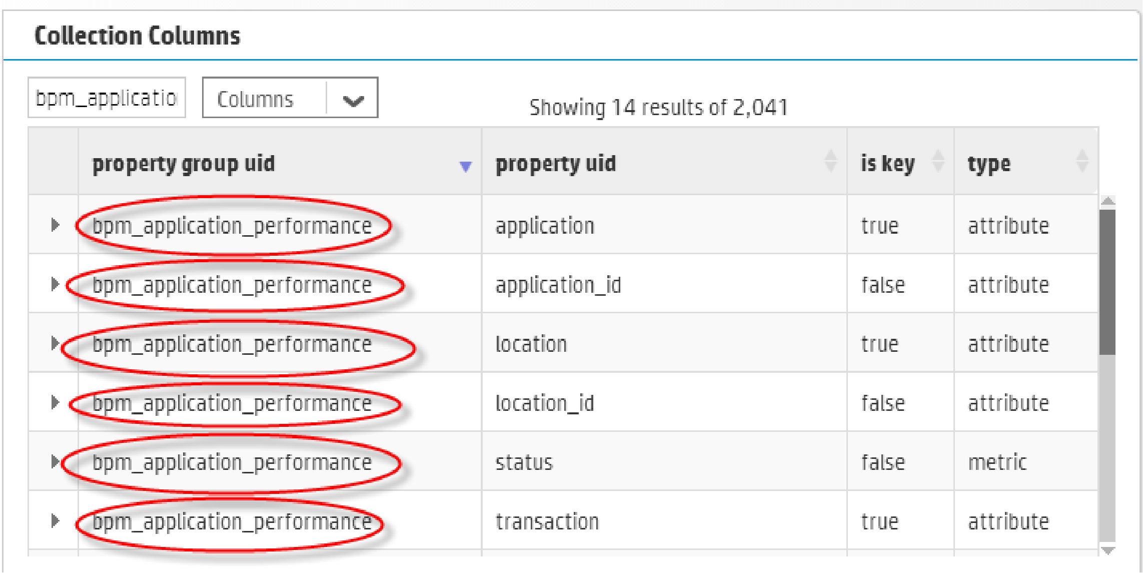


Collection Columns

Showing 2,011 results

| | property group uid | property uid |
|---|---|---|

b. After typing property group uid (`bpm_application_performance`) for this collection in the **Collection Columns Filter**, you should see information for this collection.

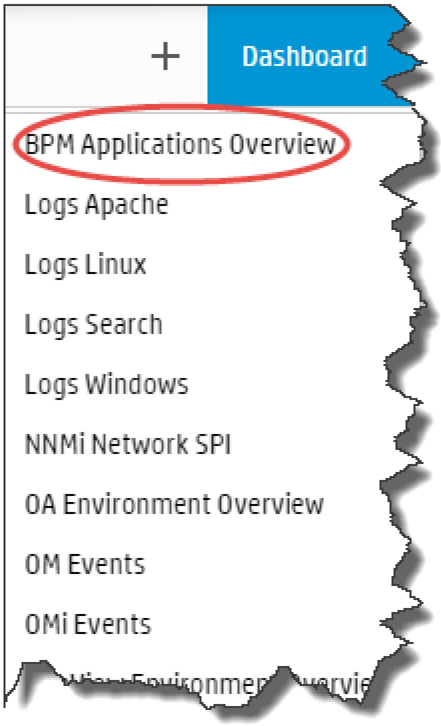


Collection Columns

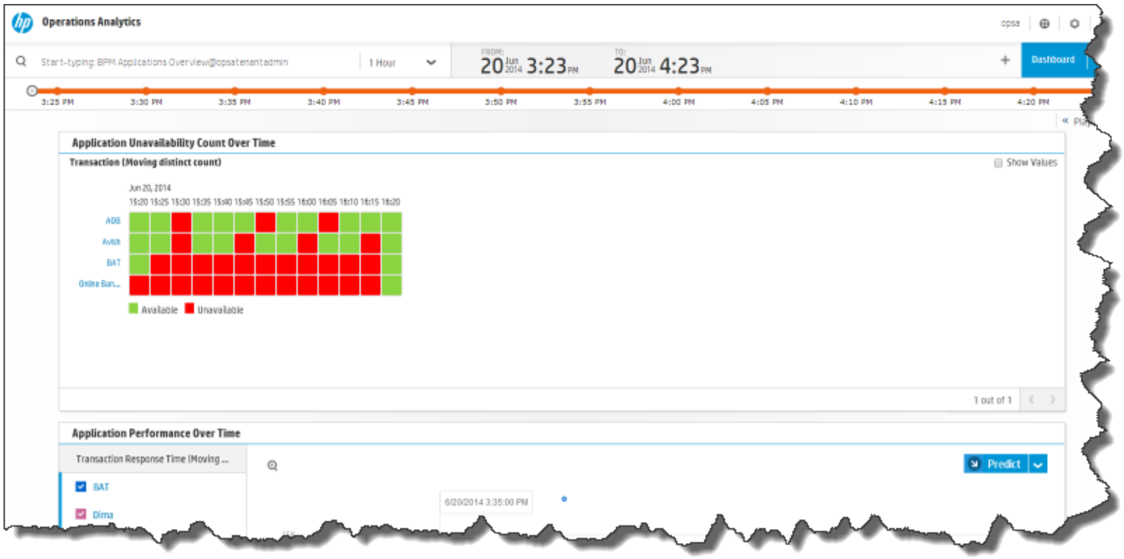
Showing 14 results of 2,041

| | property group uid | property uid | is key | type |
|---|---|---|---|---|
| | bpm_application_performance | application | true | attribute |
| | bpm_application_performance | application_id | false | attribute |
| | bpm_application_performance | location | true | attribute |
| | bpm_application_performance | location_id | false | attribute |
| | bpm_application_performance | status | false | metric |
| | bpm_application_performance | transaction | true | attribute |

c. From the Operations Analytics console, open the **BPM Applications Overview** dashboard to view some of the collected information for this collection:



The following is a small sample of the Business Process Monitor Collection data provided by the **BPM Applications Overview** dashboard.


Operations Analytics
opsa
Start-typing: BPM Applications Overview@opsatenantadmin
1 Hour
FROM: 20 Jun 2014 3:23 PM
TO: 20 Jun 2014 4:23 PM
+
Dashboard
3:25 PM
3:30 PM
3:35 PM
3:40 PM
3:45 PM
3:50 PM
3:55 PM
4:00 PM
4:05 PM
4:10 PM
4:15 PM
4:20 PM
Application Unavailability Count Over Time
Transaction (Moving distinct count)
□ Show Values

Jun 20, 2014

| | 15:20 | 15:25 | 15:30 | 15:35 | 15:40 | 15:45 | 15:50 | 15:55 | 16:00 | 16:05 | 16:10 | 16:15 | 16:20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ADB | 🟩 | 🟩 | 🟥 | 🟩 | 🟩 | 🟩 | 🟥 | 🟩 | 🟩 | 🟥 | 🟩 | 🟩 | 🟩 |
| Avish | 🟩 | 🟩 | 🟥 | 🟩 | 🟩 | 🟥 | 🟩 | 🟩 | 🟥 | 🟩 | 🟩 | 🟥 | 🟩 |
| BAT | 🟩 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟩 |
| Online Ban... | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟩 |

🟩 Available 🟥 Unavailable

1 out of 1
Application Performance Over Time
Transaction Response Time (Moving ...
☑ BAT
☑ Dima
Predict
6/20/2014 3:35:00 PM

4. Next Steps

   If you want to add tags to a Business Process Monitor Collection, use the `opsa-tag-manager.sh` command. See *Creating, Applying, and Maintaining Tags for Custom Collections* in the Operations Analytics Configuration Guide and the *opsa-tag-manager.sh* reference page (or the Linux manpage) for more information.

## Custom Collection

You can configure Operations Analytics to collect and process data from sources of structured data. You can also configure Operations Analytics to collection data from TCP, UDP, or JDBC data sources. These collections are described in the configuration instructions shown below.

Use the following instructions to create your custom collection.

1. Prerequisites

   Data sampling in Operations Analytics channels

   All of the Operations Analytics channels initially sample data from the data source so that it helps the users to view the sample data and create Operations Analytics meta data mapping in the **Data Configuration** page. This sample data must include at least 3 records from the data source for the sampling to succeed. The Operations Analytics sampling process stops automatically after receiving three records. The configurations you specify in the channel instance definitions must bring in a minimum of three records.

   > **Note:** Operations Analytics uses the same configuration for the production mode of the channel instance as well. So your configurations can bring in more data depending on your choice, however a minimum of three records are required. The Operations Analytics sampling process waits for three minutes for the three sample records to appear before it times out.

   **TCP**

   Before you start creating a TCP channel, note that the TCP channel supports the option to communicate with the remote data source in a secure way using SSL. To set up SSL, you must prepare the certificates and keys on your Operations Analytics Collector host. The TCP channel requires that you at least provide both certificate and key store paths. Key passphrases and a CA Certificate path might also be required depending on your choice of SSL mechanisms. To generate a simple certificate and key store, you can complete steps similar to those shown below.

   > **Note:** the steps shown below are only examples, and you might need to perform different steps depending on your choice of the SSL mechanism.

   Run the following commands from the Operations Analytics Collector host:

   a. `mkdir /home/opsa/my_certs`
   b. `cd /home/opsa/my_certs`
   c. `openssl req -x509 -batch -nodes -newkey rsa:2048 -keyout 1.key -out 1.crt`

   Do the following from the Operations Analytics console when setting up the TCP Channel in SSL mode:

   a. Set **isSSLEnabled** to `true`
   b. Set **Verify Remote Identity** to `false`
   c. Specify the **ssl certificate path** as `/home/opsa/my_certs/1.crt`
   d. Specify the **ssl key path** as `/home/opsa/my_certs/1.key`
   e. Make sure the **ssl ca cert path** is empty
   f. Make sure the **ssl key passphrase** is empty

   > **Note:** As mentioned earlier, the above steps are just an example. You might need to set **Verify Remote Identity** to `true`, specify the **key passphrase**, or configure other selections depending on your organization's security policies. If you choose not to enable SSL, traffic between the TCP

> channel and the remote data source will be visible in plain text to potential listeners.

TCP data sampling

The TCP channel can operate in **server mode**, where the channel listens for data, or in **client mode** where it connects to a remote TCP server and pulls data. If the TCP channel is configured in s**erver mode**, ensure that the TCP channel has started listening on the specified port as mentioned in the UDP section.

### UDP

UDP data sampling

The UDP channel only operates in server mode. After you enter the UDP channel instance configurations and click **Next**, it takes a few seconds for the UDP channel to start listening on the specified port. Log on to the appropriate Operations Analytics Collector host and ensure that the channel has started listening on the specified port before you send records to the UDP channel from your remote data source. All of the records sent to the UDP channel before it starts listening are lost. You can check if the UDP channel has started listening by running the following command: `netstat –ap | grep <specified port number>`. Sometimes the port number that you specified might have a service name entered in the `/etc/services` file. If that is your situation, you must use the following command: `netstat –ap | grep` *`<service name corresponding to the specified port number>`*

### JDBC

Before you begin creating a JDBC channel, you must understand the JDBC channel operation mechanism. The JDBC channel connects to the specified database and pulls the data at periodic intervals using the SQL statement that you specify. Specify the interval by making an entry in the **Schedule** field using the crontab time format.

The SQL statement you supply will be adjusted by the channel in the following way:

a. A **Start Time** filter will be added to the SQL statement by adding a where clause that specifies that the SQL Timestamp column is greater than the Start Time.

   > **Note: Start Time** has a default value when nothing is entered.

b. The channel pulls data from the database in batches. Specify the batch size by making an entry in the **Batch Size** field.

c. The JDBC channel remembers the timestamp of the last row pulled from the table in a persisted mechanism (including across channel restarts). If a restart occurs or during the next pull interval the channel pulls data from the table location where it left off.

Determining the JDBC channel batch size

Plan the JDBC channel’s batch size according to your database’s incoming data traffic speed and the size of the data in each row. The JDBC channel performs a blocking read of the batch. The batch size and data size directly affect both the memory required and the execution duration for the JDBC channel while reading the batch. You need to decide the optimal batch size based on your database’s data configuration.

> **Note:** If you anticipate your JDBC collection being greater than 1000 entries per minute (EPM), do not use a JDBC collection. Switch to using a CSV collection and use an Extract Transform Load (ETL) process for the data you are collecting.

JDBC data sampling

The JDBC channel connects to the specified database and runs the specified SQL statement to pull the records.

> **Note:** The **Start Time** specified in the JDBC form influences the running of the SQL statement. Ensure that you specify a start time (either default or your input) that would return enough data for sampling.

**File**

If you plan to work with the **File** option shown in the next step, do only one of the following before you select the **File** option:

- If you are using Operations Analytics in a distributed configuration (you are not using Operations Analytics All-in-One for HPE OneView), create a source directory in the following location on each selected collector host (for each selected Operations Analytics Collector Appliance): `/opt/HP/opsa/data/<directory name>`.
- If you are using Operations Analytics All-in-One for HPE OneView, create a source directory in the following location on the Operations Analytics All-in-One for HPE OneView appliance: `/opt/HP/opsa/data/<directory name>`.

2. Click one of the following:
   - **TCP**, located beneath the **Communication Protocols** heading.

     > **Note:** For data collections based on a TCP channel.

   - **UDP**, located beneath the **Communication Protocols** heading.

     > **Note:** For data collections based on a UDP channel.

   - **JDBC**, located beneath the **Databases** heading.

     > **Note:** For data collections from HPE Vertica, Microsoft SQL Server, or Oracle.
     >
     > For JDBC data collections, use the most current driver for the database version you are using.

   - **File**, located beneath the **Filesystem** heading.

3. Complete the **Source Data** step.

   For descriptions of the entry fields, hover over the ? icon shown in the Operations Analytics console.

   When completing this step, if Operations Analytics displays errors related to parsing the data with the selected data format, see *Troubleshooting Collections Manager Error Messages* in the *HPE Operations Analytics Configuration Guide*.

   When editing the **SQL Statement** field for a JDBC collection, Operations Analytics disallows commands considered to be "write" commands that might alter the collected data. Operations Analytics permits commands considered to be "read" commands. The **SQL Statement** field includes automatic statement validation for compliance with permitted and disallowed commands. This validation includes, and is not limited to, the following disallowed commands and characters:

- Disallowed commands: `update`, `insert`, `delete`, `create`, `into`, `drop`, `truncate`, `grant`, or `revoke`

  > **Note:** To view or modify these disallowed commands, edit the `/opt/HP/opsa/logstash/sql/blacklist.conf` file on the Operations Analytics Server.

- Disallowed special characters: `;`, `#`, or |

  > **Note:** This list of characters is disallowed on the Operations Analytics Server and the Operations Analytics Collector hosts. This list of disallowed characters cannot be modified.
  >
  > You can use these characters inside of strings as shown by the use of the `#` character in the following example:
  >
  > `select * from customers WHERE Country='the #1 country'`

> **Note:** After you publish a Custom collection containing an **SQL Statement**, **Collector Hosts**, **Name**, **Data Format**, or **Mode** field, you can no longer modify any of those fields when editing that collection.

> **Note:** After you publish a Custom collection, if you decide to make collection configuration changes, you must wait up to two minutes for Operations Analytics to process the initial data before editing that collection.

About the Data Format Selection and Morphline

**Apache Morphline** uses rich configuration files that make it easy to define data transformations. If you are familiar with using Apache Morphline, and have specific JSON configuration files tailored to your data formats, you can use this in Operations Analytics by placing these files in the `/opt/HP/opsa/conf/collection/server/format.content/` folder on the Operations Analytics Server Appliance. The configuration files you place in this directory will show up as selections in the **Data format** pull-down menu the next time you refresh the browser.

- For Operations Analytics, that means the **Data Format** selection step in this section supports the following data formats:.
  - Comma Separated
  - Pipe Separated
  - Colon Separated
  - Semicolon Separated
  - Generic_JSON: JavaScript Object Notation (JSON)
- During the **Data Format** selection step, select a format that needs to be applied to parse the input data you placed in the **Source data directory** you provided in an earlier step.

4. Complete the **Data Configuration** step. By analyzing a sample of the data you provided, Operations Analytics provides default values for this collection. This step provides you a chance to review the defaults, then make changes for correctness.

| Name | Description |
|---|---|
| **Relevant Columns** | Select the data columns for the data you want this collection to retain. Deselect those data columns you do not want this collection to retain. |
| **Timestamp column** | Select the timestamp value you want to use for this collection. |
| **Timestamp format** | This value changes with the timestamp value you select and supports the timestamp value in the **Timestamp column** field.<br>Operations Analytics attempts to determine the correct timestamp format from the data you placed in the **Source data directory**. If it cannot make that determination, you must type the correct value into the **Timestamp format** field.<br>**Note:** If you must type this value, the value you enter must be accurate and match the timestamp format as it appears in the data column you selected for the **Timestamp column**. You can view the timestamp data directly in by viewing the table column for the value shown for the **Timestamp column**.<br>**Tip:** See the Java Platform, Standard Edition 7 API Specification for examples of supported date and time (timestamp) formats. |

Operations Analytics provides an editing tool for the **Label**, **Type**, **Tags**, **Key**, **Data type**, and **Units** table rows. Edit the table, making any supported changes you need.

> **Note:** If Operations Analytics could not determine a data column's type, it automatically assigns the type as `metric`. Use the editing tool to make any necessary changes to the assigned type.

> **Note:** When selecting data columns to be **Key** fields, set no more than three columns to a Key value of **true**.

5. Use the **Preview** step to view the resulting dashboard from the sampled data and with the changes you made in the **Data Configuration** step. If the dashboard does not show data as you would expect, click **Prev** to review and make additional changes for correctness. After you are satisfied with the dashboard results, click **Next**.
6. In the **Summary** step, review the details to understand how to view your data after it is published.

   > **Tip:** To view additional information about a collection after publishing it, select the collection from the Collection Manager, then click **View**.

7. Click **Publish** (located in the upper right of the Operations Analytics console) to create and publish this collection and create the preview dashboard from the **Preview** step.

> **Note:** After you complete these steps and publish a collection and its associated dashboard, you can fine tune the query results by editing the generated AQL in the dashboard query editor.

8. Optional: To validate the collection results, do the following:
   a. From the Operations Analytics console, view the **OpsA Health** dashboard. Check that the row count for this collection name shows green in the **Row Count of Collected Metrics and Logs** graph.
   b. From the Operations Analytics console, view the **OpsA Meta Info** dashboard:

      Enter the property group uid for this collection in the **Collection Columns Filter**. The property group uid is the name of the string (in the form of `custom_metric_<collectionname>`.

      This verifies that the collection published successfully.
9. Optional: If this collection includes events, you can enable Event Analytics for these events in order to calculate and present the most significant messages for a selected time range. Do the following:
   a. In **Collections Manager** select this custom collection.
   b. Click **Event Analytics**.

      See "Log and Event Analytics" on page 39 for more information.
10. Optional: To enable the topology feature to recognize hosts coming from this collection, perform the following steps:
   a. Enable the JMX console by changing the suffix of the following file on the server applicance from **.tx** to **.txt**:

      **/opt/HP/opsa/conf/jmxNotHardened.tx**
   b. Wait five minutes before attempting to log on to the JMX console.
   c. Log in to the JMX console using the following syntax:

      **http://<server_URL>:8081**

      The default user name and password is **opsaadmin**
   d. Locate the OpsA Infrastructure Settings area.
   e. Locate the **java.lang.String get GLOBALSettingDefaultValue** item.
      i. Set the value to **opsa-customtopology-settings**.
      ii. Invoke the function and copy the list of values in the results to a text file
      iii. Add a line to represent the custom collection using the following syntax:

         <collection_name>, <field from collection tagged as host>
   f. Locate the **java.lang.String set GLOBALSettingDefaultValue** item
      i. Set the value of **contextName** to **opsa-customtopology-settings**.
      ii. Set the value of **settingName** to **opsa.customtopology.nodegroup.link_tags**.
      iii. Copy the list of values from the text file you saved to the **newValue** field.
11. Let the collection run for up to five minutes. From the Operations Analytics console, open the ***<collectionname>*** dashboard to view some of the collected information for this collection:

## NNM iSPI Performance for Metrics Component

Use the information in this section when configuring an NNM iSPI Performance for Metrics Component Collection.

1. Collector Host

   Select the fully-qualified domain name or IP address of the common collector that will collect data for this collection.
2. Source data directory
   Specify the source directory in which the data resides. Any examples in this section reference this entry as <*source directory*>.

   For example, suppose that this collection relies on data being collected from the `/opt/HP/opsa/data/netcomponent` directory. Follow the instructions below for mounting this directory:

   For the Collector Appliance to access raw metric information from the NNM iSPI Performance for Metric's component health extension pack, you must export these metrics to CSV files. Run the following command on the NNM iSPI Performance for Metric server to export these metrics to CSV files in the `/csvexports` directory:

   - *Windows (Raw Information)*:
     `<Install_Dir>\NNMPerformanceSPI\bin\configureCsvExport.ovpl -p Component_Health -a "Raw,<Target-Dir>"`
   - *UNIX: (Raw Information)*: `/opt/OV/NNMPerformanceSPI/bin/configureCsvExport.ovpl -p Component_Health -a "Raw,<Target-Dir>"`

   **Note:** You must make the exported component health metrics available on the Operations Analytics Collector Appliance in the `/opt/HP/opsa/data/netcomponent` directory.

   If you want to use a different directory than `/opt/HP/opsa/data/netcomponent`, do the following:

   a. Edit the following collection template:
   `/opt/HP/opsa/conf/collection/server/config.templates/nnmispi/1.0/netcomponent/component/nnmispi_netcomponent_component_collection.xml`.

   b. Specify a different directory for the `sourcedir` attribute.

   **Note:** The `opsa` user on the Operations Analytics Collector Appliance must have read and write access to the component health metric files in the Operations Analytics Collector Appliance to move them to the processed directory. The process directory is `<source directory>_processed` based on the path you entered earlier. So if you entered `/opt/HP/opsa/data/mynnmcollection` earlier as the source directory, the process directory would be `/opt/HP/opsa/data/mynnmcollection _ processed`.

   For example, to configure read and write access to the component health metric files to the Operations Analytics Collector Appliance when the files are located on a Windows server, do the following:

   a. On a Windows server, navigate to **Computer Management** > **System Tools** > **Shares** > **Shared Folders**.

   b. Right-click beneath shares and open the new share wizard.

   c. Create shares for the directories in which the .csv files are stored.

   d. From the Operations Analytics Collector Appliance, add the correct entries to the `/etc/fstab` file. Use the following entries as a model:

   ```
   //10.17.18.19/final /opt/HP/opsa/data/nnm cifs
   username=administrator,password=password,uid=opsa,rw 0 0
   //10.15.14.13/componentfinal /opt/HP/opsa/data/netcomponent cifs
   ```

```
username=admin,password=passwd,uid=opsa,rw 0 0
//10.15.14.13/interfacefinal /opt/HP/opsa/data/netinterface cifs
username=admin,password=passwd,uid=opsa,rw 0 0
```

e. Use the `mount -a` command to get the directories mounted.

Using another example, to configure read and write access to the NNMi files from the Operations Analytics Collector Appliance when the files are located on a Linux server, do the following:

a. Make sure the `/var/opt/OV/shared/nnm/databases/custompoller/export/final` directory is enabled for export on the NNMi server.

b. Run the following command from the Operations Analytics Collector Appliance to make the files exported from NNMi available on the Operations Analytics Collector Appliance:

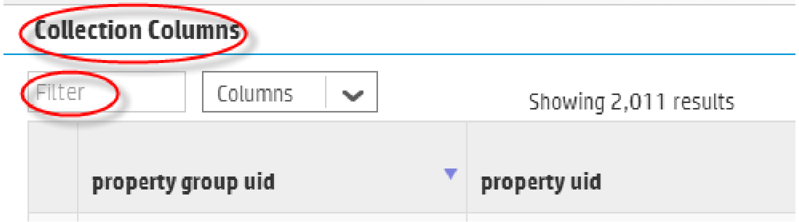
```
mount <IP address of NNMi
Server>://var/opt/OV/shared/nnm/databases/custompoller/export/final
/opt/HP/opsa/data/nnm
```

3. Click **Create Collection** to create and publish a new collection or **Override Collection** to modify an existing collection. The NNM iSPI Performance for Metrics Component Collection reads data from the CSV files within 60 seconds of the file being placed in the source directory.

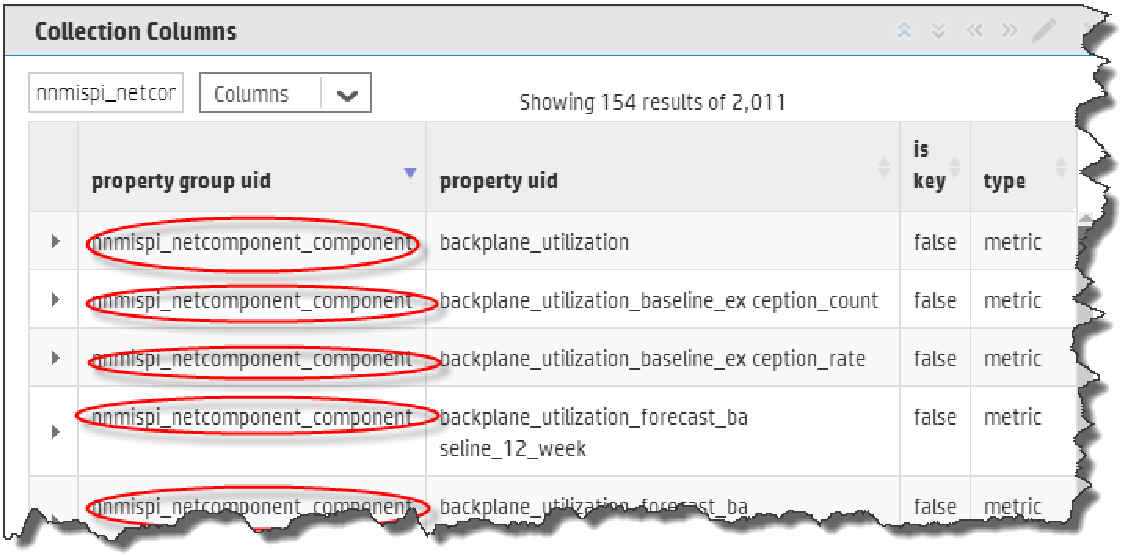
4. Validate the Collection Results

   Let the collection run for five minutes or longer. From the Operations Analytics console, view the **OpsA Meta Info** dashboard. Look for the **property group uid** for the collection you just created and published.

   a. Type the property group uid (`nnmispi_netcomponent_component`) for this collection in the **Collection Columns Filter**:



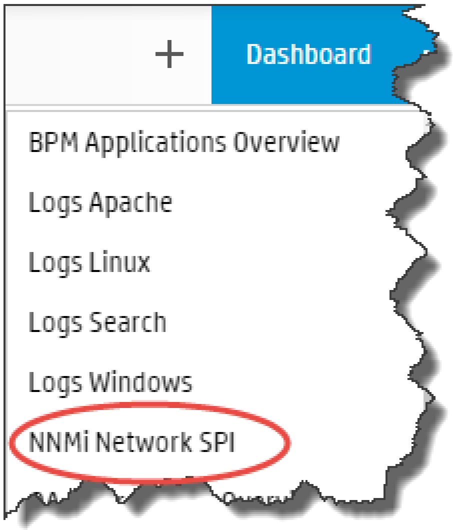
   b. After typing property group uid (`nnmispi_netcomponent_component`) for this collection in the **Collection Columns Filter**, you should see information for this collection.



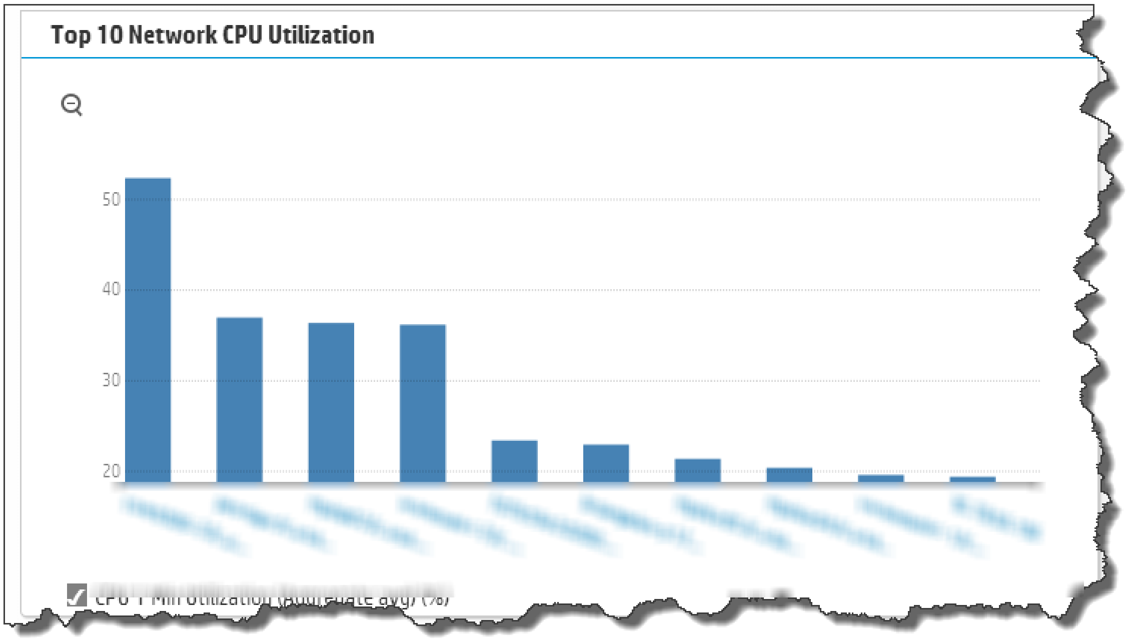
Showing 154 results of 2,011

| property group uid | property uid | is key | type |
|---|---|---|---|
| nnmispi_netcomponent_component | backplane_utilization | false | metric |
| nnmispi_netcomponent_component | backplane_utilization_baseline_ex ception_count | false | metric |
| nnmispi_netcomponent_component | backplane_utilization_baseline_ex ception_rate | false | metric |
| nnmispi_netcomponent_component | backplane_utilization_forecast_ba seline_12_week | false | metric |
| nnmispi_netcomponent_component | backplane_utilization_forecast_ba | false | metric |

c. From the Operations Analytics console, open the **NNMi Network SPI** dashboard to view some of the collected information for this collection:



The following is a small example of NNM iSPI Performance for Metrics Component Collection data provided by the **NNMi Network SPI** dashboard.



5. Next Steps
   a. 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 AQL Developer Guide for more information.
   b. If you want to add tags to an NNM iSPI Performance for Metrics Component Collection, use the opsa-tag-manager.sh command. See *Creating, Applying, and Maintaining Tags for Custom Collections* in the Operations Analytics Configuration Guide and the *opsa-tag-manager.sh* reference page (or the Linux manpage) for more information.

## NNM iSPI Performance for Metrics Interface

Use the information in this section when configuring an NNM iSPI Performance for Metrics Interface Collection.

1. Specify Collector Host

   Select the fully-qualified domain name or IP address of the common collector that will collect data for this collection.

2. Source data directory
   Specify the source directory in which the data resides. Any examples in this section reference this entry as <*source directory*>.

   For example, suppose that this collection relies on data being collected from the `/opt/HP/opsa/data/netinterface` directory. Follow the instructions below for mounting this directory:

   For the Collector Appliance to access live metric information from the NNM iSPI Performance for Metric's interface health extension pack, you must export these metrics to CSV files. Run the following command on the NNM iSPI Performance for Metric server to export these metrics to CSV files in the `/csvexports` directory:

   - *Windows (Raw Information)*:
     ```
     <Install_Dir>\NNMPerformanceSPI\bin\configureCsvExport.ovpl -p Interface_Health -a
     "Raw,<Target_Directory">
     ```

- *UNIX (Raw Information*):

```
/opt/OV/NNMPerformanceSPI/bin/configureCsvExport.ovpl -p Interface_Health -a
"Raw,<Target_Directory">
```

> **Note:** You must make the exported interface health metrics available on the Operations Analytics Collector Appliance in the `/opt/HP/opsa/data/netinterface` directory.
> If you want to use a different directory than `/opt/HP/opsa/data/netinterface`, do the following:
>
> a. Edit the following collection template:
> `/opt/HP/opsa/conf/collection/server/config.templates/nnmispi/1.0/netinterface/interface/nnmispi_netinterface_interface_collection.xml`.
> b. Specify a different directory for the `sourcedir` attribute.

> **Note:** The `opsa` user on the Operations Analytics Collector Appliance must have read and write access to the interface health metric files in the Operations Analytics Collector Appliance to move them to the processed directory. The process directory is `<source directory>_processed` based on the path you entered earlier. So if you entered `/opt/HP/opsa/data/mynnmcollection` earlier as the source directory, the process directory would be `/opt/HP/opsa/data/mynnmcollection _ processed`.
>
> For example, to configure read and write access to the interface health metric files to the Operations Analytics Collector Appliance when the files are located on a Windows server, do the following:
>
> a. On a Windows server, navigate to **Computer Management** > **System Tools** > **Shares** > **Shared Folders**.
> b. Right-click beneath shares and open the new share wizard.
> c. Create shares for the directories in which the .csv files are stored.
> d. From the Operations Analytics Collector Appliance, add the correct entries to the `/etc/fstab` file. Use the following entries as a model:
>
> ```
> //10.17.18.19/final /opt/HP/opsa/data/nnm cifs
> username=administrator,password=password,uid=opsa,rw 0 0
> //10.15.14.13/componentfinal /opt/HP/opsa/data/netcomponent cifs
> username=admin,password=passwd,uid=opsa,rw 0 0
> //10.15.14.13/interfacefinal /opt/HP/opsa/data/netinterface cifs
> username=admin,password=passwd,uid=opsa,rw 0 0
> ```
>
> e. Use the `mount -a` command to get the directories mounted.
>
> Using another example, to configure read and write access to the NNMi files from the Operations Analytics Collector Appliance when the files are located on a Linux server, do the following:
>
> a. Make sure the `/var/opt/OV/shared/nnm/databases/custompoller/export/final` directory is enabled for export on the NNMi server.
> b. Run the following command from the Operations Analytics Collector Appliance to make the files ex ported from NNMi available on the Operations Analytics Collector Appliance:
>
> ```
> mount <IP address of NNMi
> Server>://var/opt/OV/shared/nnm/databases/custompoller/export/final
> /opt/HP/opsa/data/nnm
> ```

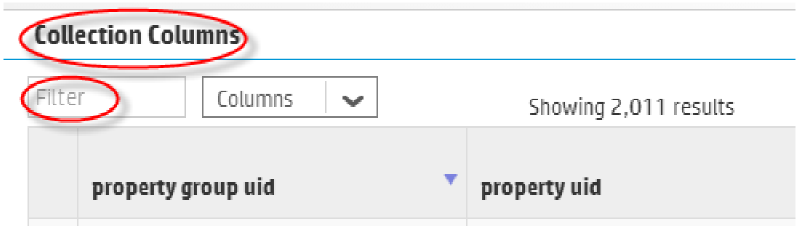
3. Click **Create Collection** to create and publish a new collection or **Override Collection** to modify an existing collection. The NNM iSPI Performance for Metrics Interface Collection reads data from the CSV

files within 60 seconds of the file being placed in the source directory.

4. Validate the Collection Results

   Let the collection run for five minutes or longer. From the Operations Analytics console, view the **OpsA Meta Info** dashboard. Look for the **property group uid** for the collection you just created and published.

   a. Type the property group uid (`nnmispi_netinterface_interface`) for this collection in the **Collection Columns Filter**:

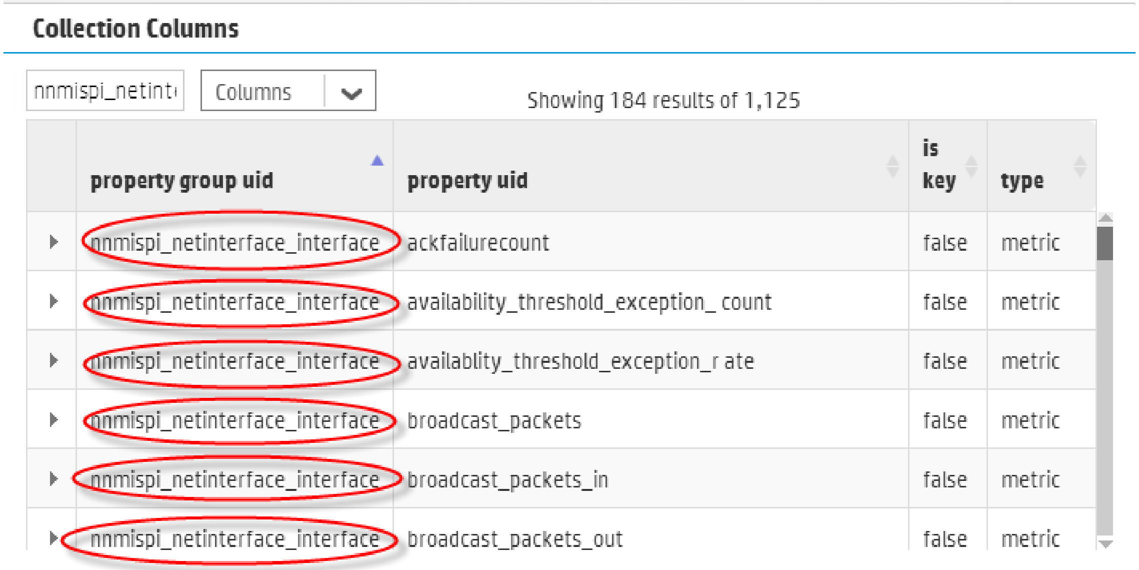


Collection Columns

Filter | Columns | Showing 2,011 results

| property group uid | property uid |
|---|---|

   b. After typing the property group uid (`nnmispi_netinterface_interface`) for this collection in **Collection Columns Filter**, you should see information in the resulting table:

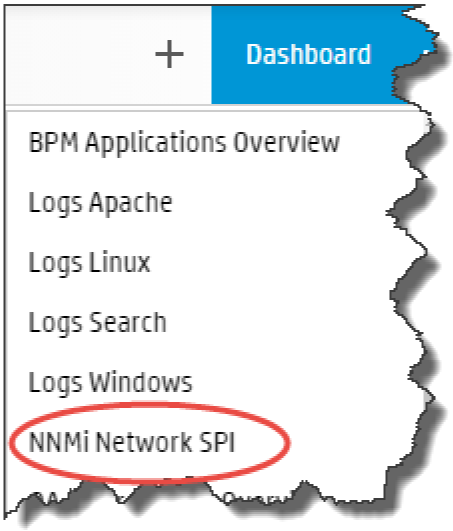


Collection Columns

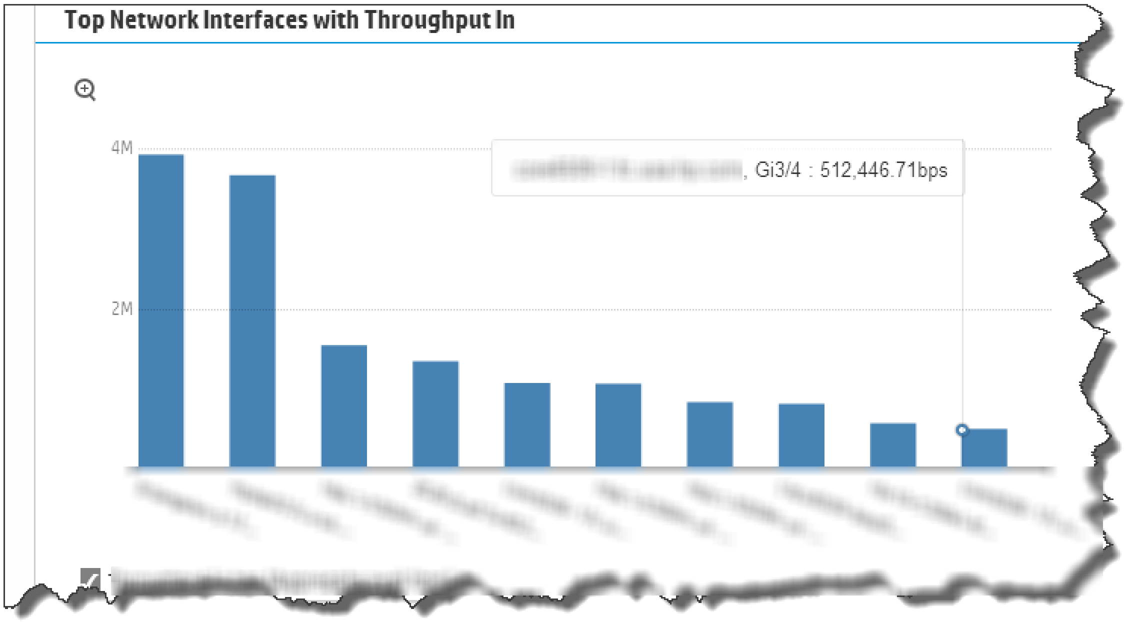
nnmispi_netint | Columns | Showing 184 results of 1,125

| property group uid | property uid | is key | type |
|---|---|---|---|
| nnmispi_netinterface_interface | ackfailurecount | false | metric |
| nnmispi_netinterface_interface | availability_threshold_exception_ count | false | metric |
| nnmispi_netinterface_interface | availablity_threshold_exception_r ate | false | metric |
| nnmispi_netinterface_interface | broadcast_packets | false | metric |
| nnmispi_netinterface_interface | broadcast_packets_in | false | metric |
| nnmispi_netinterface_interface | broadcast_packets_out | false | metric |

   c. From the Operations Analytics console, open the **NNMi Network SPI** dashboard to view some of the collected information for this collection:



The following is a small example of NNM iSPI Performance for Metrics Interface data provided by the **NNMi Network SPI** dashboard.


Top Network Interfaces with Throughput In
4M
2M
[redacted], Gi3/4 : 512,446.71bps

5. Next Steps

   a. 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 AQL Developer Guide for more information.

   b. If you want to add tags to an NNM iSPI Performance for Metrics Interface Collection, use the opsa-tag-manager.sh command. See *Creating, Applying, and Maintaining Tags for Custom Collections* in the Operations Analytics Configuration Guide and the *opsa-tag-manager.sh* reference page (or the Linux manpage) for more information.

## NNMi Custom Poller

Use the information in this section when configuring an NNMi Custom Poller Collection.

1. Specify the Collector Host.

   In the Collector Host field, select the fully-qualified domain name or IP address of the common collector that will collect data for this collection.
2. Source data directory
   Specify the source directory in which the data resides. Any examples in this section reference this entry as <*source directory*>.

   For example, suppose that the NNMi Custom Poller Collection collects data from the `/opt/HP/opsa/data/nnm` directory. To enable NNMi to export Custom Poller collections, do the following:

   a. Using the NNMi console, enable NNMi to export custom poller collections to make the metrics from your collections available for Operations Analytics. Configuring NNMi to export custom poller collections enables NNMi to export metrics, such as CSV files, into the following directory:

      - *Windows*:
        `<Install_Dir>\ProgramData\HP\HP BTO Software\shared\nnm\databases\custompoller\export\final`
      - *UNIX*:
        `/var/opt/OV/shared/nnm/databases/custompoller/export/final`

      See the *HPE Network Node Manager i Deployment Reference*, the *HPE NNMi Help*, or the *HPE Network Node Manager i Software Step-by-Step Guide to Custom Poller White Paper* for more information.

   b. The default configuration for the custom poller collection template is for Operations Analytics to read all of the files having file names that match the `*.csv*` or `*.gz*` pattern. If you need the collector to read a different set of files, the Operations Analytics administrator must edit the appropriate custom poller collector template file and specify a different file pattern. To change the pattern, edit the custom poller collection template and make the value changes you must make to the `filepattern=` tag.

> **Note:** You must make the files exported from the `/var/opt/OV/shared/nnm/databases/custompoller/export/final` directory on NNMi available on the Operations Analytics Collector Appliance in the `/opt/HP/opsa/data/nnm` directory.
>
> If you want to use a different directory than `/opt/HP/opsa/data/nnm`, do the following:
>
> a. Edit the following collection template:
> `/opt/HP/opsa/conf/collection/server/config.templates/nnm/1.0/netperf/mib/nnm_netperf_mib_collection.xml`.
>
> b. Specify a different directory for the `sourcedir` attribute.

> **Note:** The `opsa` user on the Operations Analytics Collector Appliance must have read and write access to the NNMi files on the Operations Analytics Collector Appliance to move them to the processed directory. The process directory is `<source directory>_processed` based on the path you entered earlier. So if you entered `/opt/HP/opsa/data/mynnmcollection` earlier as the source directory, the process directory would be `/opt/HP/opsa/data/mynnmcollection _processed`.
>
> For example, to configure read and write access to the NNMi files to the Operations Analytics Collector Appliance when the files are located on a Windows server, do the following:
>
> a. On a Windows server, navigate to **Computer Management** > **System Tools** > **Shares** > **Shared Folders**.

b. Right-click beneath shares and open the new share wizard.

c. Create shares for the directories in which the .csv files are stored.

d. From the Operations Analytics Collector Appliance, add the correct entries to the `/etc/fstab` file. Use the following entries as a model:

```
//10.17.18.19/final /opt/HP/opsa/data/nnm cifs
username=administrator,password=password,uid=opsa,rw 0 0
//10.15.14.13/componentfinal /opt/HP/opsa/data/netcomponent cifs
username=admin,password=passwd,uid=opsa,rw 0 0
//10.15.14.13/interfacefinal /opt/HP/opsa/data/netinterface cifs
username=admin,password=passwd,uid=opsa,rw 0 0
```

e. Use the `mount -a` command to get the directories mounted.

Using another example, to configure read and write access to the NNMi files from the Operations Analytics Collector Appliance when the files are located on a Linux server, do the following:

a. Make sure the `/var/opt/OV/shared/nnm/databases/custompoller/export/final` directory is enabled for export on the NNMi server.

b. Run the following command from the Operations Analytics Collector Appliance to make the files exported from NNMi available on the Operations Analytics Collector Appliance:

```
mount <IP address of NNMi
Server>://var/opt/OV/shared/nnm/databases/custompoller/export/final
/opt/HP/opsa/data/nnm
```

3. Complete the Configuration

   After you complete the steps in this section, the NNMi Custom Poller reads data from the CSV files within 60 seconds of the file being placed in the source directory. You can use an NNMi Custom Poller to collect numeric metrics from any NNMi Custom Poller MIB expression.

   *Windows:* `*Install_Dir*/ProgramData/HP/HP BTO Software/shared/nnm/databases/custompoller/export/final`

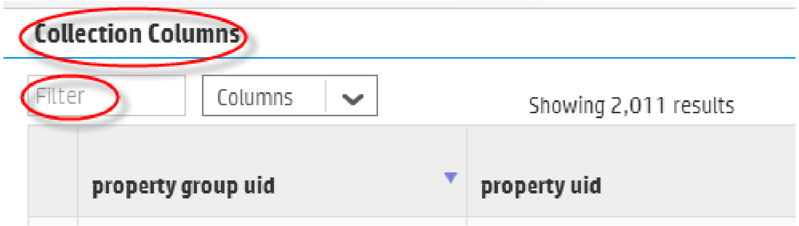
   *UNIX:* `/var/opt/OV/shared/nnm/databases/custompoller/export/final`

   Click **Create Collection** to create and publish a new collection or **Override Collection** to modify an existing collection.

4. Validate the Collection Results

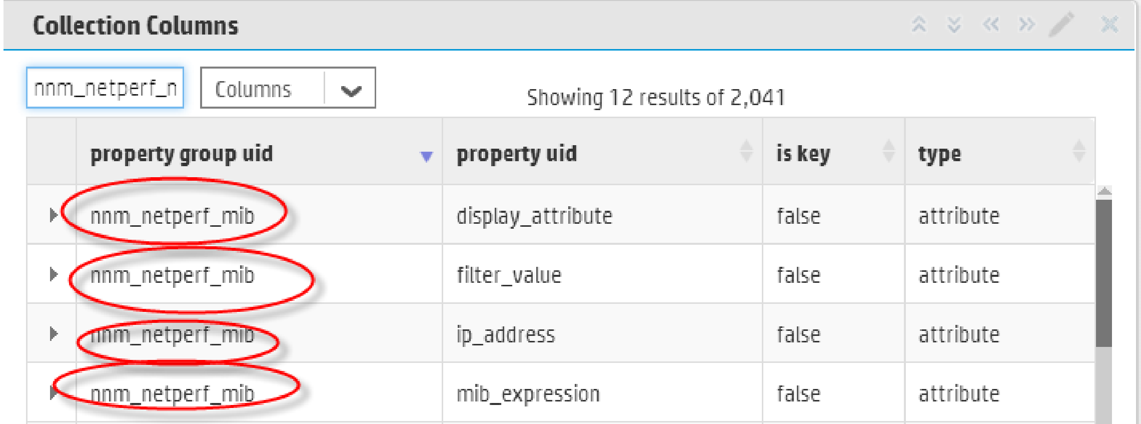
   Let the collection run for five minutes or longer. From the Operations Analytics console, view the **OpsA Meta Info** dashboard. Look for the **property group uid** for the collection you just created and published.

   a. Type the property group uid (`nnm_netperf_mib`) for this collection in the **Collection Columns Filter:**



   b. After typing property group uid (`nnm_netperf_mib`) for this collection in the **Collection Columns**

**Filter**, you should see information for this collection.



Showing 12 results of 2,041

| property group uid | property uid | is key | type |
|---|---|---|---|
| nnm_netperf_mib | display_attribute | false | attribute |
| nnm_netperf_mib | filter_value | false | attribute |
| nnm_netperf_mib | ip_address | false | attribute |
| nnm_netperf_mib | mib_expression | false | attribute |

5. Next Steps

   a. Create dashboards and query panes for the data you are now collecting. See "Dashboards and Query Panes" on page 12 for more information.

   b. 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 AQL Developer Guide for more information.

   c. If you want to add tags to an HPE NNMi Custom Poller collection, use the opsa-tag-manager.sh command. See *Creating, Applying, and Maintaining Tags for Custom Collections* in theOperations Analytics Configuration Guide and the *opsa-tag-manager.sh* reference page (or the Linux manpage) for more information.

## Operations Agent

Use the information in this section when configuring an Operations Agent Collection.

1. Specify Collection Details

| Name | Description |
|---|---|
| **Collector Host** | Select the fully-qualified domain name or IP address of the common collector that will collect data for this collection. |
| **Import agents from OMi** | Select this option to extract the list of agents from OMi. This information is stored on the RTSM database associated with the OMi instance, therefore you must specify the location and credentials of the RTSM database server.<br>**Note:** You can use this option in addition to manually specifying agents.<br>**Existing RTSM credentials.** Use this to select the RTSM credentials you used when creating a different collection. Otherwise, enter the RTSM host name, user name, password, port, and specify whether you want to use a secure connection.<br>**OMi node group.** If this is not specified, all agents that exist in the RTSM database will be imported. If you specify an OMi node group, only the agents in the specified node group will be imported.<br>**Verify.** Verify connectivity to the RTSM database and how many agents will be imported. This also displays a link to the fully-qualified domain names of the imported agents. |
| **Add agents manually** | Select this option to specify each agent you want to add manually.<br>**Note:** You can use this option in addition to automatically importing agents.<br>**Agents List.** Specify the fully-qualified domain name of an OA server from which you want to collect data. To specify additional agents, use the **Add** button to display additional fields. Alternatively, you can specify more than one agent in one field if they are separated by spaces. |

| Name | Description |
|---|---|
| **Create collection without correctness validation** | Select this check box if you want to create a collection without validating that it can connect to the data source. This is useful for creating a collection with a non-existing data source, then manually copying data to data input folders on the Operations Analytics collector.<br>This action only applies to agents specified manually. It does not skip the validation for the RTSM credentials. |

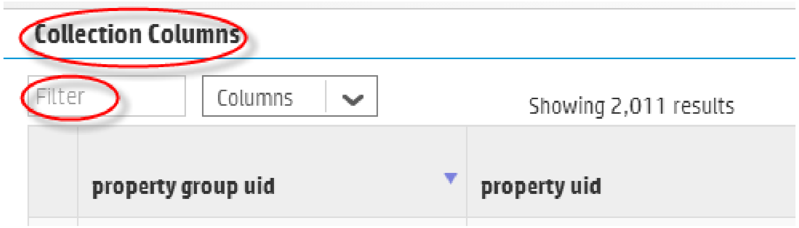
2. Click **Create Collection** to create and publish a new collection or **Override Collection** to modify an existing collection.

   The Operations Agent Collection collects global system information on the host that is running the Operations Agent. After you complete the steps in this section, the Operations Agent Collection collects raw metrics every 15 minutes, with 5 minute data granularity.

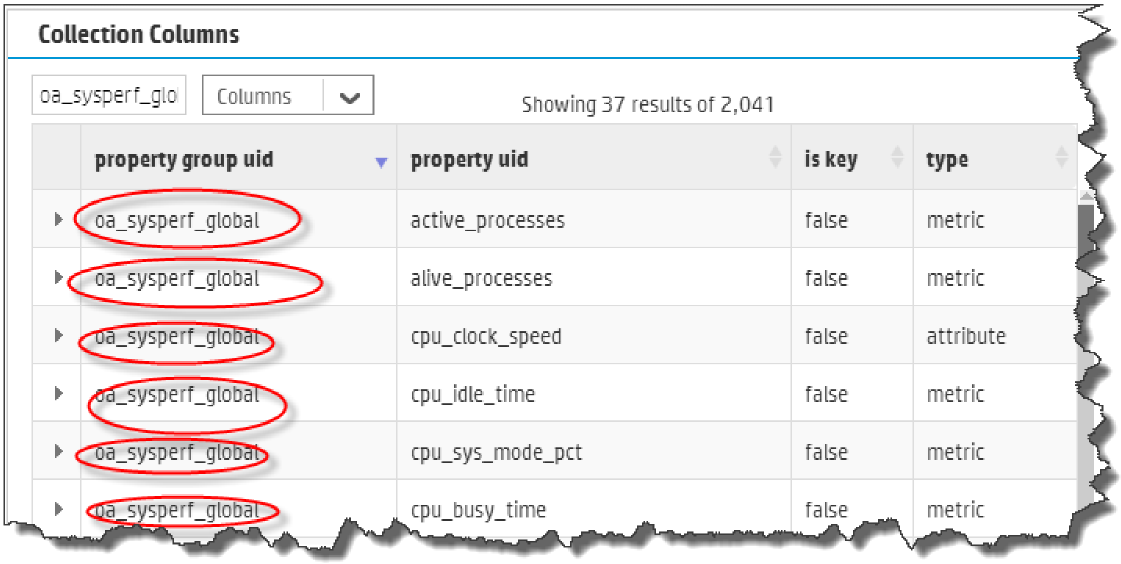
3. Validate the Collection Results

   Let the collection run for five minutes or longer. From the Operations Analytics console, view the **OpsA Meta Info** dashboard. Look for the **property group uid** for the collection you just created and published.

   a. Type the property group uid (`oa_sysperf_global`) for this collection in the **Collection Columns Filter:**

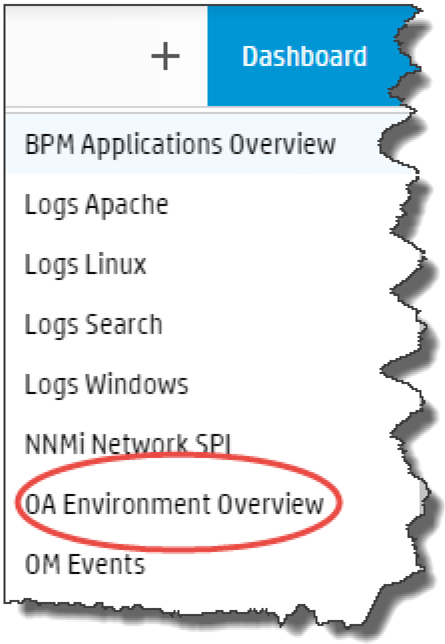


   b. After typing property group uid (`oa_sysperf_global`) for this collection in the **Collection Columns Filter**, you should see information for this collection.

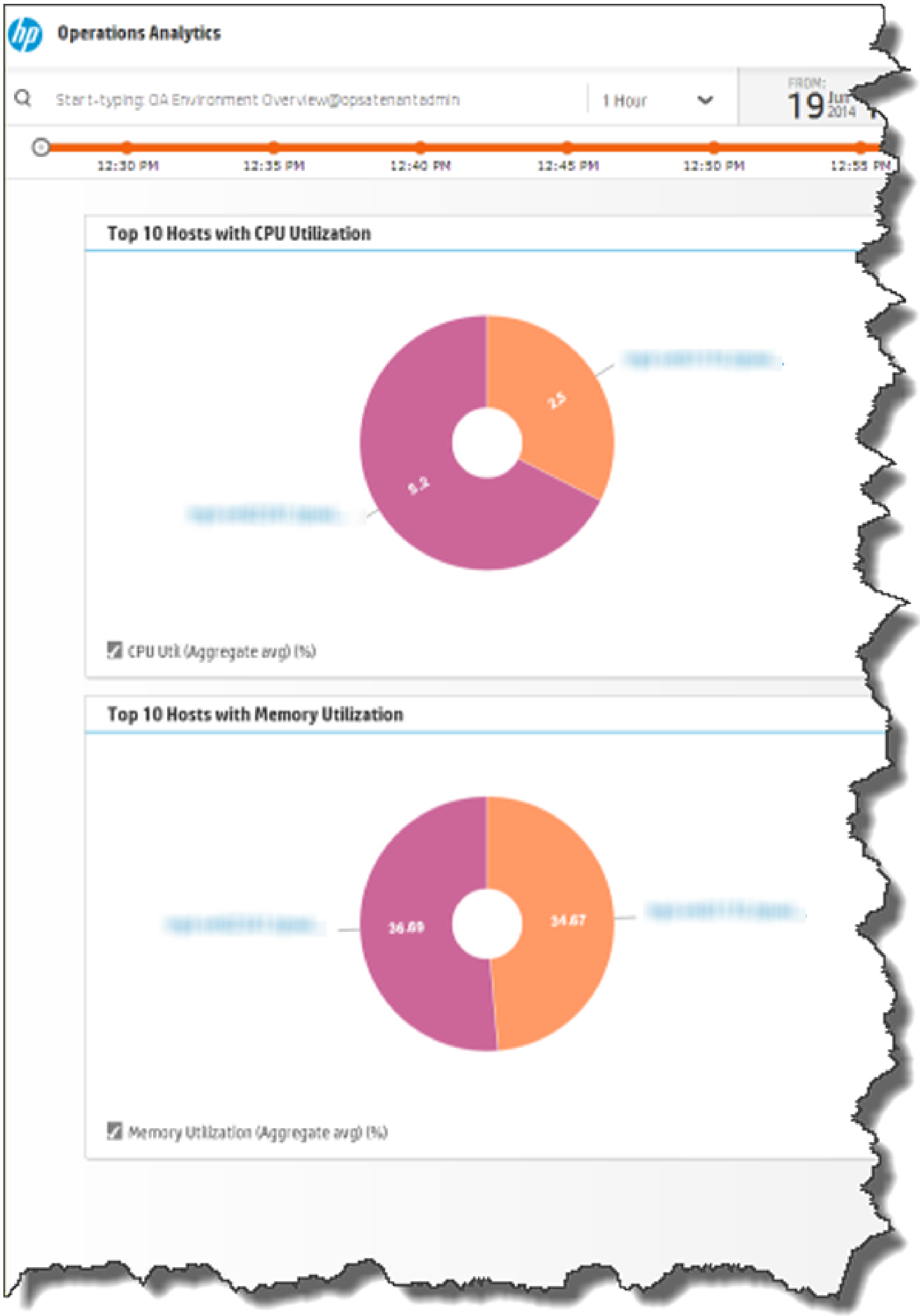


| property group uid | property uid | is key | type |
|---|---|---|---|
| oa_sysperf_global | active_processes | false | metric |
| oa_sysperf_global | alive_processes | false | metric |
| oa_sysperf_global | cpu_clock_speed | false | attribute |
| oa_sysperf_global | cpu_idle_time | false | metric |
| oa_sysperf_global | cpu_sys_mode_pct | false | metric |
| oa_sysperf_global | cpu_busy_time | false | metric |

c. From the Operations Analytics console, open the **OA Environment Overview** dashboard to view some of the collected information for this collection:



The following is a small sample of Operations Agent Collection data provided by the **OA Environment Overview** dashboard.


Operations Analytics
Start-typing: OA Environment Overview@opsatenantadmin
1 Hour
FROM:
19 Jun 2014
12:30 PM
12:35 PM
12:40 PM
12:45 PM
12:50 PM
12:55 PM
Top 10 Hosts with CPU Utilization
2.5
5.2
☑ CPU Util (Aggregate avg) (%)
Top 10 Hosts with Memory Utilization
36.69
34.67
☑ Memory Utilization (Aggregate avg) (%)

4. Next Steps

   If you want to add tags to an Operations Agent Collection, use the `opsa-tag-manager.sh` command. See *Creating, Applying, and Maintaining Tags for Custom Collections* in the Operations Analytics Configuration Guide and the *opsa-tag-manager.sh* reference page (or the Linux manpage) for more information.

## Operations MP

Use the information in this section when configuring an Operations MP Collection. This includes **Operations MP for MS ActiveDirectory, MS Exchange, MS SQL Server, and Oracle Database**. These collections take specific metric information (different metrics for each of the collections) from Operations Agents. As Operations Analytics cannot identify which agents are installed on which servers, you must specify which agents are relevant for these collections manually or by using an OMi node group. Otherwise, you must import the metric information from all agents associated with your OMi environment.

1. Specify Collection Details

| Name | Description |
|---|---|
| **Collector Host** | Select the fully-qualified domain name or IP address of the common collector that will collect data for this collection. |
| **Import agents from OMi** | Select this option to extract the list of agents from OMi. This information is stored on the RTSM database associated with the OMi instance, therefore you must specify the location and credentials of the RTSM database server.<br>**Note:** You can use this option in addition to manually specifying agents.<br>**Existing RTSM credentials.** Use this to select the RTSM credentials you used when creating a different collection. Otherwise, enter the RTSM host name, user name, password, port, and specify whether you want to use a secure connection.<br>**OMi node group.** If this is not specified, all agents that exist in the RTSM database will be imported. If you specify an OMi node group, only the agents in the specified node group will be imported.<br>**Verify.** Verify connectivity to the RTSM database and how many agents will be imported. This also displays a link to the fully-qualified domain names of the imported agents. |
| **Add agents manually** | Select this option to specify each agent you want to add manually.<br>**Note:** You can use this option in addition to automatically importing agents.<br>**Agents List.** Specify the fully-qualified domain name of an OA server from which you want to collect data. To specify additional agents, use the **Add** button to display additional fields. Alternatively, you can specify more than one agent in one field if they are separated by spaces. |

| Name | Description |
|---|---|
| **Create collection without correctness validation** | Select this check box if you want to create a collection without validating that it can connect to the data source. This is useful for creating a collection with a non-existing data source, then manually copying data to data input folders on the Operations Analytics collector.<br>This action only applies to agents specified manually. It does not skip the validation for the RTSM credentials. |

2. Click **Create Collection** to create and publish a new collection or **Override Collection** to modify an existing collection.

   The Operations MP Collections collect metric information on the host that is running the Operations Agent. After you complete the steps in this section, the Operations MP Collection collects raw metrics every 15 minutes, with 5 minute data granularity.

3. Validate the Collection Results

   Let the collection run for 30 minutes (this time may vary). From the Operations Analytics console, view the **Operations MP** dashboard associated with your collection and verify that there is data.

4. Next Steps

   If you want to add tags to an Operations MP Collection, use the `opsa-tag-manager.sh` command. See *Creating, Applying, and Maintaining Tags for Custom Collections* in the Operations Analytics Configuration Guide and the *opsa-tag-manager.sh* reference page (or the Linux manpage) for more information.

## Operations Manager Events (Unix)

Use the information in this section when configuring an Operations Manager Events (Unix) Collection.

> **Note:** To use this collection to support Oracle RAC, perform the following prerequisites:
>
> 1. Copy the `tnsnames.ora` file from the Oracle server to the following locations:
>
>    Operations Analytics Server: `/opt/HP/opsa/conf/collection/tnsnames.ora`
>
>    Operations Analytics Collector: `/opt/HP/BSM/PMDB/config/tnsnames.ora`
>
> 2. Rename the `tnsnames.ora` files:
>
>    Operations Analytics Server: `/opt/HP/opsa/conf/collection/bsm-tnsnames.ora`
>
>    Operations Analytics Collector: `/opt/HP/BSM/PMDB/config/bsm-tnsnames.ora`
>
> 3. Continue with the procedure for configuring an Operations Manager Events (Unix) collection.

1. Specify Collection Parameters

| Name | Description |
|---|---|
| **Collector Host** | Select the fully-qualified domain name or IP address of the common collector that will collect data for this collection. |
| **Database Host Name** | Determine the fully-qualified domain name for the server housing the HPOM database. |
| **Database Type** | `ORACLE` |
| **Database Port** | Determine the port number to use for accessing the HPOM server (the default port is `1521`). |
| **Database User Name** | Determine the HPOM user name (the default is opc_op). This is the user name to use for connecting to the HPOM database. This is a database user not a system or HPOM application user. |
| **Database Password** | Determine the password for the HPOM user name. This is the password Operations Analytics uses to connect (using JDBC) to fetch the events directly from the HPOM schema. |
| **Database Instance Name** | Determine the instance name of the OM database (the default is `openview`). If you are using Oracle RAC, use the service name in this field. |
| **Database Name** | Determine the HPOM database name. |
| **Create collection without correctness validation** | Select this check box if you want to create a collection without validating that it can connect to the data source. This is useful for creating a collection with a non-existing data source, then manually copying data to data input folders on the Operations Analytics collector. |

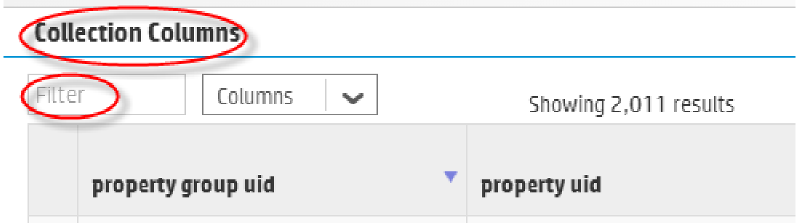
2. Click **Create Collection** to create and publish a new collection or **Override Collection** to modify an existing collection.

   The Operations Manager Events (Unix) Collection collects events every 15 minutes, and collects all OM events that occurred since the last poll.

3. Validate the Collection Results

   Let the collection run for five minutes or longer. From the Operations Analytics console, view the **OpsA Meta Info** dashboard. Look for the **property group uid** for the collection you just created and published.

   a. Type the property group uid (`om_events_omevents`) for this collection in the **Collection Columns Filter**:

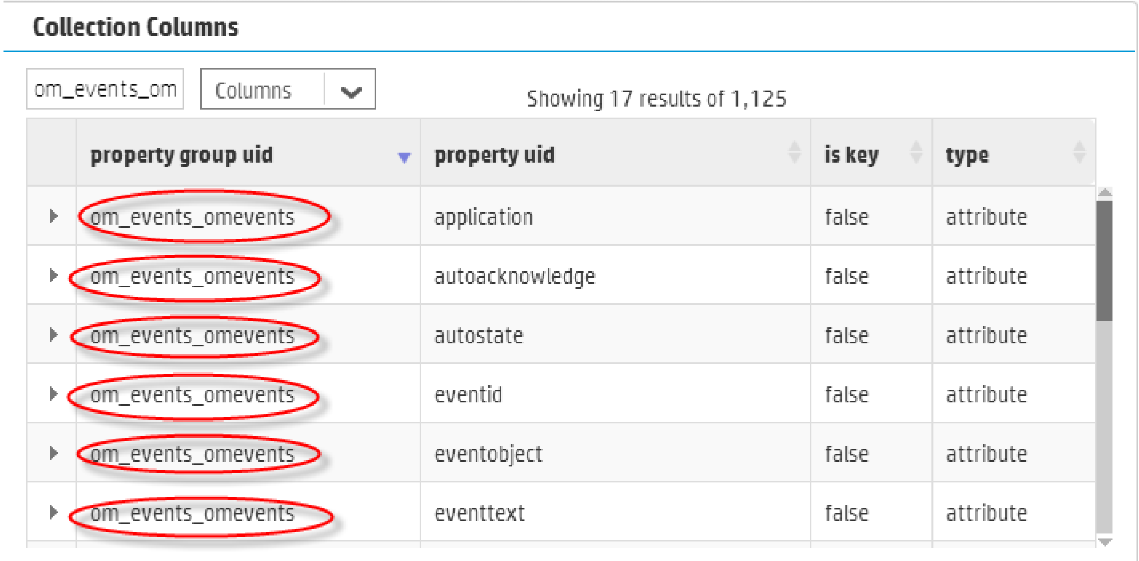


Collection Columns

Showing 2,011 results

| | property group uid | property uid |
|---|---|---|

b. After typing property group uid (`om_events_omevents`) for this collection in the **Collection Columns Filter**, you should see information for this collection.

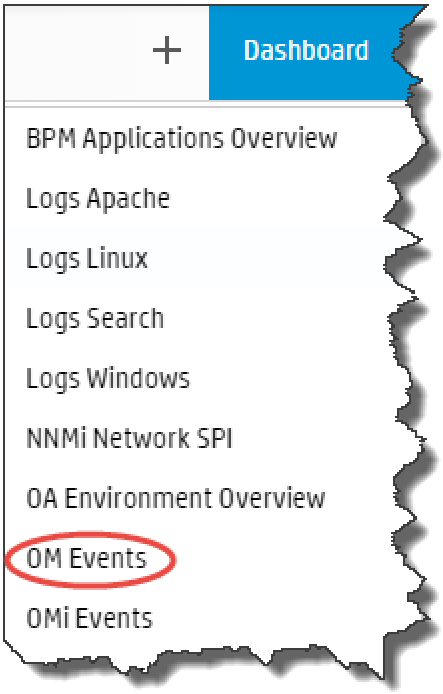


Collection Columns

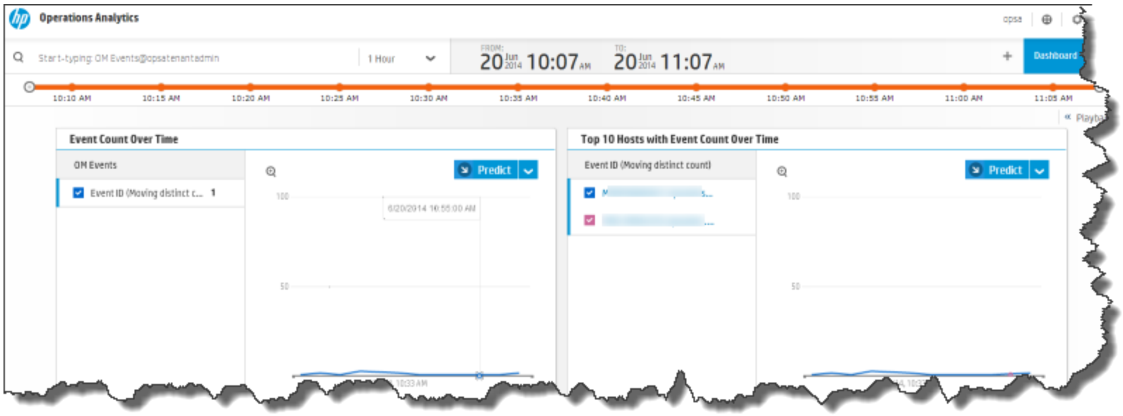
Showing 17 results of 1,125

| | property group uid | property uid | is key | type |
|---|---|---|---|---|
| ▸ | om_events_omevents | application | false | attribute |
| ▸ | om_events_omevents | autoacknowledge | false | attribute |
| ▸ | om_events_omevents | autostate | false | attribute |
| ▸ | om_events_omevents | eventid | false | attribute |
| ▸ | om_events_omevents | eventobject | false | attribute |
| ▸ | om_events_omevents | eventtext | false | attribute |

c. From the Operations Analytics console, open the **OM Events** dashboard to view some of the collected information for this collection:



The following is a small sample of OM Events Collection data provided by the **OM Events** dashboard.



4. Next Steps

   If you want to add tags to an Operations Manager Events (Unix) Collection, use the `opsa-tag-manager.sh` command. See *Creating, Applying, and Maintaining Tags for Custom Collections* in the Operations Analytics Configuration Guide and the *opsa-tag-manager.sh* reference page (or the Linux manpage) for more information..

## Operations Manager Events (Windows)

Use the information in this section when configuring an Operations Manager Events (Windows) Collection.

**Note:** To support this collection using Oracle RAC, perform the following prerequisites:

1. Copy the `tnsnames.ora` file from the Oracle server to the following locations:

   Operations Analytics Server: `/opt/HP/opsa/conf/collection/tnsnames.ora`

   Operations Analytics Collector: `/opt/HP/BSM/PMDB/config/tnsnames.ora`
2. Rename the `tnsnames.ora` files:

   Operations Analytics Server: `/opt/HP/opsa/conf/collection/bsm-tnsnames.ora`

   Operations Analytics Collector: `/opt/HP/BSM/PMDB/config/bsm-tnsnames.ora`
3. Continue with the procedure for configuring an Operations Manager Events (Unix) collection.

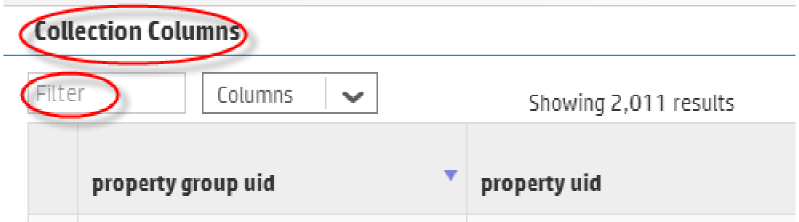
1. Specify Collection Details

| Name | Description |
|---|---|
| **Collector Host** | Select the fully-qualified domain name or IP address of the common collector that will collect data for this collection. |
| **Database Host Name** | Determine the fully-qualified domain name for the server housing the HPOM database. |
| **Database Type** | `MSSQL`. |
| **Database Port** | Determine the port number to use for accessing the HPOM database. (the default port is `1433` for SQL). |
| **Database User Name** | The user name to use for connecting to the HPOM server. This is the user name to use for connecting to the HPOM database. See *Configuring HPE Operations Manager (HPOM) (Creating a Database User Account on an HPOM Database Server)* in the Operations Analytics Configuration Guide for specific instructions about creating this user. This is a database user, not a system or HPOM application user. |
| **Database Password** | Determine the password for the HPOM user name. This is the password Operations Analytics uses to connect (using JDBC) to fetch the events directly from the HPOM schema. |
| **Database Instance Name** | Determine the instance name of the OM database (the default is `OVOPS`). If you are using Oracle RAC, use the service name in this field. |
| **Database Name** | Determine the HPOM database name. |
| **Create collection without correctness validation** | Select this check box if you want to create a collection without validating that it can connect to the data source. This is useful for creating a collection with a non-existing data source, then manually copying data to data input folders on the Operations Analytics collector. |

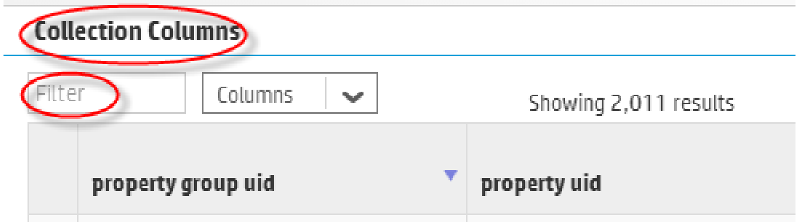
2. Click **Create Collection** to create and publish a new collection or **Override Collection** to modify an existing collection.

3. Validate the Collection Results

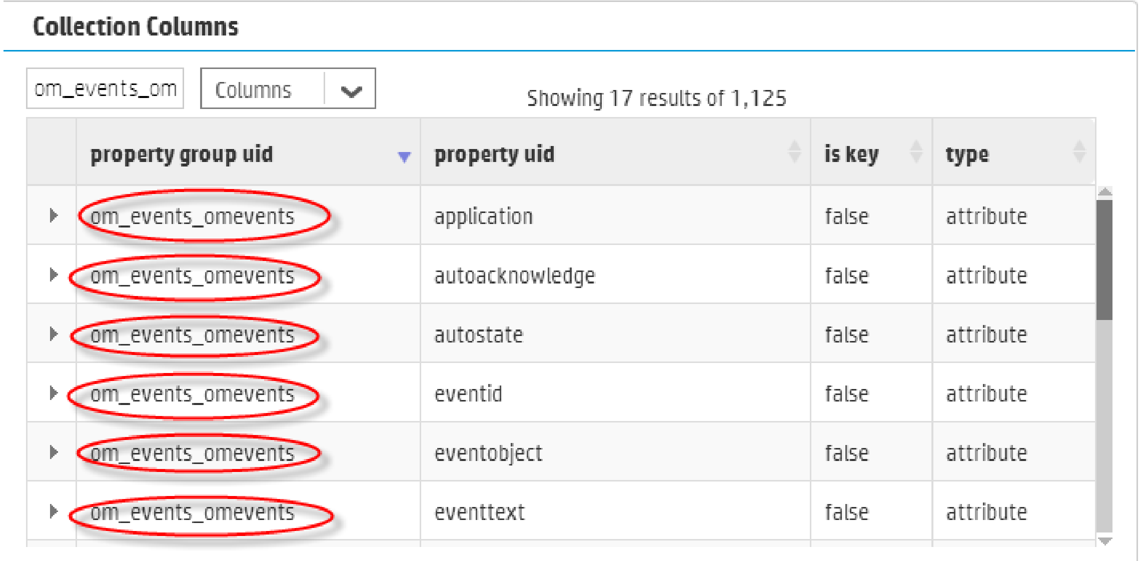
   Let the collection run for five minutes or longer. From the Operations Analytics console, view the **OpsA Meta Info** dashboard. Look for the **property group uid** for the collection you just created and published.



   a. Type the property group uid (`om_events_omevents`) for this collection in the **Collection Columns Filter**:

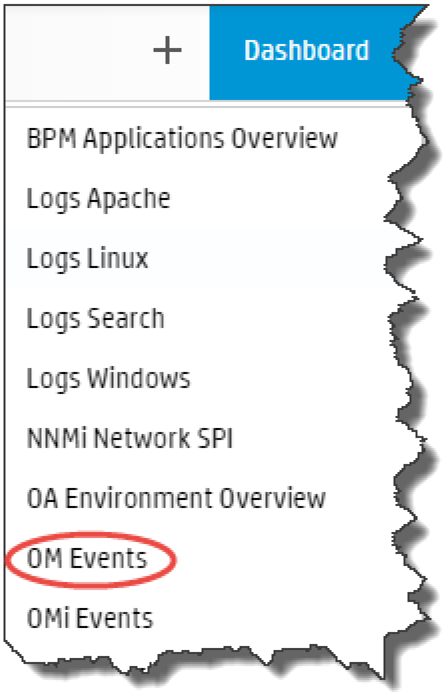


   b. After typing property group uid (`om_events_omevents`) for this collection in the **Collection Columns Filter**, you should see information for this collection.

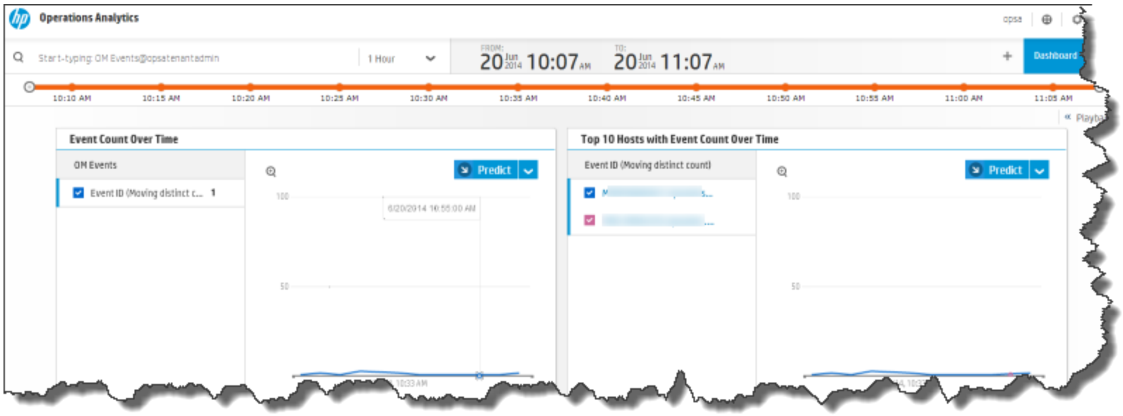


| property group uid | property uid | is key | type |
|---|---|---|---|
| om_events_omevents | application | false | attribute |
| om_events_omevents | autoacknowledge | false | attribute |
| om_events_omevents | autostate | false | attribute |
| om_events_omevents | eventid | false | attribute |
| om_events_omevents | eventobject | false | attribute |
| om_events_omevents | eventtext | false | attribute |

   c. From the Operations Analytics console, open the **OM Events** dashboard to view some of the collected information for this collection:



The following is a small sample of Operations Manager Events (Windows) Collection data provided by the **OM Events** dashboard.



4. Next Steps

   If you want to add tags to an Operations Manager Events (Windows) Collection, use the `opsa-tag-manager.sh` command. See *Creating, Applying, and Maintaining Tags for Custom Collections* in the Operations Analytics Configuration Guide and the *opsa-tag-manager.sh* reference page (or the Linux manpage) for more information.

## Operations Manager i Events

Use the information in this section when configuring an Operations Manager i Events Collection.

> **Note:** To support this collection using Oracle RAC, perform the following prerequisites:

1. Copy the `tnsnames.ora` file from the Oracle server to the following locations:

   Operations Analytics Server: `/opt/HP/opsa/conf/collection/tnsnames.ora`

   Operations Analytics Collector: `/opt/HP/BSM/PMDB/config/tnsnames.ora`
2. Rename the `tnsnames.ora` files:

   Operations Analytics Server: `/opt/HP/opsa/conf/collection/bsm-tnsnames.ora`

   Operations Analytics Collector: `/opt/HP/BSM/PMDB/config/bsm-tnsnames.ora`
3. Continue with the procedure for configuring an Operations Manager Events (Unix) collection.

**Note:** To support this collection for OMi version 10.x instead of OMi version 9.2x, do the following:

1. Edit the `/opt/HP/opsa/conf/collection/framework.properties` file
2. Change the value of

   ```
    omi.defaultversion=1.0
   ```

   to

   ```
   omi.defaultversion=1.1
   ```
3. Save your work.

1. Specify Collection Details

| Name | Description |
|---|---|
| **Collector Host** | Select the fully-qualified domain name or IP address of the common collector that will collect data for this collection. |
| **Database Host Name** | Determine the fully-qualified domain name for the server housing the OMi database. |
| **Database Type** | Choose `ORACLE` or `MSSQL`. |
| **Database Port** | Determine the port number to use for accessing the OMi database.<br>**Note:** The default port is `1433`, which is suitable for accessing most MS MQL Server installations. Oracle typically uses port 1521. |
| **Database User Name** | The name of a database user that has READ access to the OMi/Event Management schema in BSM. This is a database user, not a system user. Check with your BSM administrator or the database administration staff for the proper credentials. |
| **Database Password** | Determine the password for the OMi database username (the default is `Omi`). This is the password Operations Analytics uses to connect (using JDBC) to fetch the events directly from the OMi schema. This is a database password, not a system password. |
| **Database Instance Name** | Determine the instance name of the OMi database. If you are using Oracle RAC, use the service name in this field. |
| **Database Name** | Determine the OMi database name (the default is `OMi`). |
| **Create collection without correctness validation** | Select this check box if you want to create a collection without validating that it can connect to the data source. This is useful for creating a collection with a non-existing data source, then manually copying data to data input folders on the Operations Analytics collector. |

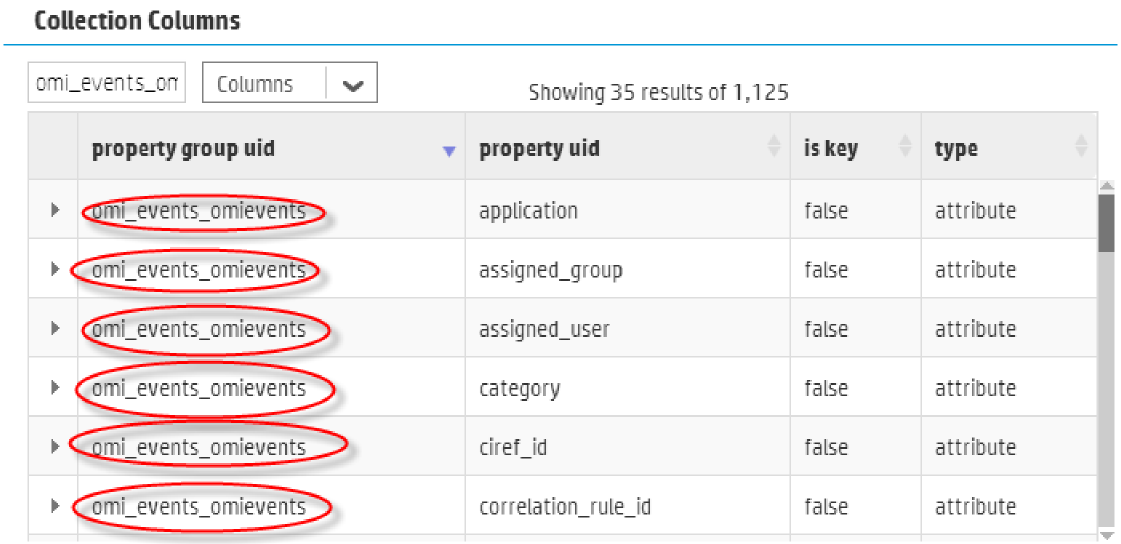
2. Click **Create Collection** to create and publish a new collection or **Override Collection** to modify an existing collection.

   The Operations Manager i Events Collection collects events every 15 minutes, and collects all OMi events that occurred since the last poll.

3. Validate the Collection Results

   Let the collection run for five minutes or longer. From the Operations Analytics console, view the dashboard. Look for the **property group uid** for the collection you just created and published.

a. After typing property group uid (`omi_events_omievents`) for this collection in the **Collection Columns Filter**, you should see information for this collection.



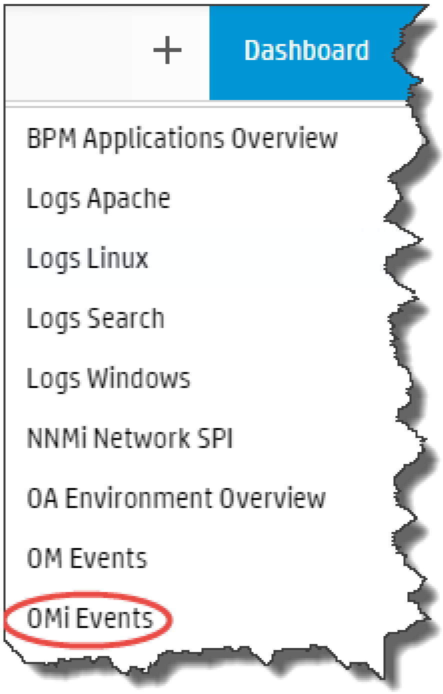
Collection Columns

omi_events_om Columns

Showing 35 results of 1,125

| property group uid | property uid | is key | type |
|---|---|---|---|
| omi_events_omievents | application | false | attribute |
| omi_events_omievents | assigned_group | false | attribute |
| omi_events_omievents | assigned_user | false | attribute |
| omi_events_omievents | category | false | attribute |
| omi_events_omievents | ciref_id | false | attribute |
| omi_events_omievents | correlation_rule_id | false | attribute |

b. From the Operations Analytics console, open the **OMi Events** dashboard to view some of the collected information for this collection:



4. Next Steps

If you want to add tags to an Operations Manager i Events Collection, use the `opsa-tag-manager.sh` command. See *Creating, Applying, and Maintaining Tags for Custom Collections* in the Operations Analytics Configuration Guide and the *opsa-tag-manager.sh* reference page (or the Linux manpage) for more information.

## Operations SPI for Oracle

Use the information in this section when configuring an Operations SPI for Oracle Collection.

1. Prerequisite

   Check that the HPE Operations Smart Plug-in for Oracle is deployed correctly, that it is running on the agent, and that metrics exist.

2. Specify Collection Details

| Name | Description |
|---|---|
| **Collector Host** | Select the fully-qualified domain name or IP address of the common collector that will collect data for this collection. |
| **Import agents from OMi** | Select this option to extract the list of agents from OMi. This information is stored on the RTSM database associated with the OMi instance, therefore you must specify the location and credentials of the RTSM database server.<br>**Note:** You can use this option in addition to manually specifying agents.<br>**Existing RTSM credentials.** Use this to select the RTSM credentials you used when creating a different collection. Otherwise, enter the RTSM host name, user name, password, port, and specify whether you want to use a secure connection.<br>**OMi node group.** If this is not specified, all agents that exist in the RTSM database will be imported. If you specify an OMi node group, only the agents in the specified node group will be imported.<br>**Verify.** Verify connectivity to the RTSM database and how many agents will be imported. |
| **Add agents manually** | Select this option to specify each agent you want to add manually.<br>**Note:** You can use this option in addition to automatically importing agents.<br>**Agents List.** Specify the fully-qualified domain name of an OA server from which you want to collect data. To specify additional agents, use the **Add** button to display additional fields. Alternatively, you can specify more than one agent in one field if they are separated by spaces. |

| Name | Description |
|---|---|
| **Create collection without correctness validation** | Select this check box if you want to create a collection without validating that it can connect to the data source. This is useful for creating a collection with a non-existing data source, then manually copying data to data input folders on the Operations Analytics collector.<br>This action only applies to agents specified manually. It does not skip the validation for the RTSM credentials. |

3. Click **Create Collection** to create and publish a new collection or **Override Collection** to modify an existing collection.

   The Operations SPI for Oracle Collection collects metrics every 15 minutes, with 5 minute data granularity.

4. Validate the Collection Results

   Let the collection run for five minutes or longer. From the Operations Analytics console, view the **OA Oracle Database SPI** dashboard and verify that there is data.

5. Next Step

   If you want to add tags to an Operations SPI for Oracle Collection, use the opsa-tag-manager.sh command. See *Creating, Applying, and Maintaining Tags for Custom Collections* in the Operations Analytics Configuration Guide and the *opsa-tag-manager.sh* reference page (or the Linux manpage) for more information.

## SiteScope

Use the information in this section when configuring a SiteScope Collection.

**Note:** See *Supported Monitor Types* in the Operations Analytics Configuration Guide for a list of supported SiteScope monitor types. If a SiteScope monitor type has only unsupported counters configured, Operations Analytics ignores that monitor type when creating the collection. Operations Analytics does not support monitor counter names longer than 128 characters. If a supported monitor's counter name is longer than 128 characters, Operations Analytics ignores that counter.

**Note:** Configuring the Custom SiteScope Collection by using the Collections Manager as described in this section automatically tags the root group in SiteScope in a way that data from all monitors will be sent to Operations Analytics.

If you want to manually select (tag) the monitors from which to receive data, (instead of using the Configuration Manager in the Operations Analytics console), you must do the following:

1. Follow the instructions in the *Configuring a Custom SiteScope Collection (Detailed Method)* section in the *Operations Analytics Configuration Guide* and use the `-ignoretag` option when running the `opsa-sis-collector-auto-conf.sh` script.
2. Follow the steps in the *Configuring SiteScope for Integrating Data with Operations Analytics (Manual Method)* section in the *Operations Analytics Configuration Guide* to manually tag the integration and the desired monitors.

1. Specify Collection Details

| Name | Description |
|---|---|
| **Collector Host** | Select the fully-qualified domain name or IP address of the common collector that collects data from the SiteScope servers.<br>**Note:** It is possible to connect one or more SiteScope servers to each Operations Analytics Collector host. Do not connect the same SiteScope server to more than one Operations Analytics Collector host. You can distribute the data load among Operations Analytics Collector hosts by connecting different SiteScope servers to different Operations Analytics Collector hosts. |
| **Use IP** | Select this option for networks that only permit the SiteScope server to connect to the Operations Analytics collector using the Operations Analytics Collector's IP address (and not its hostname). |
| **SiteScope Server** | Determine the IP address or fully-qualified domain name of the SiteScope server for which you are configuring collections. |
| **SiteScope Port** | Determine the port used to connect to the SiteScope server. This port is the same one that you use to access the SiteScope user interface. |
| **SiteScope User Name** | Determine the user name used to connect to the SiteScope server. This is typically `admin`.<br>**Note:** The SiteScope administrator can create other users that have permissions to view and edit SiteScope integrations and tags. Operations Analytics can connect as one of these users. |
| **SiteScope Password** | Determine the user name password to use when connecting to the SiteScope server. |

| Name | Description |
|---|---|
| **SiteScope LWSSO initString** | Take this value from **SiteScope UI** > **Preferences** > **General Preferences** > **LW SSO Settings** > **Communication security passphrase**.<br>**Note:** If you cannot find this **SiteScope LWSSO initString** in the user interface for the version of SiteScope you are using, you can find the string in the SiteScope file system at `<SiteScope installation directory>\conf\lwsso\lwssofmconf.xml`.<br>**Note:** You cannot leave the LWSSO field empty even if you do not use SSL communication to connect to SiteScope. |
| **UOM Folder Path** | The path to the extracted UOM files you manually placed on the Operations Analytics server. If this is not filled in, Operations Analytics will attempt to extract the UOM file from the SiteScope server automatically.<br>**Note:** A UOM file contains the list of configured monitor types for a SiteScope server, and includes the list of counters (metrics and attributes) for each monitor type. See *Configuring a Custom SiteScope Collection* in the *Operations Analytics Configuration Guide* for more information about UOM files. |
| **Use Default UOM** | Use the default UOM file provided by Operations Analytics. Try this option only if you are unable to extract the file from SiteScope. |
| **Use SSL** | Select this option if you want to enable SSL communication with the SiteScope server.<br>**Note:** After selecting this option, you will use the **SiteScope Port** shown earlier in this table to connect to the SiteScope user interface. If this port changed, use the new port to access the SiteScope user interface. |
| **Ignore tag** | Select this option if you want to bypass the tagging of all the monitors. Use it to manually tag for collection only subset of the monitors. |

| Name | Description |
|---|---|
| **Create collection without correctness validation** | Select this check box if you want to create a collection without validating that it can connect to the data source. This is useful for creating a collection with a non-existing data source, then manually copying data to data input folders on the Operations Analytics collector. |

2. Click **Create Collection** to create and publish a new collection.

   **Note:** Creating this collection takes extra time. Typically it takes 30 minutes or longer to create this collection.

   **Note:** If you receive an error stating that the Sitescope integration already exists, this may be because you have created a collection connected to this SiteScope server from a similar Operations Analytics machine in the past and did not unregister it. To resolve this issue, go to the SiteScope server user interface and manually delete the integration with this Operations Analytics tenant (the name of integration will be opsa_<tenant_name>).

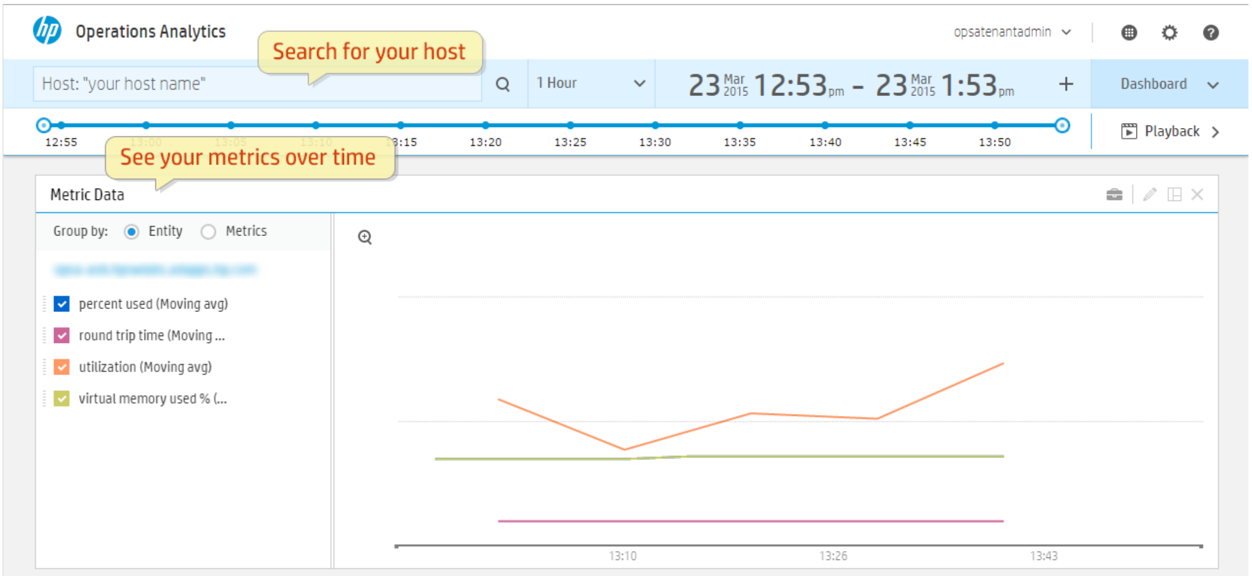
3. Next Steps
   a. Use the SiteScope dashboard to view the collection results.
   b. Create AQL functions for the data you are now collecting. See the instructions shown in the *Define Analytic Query Language (AQL) Functions* section of the AQL Developer Guide for more information.
   c. If you want to add tags to a Custom SiteScope Collection, use the `opsa-tag-manager.sh` command. See *Creating, Applying, and Maintaining Tags for Custom Collections* in the Operations Analytics Configuration Guide and the *opsa-tag-manager.sh* reference page (or the Linux manpage) for more information.

# Tagging Collection Best Practice

To make your data easier to search, you must add your desired tags to both the collection and to each preferred data column.

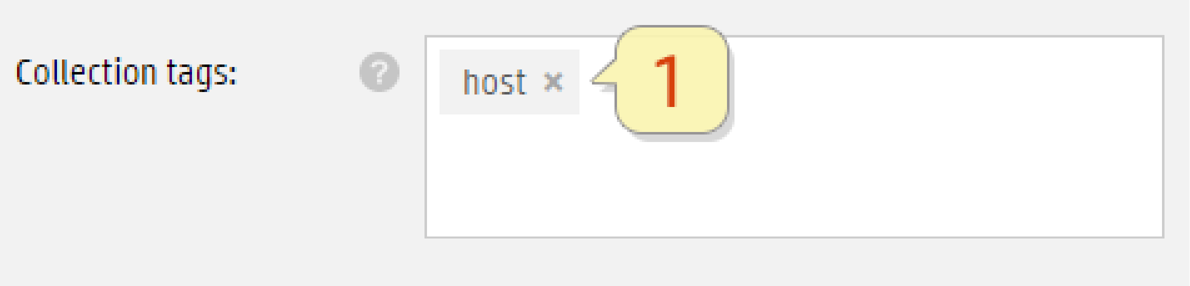
# Tagging a Collection For Searching by Host

If your data contains a host, you might prefer to search the data by host name as shown in the following image.


Operations Analytics
Search for your host
opsatenantadmin
Host: "your host name"
1 Hour
23 Mar 2015 12:53 pm - 23 Mar 2015 1:53 pm
Dashboard
12:55
13:15
13:20
13:25
13:30
13:35
13:40
13:45
13:50
Playback
See your metrics over time
Metric Data
Group by: ● Entity ○ Metrics
☑ percent used (Moving avg)
☑ round trip time (Moving ...
☑ utilization (Moving avg)
☑ virtual memory used % (...
13:10
13:26
13:43

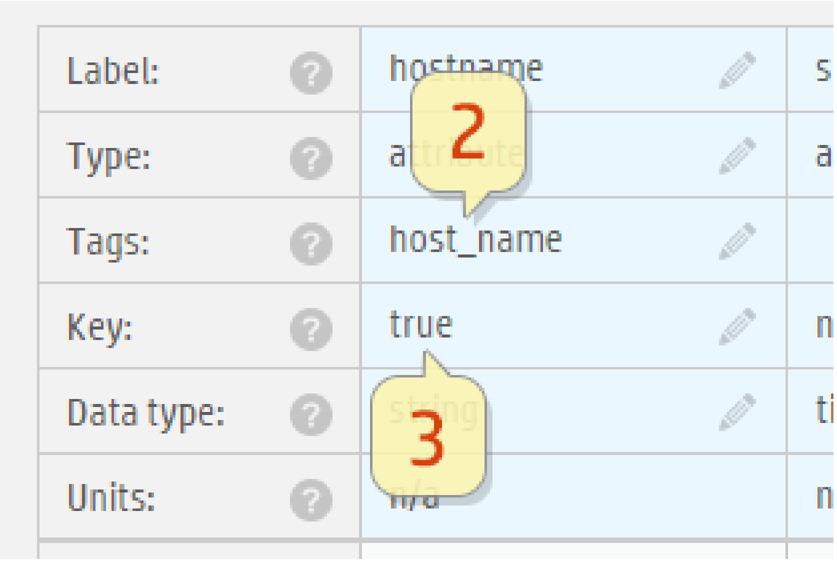
To configure this host name search, complete the following steps.

1. Add a **Host** tag to the **Collection tags** field.



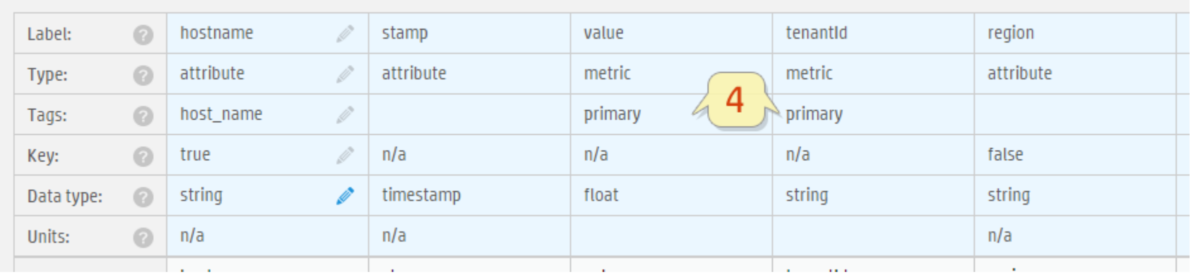
2. Add a **Host_Name** tag to the column you want tagged as a host. Your data might include several columns that contain host information. If that is the case, you must choose one column as the main host column and add the **Host_Name** tag to this column.
3. Set this column as a key.

> **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 16: Integration with HPE OneView

The information in this section is useful If you configured the Operations Analytics - HPE OneView integration. See the *HPE Operations Analytics for HPE OneView Installation, Integration, and Upgrade Guide* for more information.

Summary of the the Operations Analytics - HPE OneView integration.

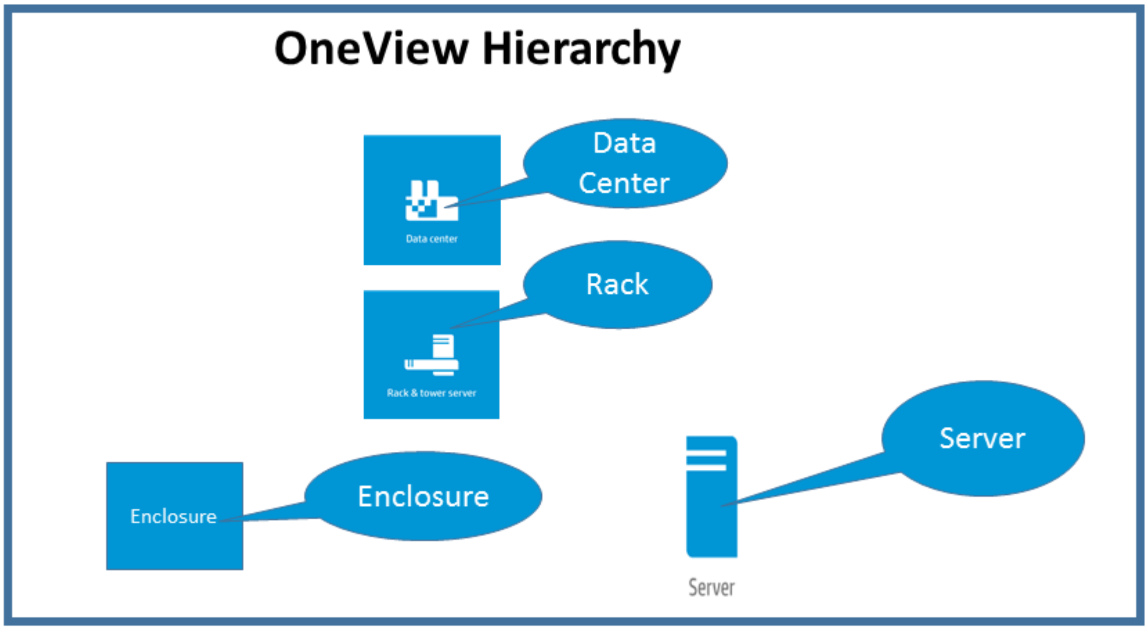
Operations Analytics’s integration with OneView provides IT professionals a summary of the converged infrastructure devices being managed by HPE OneView. With this integration Operations Analytics becomes the troubleshooting, analytic, and capacity planning arm of HPE OneView. The Operations Analytics - HPE OneView integration provides summary information for the infrastructure devices as well as doing analytics on the management data from HPE OneView, including logs, metrics, HPE OneView alerts, and topology data.

## Learn About

About the Operations Analytics - HPE OneView integration.

To configure the Operations Analytics - HPE OneView integration, see the HPE Operations Analytics for HPE OneView Installation, Integration, and Upgrade Guide.

HPE OneView organizes your system environment according to the following hierarchy :



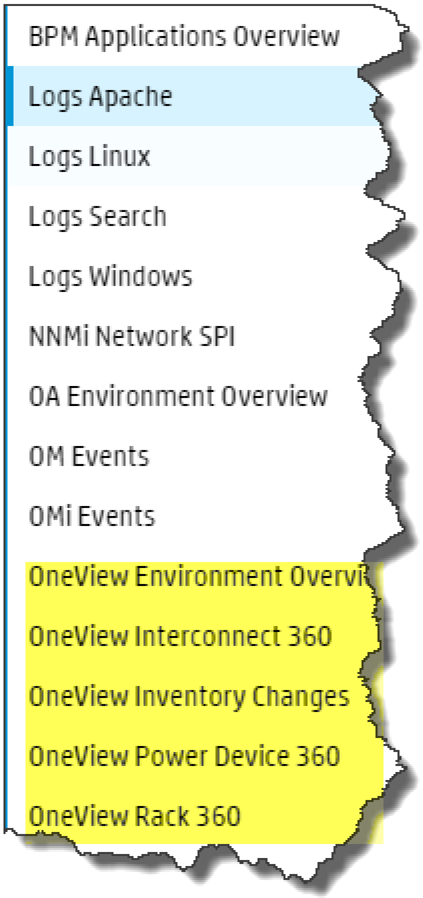
1. **Data Center**: A collection of racks and servers.
2. **Rack**: A cabinet that contains enclosures and servers.
3. **Enclosure**: An enclosure is a physical structure that can contain server blades, infrastructure hardware, and interconnects. An enclosure also includes bays for the following equipment:
   - servers
   - disk arrays
   - cpu blades
   - switches (interconnects) for network virtual connect
   - chassis elements
   - power supplies
   - fans
4. **Server**: Any single computer that is a standalone server, rack mounted, or a blade. It is monitored by HPE's Integrated Lights-Out (iLO) technology.

Consider the following definitions to better understand the OneView feature:

1. Device bays: A slot in an enclosure supplying power and network connectivity to the blade.
2. Blade: A server, disk array, or a set of CPUs.
3. Interconnects: A set of switches that provides network connectivity in a virtual fashion such that the IP and MAC addresses can be moved between two blades (for failover purposes). These switches are monitored by the virtual connect (VC) device.
4. Server profile: A configuration that you can apply to any server being managed by OneView.
5. Enclosure Groups: A logical collection of enclosures.

Navigating with HPE OneView Dashboards

**HPE OneView Dashboards**: To open any of the five main dashboards focused on data collected from the Operations Analytics - HPE OneView integration, select one of the following highlighted menu items from the Operations Analytics console:

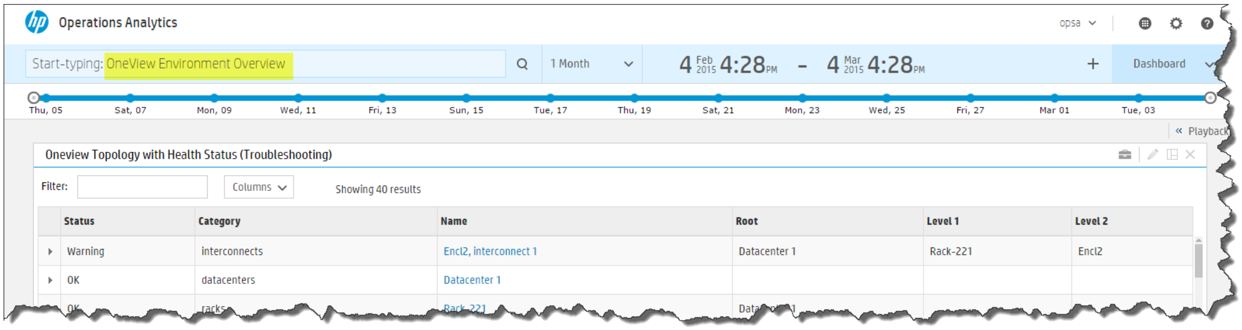


BPM Applications Overview
Logs Apache
Logs Linux
Logs Search
Logs Windows
NNMi Network SPI
OA Environment Overview
OM Events
OMi Events
OneView Environment Overvi
OneView Interconnect 360
OneView Inventory Changes
OneView Power Device 360
OneView Rack 360

After Selecting one of these dashboards, review the information that follows to see what information you can obtain from the dashboards provided by the Operations Analytics - HPE OneView integration and how to navigate among the various dashboards to troubleshoot and plan for the future capacity needs for your infrastructure.

Workflow for the OneView Environment Overview dashboard:

The following graphic shows you the OneView Environment Overview dashboard. This dashboard shows summarized management information for all the data centers currently being managed by HPE OneView. Use this dashboard as the starting point for troubleshooting your infrastructure.

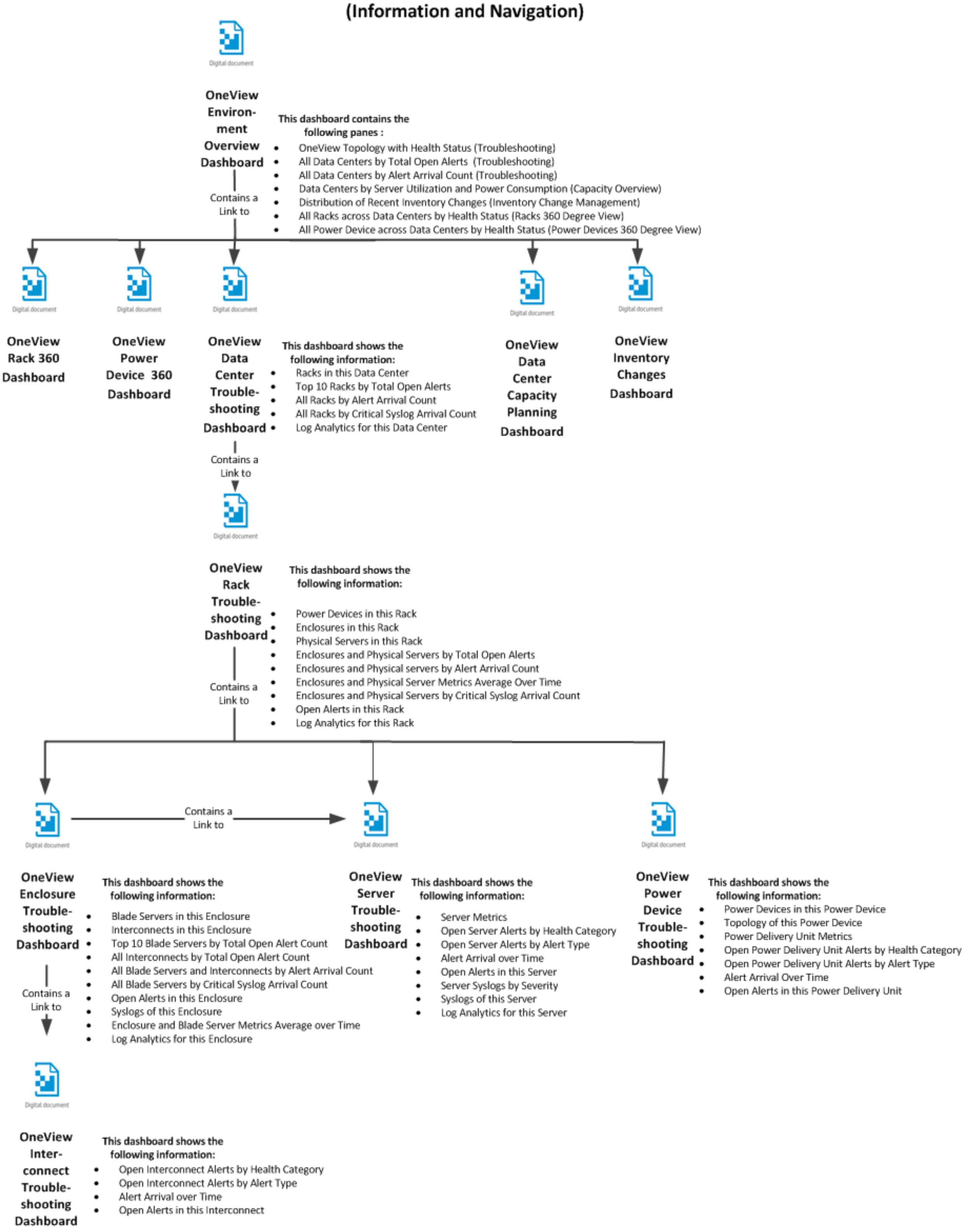


Oneview Topology with Health Status (Troubleshooting)

Filter: Columns Showing 40 results

| | Status | Category | Name | Root | Level 1 | Level 2 |
|---|---|---|---|---|---|---|
| ▸ | Warning | interconnects | Encl2, interconnect 1 | Datacenter 1 | Rack-221 | Encl2 |
| ▸ | OK | datacenters | Datacenter 1 | | | |
| | OK | racks | Rack-221 | Datacenter 1 | | |

**OneView Environment Overview Dashboard (Information and Navigation)**



**OneView Environment Overview Dashboard**

This dashboard contains the following panes :

- OneView Topology with Health Status (Troubleshooting)
- All Data Centers by Total Open Alerts (Troubleshooting)
- All Data Centers by Alert Arrival Count (Troubleshooting)
- Data Centers by Server Utilization and Power Consumption (Capacity Overview)
- Distribution of Recent Inventory Changes (Inventory Change Management)
- All Racks across Data Centers by Health Status (Racks 360 Degree View)
- All Power Device across Data Centers by Health Status (Power Devices 360 Degree View)

**OneView Rack 360 Dashboard**

**OneView Power Device 360 Dashboard**

**OneView Data Center Trouble-shooting Dashboard**

This dashboard shows the following information:

- Racks in this Data Center
- Top 10 Racks by Total Open Alerts
- All Racks by Alert Arrival Count
- All Racks by Critical Syslog Arrival Count
- Log Analytics for this Data Center

**OneView Data Center Capacity Planning Dashboard**

**OneView Inventory Changes Dashboard**

**OneView Rack Trouble-shooting Dashboard**

This dashboard shows the following information:

- Power Devices in this Rack
- Enclosures in this Rack
- Physical Servers in this Rack
- Enclosures and Physical Servers by Total Open Alerts
- Enclosures and Physical servers by Alert Arrival Count
- Enclosures and Physical Server Metrics Average Over Time
- Enclosures and Physical Servers by Critical Syslog Arrival Count
- Open Alerts in this Rack
- Log Analytics for this Rack

**OneView Enclosure Trouble-shooting Dashboard**

This dashboard shows the following information:

- Blade Servers in this Enclosure
- Interconnects in this Enclosure
- Top 10 Blade Servers by Total Open Alert Count
- All Interconnects by Total Open Alert Count
- All Blade Servers and Interconnects by Alert Arrival Count
- All Blade Servers by Critical Syslog Arrival Count
- Open Alerts in this Enclosure
- Syslogs of this Enclosure
- Enclosure and Blade Server Metrics Average over Time
- Log Analytics for this Enclosure

**OneView Server Trouble-shooting Dashboard**

This dashboard shows the following information:

- Server Metrics
- Open Server Alerts by Health Category
- Open Server Alerts by Alert Type
- Alert Arrival over Time
- Open Alerts in this Server
- Server Syslogs by Severity
- Syslogs of this Server
- Log Analytics for this Server

**OneView Power Device Trouble-shooting Dashboard**

This dashboard shows the following information:

- Power Devices in this Power Device
- Topology of this Power Device
- Power Delivery Unit Metrics
- Open Power Delivery Unit Alerts by Health Category
- Open Power Delivery Unit Alerts by Alert Type
- Alert Arrival Over Time
- Open Alerts in this Power Delivery Unit

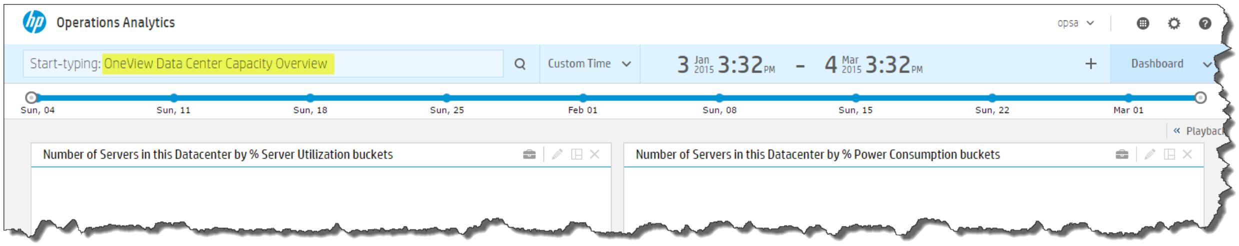
**OneView Inter-connect Trouble-shooting Dashboard**

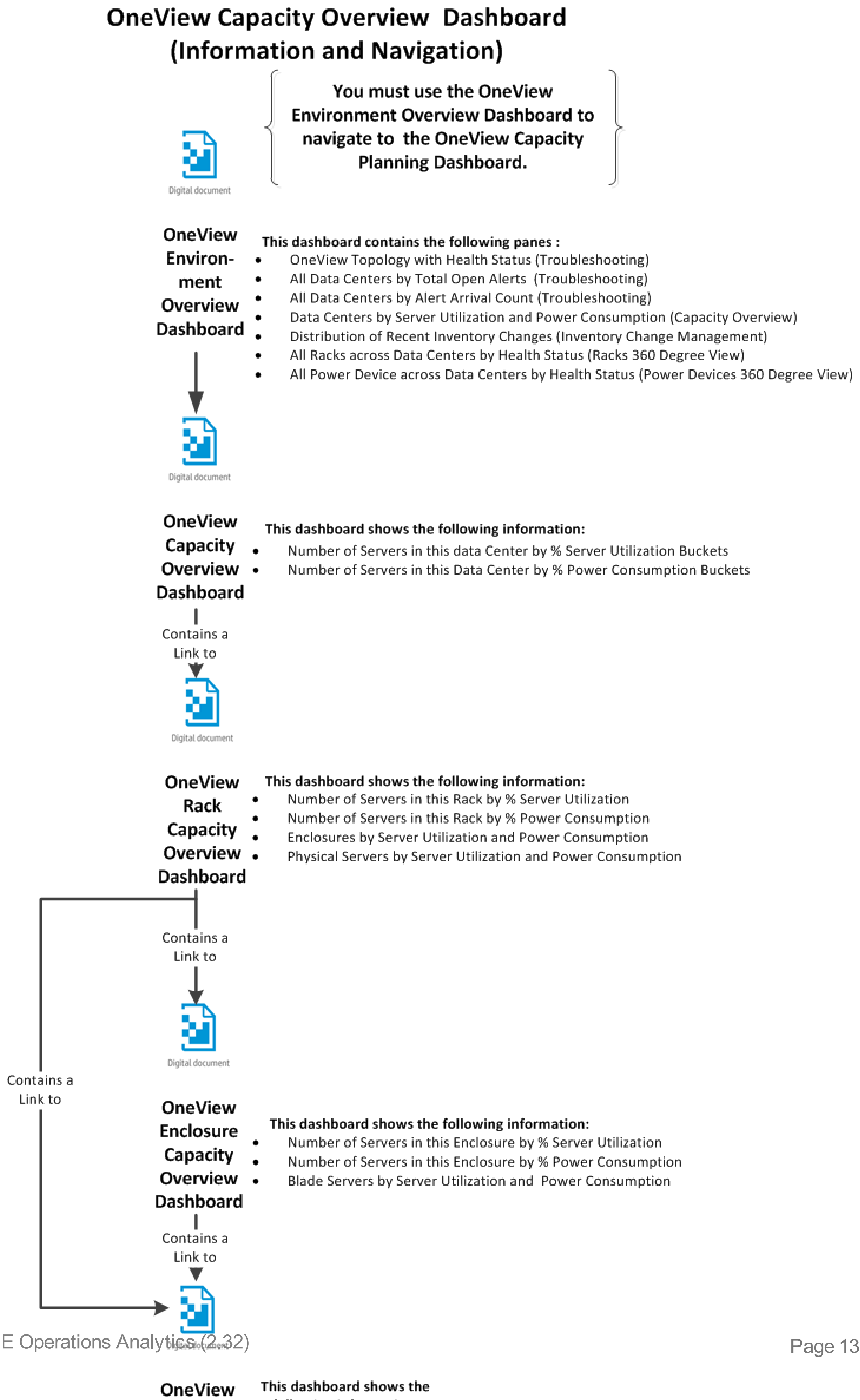
This dashboard shows the following information:

- Open Interconnect Alerts by Health Category
- Open Interconnect Alerts by Alert Type
- Alert Arrival over Time
- Open Alerts in this Interconnect

Workflow for the OneView Capacity Overview dashboard:

The following graphic shows you the OneView Capacity Overview dashboard.


Operations Analytics
opsa
Start-typing: OneView Data Center Capacity Overview
Custom Time
3 Jan 2015 3:32 PM - 4 Mar 2015 3:32 PM
Dashboard
Sun, 04
Sun, 11
Sun, 18
Sun, 25
Feb 01
Sun, 08
Sun, 15
Sun, 22
Mar 01
« Playbac
Number of Servers in this Datacenter by % Server Utilization buckets
Number of Servers in this Datacenter by % Power Consumption buckets



**OneView Capacity Overview Dashboard (Information and Navigation)**

You must use the OneView Environment Overview Dashboard to navigate to the OneView Capacity Planning Dashboard.

**OneView Environment Overview Dashboard**

**This dashboard contains the following panes :**

- OneView Topology with Health Status (Troubleshooting)
- All Data Centers by Total Open Alerts (Troubleshooting)
- All Data Centers by Alert Arrival Count (Troubleshooting)
- Data Centers by Server Utilization and Power Consumption (Capacity Overview)
- Distribution of Recent Inventory Changes (Inventory Change Management)
- All Racks across Data Centers by Health Status (Racks 360 Degree View)
- All Power Device across Data Centers by Health Status (Power Devices 360 Degree View)

**OneView Capacity Overview Dashboard**

**This dashboard shows the following information:**

- Number of Servers in this data Center by % Server Utilization Buckets
- Number of Servers in this Data Center by % Power Consumption Buckets

**OneView Rack Capacity Overview Dashboard**

**This dashboard shows the following information:**

- Number of Servers in this Rack by % Server Utilization
- Number of Servers in this Rack by % Power Consumption
- Enclosures by Server Utilization and Power Consumption
- Physical Servers by Server Utilization and Power Consumption

**OneView Enclosure Capacity Overview Dashboard**

**This dashboard shows the following information:**

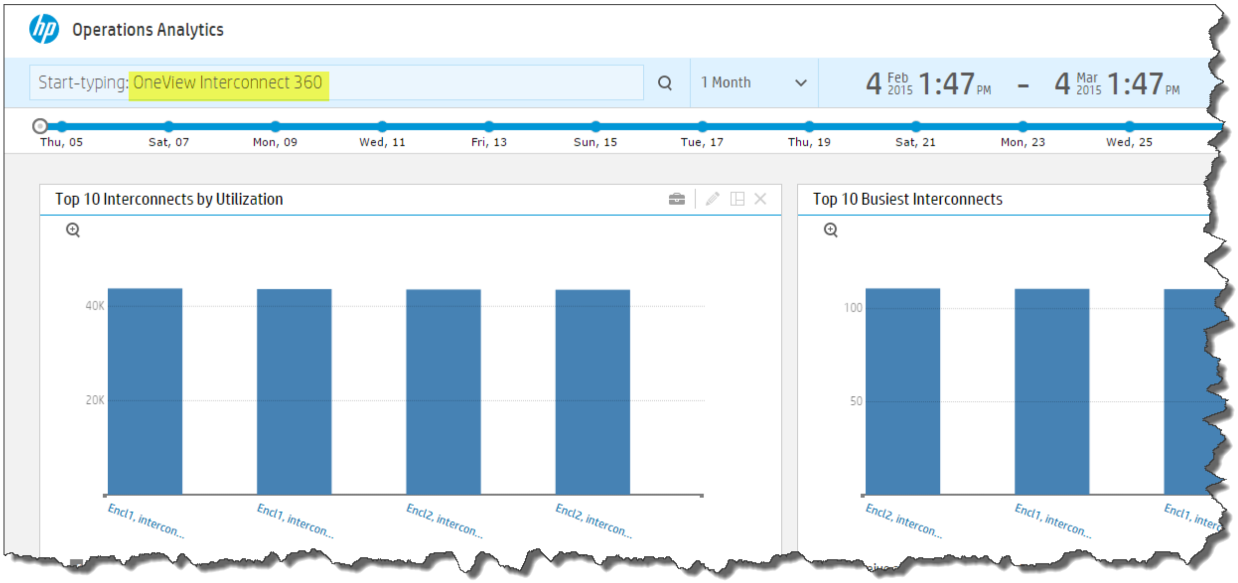
- Number of Servers in this Enclosure by % Server Utilization
- Number of Servers in this Enclosure by % Power Consumption
- Blade Servers by Server Utilization and Power Consumption

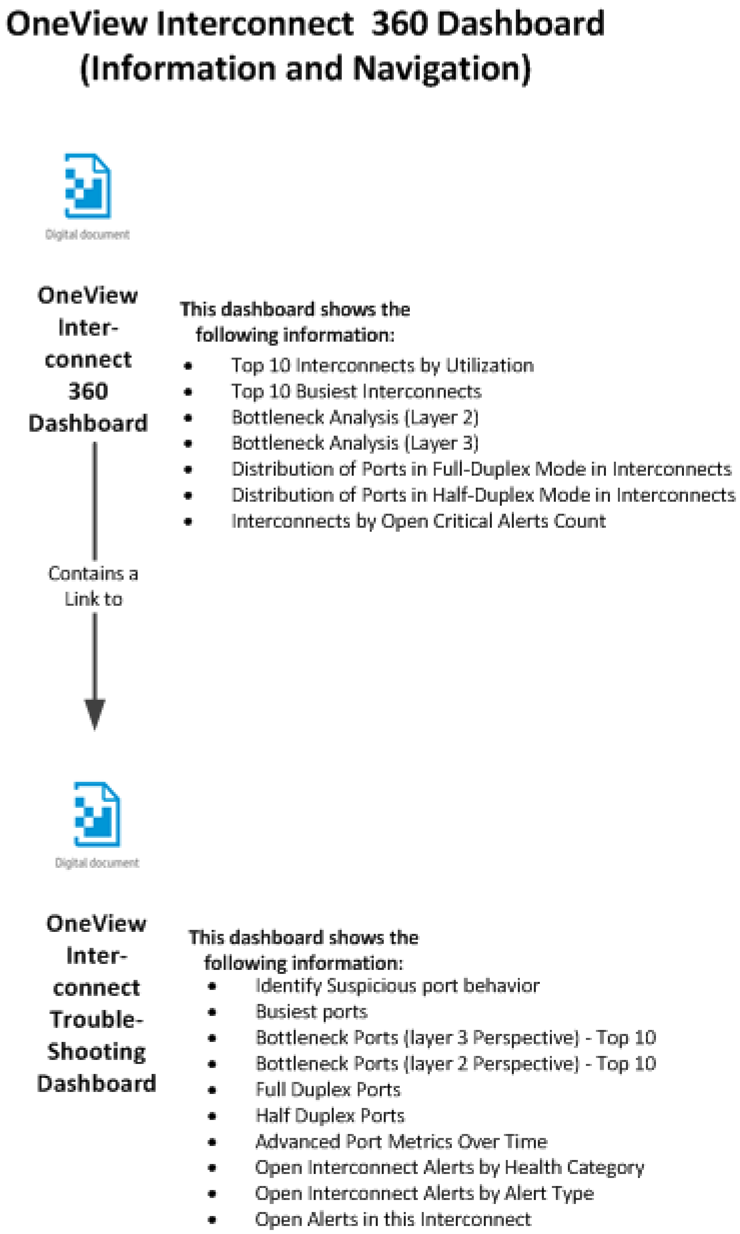
**OneView**

**This dashboard shows the**

Workflow for the OneView Interconnect 360 dashboard:

The following graphic shows you the OneView Interconnect 360 dashboard.





## OneView Interconnect 360 Dashboard (Information and Navigation)

**OneView Inter-connect 360 Dashboard**

**This dashboard shows the following information:**

- Top 10 Interconnects by Utilization
- Top 10 Busiest Interconnects
- Bottleneck Analysis (Layer 2)
- Bottleneck Analysis (Layer 3)
- Distribution of Ports in Full-Duplex Mode in Interconnects
- Distribution of Ports in Half-Duplex Mode in Interconnects
- Interconnects by Open Critical Alerts Count

Contains a Link to

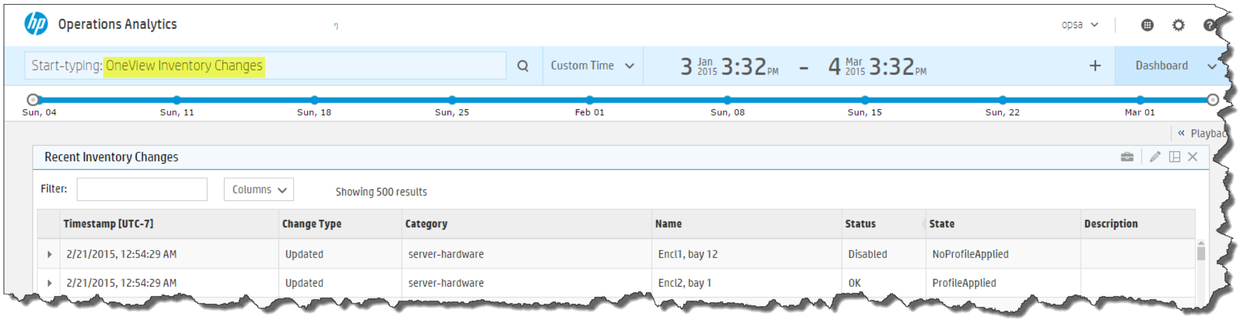
**OneView Inter-connect Trouble-Shooting Dashboard**

**This dashboard shows the following information:**

- Identify Suspicious port behavior
- Busiest ports
- Bottleneck Ports (layer 3 Perspective) - Top 10
- Bottleneck Ports (layer 2 Perspective) - Top 10
- Full Duplex Ports
- Half Duplex Ports
- Advanced Port Metrics Over Time
- Open Interconnect Alerts by Health Category
- Open Interconnect Alerts by Alert Type
- Open Alerts in this Interconnect

Workflow for the OneView Inventory Changes dashboard:

The following graphic shows you the OneView Inventory Changes dashboard.

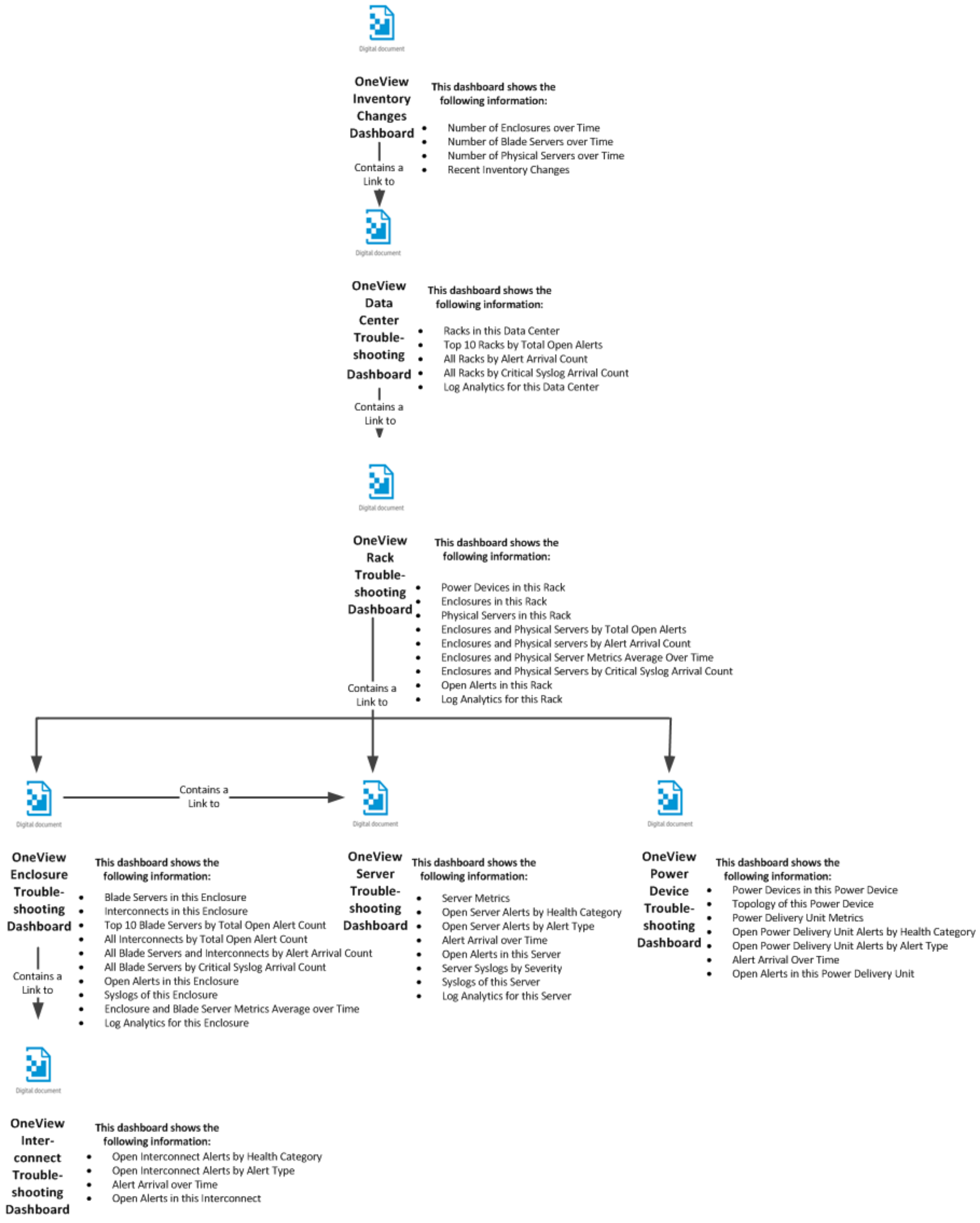


Recent Inventory Changes

Showing 500 results

| Timestamp [UTC-7] | Change Type | Category | Name | Status | State | Description |
|---|---|---|---|---|---|---|
| 2/21/2015, 12:54:29 AM | Updated | server-hardware | Encl1, bay 12 | Disabled | NoProfileApplied | |
| 2/21/2015, 12:54:29 AM | Updated | server-hardware | Encl2, bay 1 | OK | ProfileApplied | |

**OneView Inventory Changes Dashboard (Information and Navigation)**



**OneView Inventory Changes Dashboard**

This dashboard shows the following information:

- Number of Enclosures over Time
- Number of Blade Servers over Time
- Number of Physical Servers over Time
- Recent Inventory Changes

Contains a Link to

**OneView Data Center Trouble-shooting Dashboard**

This dashboard shows the following information:

- Racks in this Data Center
- Top 10 Racks by Total Open Alerts
- All Racks by Alert Arrival Count
- All Racks by Critical Syslog Arrival Count
- Log Analytics for this Data Center

Contains a Link to

**OneView Rack Trouble-shooting Dashboard**

This dashboard shows the following information:

- Power Devices in this Rack
- Enclosures in this Rack
- Physical Servers in this Rack
- Enclosures and Physical Servers by Total Open Alerts
- Enclosures and Physical servers by Alert Arrival Count
- Enclosures and Physical Server Metrics Average Over Time
- Enclosures and Physical Servers by Critical Syslog Arrival Count
- Open Alerts in this Rack
- Log Analytics for this Rack

Contains a Link to

**OneView Enclosure Trouble-shooting Dashboard**

This dashboard shows the following information:

- Blade Servers in this Enclosure
- Interconnects in this Enclosure
- Top 10 Blade Servers by Total Open Alert Count
- All Interconnects by Total Open Alert Count
- All Blade Servers and Interconnects by Alert Arrival Count
- All Blade Servers by Critical Syslog Arrival Count
- Open Alerts in this Enclosure
- Syslogs of this Enclosure
- Enclosure and Blade Server Metrics Average over Time
- Log Analytics for this Enclosure

Contains a Link to

**OneView Server Trouble-shooting Dashboard**

This dashboard shows the following information:

- Server Metrics
- Open Server Alerts by Health Category
- Open Server Alerts by Alert Type
- Alert Arrival over Time
- Open Alerts in this Server
- Server Syslogs by Severity
- Syslogs of this Server
- Log Analytics for this Server

**OneView Power Device Trouble-shooting Dashboard**

This dashboard shows the following information:

- Power Devices in this Power Device
- Topology of this Power Device
- Power Delivery Unit Metrics
- Open Power Delivery Unit Alerts by Health Category
- Open Power Delivery Unit Alerts by Alert Type
- Alert Arrival Over Time
- Open Alerts in this Power Delivery Unit

Contains a Link to

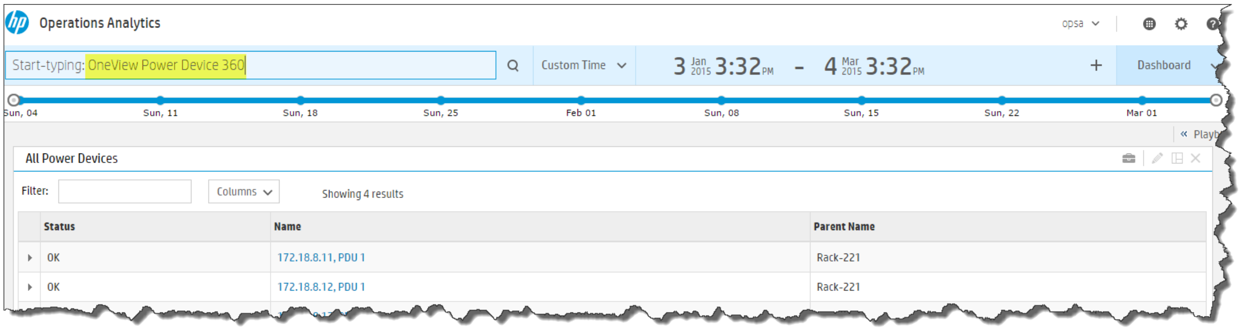
**OneView Inter-connect Trouble-shooting Dashboard**

This dashboard shows the following information:

- Open Interconnect Alerts by Health Category
- Open Interconnect Alerts by Alert Type
- Alert Arrival over Time
- Open Alerts in this Interconnect

Workflow for the OneView Power Device 360 dashboard:

The following graphic shows you the OneView Power Device 360 dashboard.

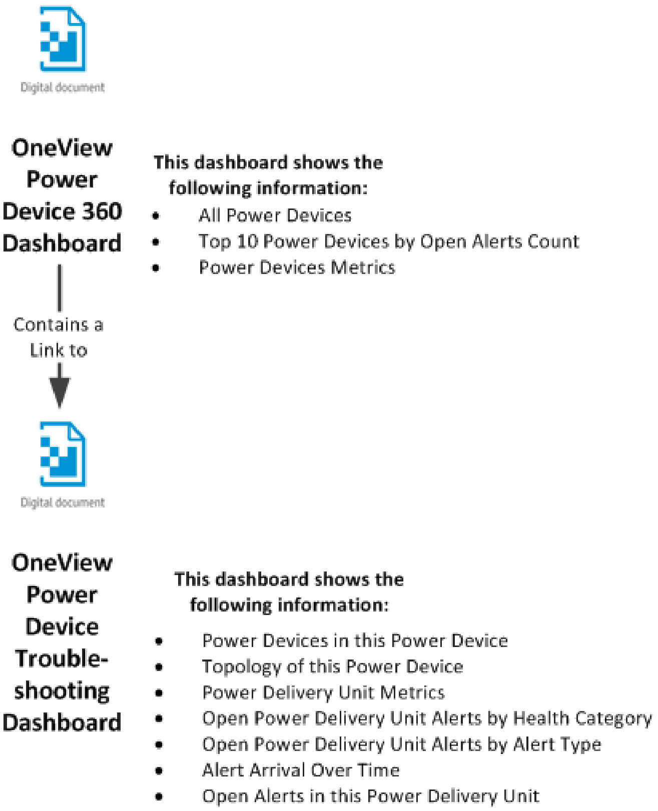


All Power Devices

Filter: Columns Showing 4 results

| Status | Name | Parent Name |
|---|---|---|
| OK | 172.18.8.11, PDU 1 | Rack-221 |
| OK | 172.18.8.12, PDU 1 | Rack-221 |

## OneView Power Device 360 Dashboard (Information and Navigation)



**OneView Power Device 360 Dashboard**

**This dashboard shows the following information:**

- All Power Devices
- Top 10 Power Devices by Open Alerts Count
- Power Devices Metrics

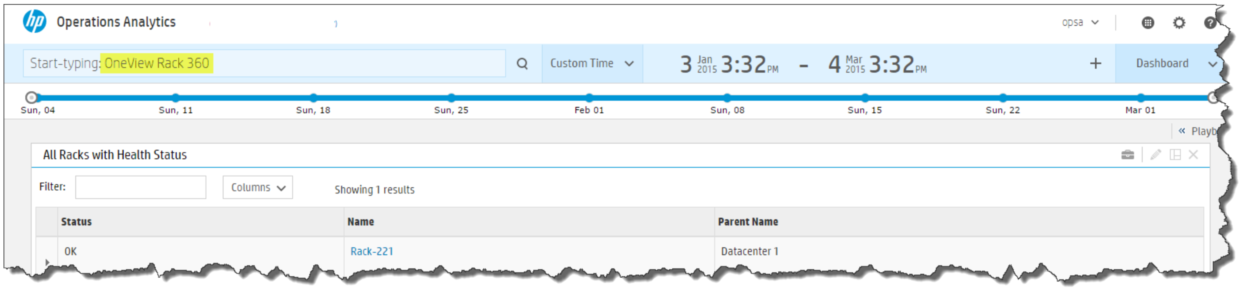
**OneView Power Device Trouble-shooting Dashboard**

**This dashboard shows the following information:**

- Power Devices in this Power Device
- Topology of this Power Device
- Power Delivery Unit Metrics
- Open Power Delivery Unit Alerts by Health Category
- Open Power Delivery Unit Alerts by Alert Type
- Alert Arrival Over Time
- Open Alerts in this Power Delivery Unit

Workflow for the OneView Rack 360 dashboard:

The following graphic shows you the OneView Rack 360 dashboard.

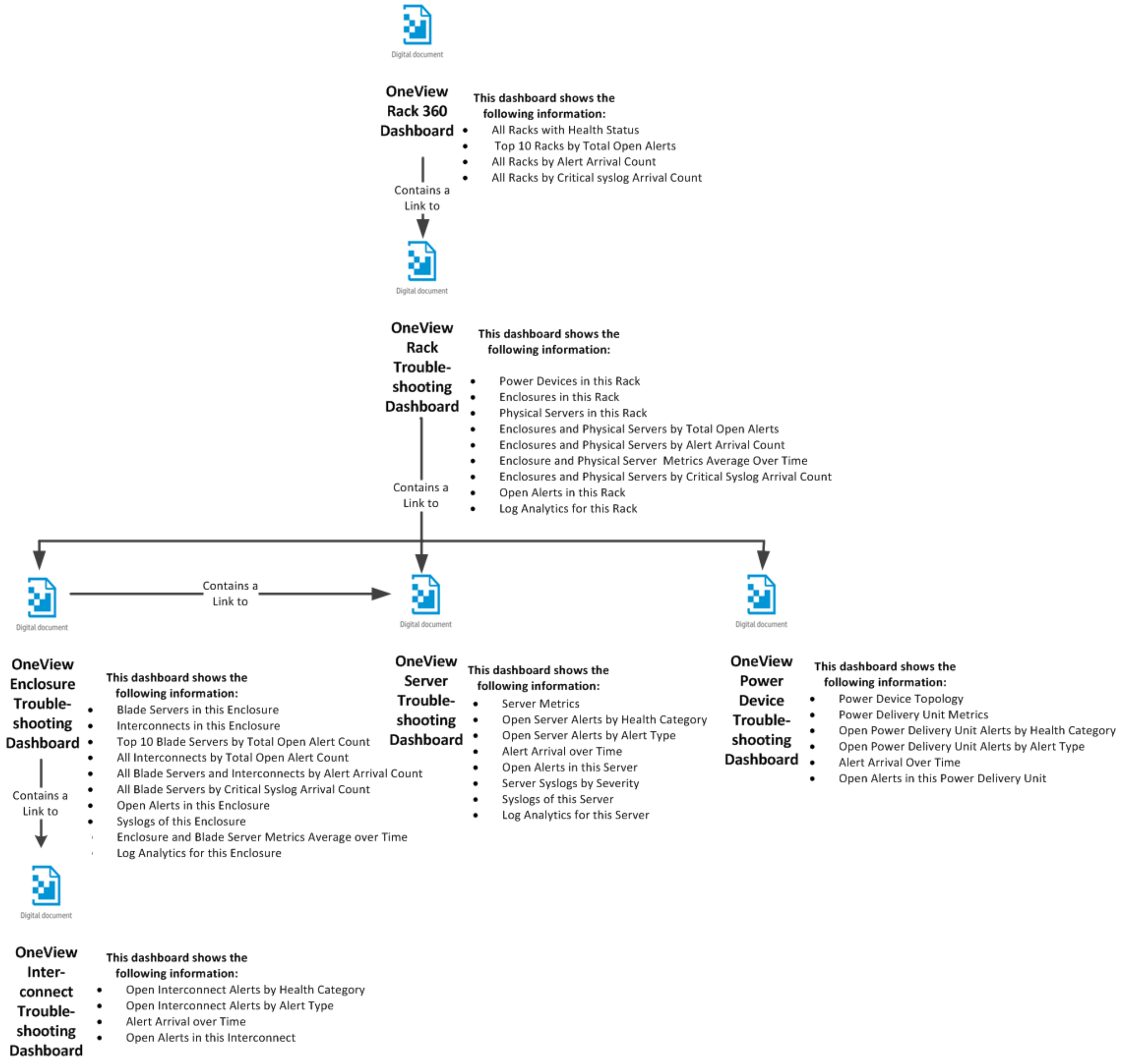


All Racks with Health Status

Filter: Columns Showing 1 results

| Status | Name | Parent Name |
|---|---|---|
| OK | Rack-221 | Datacenter 1 |

**OneView Rack 360 Dashboard (Information and Navigation)**



**OneView Rack 360 Dashboard**

This dashboard shows the following information:

- All Racks with Health Status
- Top 10 Racks by Total Open Alerts
- All Racks by Alert Arrival Count
- All Racks by Critical syslog Arrival Count

**OneView Rack Trouble-shooting Dashboard**

This dashboard shows the following information:

- Power Devices in this Rack
- Enclosures in this Rack
- Physical Servers in this Rack
- Enclosures and Physical Servers by Total Open Alerts
- Enclosures and Physical Servers by Alert Arrival Count
- Enclosure and Physical Server Metrics Average Over Time
- Enclosures and Physical Servers by Critical Syslog Arrival Count
- Open Alerts in this Rack
- Log Analytics for this Rack

**OneView Enclosure Trouble-shooting Dashboard**

This dashboard shows the following information:

- Blade Servers in this Enclosure
- Interconnects in this Enclosure
- Top 10 Blade Servers by Total Open Alert Count
- All Interconnects by Total Open Alert Count
- All Blade Servers and Interconnects by Alert Arrival Count
- All Blade Servers by Critical Syslog Arrival Count
- Open Alerts in this Enclosure
- Syslogs of this Enclosure
- Enclosure and Blade Server Metrics Average over Time
- Log Analytics for this Enclosure

**OneView Server Trouble-shooting Dashboard**

This dashboard shows the following information:

- Server Metrics
- Open Server Alerts by Health Category
- Open Server Alerts by Alert Type
- Alert Arrival over Time
- Open Alerts in this Server
- Server Syslogs by Severity
- Syslogs of this Server
- Log Analytics for this Server

**OneView Power Device Trouble-shooting Dashboard**

This dashboard shows the following information:

- Power Device Topology
- Power Delivery Unit Metrics
- Open Power Delivery Unit Alerts by Health Category
- Open Power Delivery Unit Alerts by Alert Type
- Alert Arrival Over Time
- Open Alerts in this Power Delivery Unit

**OneView Inter-connect Trouble-shooting Dashboard**

This dashboard shows the following information:

- Open Interconnect Alerts by Health Category
- Open Interconnect Alerts by Alert Type
- Alert Arrival over Time
- Open Alerts in this Interconnect

## Using the Phased Query Language with HPE OneView

With the Operations Analytics - HPE OneView integration, you have some additional PQL search query options.

The PQL search query now supports three additional search tags:

- **enclosure**: Use this tag to search for specific enclosures.
- **server_hardware**: Use this tag to search for physical servers and blade servers within enclosures.
- **power_device**: Use this tag to search for power devices.
- **interconnect**: Use this tag to search for interconnects managed by HPE OneView.

When you start a PQL search query by typing any of the tags shown above, the search bar suggests the applicable entity instances using the **withkey** string . For example,if you start typing `enclosure`, Operations Analytics shows you suggestions such as : `enclosure withkey <enclosure name> <IP address>`. Similarly for the `server_hardware` and `power_device` tags, Operations Analytics shows you applicable suggestions.

These PQL suggestions are tied to your HPE OneView environment, as the entity instances being suggested come directly from the database in which this management data or inventory data exists. As discussed earlier, the management data for HPE OneView are alerts, syslogs and metrics. After you select a suggestion from the list of suggestions, the PQL dynamically generates a dashboard for the selected entity with the panes showing the HPE OneViewmanagement data.

The dashboards from the PQL search queries contain panes of information similar to the following:

- A metrics line chart showing the applicable metrics of the selected entity (applicable for enclosures, server hardware and power devices).
- A pie chart showing enclosure syslogs by severity (applicable for enclosures and server hardware).
- A table showing enclosure syslogs (applicable for enclosures and server hardware).
- A list of enclosure alerts by health category (applicable for enclosures, server hardware, and power devices).
- A table of enclosure alerts (applicable for enclosures, server hardware, and power devices).

Operations Analytics information panes appear in the generated dashboard only when there is data available in the database for those panes.

Metric panes contain links to the corresponding troubleshooting dashboards for a given entity. For example, if a PQL search query shows a metric pane for several power devices, it will contain a link to the power device troubleshooting dashboard for those power devices.

# Tasks

Troubleshooting with OneView Dashboards

After configuring the Operations Analytics - HPE OneView integration, Operations Analytics provides the dashboards described in this section to use when troubleshooting with OneView.

- **OneView Environment Overview Dashboard**: This dashboard shows summarized management information for all the data centers currently being managed by HPE OneView. Use this dashboard as the starting point for troubleshooting your infrastructure. From here, select a data center and navigate to the OneView Data Center Troubleshooting dashboard to continue troubleshooting.
- **OneView Data Center Troubleshooting Dashboard**: This dashboard shows a 360 degree view of the selected data center, showing all of the racks residing in the data center. From here, select a rack to go to the **OneView Rack Troubleshooting** dashboard.
- **OneView Rack Troubleshooting Dashboard**: From the **OneView Rack Troubleshooting** dashboard

you can view the various aspects of the rack and select an enclosure to go to the **OneView Enclosure Troubleshooting** dashboard or select a physical server to go to the **OneView Server Troubleshooting** dashboard.

- **OneView Enclosure Troubleshooting Dashboard**: From the **OneView Enclosure Troubleshooting** dashboard, you can view the various aspects of the enclosure and select a blade server to open the **OneView Server Troubleshooting** dashboard for the selected blade. From the **OneView Enclosure Troubleshooting** dashboard you can also select an interconnect to go to the **OneView Interconnect Troubleshooting** dashboard.
- **OneView Server Troubleshooting Dashboard**: Use this dashboard to troubleshoot a blade server or a physical server.
- **OneView Interconnect Troubleshooting Dashboard**: Use this dashboard to troubleshoot the selected interconnect.
- **Start-Typing bar**: As a shortcut, use Operations Analytics **Start-typing** bar to search for a Oneview managed entity and quickly open its troubleshooting or analytics page.

# Chapter 17: Content Packs

You can combine additional information with the data collected by Operations Analytics by using the content packs shown in the following location: Operations Analytics Content Packs (https://hpln.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 18: Configuring LDAP Server Authentication for Operations Analytics

The Operations Analytics console supports Lightweight Access Directory Protocol (LDAP) for user authentication. The instructions in this section explain how to configure Operations Analytics to connect to an LDAP server to validate Operations Analytics users. Only a Super Admin User, opsaadmin by default, can configure Operations 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 Analytics does the following to authenticate users when multiple LDAP servers exist:
  >
  > - Operations Analytics does not contact LDAP servers in any specific order.
  > - Operations 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 opsaadmin 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 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 username and 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 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 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. 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 Analytics console, create an Operations 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 Analytics console. Enter information into this form to provide mapping that enables automatic user profile creation in Operations 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 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 Analytics. All of the Operations 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 user name and 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 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. Exit the `opsa-server-manager.sh` script.

2. Run the following command to check that the LDAP information you added to Operations Analyticsis 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 Analytics console, create an Operations 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 Analytics console. Enter information into this form to provide mapping that enables automatic user profile creation in Operations 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**.

See the *opsa-ldap-configuration-manager.sh* and *opsa-ldap-group-mapping-manager.sh* reference pages (or the Linux man pages) for more information.

# Chapter 19: 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 Management**.

## Learn About

### About User Accounts

As an Operations Analytics administrator, you must configure a User Account for each user who needs to access the Operations 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 147, **opsa-tenant-manager.sh** (available from help > reference pages), and "Configuring Tenants and Collections" in the HPE Operations Analytics Configuration Guide .

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 Analytics from a specific user account, Operations Analytics denies access to users attempting access with this user account. This account restriction lasts for ten minutes. If you have any Operations Analytics access problems, discuss them with your Operations 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 HPE Operations Analytics Configuration Guide.

### About User Groups

User Groups are pre-defined in Operations 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 Analytics graphical user interface.

- You cannot add a new User Group to Operations Analytics.
- A User Account was assigned to the **Super Admin** User Group when Operations Analytics was installed.
- See **opsa-tenant-manager.sh** (available from help > reference pages) and "Configuring Tenants and Collections" in the HPE Operations Analytics Configuration Guide for information about assigning a user to a User Group.

### Pre-defined User Groups

| User Group | Description | Supported Tasks |
|---|---|---|
| Super Admin | **Note:** Operations Analytics permits only one Super Admin user.<br>The user account assigned to this user group has access to the following information for each tenant defined:<br>• User Accounts<br>• User Groups | Add, modify, and delete tenants.<br>Add, modify, and delete user accounts assigned to the Tenant Admin user group. |
| Tenant Admin | User accounts assigned to this User Group have access to the following information only for the tenant to which they are assigned:<br>• Collectors<br>• Collections<br>• Meta Data<br>• Tags<br>• User Accounts<br>• User Groups | Add, modify, and delete user accounts.<br>Manage the collectors, collections, meta data, and tags for a specified tenant. |
| User | User accounts assigned to this User Group have access to the Operations Analytics graphical user interface and to only the meta data and data for the tenant to which they are assigned. | Access and perform tasks using the Operations Analytics Dashboards.<br>**Note:** Users assigned to this user group can also add and delete tags from a collection. See **opsa-tag-manager.sh** (available from help > reference pages) and "Configuring Tenants and Collections" in the HPE Operations Analytics Configuration Guide for more information. |

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 Analytics supports multi-tenancy. This means one instance of Operations 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 Analytics, by default Operations Analytics creates the **opsa_default** tenant.

To create one or more tenants, see **opsa-tenant-manager.sh** (available from help > reference pages) and "Configuring Tenants and Collections" in the HPE Operations Analytics Configuration Guide .

# Tasks

## Add a User Account

1. Click ⚙**Settings** and select **Users Manager**.

   Operations Analytics displays 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 Analytics displays the **Add User** form with options for LDAP or Local Authentication.

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.

4. Finish entering your passwords for a locally authentication user, then click **Add**.

   Operations 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.

You can also add a user account using the opsa-user-manager.sh script. Run the following command for creating a local user:
$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*>

Run the following command for creating a new LDAP authenticated user:
$OPSA_HOME/bin/opsa-user-manager.sh -add -loginUser <*Super Admin or Tenant Admin User Name*> -loginPassword <*password*> -newUser <*new username*> -ldapAuthenticated *user role* [-tenant *tenant*]

> **Note:** The –tenant and –role parameters are required only for the Super Admin User.

> **Note:** See the opsa-user-manager.sh reference page (or the Linux manpage) 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 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 manpage) for more information.

## Add a Tenant

As an Operations 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 Analytics.
> - If you do not configure one or more tenants, Operations 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 and a tenant admin**:

1. Click ⚙**Settings** and select **Users Manager**.

   Operations Analytics displays 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 Analytics displays 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:** Operations Analytics 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:

   - 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.

7. Click **OK** to add the Tenant Admin.

# Chapter 20: 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 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 78.

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 21: Administrator Tasks

As an Operations Analytics administrator, you perform the tasks described in the table below to enable Operations Analytics users to proactively manage and troubleshoot IT operations problems.

For example, after you have initially installed and configured Operations Analytics, you might find that you want to use additional data sources and configure the associated collections.

### Administrator Tasks

| Category | Task | Location in Documentation | Command |
|---|---|---|---|
| Maintain Collections and Collectors | Plan for each new data source and subsequent collection configuration. | "Planning Your Deployment" in the HPE Operations Analytics Installation Guide. | |
| | *In multiple Operations Analytics server environments only*. Designate the Operations Analytics server from which to configure all collections. | "Configuring Tenants and Collections" in the HPE Operations Analytics Configuration Guide. | |
| | Create the collection template for each additional collection. | "Adding a New HPE Operations Analytics Collection" in the HPE Operations Analytics Configuration Guide. | **opsa-collection-config.sh** (available from help > reference pages) |
| | Configure your collection templates to match your IT environment. | "Configuring Tenants and Collections" in the HPE Operations Analytics Configuration Guide. | **opsa-collection-config.sh** (available from help > reference pages) |
| | *Optional*. Add one or more tenants | "Add a Tenant" on page 149<br>"Creating a Tenant" in the HPE Operations Analytics Configuration Guide. | **opsa-tenant-manager.sh** (available from help > reference pages) |
| | *Optional*. Delete one or more tenants.<br>**Note:** Be sure to remove a collection registration for any tenant that will be removed. | "Deleting a Tenant" and "Remove a Collection Registration for a Tenant" in the HPE Operations Analytics Configuration Guide. | **opsa-tenant-manager.sh** (available from help > reference pages) |
| | *Optional*. Associate each collection with a tenant.<br>**Note:** You must first create the tenant to which you want to associate a collection. | "Configuring Tenants and Collections" in the HPE Operations Analytics Configuration Guide. | **opsa-tenant-manager.sh** (available from help > reference pages) |

### Administrator Tasks , continued

| Category | Task | Location in Documentation | Command |
|---|---|---|---|
| | *Optional.* For each tenant, create a user account for the **Tenant Admin** and **User** User Groups. | "Manage Users and Tenants" on page 145<br>"Configuring Tenants and Collections" in the HPE Operations Analytics Configuration Guide. | **opsa-tenant-manager.sh** (available from help > reference pages) |
| | Configure a collector for each new collection. | "Configuring Tenants and Collections" in the HPE Operations Analytics Configuration Guide. | **opsa-collection-config.sh** (available from help > reference pages) |
| | Configure additional collectors for one or more existing collections. | "Installing and Configuring the Operations Analytics Collector Appliance using the VMware vSphere Client" in the HPE Operations Analytics Installation Guide and "Configuring Tenants and Collections" in the HPE Operations Analytics Configuration Guide. | **opsa-collection-config.sh** (available from help > reference pages) |
| | Back up your collection configuration on the Operations Analytics server. The collection configuration directory is:<br>`/opt/HP/opsa/conf/collection` | "Configuring Tenants and Collections" in the HPE Operations Analytics Configuration Guide. | |
| | Troubleshoot collection problems | "Troubleshooting Operations Analytics Collections" in the HPE Operations Analytics Configuration Guide. | |
| | Communicate collection names and meta data information to your users. | See "Communicating Collection Names and Meta Data Information to your Users" in the HPE Operations Analytics Configuration Guide. | |
| | Set collection retention periods. | See "Setting Collection Retention Periods" in the HPE Operations Analytics Configuration Guide. | |

**Administrator Tasks , continued**

| Category | Task | Location in Documentation | Command |
|---|---|---|---|
| Define a Service | View the collection information stored in Operations Analytics. | "How to View Collection Information" on page 78 | |
| | Topology Manager enables you to group together hosts that are of interest to you, and view them in Operations Analytics as a **service**. You can group hosts together based on their function, their location, or any other grouping that is meaningful to you when organizing your services. | "Topology Manager" on page 59 | |
| Create AQL Functions | *Optional*. Write Analytic Query Language (AQL) functions using a text editor. | AQL Developer Guide | |
| Import AQL Functions | *Optional.* Import your AQL functions. | AQL Developer Guide | **opsa-aql-module-manager.sh** (available from help > reference pages) |
| Maintain User Accounts | Add, modify, or delete one or more user accounts. | "Manage Users and Tenants" on page 145<br>"Maintaining User Accounts" in the HPE Operations Analytics Configuration Guide. | |
| Maintain HP Operations Analytics | Check the system health of Operations Analytics. | "Check the Health of Operations Analytics" on the next page<br>"Checking Operations Analytics System Health" in the HPE Operations Analytics Configuration Guide. | |
| | Back up the Operations Analytics database. | "Maintaining the HPE Operations Analytics Database" in the HPE Operations Analytics Configuration Guide. | |
| | View license information. | Access Help and About Information from the help menu. | |

# Check the Health of Operations Analytics

Operations Analytics provides two methods for checking the health of servers running the Operations Analytics service:

## Command Line Interface

The table below describes the commands used to check the status of Operations Analytics:

| Command | Description |
|---|---|
| opsa-server status | Check the status of the Operations Analytics service<br>**Note:** The opsa-server command must be run on the Operations Analytics server. |
| opsa-collector status | Checks the status of the collector service on the Collector Appliance.<br>**Note:** The opsa-collector command must be run on the Operations Analytics Collector Appliance. |
| opsa-loader status | Checks the status of the loader service on the Collector Appliance.<br>**Note:** The opsa-loader command must be run on the Operations Analytics Collector Appliance. |

## OpsaSystemHealth Dashboard

Use the OpsaSystemHealth dashboard to investigate the health of the Operations 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. Also see "Checking Operations Analytics System Health" in the HPE Operations Analytics Configuration Guide for the configuration steps required to display this dashboard information.

| Query Pane | Description | Required Software |
|---|---|---|
| Host System Metrics over Time | Use this visualization to determine server health for the Operations Analytics servers.<br>Displays the average value over time for the following metrics for each server running the Operations Analytics service:<br>• System up time<br>• CPU utilization | HPE Operations Agent |

| Query Pane | Description | Required Software |
|---|---|---|
| Service Topology | Use this visualization to determine the servers running Operations Analytics software.<br>Displays topology information for the Operations Analytics service, including the following servers:<br>• Operations Analytics server<br>• Operations Analytics collector servers<br>• HPE logger servers<br>• HPE Vertica database servers<br>Also displays the CPU utilization and system up time for each of the Operations Analytics servers. | Operations 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+) | Use this visualization to troubleshoot any Operations Analytics log file error messages.<br>Displays all log file messages for servers running the Operations Analytics service. | Operations Analytics only |

# Glossary

## A

**attribute**

A descriptor stored in a collection for an entity, such as host_name.

## C

**category**

A folder that is used to organize your AQL modules.

**collections**

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

## D

**Database schema**

Table, column, attribute, and data type information per collection.

## K

**Knowledge Content**

An xml file that configures a predefined dashboard. Each Knowledge Context includes a name, the entities for which the dashboard displays information, phrases to help identify the Knowledge Context, as well as the queries that return the dashabord and any filters to use before the data is returned.

## M

**metric**

Typically a measurement stored in a collection. For example, CPU utilization.

## O

**outlier**

A data point that is outside of the normal range based on the data collected to date.

## Q

**query pane**

Displays the results of an Analytic Query Language (AQL) query, AQL function, or AQL expression. If you use the Phrased Query Language (PQL) in your search, HP Operations Analytics converts the PQL query to one or more AQL queries and subsequent query panes.

## R

**raw logs**

Log files that contain messages as they appear in the log source from which they are collected. These log files must be configured using the log file management software supported by HP Operations Analytics. See the HP Operations Analytics Support Matrix for more information.

**raw metrics**

Metrics to which an overall aggregate or moving aggregate analytic function is applied.

## S

**structured log files**

Fragments of log file data that are stored as collections in HP Operations Analytics. Structured logs are log files that are configured as collections. These collections are created so that users can perform analytics on the log file contents. For example, you might want to query for all outliers by host name and application for a particular time range.

## T

**tag**

A word or phrase that is associated with a metric, topology, event, or log file attribute that is stored as part of a collection in HP Operational Analytics. These tags can be used in the HP Operational Analtyics search query as synonyms for the attributes stored in HP Operational Analytics collection tables. They are also used to make metrics display names more meaningful. Tags are provided by HP Operational Analytics and can also be defined by the HP Operational Analytics administrator.

# 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 HPE Operations Analytics Help (Operations Analytics 2.32)**

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 sw-doc@hpe.com.

We appreciate your feedback!