



# Operations Bridge Analytics

Software Version: 3.03

## Troubleshooting Guide

Document Release Date: December 2017

Software Release Date: November 2017



**Hewlett Packard**  
Enterprise

## Legal Notices

### Warranty

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

The information contained herein is subject to change without notice.

### Restricted Rights Legend

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

### Copyright Notice

© 2016 - 2017 Hewlett Packard Enterprise Development LP

### Trademark Notices

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

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

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

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

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

iPad® and iPhone® are trademarks of Apple Inc.

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

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

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

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

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

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

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

UNIX® is a registered trademark of The Open Group.

## Documentation Updates

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

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

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

## Support

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

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

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

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

# Contents

Troubleshooting .....	4
General Troubleshooting .....	4
Collection Troubleshooting .....	6
Integration Troubleshooting .....	11
Send documentation feedback .....	15

# Troubleshooting

This section provides information to help you to diagnose and solve problems with OBA.

["General Troubleshooting" below](#)

["Collection Troubleshooting" on page 6](#)

["Integration Troubleshooting" on page 11](#)

## General Troubleshooting

This section includes some general troubleshooting tips and techniques for resolving Operations Bridge Analytics issues.

**Problem:** When I log on to an OBA Application Server or OBA Collector host as an opsa user, I receive an Account locked due to <n> failed logins message, yet I know the password I supplied is correct.

**Solution:** This message indicates that you need to wait some period of time after the last failed attempt to try to log on again. However, for the this opsa user, this message means you are really supplying the wrong password. Obtain the correct password for the opsa user and try again. You will be able to log on immediately by using the correct password.

---

**Problem:** I am using an integration between Operations Bridge Analytics and Logger and suspect that my Logger collection is missing some log data.

**Solution:** Configuring Logger to use the **TCP Forwarding** feature, also known as CEF forwarding, is more reliable.

---

**Problem:** I use the logrotate Linux command with the copytruncate feature to rotate the logs for a product that has its logs collected by Operations Bridge Analytics. Are there any logrotate command limitations I should be aware of?

**Solution:** Using the logrotate command's copytruncate feature is strongly discouraged:

- In high load scenarios, lines were missed in the short time frame right before the rotation.
  - When using a pattern for the logfile name, every line is sent twice to the OBA Application Server.
-

**Problem:** I installed Operations Bridge Analytics, which installed Operations Agent over the top of an existing Operations Agent installation, without error. The Operations Bridge Analytics issue is that I cannot set up any Operations Agent or OMi collections.

**Solution:** The only known remedy is to complete a new Operations Bridge Analytics installation on a server that has a fresh operating system installed with no other software applications installed, such as HPE Operations Agent.

---

**Problem:** How can I verify that a Source Type published successfully?

**Solution:** Do the following:

1. From the Operations Bridge Analytics console, view the Meta Info dashboard:
  2. Enter the property group `uid` for this Source Type in the **Collection Columns** Filter. The property group `uid` is the name of the string (in the form of `<source type name>_logstash_metrics`).
  3. If the resulting table shows data, then the Source Type published successfully.
- 

**Problem:** How do I enable the topology feature to recognize hosts coming from a Source Type?

**Solution:** To enable the topology feature to recognize hosts coming from a Source Type, do the following:

1. Enable the JMX console by changing the suffix of the following file on the application server appliance from `.tx` to `.txt`:

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

2. Wait five minutes before attempting to log on to the JMX console.
3. Log on to the JMX console by using the following syntax:

**`http://<application_server_FQDN>:8081`**

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

4. Locate the OBA Infrastructure Settings area.
5. Locate the **`java.lang.String get GLOBALSettingDefaultValue`** item.
  - a. Set the value to **`opsa-customtopology-settings`**.
  - b. Invoke the function and copy the list of values in the results to a text file
  - c. Add a line to represent the custom collection using the following syntax:

*`<collection_name>, <field from collection tagged as host>`*

6. Locate the **java.lang.String set GLOBALSettingDefaultValue** item.
  - a. Set the value of **contextName** to **opsa-customtopology-settings**.
  - b. Set the value of **settingName** to **opsa.customtopology.nodegroup.link\_tags**.
  - c. Copy the list of values from the text file you saved to the **newValue** field.

The topology feature now recognizes hosts coming from this Source Type.

---

**Problem:** After the installation, OBA does not display Metric data.

**Solution:** Reboot the collector.

## Collection Troubleshooting

To troubleshoot your collections, you can check a collector's status, investigate why a collection is not collecting data, check the log messages, and look into why you might receive unparsed messages.

### Check a collector's status

To check a collector's status, do the following:

- Run the following command from an OBA Application Server to list the collections deployed to that OBA Collector host:
 

```
$OPSA_HOME/bin/opsa-collection-config.sh -list -collectorhost <collector hostname> -username opsatenantadmin
```
- Run the following commands from an OBA Collector host to check the status of collector sources and processes:
  - `$OPSA_HOME/bin/opsa-collector status`
  - `$OPSA_HOME/bin/opsa-loader status`
- Run the following command from an OBA Application Server to check the status of the collector sources and processes configured on an OBA Collector host:
 

```
$OPSA_HOME/bin/opsa-collection-config.sh -status -collectorhost <collector hostname> -username opsatenantadmin
```

## Troubleshoot the absence of collection data

The information in this section helps you troubleshoot collections that have been published to an OBA Collector host, but are not collecting data. This troubleshooting takes place on the OBA Collector host.

If you restart the `opsa-loader` process, after configuring a collection, data may be lost. This is a known issue.

After configuring a collection, open the Health Overview Dashboard and check **MOVING\_TOTAL (collector\_rows)** to see if it contains a row for each newly configured collection. If any of your newly configured collections are not present, you might need to restart the collector using the following command: `$OPSA_HOME/bin/opsa-collector start`

- Always run the following commands to check that the collector and data loader are functioning correctly.

```
$OPSA_HOME/bin/opsa-collector status
```

```
$OPSA_HOME/bin/opsa-loader status
```

- Look for any error messages in the `/opt/HP/opsa/log/opsa-collector.log` and `/opt/HP/opsa/log/loader.log` files.
- If you want to adjust the logging levels, edit the `/opt/HP/opsa/conf/opsa-collector/log4j/opsa-collector-log.properties` file and set the following properties:

```
log4j.logger.com.hp.opsa.collector = DEBUG
```

```
log4j.logger.com.hp.opsa.collector.common = DEBUG
```

```
log4j.logger.com.hp.opsa.collector.agent = DEBUG
```

```
log4j.logger.com.hp.opsa.collector.server = DEBUG
```

- If the following collections do not collect data, check the associated log files:
  - Operations Agent or Operations Smart Plug-in for Oracle Collections
    - `/opt/HP/BSM/PMDB/log/collections.log`
    - `/opt/HP/BSM/PMDB/log/hpacollector.log`
  - Operations Manager (HPOM) or Operations Manager i (OMi) Collections
    - `/opt/HP/BSM/PMDB/log/collections.log`
    - `/opt/HP/BSM/PMDB/log/dbcollector.log`
  - Any of associated BSM RTSM Collections
    - `/opt/HP/BSM/PMDB/log/collections.log`
    - `/opt/HP/BSM/PMDB/log/topologycollector.log`

- Custom SiteScope Collection: If the Custom SiteScope Collection does not collect data, do the following:
  - Check the `%SITESCOPE_HOME%/log/error.log` and `%SITESCOPE_HOME%/log/data_integration.log` files on the SiteScope server for any error messages about not being able to push SiteScope data to an OBA Collector host.
  - Check the OBA Collector host data integration to make it is configured correctly on the SiteScope server. See [Configuring Collections](#) for more information.
- For the following collections, look in the specific processed folder to check that the collector is collecting data for that collection:
  - Operations Agent Collection: `/opt/HP/opsa/data/pa_processed/<tenant>`
  - Operations Smart Plug-in for Oracle Collection: `/opt/HP/opsa/data/ora_pa_processed/<tenant>`
  - NNMi Custom Poller Collection: `/opt/HP/opsa/data/nnm_processed/<tenant>`

The NNMi Custom Poller collector needs to have read/write access to the NNMi CSV files to move them to the processed directory. If the collector cannot move them, the NNMi Custom Poller CSV files will be reprocessed the next time the collector starts up. See [Configuring Collections](#) for more information.
  - NNM ISPi Performance for Metrics Interface Health
 

Collection: `/opt/HP/opsa/data/netinterface_processed/<tenant>`

The NNM ISPi Performance for Metrics Interface Health collector needs to have read/write access to the NNM ISPi Performance for Metrics Interface Health CSV files to move them to the processed directory. If the collector cannot move them, the NNM ISPi Performance for Metrics Interface Health CSV files will be reprocessed the next time the collector starts up. See [Configuring Collections](#) for more information.
  - NNM ISPi Performance for Metrics Component Health
 

Collection: `/opt/HP/opsa/data/netcomponent_processed/<tenant>`

The NNM ISPi Performance for Metrics Component Health collector needs to have read/write access to the NNM ISPi Performance for Metrics Component Health CSV files to move them to the processed directory. If the collector cannot move them, the NNM ISPi Performance for Metrics Component Health CSV files will be reprocessed the next time the collector starts up. See [Configuring Collections](#) for more information.
  - Operations Manager (HPOM ) Collections: `/opt/HP/opsa/data/om_events_processed/<tenant>`

- Operations Manager i (OMi) Collections: /opt/HP/opsa/data/omi\_events\_processed/<tenant>
- Custom SiteScope Collection:  
/opt/HP/opsa/data/sis\_processed/<tenant>  
Look for collected Customer SiteScope Collection data in /opt/HP/opsa/data/SIS\_GDIAPI\_DATA/<tenant>.
- Custom Collection: <custom source parent directory>\_processed/<tenant>

**Note:** The Custom CSV collector needs to have read/write access to the Custom CSV files to move them to the processed directory. If the collector cannot move them, the Custom CSV files will be reprocessed the next time the collector starts up. See [Configuring Collections](#) for more information.

- To check if data is being loaded into the Operations Bridge Analytics database, look at the files in the /opt/HP/opsa/data/load/<tenant> directory. Files with a .working extension are files to which the collector is actively writing. Working files should never be older than 10 minutes. So any files with a .csv extension are ready to be loaded into the Operations Bridge Analytics database. If the system is functioning correctly, there should not be any \*.csv files older than 10 minutes as well.

If you do not find any files with a .csv extension in the /opt/HP/opsa/data/load/<tenant> directory, do the following:

- Check for any CSV files that were successfully loaded into the Operations Bridge Analytics database by looking in the /opt/HP/opsa/data/archive/<tenant> directory.
- If you do not see files for the collection in question, check to see if the data loader has rejected the load files by looking in the /opt/HP/opsa/data/failed\_to\_load directory.

## Troubleshoot configurations from the OBA application server

To troubleshoot collector and collection configuration, do the following from the OBA Application Server:

- If you completed the instructions to set up Operations Bridge Analytics System Health in [Check the Status of Operations Analytics Servers](#) and installed and configured the Operations Bridge Analytics Log File Connector on the OBA Collector hosts (to collect Operations Bridge Analytics log files), you can check the Health Overview dashboard and look for ERROR and WARN severity log messages.
- Look in the /opt/HP/opsa/log/collection\_config.log file for any errors and warnings.

- If you want to adjust the logging level, edit the `/opt/HP/opsa/conf/opsa-collector/log4j/opsa-collector-log.properties` file and set the following properties. Then reconfigure the collection and view the results.
  - `log4j.logger.com.hp.opsa.collection.config=DEBUG,coll_cfg`
  - `log4j.logger.com.hp.opsa.collector=DEBUG,coll_cfg`

## Messages appear as unparsed messages without appearing in collections

**Problem:** You configure a new source type using the Source Type Manager and you define one or more fields calculated as arithmetic functions of other fields. You notice that some events do not enter the expected Operations Bridge Analytics collections, but appear as unparsed messages.

**Reason:** If Operations Bridge Analytics receives an event or message that has null as a value for one or more of the fields used in the arithmetic function you are using, it will not parse the entire event or message.

**Note:** To view unparsed messages, open the Health Overview dashboard and view the messages shown in the **Unparsed Messages** section.

Here are some ways to notice this issue:

- You know how many log messages and events the source emits per time period and you notice that this number is larger than the entries that appear in the collection.
- You create an AQL query for the `opsa_unparsed_messages` collection and see all the messages and events that were not parsed. If you see messages in this collection it means that these messages and events are absent from the expected collection.

**Workaround:** Do not use arithmetic functions when working with fields that you expect will contain a null value part of the time. Instead, the calculated fields should be created during an earlier stage of the data flow. For example, do the calculation in the SQL query of a JDBC source.

## Collectors are currently not reachable

**Problem:** The red alarm bell at the top right in the Operations Bridge Analytics console displays the message: "The following collectors are currently not reachable: `<collector>`"

**Reason:** Collectors form a Kafka cluster. This error message is displayed if Kafka is not running on one or more registered collectors, which means that they are down.

**Solution:** If a collector that is down cannot be recovered, check if the machine is running. Then check if the OBA processes are running by running the `opsa status` command. Finally, restart OBA by running the `opsa restart` command.

If none of these steps remedies the problem, you must take disaster recovery actions. The disaster recovery actions depend on the number of collectors that form the Kafka cluster, and the number of collectors that are down:

- If the cluster consists of only one collector, the cluster cannot operate anymore if the collector is down. If it is not possible to recover the machine, the Kafka cluster remains unrecoverable and you must take disaster recovery actions.
- If the cluster consists of multiple collectors, the cluster can handle the loss of one collector. However, if more than one collector is down, the Kafka cluster cannot operate anymore. If the collectors cannot be recovered, the Kafka cluster remains unrecoverable and you must take disaster recovery actions.

If a collector cannot be recovered, you must properly decommission it. As soon as this happens, the cluster's fault tolerance is restored.

**Example:** You have a Kafka cluster with three collectors. One of them becomes unavailable and cannot be recovered. There is no more fault tolerance now. As soon as you decommission the unavailable collector, the cluster's fault tolerance is restored.

Do not add any collectors while others are down, as this can result in problems. Before you add collectors, either make sure that all existing collectors are up and running, or decommission collectors that cannot be recovered.

For instructions on how to decommission a collector and/or perform disaster recovery, see [Decommission collectors and perform disaster recovery](#).

## Integration Troubleshooting

See the section below for information about how to resolve certificate errors when integrating Operations Bridge Analytics with OMi.

The OMi dashboard integration results in a certificate error

For the information in this section, consider the following:

- You completed the instructions shown in [BSM and OMi Integrations](#).
- You configured Single Sign-on as required. For more information, see the *HPE Operations Bridge Analytics User Guide*.

When using a browser, you might see a certificate error when navigating from OMi to an Operations Bridge Analytics dashboard from outside the virtual environment. Depending on the browser, different solutions are available:

#### Mozilla Firefox

1. Export the certificate from the browser.
  - a. Open Operations Bridge Analytics in the browser.
  - b. Navigate from OMi to an Operations Bridge Analytics dashboard from outside the virtual environment to see the certificate error you have been experiencing.
  - c. Select **Certificate error** > **View certificates**.
  - d. Select the **Details** tab.
  - e. Select **Copy to File...**
  - f. Select the following format: **Base-64 encoded X.509 (.CER)**.
  - g. Select **Next**.
  - h. Enter *Filename*.
  - i. Select **Next/Finish**.
2. Import the Base-64 encoded X.509 (.CER) version of the certificate into the browser.
  - a. Click **Open menu** in the upper right of the browser.
  - b. Open **Options**; then select **Advanced**.
  - c. Click **View Certificates**.
  - d. Click **Servers**.
  - e. Click **Add Exception** and add the fully qualified domain name of the OBA Application Server.
  - f. Navigate to **View Certificates** > **Servers** again.
  - g. Click **Import ...** and import the Base-64 encoded X.509 (.CER) version of the certificate that you exported earlier into the Firefox browser.

## Internet Explorer

1. Export the certificate from the browser.
  - a. Open Operations Bridge Analytics in the browser.
  - b. Navigate from OMi to an Operations Bridge Analytics dashboard from outside the virtual environment to see the certificate error you have been experiencing.
  - c. Select **Certificate error > View certificates**.
  - d. Select the **Details** tab.
  - e. Select **Copy to File...**
  - f. Select the following format: **Base-64 encoded X.509 (.CER)**.
  - g. Select **Next**.
  - h. Enter *Filename*.
  - i. Select **Next/Finish**.
2. Import the Base-64 encoded X.509 (.CER) version of the certificate into the browser.
  - a. Select **Start > Run** and run the **mmc.exe** command to open a **mmc console**.
  - b. Select **File > Add/remove Snap-in...**
  - c. After a new window opens, select **Certificates > Add**.
  - d. Select **Computer Account**, then click **Next**.
  - e. Select **Local Computer**, then click **Finish**.
  - f. Click **OK** to complete this task.
  - g. Select **Certificates (Local Computer)** to complete this task.
  - h. Right-click **Trusted Root Certification Authorities**, then select **All Tasks > Import** to open the **Certificate Import Wizard**.
  - i. Click **Next**.
  - j. Browse to the location to which you exported the certificate file during Step 1.
  - k. Follow the steps of the interactive wizard to complete the certificate import. For example, you might select **Next > Next > Finish** to complete the certificate import.
  - l. After the **Certificate Import Wizard** informs you that the import was successful, click **OK**.
  - m. You are finished. Close the **mmc console**.

Now you should no longer see a certificate error when navigating from OMi to an Operations Bridge Analytics dashboard from outside the virtual environment.

# Send documentation feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

## **Feedback on Troubleshooting Guide (Operations Bridge Analytics 3.03)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to [ovdoc-asm@hpe.com](mailto:ovdoc-asm@hpe.com).

We appreciate your feedback!