

HP Operations Analytics

Software Version: 2.31

Operations Analytics 2.20 to 2.31 Upgrade Guide

Document Release Date: November 2015
Software Release Date: September 2015



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2015 Hewlett-Packard Development Company, L.P.

Trademark Notices

Microsoft and Windows are 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.hp.com/group/softwaresupport/search-result?keyword=>.

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

Support

Visit the HP Software Support web site at: <https://softwaresupport.hp.com>

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

HP 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 web site to:

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

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

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

HP Software Integrations, Solutions and Best Practices

Visit the Integrations and Solutions Catalog at <https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01702710> to explore how the products in the HP Software catalog work together, exchange information, and solve business needs.

Visit the Cross Portfolio Best Practices Library at <https://hpin.hp.com/group/best-practices-hpsw> to access a wide variety of best practice documents and materials.

Contents

Chapter 1: Introduction to Upgrading Operations Analytics	4
Chapter 2: Environment Variables used in this Document	5
Chapter 3: Upgrade Infrastructure and Specifications	6
Chapter 4: Vertica Upgrade	8
Chapter 5: Upgrade Steps	9
Chapter 6: Roll Back Due to Errors	20
Chapter 7: Support Considerations	22
Preserving Operations Analytics Log Files	22
Send Documentation Feedback	23

Chapter 1: Introduction to Upgrading Operations Analytics

This document shows you how to upgrade Operations Analytics from version 2.20 to version 2.31. The upgrade steps shown in this document support one or more Operations Analytics Server Appliances along with the associated Collector Appliances used in your Operations Analytics configuration.

Chapter 2: Environment Variables used in this Document

This document refers to the following environment variables and other useful directories when explaining upgrade instructions for the Operations Analytics Software, including the Operations Analytics Server Appliance and the Operations Analytics Collector Appliance.

Table 1: Environment Variables

Variable Name	Path	Operations Analytics Server Appliance or Collector Appliance
OPSA_HOME	/opt/HP/opsa	Server and Collector Appliances
JAVA_HOME	/opt/HP/opsa/jdk	Server and Collector Appliances

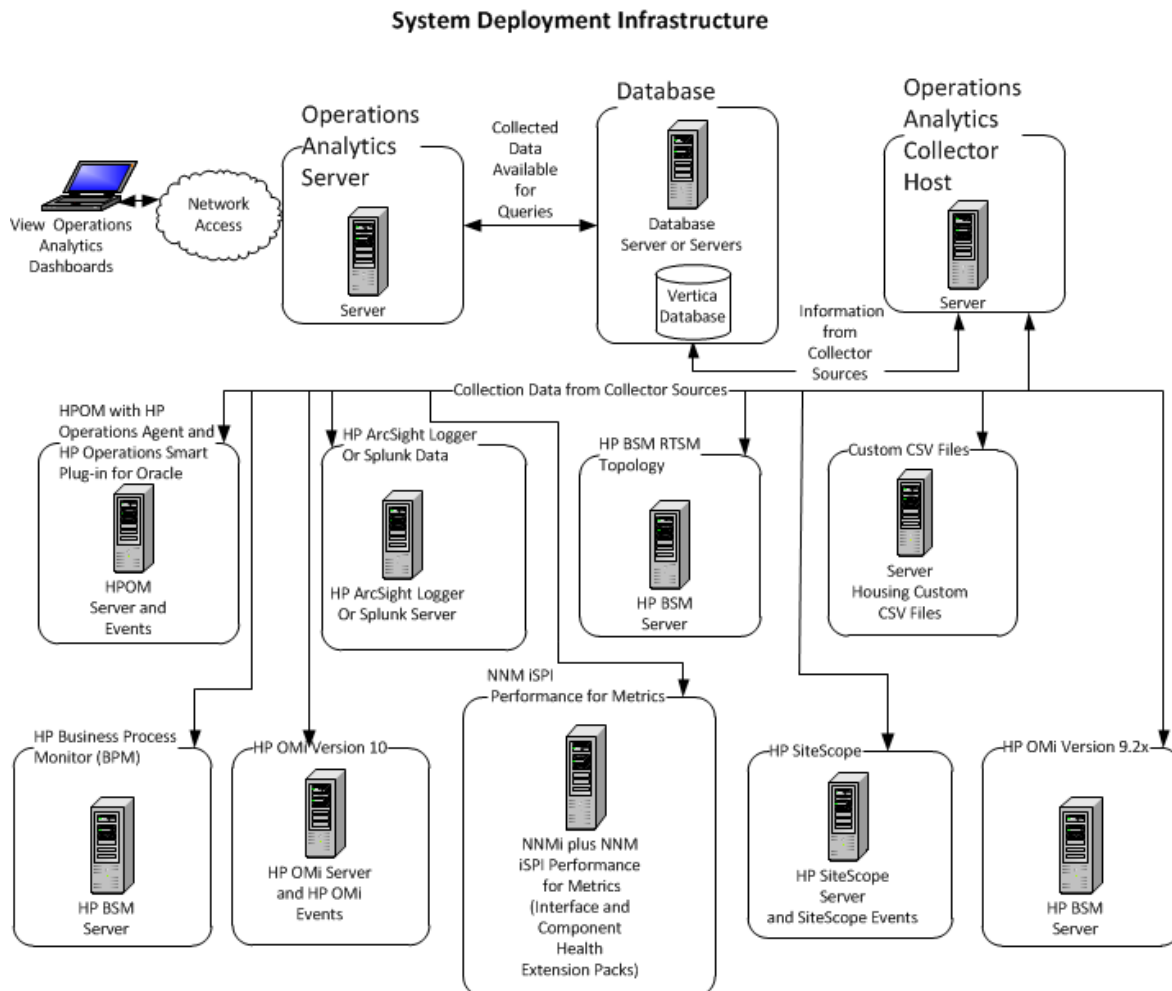
Table 2: Other Useful Directories

Folder Name	Path	Operations Analytics Server Appliance or Collector Appliance
JBOSS Home Directory	/opt/HP/opsa/jboss	Server Appliance
JDK Folder	/opt/HP/opsa/jdk	Server and Collector Appliances
scripts Folder	/opt/HP/opsa/scripts	Server and Collector Appliances
conf Folder	/opt/HP/opsa/conf	Server and Collector Appliances
data Folder	/opt/HP/opsa/data	Server and Collector Appliances
log Folder	/opt/HP/opsa/log	Server and Collector Appliances
lib Folder	/opt/HP/opsa/lib	Server and Collector Appliances
bin Folder	/opt/HP/opsa/bin	Server and Collector Appliances
upgrade Folder	/opt/HP/opsa/upgrade	Server and Collector Appliances
Vertica Database Installation Folder	/opt/vertica	Server and Collector Appliances have the Vertica client installed in this folder

Chapter 3: Upgrade Infrastructure and Specifications

The Operations Analytics Server Appliances and Collector Appliances are distributed as shown in the following diagram.

Note: The following diagram shows a single Operations Analytics Server Appliance and Collector Appliance in a distributed configuration. You can upgrade Operations Analytics configurations that use more than one Operations Analytics Server Appliance or Collector Appliance.



This document supports the configurations and actions shown in this section when upgrading to Operations Analytics 2.31.

Note: See the *Operations Analytics Support Matrix* for the hardware and operating system requirements for Operations Analytics.

The following upgrade instructions support a distributed system deployment of Operations Analytics:

- You must upgrade all Operations Analytics appliances.
- These instructions do not support upgrading the Operations Analytics All-in-One Appliance.
- Do not upgrade your Logger servers during this upgrade. The Vertica servers will be upgraded as part of the procedure later in this guide.
- Do not connect an Operations Analytics Server or Collector Appliance running version 2.20 after you complete this upgrade.

Consider the following when planning your upgrade:

- The upgrade supports upgrading all tenants.
- The upgrade **does not support** using a staging process.

Note: Staging is a way to upgrade so that you can compare the behavior of Operations Analytics 2.20 to Operations Analytics 2.31 in parallel. Although a staging approach is not supported, the idea would be to run both systems in staging until you are satisfied with the results. Again, a staging process is not currently supported.

- The upgrade supports Operations Analytics 2.20 data structure changes to incorporate any new data definitions for Operations Analytics 2.31.
- The upgrade retains Operations Analytics data and configuration, including custom CSV data collection and configuration information.
- The upgrade comprises both manual and automated steps.
- The upgrade can result in up to two hours of missing data collections and downtime.

Chapter 4: Vertica Upgrade

In order to use Operations Analytics 2.31, you must upgrade Vertica to version 7.1.1. This procedure provides a high level workflow for how to upgrade Vertica 6.1.3 to 7.1.1. For more details, see the Vertica documentation.

Note: During the Vertica upgrade, Operations Analytics will be temporarily unavailable, but no data loss is expected.

This should be done in two steps. Use Vertica documentation to follow the upgrade procedure.

1. Locate the Vertica upgrade RPM's in the **HP_OpsA_2.31_Vertica_Integration.zip**.

- The Vertica 7.0.2 RPM's are located in the **vertica_upgrade** directory in the zip file.
- The Vertica 7.1.1 RPM's are located in the **vertica** directory in the zip file.

2. Upgrade Vertica from 6.1.3 to 7.0.2

Use the vertica documentation http://my.vertica.com/docs/7.0.x/PDF/HP_Vertica_7.0.x_Install_Guide.pdf

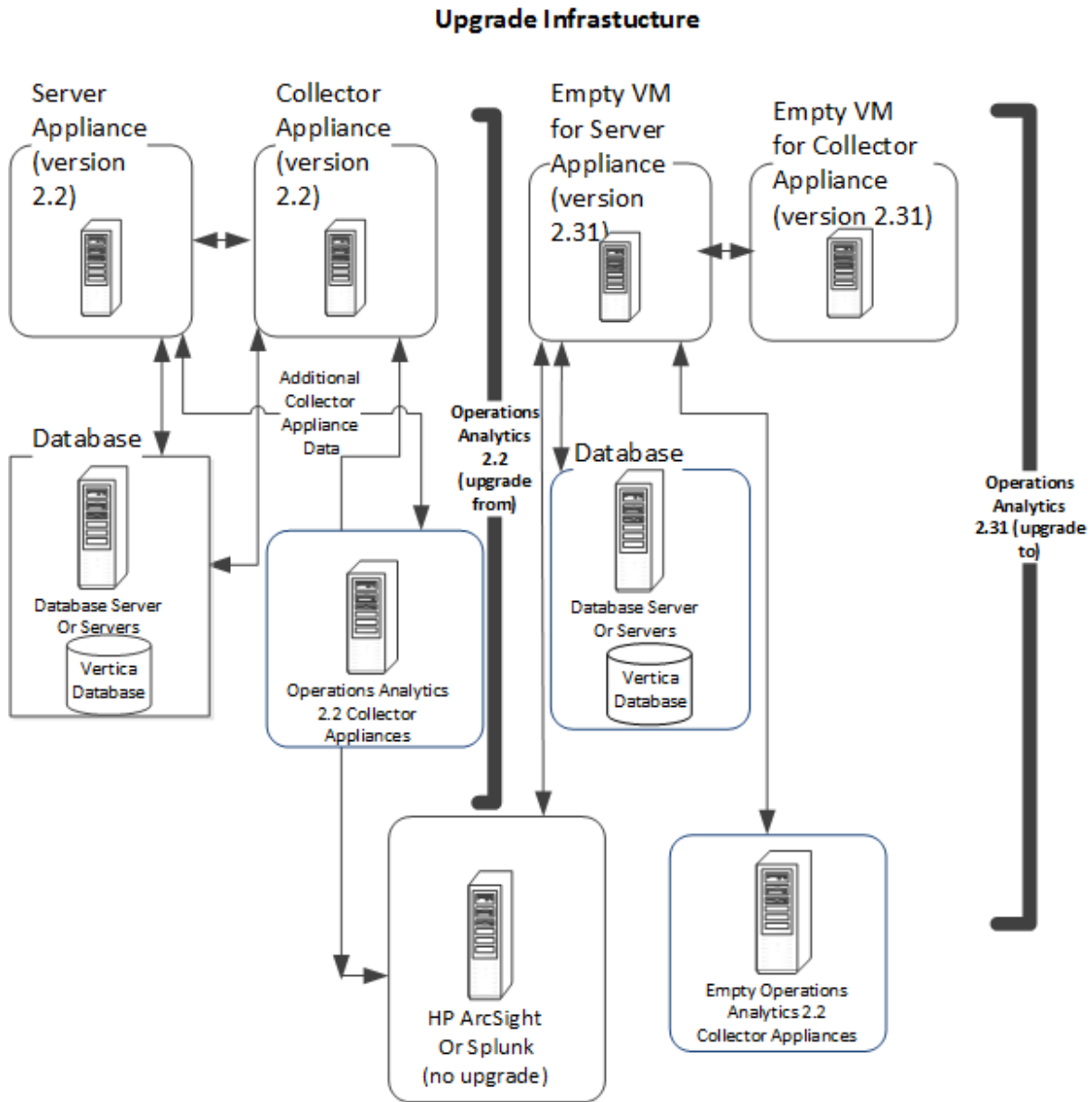
3. Verify that Operations Analytics 2.20 is working properly with Vertica 7.0.2. This can be verified by logging in to Operations Analytics and looking for data that has come in after the upgrade.
4. Upgrade Vertica from 7.0.2 to 7.1.1

Use the vertica documentation <https://my.vertica.com/docs/7.1.x/HTML/Content/Authoring/InstallationGuide/InstallingVertica/UpgradingHPVerticaToANewVersion.htm>

5. Verify that Operations Analytics 2.20 is working properly with Vertica 7.1.1. This can be verified by logging in to Operations Analytics and looking for data that has come in after the upgrade.
6. Give Vertica and Operations Analytics at least two hours to upload buffered data that has built up during the upgrade process before continuing with the Operations Analytics upgrade.

Chapter 5: Upgrade Steps

Complete the following steps to upgrade from Operations Analytics 2.20 to Operations Analytics 2.31. Use the following diagram while completing these steps.



Note: The instructions in this section cite reference pages and Linux manpages. These reference pages and manpages show details of how to use the Operations Analytics command line tools. To view reference pages or Linux manpages, do one of the following:

- **Reference Pages:** From the upper right side of the Operations Analytics console, click ? > **Reference Pages** to view a list of reference pages.
- **Manpages:** From a command prompt, enter `man <command line name>` to see the manpage for a command.

1. We recommend backing up the Vertica database used by Operations Analytics 2.20 before starting the upgrade.
2. Prepare the new machines for the Operations Analytics Server Appliance and Collector Appliances and install the new Operations Analytics 2.31 Server and Collector Appliances.

Note: You must manually make any changes done to the operating system parameters for Operations Analytics 2.20 servers to the machines you plan to use for Operations Analytics 2.31. These operating system parameter changes are not updated automatically by the upgrade process.

3. Delete the contents of the `/opt/HP/opsa/upgrade` directory on the Operations Analytics 2.20 Server Appliance.
4. Copy the contents of the `/opt/HP/opsa/upgrade` directory from the 2.31 server appliance to the same directory on the 2.20 server appliance.
5. Copy the contents of the `/opt/HP/opsa/conf/splunk` directory from the 2.20 server appliance to the same directory on the 2.31 server appliance.
6. From the Operations Analytics 2.20 Server Appliance, run the `chmod 777` command on the `/opt/HP/opsa/upgrade` folder and the files it contains.
7. Using a text editor, edit the `/opt/HP/opsa/upgrade/host_map.properties` file on the Operations Analytics 2.20 Server Appliance, listing all of the servers you must upgrade. Use the following lines as a guide to enter content into this file:

```
server_1_ip_old=10.60.164.34
server_1_hostname_old=hostname1.<domain>
collector_1_ip_old=10.60.188.108
collector_1_hostname_old=hostname2.<domain>
server_1_ip_new=10.60.164.195
server_1_hostname_new=hostname3.<domain>
collector_1_ip_new=10.60.164.196
collector_1_hostname_new=hostname4.<domain>
```

Note: Make sure all host names are in lower case letters.

8. If you have a BPM collection, perform the following procedure.
 - a. Log in to the Operations Analytics server as the **opsa** user.
 - b. Switch to the root user and change the root user password.
 - c. Open the file **/etc/ssh/sshd_config** for editing using the following command:

```
vi /etc/ssh/sshd_config
```
 - d. Locate the line with the text **PermitRootLogin no** and add a **"#"** symbol at the beginning of the line as follows:

```
# PermitRootLogin no
```
 - e. Restart the sshd service by running the following command:

```
/etc/init.d/sshd restart
```
 - f. Copy the line for the BPM host from the **/etc/hosts** file from each Operations Analytics 2.20 Collector Appliance to the **/etc/hosts** file on each corresponding Operations Analytics 2.31 Collector Appliance using the following format: `10.1.2.3 server.location.domain.com`.
9. **Important:** Run the following command from the Operations Analytics Appliance Server to create rollback backup tables for the Operations Analytics 2.20 database (in case you need to roll back to the original Operations Analytics 2.20 configuration). This command also records the upgrade start time.

Note: If you are upgrading with multiple servers, run this command from **only one** of the Operations Analytics Server Appliances.

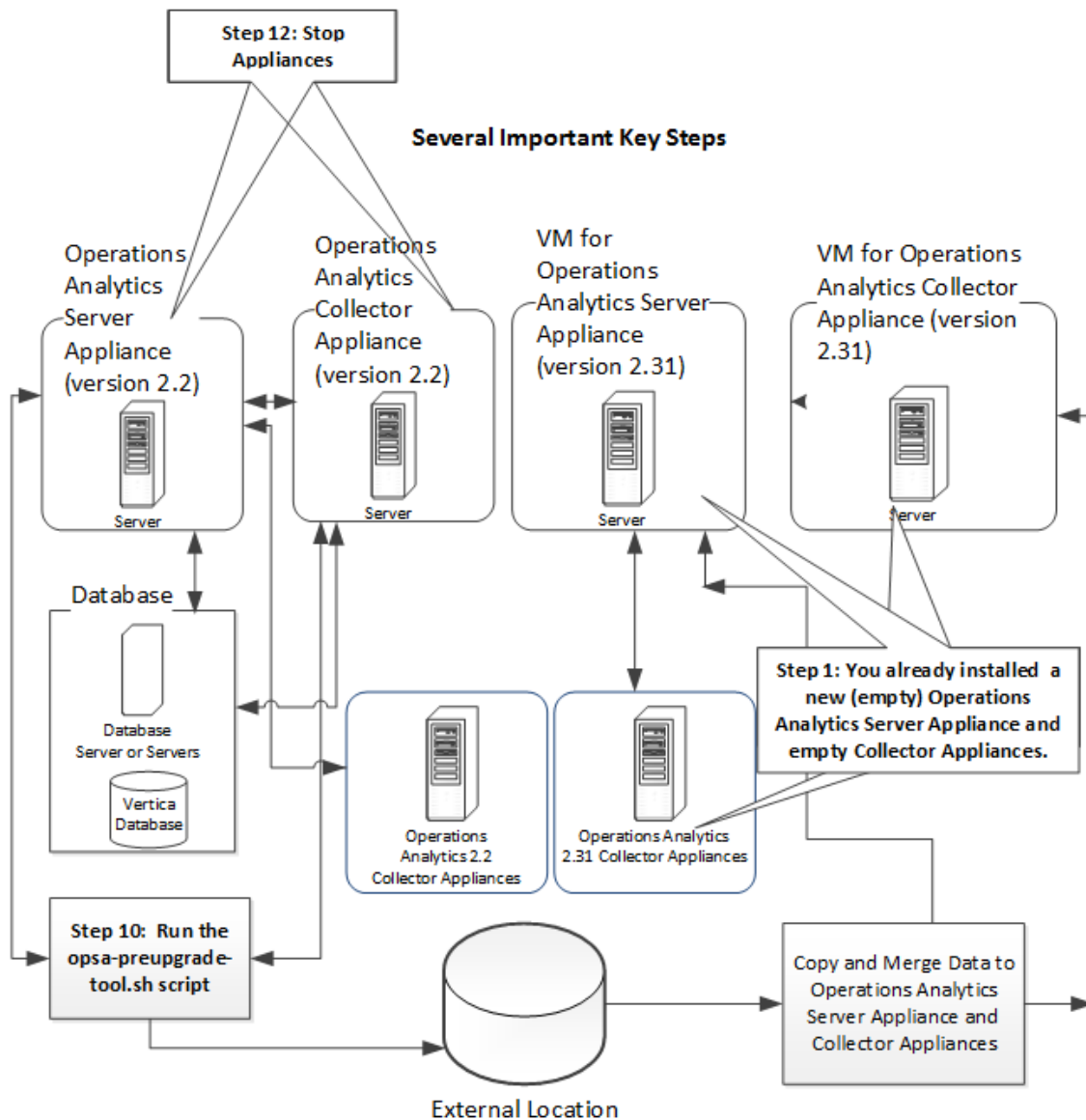
```
/opt/HP/opsa/upgrade/opsa-server-rollback.sh
```

- a. The `opsa-server-rollback.sh` script prompts you for the Vertica dbadmin user password which was dbadmin during the initial Vertica installation.
- b. When prompted with the next question, answer **yes**.

See the `opsa-server-rollback.sh` reference page (or the Linux manpage) for more information.

Note: You must not make configuration changes to Operations Analytics after completing this step.

Complete the following steps to continue upgrading to Operations Analytics 2.31. Use the following diagram while completing these steps.



10. From the Operations Analytics 2.20 Server Appliance, run the following command to collect the information you need to complete this upgrade. See the *opsa-preupgrade-tool.sh* reference page (or the Linux manpage) for more information.
 - a. As the *opsa* user, run the *opsa-preupgrade-tool.sh* script on the Operations Analytics 2.20 Server Appliance. Use the following syntax: `/opt/HP/opsa/upgrade/opsa-preupgrade-tool.sh server X`, where *server X* matches the appropriate server number shown in the *host_map.properties* file or 1 when you are not upgrading with multiple servers.
 - b. You will see a message similar to the following:

```
Wed Feb 26 14:00:17 UTC 2014 OPSA_HOME is set to /opt/HP/opsa
Wed Feb 26 14:00:17 UTC 2014
```

```
Wed Feb 26 14:00:17 UTC 2014 ---- opsa-server preupgrade tool validation ---  
--  
Wed Feb 26 14:00:17 UTC 2014  
Wed Feb 26 14:00:17 UTC 2014 server_1_ip_old 10.60.164.44 is valid  
Wed Feb 26 14:00:17 UTC 2014 server_1_ip_new 10.60.164.101 is valid  
Wed Feb 26 14:00:17 UTC 2014 collector_1_ip_old 10.60.164.82 is valid  
Wed Feb 26 14:00:17 UTC 2014 collector_1_ip_new 10.60.164.107 is valid  
Wed Feb 26 14:00:17 UTC 2014 server_1_hostname_old host1.thislab.ad is not  
accessible  
Wed Feb 26 14:00:17 UTC 2014 server_1_hostname_new host2.thislab.ad is not  
accessible  
Wed Feb 26 14:00:17 UTC 2014 collector_1_hostname_old host3.thislab.ad.ad is  
not accessible  
Wed Feb 26 14:00:17 UTC 2014 collector_1_hostname_new host4.thislab.ad.ad is  
not accessible  
Wed Feb 26 14:00:17 UTC 2014 server_2_ip_old 10.60.164.94 is valid  
Wed Feb 26 14:00:17 UTC 2014 collector_2_ip_old 10.60.164.78 is valid  
Wed Feb 26 14:00:17 UTC 2014 collector_2_ip_new 10.60.164.109 is valid  
Wed Feb 26 14:00:17 UTC 2014 server_2_hostname_old host1.thislab.ad.ad is  
not accessible  
Wed Feb 26 14:00:17 UTC 2014 collector_2_hostname_old  
ACEVM139201827.devlab.ad is not accessible  
Wed Feb 26 14:00:17 UTC 2014 collector_2_hostname_new  
ACEVM139333687.devlab.ad is valid  
Wed Feb 26 14:00:17 UTC 2014  
Wed Feb 26 14:00:17 UTC 2014 Some servers in host_map.properties are not  
accessible  
Wed Feb 26 14:00:17 UTC 2014 The accessibility is not mandatory for the  
upgrade process but please verify the file has the correct details before  
continuing  
You may stop now and rerun the script. Do you wish to continue now?
```

- c. Examine the host list from the previous step and verify that the list of IP addresses and host names are accurate, and that those IP addresses and host names that are not accessible are intentionally configured that way. Select **yes** after you are confident that the list is accurate, and you will be asked to enter the opsa user password for the Linux file system.

Note: Correct any problems you find when reviewing the host list from the previous step, then rerun the `/opt/HP/opsa/upgrade/opsa-preupgrade-tool.sh server 1` command before continuing with the upgrade.

- d. After the `opsa-preupgrade-tool.sh` script finishes, you should see the following message:

```
preupgrade_<IP Address>.tar.gz 100% 108KB 107.6KB/s 00:00  
host_map.properties 100% 110 0.1KB/s 00:00  
opsa-server preupgrade tool end
```

See the *opsa-preupgrade-tool.sh* reference page (or the Linux manpage) for more information.

11. Verify that the following files exist on the Operations Analytics 2.31 Server Appliance:

- `/opt/HP/opsa/upgrade/preupgrade<2.20 servername>.tar.gz`
- `/opt/HP/opsa/upgrade/host_map.properties`
- `/opt/HP/opsa/upgrade/OpsaVersion.prp`

Note: If these files do not exist, manually copy them from the Operations Analytics 2.20 Server Appliance. The first two files can be found in the same location in every version, but the `OpsaVersion.prp` file was located in the `/opt/HP/opsa/` directory before version 2.31.

12. Stop the Operations Analytics 2.20 Server Appliance and Collector Appliances:

a. Log in to the 2.20 server appliance as the root user and run the following command:

```
/opt/HP/opsa/bin/opsa stop
```

b. Log in to the 2.20 collector appliance as the root user and run the following command:

```
/opt/HP/opsa/bin/opsa stop
```

Note: After completing this step, Operations Analytics is no longer collecting information.

13. As the `opsa` user, run the following command from each of the Operations Analytics 2.31 Server Appliances and follow the interactive instructions:

```
/opt/HP/opsa/bin/opsa-server-postinstall.sh -upgrade
```

- When the script asks you to enter the database details, use the default entries from the script.
- When the script asks for the database password, enter the password for the Vertica `dbadmin` user.
- When the script asks whether the database schema exists, enter **yes**.
- After the command finishes, you should see a message similar to the following:

```
2014-02-09 15:00:39,990 [main] (PostInstallConfiguration.java:218) INFO -  
Post installation configuration completed successfully
```

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

14. For every custom CSV collection you defined in Operations Analytics 2.20, you must repeat the following steps on each Operations Analytics 2.31 Collector Appliance:

- a. Create the following directory on each Operations Analytics 2.31 Collector Appliance:
`/opt/HP/opsa/data/<mySourceDirectory>`
- b. Run the following command from each Operations Analytics 2.31 Collector Appliance to set the correct file ownership:
`chown opsa /opt/HP/opsa/data/<mySourceDirectory>`

15. As the opsa user, run the following command from each of the Operations Analytics 2.31 Collector Appliances: `/opt/HP/opsa/bin/opsa-collector-postinstall.sh`

Note: The script asks you to type the Vertica hostname and to enter the dbadmin password. Enter no when asked if you want to configure an OpsA Flex connector for Arcsight Logger.

Note: After the command finishes, you should see a message similar to the following:
2014-02-09 15:06:25,880 [main] (CollectorPostInstallConfiguration.java:115) INFO -Post installation configuration completed successfully

See the *opsa-collector-postinstall.sh* reference page (or the Linux manpage) for more information.

16. On the Operations Analytics Collector Appliance, restart the collector by running the following command:

```
opsa-collector restart
```

17. If your original 2.20 environment was using user authentication, and you would like to configure it in the new 2.31 environment as well, perform the procedures specified in *Configuring User Authentication using Public Key Infrastructure (PKI) to Access Operations Analytics* in the *Operations Analytics Configuration Guide* before continuing with the upgrade steps.
18. As the opsa user, run the following command from each of the Operations Analytics 2.31 Server Appliances:

```
/opt/HP/opsa/upgrade/opsa-server-postupgrade.sh
```

Note: The command in this step can take up to 90 minutes to complete, depending on the complexity of the Operations Analytics configuration.

After the command in this step finishes, you should see a message similar to the following:

```
2014-02-09 15:57:14,961 [main] (PostUpgradeConfiguration.java:81) INFO - Post upgrade configuration completed successfully
```

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

19. Restart the Operations Analytics servers as follows:

- a. Log in to the Operations Analytics 2.31 Server Appliance as the root user and run the following command:

```
/opt/HP/opsa/bin/opsa restart
```

- b. Log in to the Operations Analytics 2.31 Collector Appliance as the root user and run the following command:

```
/opt/HP/opsa/bin/opsa restart
```

20. If you are migrating Operations Analytics Collector Appliances that connect to NNMi for collecting NNMi custom poller data, do the following on the Operations Analytics 2.31 Collector Appliance similar to how you did this on the Operations Analytics 2.20 Collector Appliance:

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/nm_netperf_mib_collection.xml
```

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

If you want to use a different directory than `/opt/HP/opsa/data/nnm`, do the following: 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 default process directory is `/opt/HP/opsa/data/nnm_processed`.

21. If you are migrating Operations Analytics Collector Appliances that connect to NNMi for NNM ISPI Performance for Metrics Component Health data, do the following on the Operations Analytics 2.31 Collector Appliance similar to how you did this on the Operations Analytics 2.20 Collector Appliance:

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.

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 default process directory is `/opt/HP/opsa/data/netcomponent_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:

Note: Only complete steps a through c if you made a change to NNMi.

- 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/nm 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.
22. If you are migrating Operations Analytics Collector Appliances that connect to NNMi for collecting NNM ISPi Performance for Metrics Interface Health data, do the following on the Operations Analytics 2.31 Collector Appliance similar to how you did this on the Operations Analytics 2.20 Collector Appliance::

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.

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 default process directory is `/opt/HP/opsa/data/netinterface_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:

Note: Only complete steps a through c if you made a change to NNMI.

- 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.
23. Check that the Operations Analytics Collector Appliances are connected, and that new data is appearing in the Operations Analytics console.
 - a. Run the following command from the Operations Analytics Server Appliance to check the status of the collector sources configured on an Operations Analytics Collector Appliance:

```
$OPSA_HOME/bin/opsa-collection-config.sh -list -collectorhost <collector
hostname> -username <Tenant Admin User>
```
 - b. Check the dashboards for your collections to make sure they are collecting data.
 24. Verify that SiteScope data is coming in to Operations Analytics from all SiteScope sources. If this is not happening, try unregistering and reregistering the SiteScope collection.

25. Restart all processes on the 2.31 Operations Analytics Server and Collector hosts.
26. If you would like to configure user authentication on the 2.31 environment **and your original 2.20 environment was not using user authentication**, see *Configuring User Authentication using Public Key Infrastructure (PKI) to Access Operations Analytics* in the *Operations Analytics Configuration Guide*.
27. If you had TCP/CEF forwarding enabled in Logger before the upgrade, configure the Logger forwarder to point to the new Operations Analytics Collector host.

Caution: Do not connect an Operations Analytics Collector Appliance running version 2.20 after you complete this upgrade.

Chapter 6: Roll Back Due to Errors

If errors occur during the upgrade steps or if Operations Analytics 2.31 is running (following the upgrade) and you suspect errors that originated from the upgrade, you might need to roll back your system.

Note: The steps in this section return your Operations Analytics 2.20 system back to the state it was in before the upgrade. These steps will not remove or restore any of the tenant schemas that were removed from or created on the new system.

To roll back your system to the previous state, do the following:

1. Stop the Operations Analytics 2.31 Server Appliance and Collector Appliances:
 - a. Log in to the 2.31 server appliance as the root user and run the following command:

```
opsa stop
```
 - b. Log in to the 2.31 collector appliance as the root user and run the following command:

```
opsa stop
```
2. Run the following command from the Operations Analytics 2.31 Server Appliance:

```
/opt/HP/opsa/upgrade/opsa-rollback-tool.sh server 1
```

 - a. Verify that the IP addresses and names are correct.
 - b. Enter **yes** after you see a message similar to the following:

```
<timestamp> The accessibility is not mandatory for the rollback process but please verify the file has the correct details before continuing. You may stop now and rerun the script. Do you wish to continue now?
```
 - c. Enter **yes** when asked if you are sure you want to continue connecting.
 - d. Enter the opsa password for the Operations Analytics 2.20 Server Appliance.
 - e. If the copy to the Operations Analytics 2.20 Server Appliance fails, copy the `prerollback*.tar.gz` file to `/opt/HP/opsa/upgrade/` on the Operations Analytics 2.20 Server Appliance.
 - f. Repeat these steps for all of the Operations Analytics 2.31 Server Appliances.
3. Run the following command from the Operations Analytics 2.20 Server Appliance:

```
/opt/HP/opsa/upgrade/opsa-server-rollback.sh
```

- a. Enter the Vertica administrator password.
 - b. Enter **no** after you see a message similar to the following: Do you want to perform metadata backup before upgrade [yes/[no]]:
 - c. Enter **yes** after you see a message similar to the following: Do you want to rollback the upgrade [yes/[no]]:
 - d. Repeat these steps for all of the Operations Analytics 2.20 Server Appliances.
4. Run the appropriate commands on all of the Operations Analytics 2.20 Server and Collector Appliances:
 - Log in to the 2.20 server appliance as the root user and run the following command:

```
opsa start
```
 - Log in to the 2.20 collector appliance as the root user and run the following command:

```
opsa start
```
 5. The rollback should complete within five minutes.

Chapter 7: Support Considerations

This chapter contains information about special cases you might consider during your upgrade.

Preserving Operations Analytics Log Files

You might decide to preserve the Operations Analytics 2.20 log files during your upgrade. To do so, complete the following steps on each of the Operations Analytics 2.20 Server and Collector appliances:

1. Run the `/opt/HP/opsa/upgrade/opsa-logcopy-tool.sh` script on the target server.

Note: The `opsa-logcopy-tool.sh` script creates the `logfiles_<current date time>.tar.gz` in the `/opt/HP/opsa/upgrade` folder.

2. Manually copy the `logfiles_<current date time>.tar.gz` file to a folder of your choice for support purposes.

See the `opsa-logcopy-tool.sh` reference page (or the Linux manpage) for more information.

Send Documentation Feedback

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

Feedback on Operations Analytics 2.20 to 2.31 Upgrade Guide (Operations Analytics 2.31)

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@hp.com.

We appreciate your feedback!