

HP Operations Analytics

Software Version: 2.20

Operations Analytics Quick Start Guide

Document Release Date: February 2015
Software Release Date: December 2014



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 2013 - 2014 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 Solutions & Integrations and Best Practices

Visit HP Software Solutions Now at <https://h20230.www2.hp.com/sc/solutions/index.jsp> 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://hpln.hp.com/group/best-practices-hpsw> to access a wide variety of best practice documents and materials.

Contents

Chapter 1: Operations Analytics System Requirements	4
Known Issues and Workarounds	4
Chapter 2: Installing and Configuring Operations Analytics	5
Task 1: Installing and Configuring the Vertica Software	5
Task 2: Installing and Configuring HP ArcSight Logger	9
Prerequisites for Installation	10
Using the Console Mode to Install HP ArcSight Logger	10
Configuration Steps: Connecting to HP ArcSight Logger for the First Time	12
Task 3: Installing the Operations Analytics Server Appliance using the VMware vSphere Client	13
Task 4: Installing the Operations Analytics Collector Appliance using the VMware vSphere Client	14
Post-Installation Configuration Steps for Operations Analytics	16
Post-Installation Steps for the Operations Analytics Server Appliance	16
Prerequisite: Setting up the Vertica Database	17
Running the Post-Installation Script	17
Post-Installation Steps for the Operations Analytics Collector Appliance	20
Accessing Operations Analytics for the First Time	21
Task 6: Gathering Collection Information	22
Task 7: Configuring Collections	24
Configuring Log Analytics for Logger	27
Configuring Log Analytics for Splunk	33
Chapter 3: Using Operations Analytics	35
Getting Started	35
More Information	35
Send Documentation Feedback	37

Chapter 1: Operations Analytics System Requirements

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

Note: Any command examples shown in this document as being run by an `opsa` user can also be run by a root user.

Note: `$OPSA_HOME` is set to `/opt/HP/opsa` in the OpsA Server Appliance

Known Issues and Workarounds

Browsers: OpsA does not support Internet Explorer 10. Use Internet Explorer 9, Google Chrome, or Firefox 31 ESR.

Vertica: OpsA includes `vertica-6.1.3-12.x86_64.RHEL5.rpm` for the Vertica installation and `vertica-R-lang-6.1.3-12.x86_64.RHEL5.rpm` for the R Language Pack from Vertica. Use these packages for optimum Vertica performance.

Operations Analytics Log File Connector for Arcsight Logger Installation: During post installation steps for both the OpsA Server and Collector appliances, OpsA provides an option for you to install the Operations Analytics Log File Connector for Arcsight Logger (also known as the Flex Connector). If you choose to install this connector, OpsA might print a message that includes something similar to the following: `INFO - touch: cannot touch `/var/lock/subsys/arc_sdkmultifolderreader': Permission denied`. You can safely ignore this message, as the Operations Analytics Log File Connector for Arcsight Logger installation ignores this issue and installs correctly.

Note: Any time you use the `opsa-server-postinstall.sh` or `opsa-collector-postinstall.sh` scripts to install the Operations Analytics Log File Connector for Arcsight Logger, you might see the issue just described. You can safely ignore this message, as the Operations Analytics Log File Connector for Arcsight Logger installation ignores this issue and installs correctly.

Chapter 2: Installing and Configuring Operations Analytics

Operations Analytics (OpsA) is a unique platform for both simple and complex IT operational problem-solving. Use OpsA to access, combine, and compare the metric, topology, event, and log file data that your OpsA administrator configures to be collected from diverse sources in your IT environment. Because this data is collected from multiple domains, Operations Analytics enables you to identify answers to problems that are not easily solved using other methods. See the *Operations Analytics Help* for more information.

Read this guide to understand the concepts required to install, configure, and use OpsA most effectively, including helpful tips and how to set up collections after installation.

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

This chapter guides you through the process of installing and configuring OpsA. For more detailed information about installing OpsA, see the *Operations Analytics Installation and Configuration Guide*.

There are seven main categories for the installation tasks you need to complete:

1. ["Task 1: Installing and Configuring the Vertica Software" below](#)
2. ["Task 2: Installing and Configuring HP ArcSight Logger" on page 9](#)
3. ["Task 3: Installing the Operations Analytics Server Appliance using the VMware vSphere Client" on page 13](#)
4. ["Task 4: Installing the Operations Analytics Collector Appliance using the VMware vSphere Client" on page 14](#)
5. ["Post-Installation Configuration Steps for Operations Analytics" on page 16](#)
6. ["Task 6: Gathering Collection Information" on page 22](#)
7. ["Task 7: Configuring Collections" on page 24](#)

Task 1: Installing and Configuring the Vertica Software



To install Vertica as a multiple node cluster with OpsA-related extensions, do the following:

1. Download the `Documentation_OSRB_Third_parties_A7X14-88005.zip` file and copy the following compressed Vertica installation file from the `installations` folder to a temporary location: `opsa-vertica-<version>.tar.gz`
2. From the temporary location, extract the `opsa-vertica-<version>.tar.gz` file using the following command: `tar -zxvf opsa-vertica-<version>.tar.gz`

Note: This `opsa-vertica-<version>.tar.gz` file contains the necessary files to support setting up Vertica in a cluster mode as shown in the steps in this section.

3. Install Vertica as a cluster mode using the `vertica-R-lang-6.1.3-12.x86_64.RHEL5.rpm` file along with the other files extracted from the `opsa-vertica-<version>.tar.gz` file during the previous step. For full installation details see the Vertica Installation Guide at http://my.vertica.com/docs/7.1.x/HTML/index.htm#Authoring/InstallationGuide/Other/InstallationGuide.htm%3FTocPath%3DInstallation%20Guide%7C_____0.
4. Complete the remaining steps in this section for each one of the Vertica cluster nodes. Copy the following files from the `integrations` folder in the media to the `/home` directory:

- `GammaDistribution.R`
- `MASS_7.3-23.tar.gz`
- `libgfortran-4.1.2-52.el5_8.1.x86_64.rpm`
- `create_R_GammaDist.sh`
- `vertica-R-lang-6.1.3-12.x86_64.RHEL5.rpm`

Note: This file must contain the Vertica version in the file name. The Vertica version must be the same version as the Vertica that is installed.

5. Run the following command to create the link to the R-Vertica function: `ln -s /home/dbadmin/home_vertica`

Note: This command will not work without an Internet connection. Make sure you have an Internet connection before running this command.

6. Run the following command to set the correct folder permissions: `chmod 770 /home_vertica`
7. Run the following command from the `/home` directory to copy the `GammaDistribution.R` file to the `/home_vertica` directory:
`cp GammaDistribution.R /home_vertica`
8. Run the following command to install a group package to enable the MASS statistics Library to

compile:

```
yum groupinstall 'Development tools'
```

Note: This command will not work without an Internet connection. Make sure you have an Internet connection before running this command. The alternative approach is to download the R Language Pack using a computer that has an Internet connection and install it manually.

9. Run the following command to start the R Language Pack installation:

```
rpm -Uvh vertica-R-lang_VERSION.rpm
```

After the installation completes, the R Language Pack installation is done.
10. Verification: To verify the R Language Pack installation, do the following:
 - a. Run the following command:

```
rpm -qa | grep -i vertica-R
```
 - b. If you see a message similar to the following, the installation was successful:

```
vertica-R-lang-VERSION
```
11. Complete the following steps to install the MASS package:
 - a. Run the following command to set the correct permissions:

```
chmod 770 MASS_7.3-23.tar.gz
```
 - b. Copy the `/home/MASS_7.3-23.tar.gz` file to `/root/MASS_7.3-23.tar.gz`
 - c. Run the following command:

```
/opt/vertica/R/bin/R CMD INSTALL /root/MASS_7.3-23.tar.gz
```
12. Run the following command for each one of the Vertica cluster nodes to set the correct permissions:

```
chmod 777 /home/create_R_GammaDist.sh
```
13. Run the following command as the dbadmin user to create and start opsadb:

```
/opt/vertica/bin/adminTools -t create_db -d opsadb -p dbadmin --hosts=127.0.0.1
```
14. Run the following command to switch to the dbadmin user:

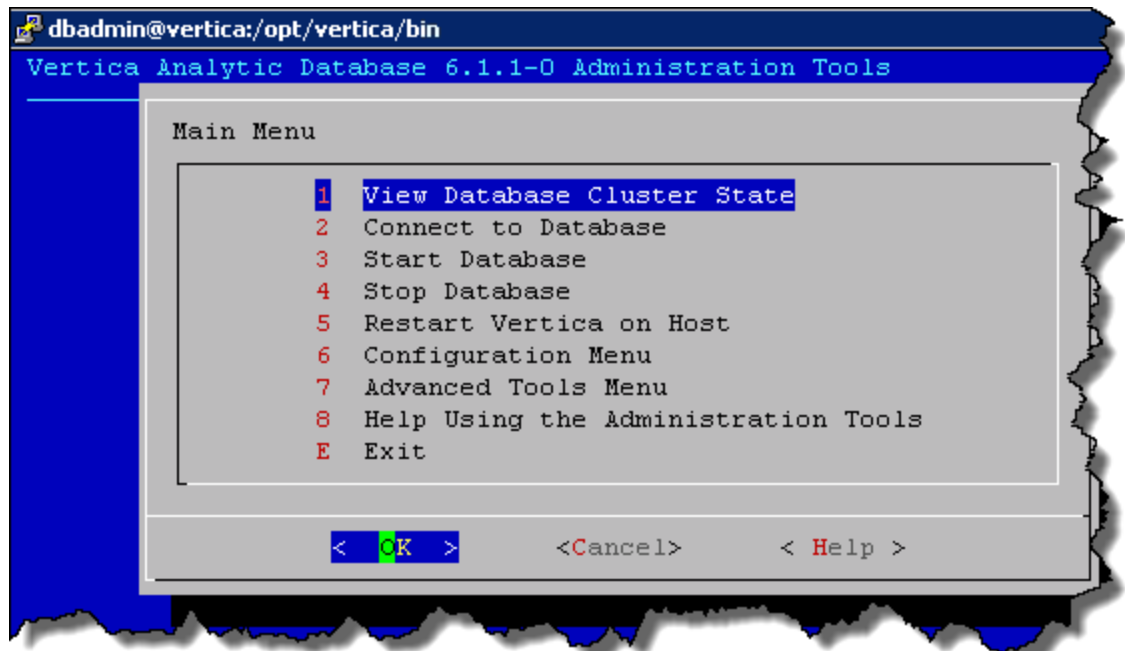
```
su - dbadmin
```
15. From the `/home` directory, run the following command:

```
./create_R_GammaDist.sh
```
16. The Vertica database admin user is `dbadmin`, and its default password is `dbadmin`. It is recommended that you change the default password now. Do the following to change the password:
 - a. Run the following command to log on to the `opsadb` database using the `vsq1` tool:

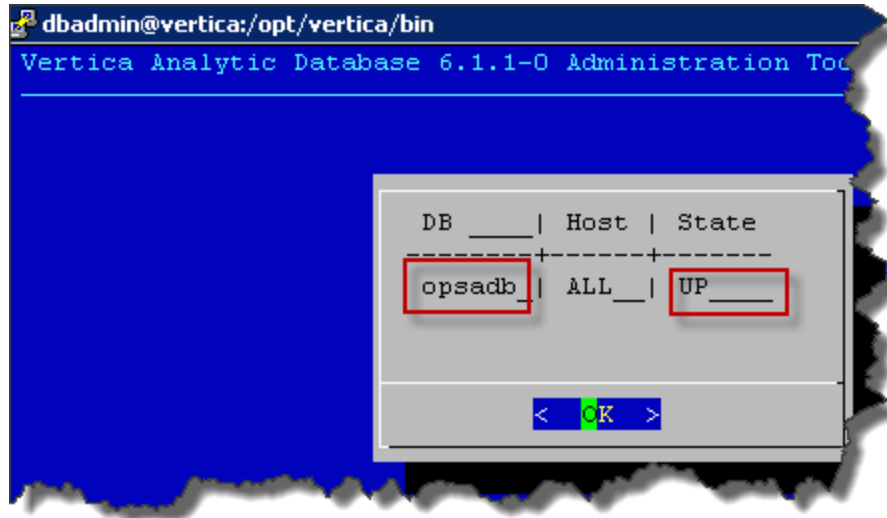
```
/opt/vertica/bin/vs1 -h hostname -p 5433 -U dbadmin -w dbadmin -d opsadb
```

Note: `opsadb` is the Vertica database created during the Vertica installation.

- b. Run the following command to change the password:
`alter user dbadmin identified by '<new password>';`
 - c. Enter `\q` to quit the `vsq` tool.
17. Do the following to check the database:
- a. Run the `su -dbadmin` command.
 - b. Run the `/opt/vertica/bin/adminTools` command. You should see a screen similar to the following:



- c. The opsadb database should have been created during the installation. Enter 1 to view the state of the database; then click **OK**. You should see a screen similar to the following if the opsadb database is running:



- d. Click **OK** twice to exit the adminTools interactive command.

Note: If you need to stop or restart the database, you can always do it from the first screen shown in this step. You can also (carefully) complete other administrative operations using this tool.

In Vertica, load balancing supports multiple client connections through a single Virtual IP (VIP) address that is shared among all nodes in a cluster. This is useful for balancing incoming client requests across nodes, as well as preventing node exclusion from clients in the case of node failure.

Task 2: Installing and Configuring HP ArcSight Logger



Review the HP *Operations Analytics Software Support Matrix* for the supported platforms and browsers for HP ArcSight Logger.

You can be logged in as a root user or a non-root user on the system on which you are installing the software. When you install the software as a root user, you can select the port on which HP ArcSight Logger listens for secure web connections. However, when you install it as a non-root user, HP ArcSight Logger can only listen for connections on port 9000. You cannot configure the port to a

different value. Additionally, you can configure HP ArcSight Logger to start as a service when you install as a root user.

Prerequisites for Installation

- You must have downloaded the HP ArcSight Logger installation package.
- You need a separate license file for each instance of HP ArcSight Logger. A license file is uniquely generated for each Enterprise version download.
- Make sure a non-root user account exists on the system on which you are installing HP ArcSight Logger. The non-root user must also be a non-system user with login permissions.
- Decide whether to install Logger while logged in as root or as a non-root user. Your installation options vary depending on which user you choose.
 - When you install as root, a non-root user account is still required.
 - When you install as root, you can choose to configure HP ArcSight Logger to start as a service and select the port on which HP ArcSight Logger listens for secure web connections.
 - When you install as a non-root user, HP ArcSight Logger can only listen for connections on port 9000. You cannot configure the port to a different value.
 - When upgrading, you cannot change the previous installation to a root-user installation. You will need to use the previously configured port 9000 for accessing HP ArcSight Logger software.
- The hostname of the server on which you are installing HP ArcSight Logger cannot be localhost. If it is, change the hostname before proceeding with the installation.
- You must not have an instance of MySQL installed on the Linux server on which you will install HP ArcSight Logger. If an instance of MySQL exists on that server, uninstall it before installing HP ArcSight Logger.
- If you want to use the GUI mode of installation and will be installing HP ArcSight Logger over an SSH connection, make sure that you have enabled X window forwarding using the `-X` option so that you can view the screens of the installation wizard. If you will be using PuTTY, you will also need an X client on the machine from which you are connecting to the Linux machine.
- Installation on 64-bit systems requires `glibc-2.12-1.25.el6.i686` and `nsssoftokn-freebl-3.12.9-3.el6.i686`. Install these packages if the installation fails with the following error message: `Installation requirements not met. Pre-install check failed: 32-bit compatibility libraries not found.`

Using the Console Mode to Install HP ArcSight Logger

Make sure the server on which you will be installing HP ArcSight Logger complies with the platform requirements listed in the Release Notes for your version, and that the prerequisites listed in ["Prerequisites for Installation"](#) are met.

You can install HP ArcSight Logger as a root user or as a non-root user. See "[Prerequisites for Installation](#)" for details and restrictions.

To install HP ArcSight Logger on a separate server from the Operations Analytics server, use the following instructions:

1. Run these commands from the directory where you copied the HP ArcSight Logger software:

```
chmod +x ArcSight-logger-5.5.0.XXXX.0.bin  
./ArcSight-logger-5.5.0.XXXX.0.bin -i console
```

2. The installation wizard launches in command-line mode, as shown below. Press **Enter** to continue.

```
InstallAnywhere will guide you through the installation of HP ArcSight Logger  
5.5.It is strongly recommended that you quit all programs before continuing  
with this installation.
```

```
Respond to each prompt to proceed to the next step in the installation. If you  
want to change something on a previous step, type 'back'.
```

```
You may cancel this installation at any time by typing 'quit'
```

```
PRESS <ENTER> TO CONTINUE:
```

3. The next screens display license information. Installation and use of HP ArcSight Logger 5.5 requires acceptance of the license agreement. Press Enter to display each part of the license agreement, until you reach the following prompt:

```
DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N):
```

4. Type Y and press Enter to accept the terms of the License Agreement.
5. Follow the prompts to complete the Logger installation.

Note: Use the information in this table to complete the Logger installation.

Field	Notes
Non-root user name	This user must already exist on the system.
HTTPS port	The port number to use when accessing the HP ArcSight Logger UI. You can keep the default HTTPS port (443) or enter any other port that suits your needs. If the port you specify is already in use, you will be asked to select a different port. If you specify any port except 443, users will need to enter that port number in the URL they use to access the HP ArcSight Logger UI.

Field	Notes
Configure HP ArcSight Logger as a service	Indicate whether to configure HP ArcSight Logger to run as a service. Select this option to create a service called arcsight_HP ArcSight Logger, and enable it to run at levels 2, 3, 4, and 5. If you do not enable HP ArcSight Logger to start as service during the installation process, you can still do so later. For instructions on how to enable HP ArcSight Logger to start as a service, see <i>System Settings</i> in the <i>ArcSight Logger Quick Start Guide</i> .

Configuration Steps: Connecting to HP ArcSight Logger for the First Time

The HP ArcSight Logger user interface is a web browser application using Secure Sockets Layer (SSL) encryption. Users must be authenticated with a name and password before they can use the interface.

To connect and log into Logger, do the following:

1. Use the following URL to connect to Logger through a supported browser:

`https://<hostname or IP address>:<configured_port>`

where the `hostname or IP address` is the system on which Logger is installed, and `configured_port` is the port specified during the Logger installation.

After you connect, the Log on screen is displayed.

2. Use the following default credentials if you are connecting for the first time or have not yet changed the default credentials:

Username: admin

Password: password

3. If you already have an account, enter your user name and password, then click **Login**.
4. After you have successfully logged in, go to the *Configuring Logger* section of the *HP ArcSight Logger Administrator's Guide* for information about how to set up Logger to start receiving events.

Note: You will need to configure HP ArcSight Logger to collect the log files in which you are interested. This includes setting up the Operations Analytics Log File Connector for HP ArcSight Logger. See the *Configuring Logger* section of the *HP ArcSight Logger Administrator's Guide* and the *Configuring the Operations Analytics Log File Connector for HP ArcSight Logger* section of the *Operations Analytics Configuration Guide* for more information.

Note: If there is an ArcSight connector available to collect the type of log file you must collect, use that connector. Only use the Operations Analytics Log File Connector for HP ArcSight Logger if an

existing ArcSight connector does not meet your needs.

Task 3: Installing the Operations Analytics Server Appliance using the VMware vSphere Client



To install and configure the Operations Analytics Server Appliance using the VMware vSphere Client, do the following:

1. Log on to the VMware vSphere Client.
2. Select **File** -> **Deploy OVF Template**.
3. Enter the URL or the file path of the HP_opsa_Server_OVF10.ova file, based on where the OVA file is located; then click **Next**.
4. Review the product summary; then click **Next**.
5. Review the licensing agreement; then click **Next**.
6. Specify a name and location for the deployed template.
7. Follow the instructions to select the host or cluster on which you want to deploy the Server Appliance; then click **Next**.
8. Select a resource pool.
9. Select the destination storage for the Server Appliance files; then click **Next**.
10. Select the format on which you want to store the virtual disks; then click **Next**.
11. Select a destination network; then click **Next**.
12. Enter the network properties by specifying the field values shown in the following table.

Note: If you are using VMware Vcenter 5.x for this installation, a User Interface appears to help you enter these values. If the User Interface does not appear, see the *User's Guide to Deploying vApps and Virtual Appliances*, available from http://www.vmware.com/support/developer/studio/studio26/va_user.pdf (page 17) for network configuration instructions.

Network Properties

Address Type	Field	Value
DHCP	All Fields	Leave all fields blank. Note: The Operations Analytics installation needs either static IP addresses or permanently-leased DHCP IP addresses.
Static	DNS	The fully-qualified domain name or IP address of the DNS Server.
	Default Gateway	The fully-qualified domain name or IP address of the network's default gateway.
	IP Address	The IP address of the server.
	Network Mask	The network mask for your network.

13. Specify the virtual appliance Host Name and Timezone settings; then click **Next**.
14. Click **Finish**.
15. Power on the virtual appliance.

Note: After you deploy the virtual appliance, you should upgrade the VMWare Tools for the appliance as described in the VMWare Upgrade Instructions. At this printing, you can obtain this document using the following link: <http://pubs.vmware.com/vsphere-50/index.jsp#com.vmware.vmtools.install.doc/GUID-08BB9465-D40A-4E16-9E15-8C016CC8166F.html>

Task 4: Installing the Operations Analytics Collector Appliance using the VMware vSphere Client



To install and configure the Operations Analytics Collector Appliance using the VMware vSphere Client, do the following:

1. Log on to the VMware vCenter server or directly to the VMWARE ESX server using the VMware vSphere Client.

2. Select **File -> Deploy OVF Template**.
3. Point your web browser to the following location: `http://<path to file>/HP_Neutron1_OVF10.ova`; then click **Next**.
4. Specify a name and location for the deployed template.
5. Select the host or cluster on which you want to deploy the Collector Appliance; then click **Next**.
6. Select a resource pool.
7. Select the destination storage for the Collector Appliance files; then click **Next**.
8. Select the format on which you want to store the collector's virtual disks; then click **Next**.
9. Select a destination network; then click **Next**.
10. Enter the network properties by specifying the field values shown in the following table.

Note: If you are using VMware Vcenter 5.x for this installation, a User Interface appears to help you enter these values.

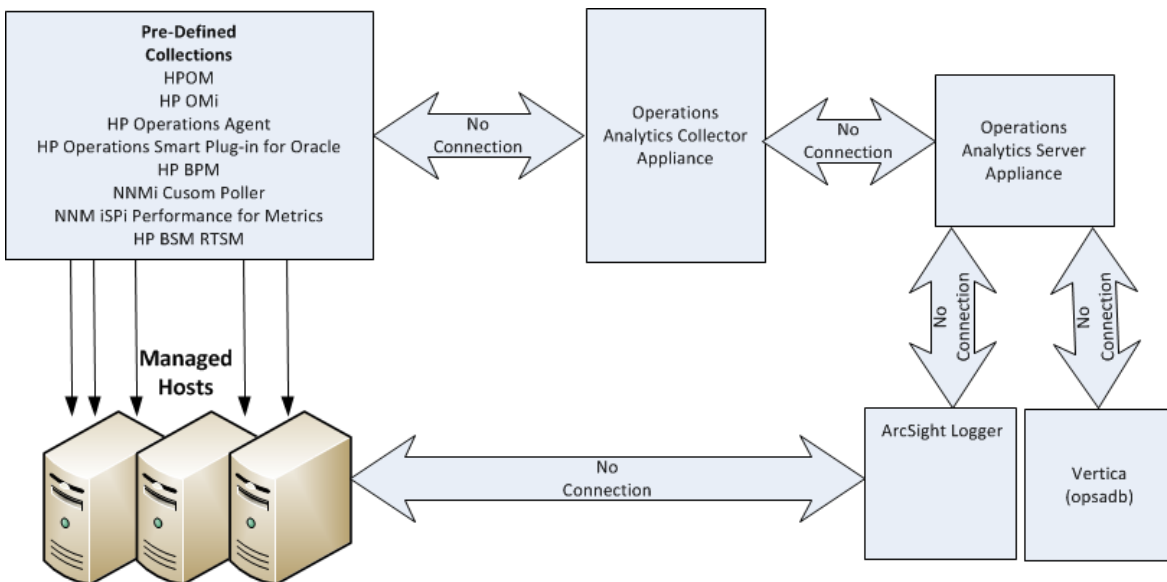
Network Properties

Address Type	Field	Value
DHCP	All Fields	Leave all fields blank. Note: The Operations Analytics installation needs either static IP addresses or permanently-leased DHCP IP addresses.
Static	DNS	The fully-qualified domain name or IP address of the DNS Server.
	Default Gateway	The fully-qualified domain name or IP address of the network's default gateway.
	IP Address	The IP address of the server.
	Network Mask	The network mask for your network.

11. Specify the VA Host Name and Timezone settings; then click **Next**.
12. Select the **Power on after deployment** option; then click **Finish**.

Post-Installation Configuration Steps for Operations Analytics

The post installation script (`opsa-server-postinstall.sh` script) completes the final configuration steps for the different application components used by Operations Analytics (OpsA). The `opsa-server-postinstall.sh` script configures communication among the distributed components of OpsA. The following diagram shows the missing communication connections that the `opsa-server-postinstall.sh` script will soon create.



To finish the post-installation configuration steps and configure the communication connections for OpsA, complete the actions in this section.

Post-Installation Steps for the Operations Analytics Server Appliance

Complete the following post-installation configuration steps on the OpsA Server Appliance.

Note: If you run the `opsa-server-postinstall.sh` script using an already configured Vertica database, the `opsa-server-postinstall.sh` script does not complete. It shows you a message explaining how to run the `opsa-server-postinstall.sh` script to remedy an already configured Vertica database.

Prerequisite: Setting up the Vertica Database

OpsA uses database schemas to organize the data for administration and by individual tenants. OpsA requires the creation of a database user that has access to the Vertica database. If this database user is a superuser, then the creation of the schemas and the setting of the `MaxClientSessions` configuration parameter (discussed below) happen without any further work (OpsA does the schema creation and the `MaxClientSessions` configuration parameter setting).

Note: This required database user does not have to be a superuser. However, if this created database user is not a superuser, then the Vertica database administrator must create database schemas before configuring the OpsA or any OpsA tenants.

Before running the `.sh` script, do one of the following:

- **Option 1:** Verify that the Vertica database administrator created a database user, superuser, that has access to the Vertica database. Continue with ["Running the Post-Installation Script" below](#).
- **Option 2:** If the Vertica database administrator did not create a database user, superuser, complete the following steps using the sql statements to create a database user (`<newusername>`), password (`<password>`), and the two schemas (`opsa_admin` and `opsa_default`), specifying user `<newusername>` as the owner of the schemas:
 - a. `create user <newusername> identified by '<password>';`
 - b. `create schema if not exists opsa_admin authorization <newusername>;`
 - c. `create schema if not exists opsa_default authorization <newusername>;`
 - d. `grant all on schema opsa_default to <newusername>;`
 - e. `grant all on schema opsa_admin to <newusername>;`
 - f. `grant usage on schema PUBLIC to <newusername>;`
 - g. `select SET_CONFIG_PARAMETER('MaxClientSessions', 200);`

Continue with ["Running the Post-Installation Script" below](#).

Running the Post-Installation Script

Complete the following post-installation configuration steps on the Server Appliance:

1. Log on as an `opsa` user to the OpsA server (the default password is `opsa`).

Note: Note: The first time you log on, you will need to change the default password.

2. Run the `$OPSA_HOME/bin/opsa-server-postinstall.sh` script (interactive mode).
3. The `opsa-server-postinstall.sh` script prompts for following information, and includes a default value surrounded by brackets. To accept the default value, click **Enter** for each prompt.

- Vertica database host name
- Vertica database port number
- Vertica database name
- Vertica database user name

Note: Note: Use either `dbadmin` or the `<newusername>` you created earlier.

- Vertica database password

Note: Note: The `opsa-server-postinstall.sh` script shows an error message if any of the following problems exist:

- Vertica is not installed on the specified host.
- Vertica is down.
- The port number you specified for Vertica is not open.
- You entered the wrong Vertica username or password.
- The default tenant name, `opsa_default`, does not exist.

Correct these problems and rerun the `opsa-server-postinstall.sh` script.

For Vertica administration issues, run the `/opt/vertica/bin/adminTools` command and view the cluster state. If the state is `down`, you might need to restart the database. See ["Task 1: Installing and Configuring the Vertica Software" on page 5](#) for more information.

4. The `opsa-server-postinstall.sh` script prompts you with the following message: Is the database created and running on host [yes/no]:
If the database is created and running, enter `yes`; If the database is not created and running, enter `no` to stop the post install configuration script.

Note: The `opsa-server-postinstall.sh` script assumes the `opsadb` database is available on the Vertica server and does not create the `opsadb` database on the Vertica server.

Note: If you already have the opsadb schema installed from a previous installation, you must delete it. The opsadb schema installed from a previous installation, you must delete it. The `opsa-server-postinstall.sh` script does not support connection to an existing database schema. You must drop the old opsadb database and create a new one before running the `opsa-server-postinstall.sh` script. See the *Vertica Enterprise Edition 6.1 Administrator's Guide* for more information

5. If this is the first time running the `opsa-server-postinstall.sh` script on this server, it prompts you to change the passwords for the opsadmin, opsatenantadmin, and opsa default application users. Follow the interactive instructions carefully to reset these passwords, and note the password values you set for later use.

Note: If you are running the `opsa-server-postinstall.sh` script to add additional servers, it does not require you to change these passwords.

Note: The passwords you set must contain at least 13 characters, both upper and lower case characters, and a digit character.

6. The `opsa-server-postinstall.sh` script prompts you to configure logger details for opsa_default [yes/[no].

Note: If you enter no, you can always use the `opsa-logger-config-manager.sh` script to configure HP ArcSight Logger at a later time.

7. The `opsa-server-postinstall.sh` script prompts you for the type of logger software you plan to use (ArcSight or Splunk).
8. The `opsa-server-postinstall.sh` script prompts you for following information, and includes a default value. To accept the default value, click **Enter** for each prompt.
 - Logger host name
 - Logger Webservice port
 - Logger Webservice username
 - Logger Webservice password

Note: These Logger details will be persisted to the database using the opsadb schema. If the log management software is arcsight, you can configure more than one Logger using the opsadb schema. The `opsa-server-postinstall.sh` script prompts you with the following message: Do you want to add more Logger configuration for 'opsadb' [yes/no]: If you enter yes, you can add one

more Logger configuration for the `opsa_default` schema and tenant.

If the log management software is `splunk` you can only add one set of Splunk configuration details. The `opsa-server-postinstall.sh` script does not prompt you for more than one set of Splunk configuration details.

9. If the log management software is HP ArcSight Logger, you can configure more than one Logger using the `opsa_default` schema. The `opsa-server-postinstall.sh` script prompts with the following message:

```
Do you want to add more Logger configuration for 'opsa_default' [yes/no]:
```

If you enter **yes**, you can add one more Logger configuration for the `opsa_default` schema and tenant.

10. The `opsa-server-postinstall.sh` script prompts you to decide if you want to Configure the OPSA Flex connector for ArcSight Logger [yes/no]. For the remainder of these instructions the name for the OPSA Flex connector will be the Operations Analytics Log File Connector for HP ArcSight Logger. If you enter `no`, that completes the installation. If you enter `yes`, do the following:
 - a. Review the list of Logger hosts already configured for the `opsa_default` tenant.
 - b. Enter the serial number of the Logger host for which you want to configure the Operations Analytics Log File Connector for HP ArcSight Logger.

That completes the post-installation configuration steps for the OpsA Server Appliance.

Post-Installation Steps for the Operations Analytics Collector Appliance

Complete the following post-installation configuration steps on the Operations Analytics (OpsA) Collector Appliance.

1. Log on as a `opsa` user to the OpsA Collector Appliance (the default password is `opsa`).
2. Run the `$OPSA_HOME/bin/opsa-collector-postinstall.sh` script (interactive mode).
3. The `opsa-collector-postinstall.sh` script prompts for following Vertica database host details (where the `opsadb` database is created information, and includes the default values shown in the following list. To accept the default value, click **Enter** for each prompt.
 - Vertica database host name
 - Vertica database port number

- Vertica database name
- Vertica database user name
- Vertica database password (dbadmin, unless you reset this password earlier)

Note: The `opsa-collector-postinstall.sh` script shows an error message if any of the following problems exist:

- Vertica is not installed on the specified host.
- Vertica is down.
- The port number you specified for Vertica is not open.
- You entered the wrong Vertica username or password.
- The default tenant name, `opsa_default`, does not exist.

Correct these problems and rerun the `opsa-collector-postinstall.sh` script.

For Vertica administration issues, run the `/opt/vertica/bin/adminTools` command and view the cluster state. If the state is `down`, you might need to restart the database. See "[Task 1: Installing and Configuring the Vertica Software](#)" on page 5 for more information.

4. The `opsa-collector-postinstall.sh` script prompts you to decide if you want to Configure the OPSA Flex connector for ArcSight Logger [yes/no]. For the remainder of these instructions the name for the OPSA Flex connector will be the Operations Analytics Log File Connector for HP ArcSight Logger. If you enter `no`, that completes the installation. If you enter `yes`, do the following:
 - a. Review the list of Logger hosts already configured for the `opsa_default` tenant.
 - b. Enter the serial number of the Logger host for which you want to configure the Operations Analytics Log File Connector for HP ArcSight Logger.

That completes the post-installation configuration steps for the OpsA Collector Appliance.

Accessing Operations Analytics for the First Time

To log on to Operations Analytics (OpsA):

1. Access the following URL: **`http://IP Address or fully-qualified domain name of the OpsA Server:8080/opsa`**
2. After the OpsA log on screen appears, log on to OpsA using the credentials you configured when

running the `opsa-server-postinstall.sh` script in "[Post-Installation Configuration Steps for Operations Analytics](#)" on page 16.

Task 6: Gathering Collection Information



Based on the collections you need to configure, gather the information and complete the actions shown in the following table before proceeding:

Information to Collect

Collection	Actions
HP Operations Smart Plug-in for Oracle	Obtain the list of nodes running HP Operations Smart Plug-in for Oracle.
Operations Agent	Obtain the list of nodes running Operations Agent.
NNM ISPi Performance for Metrics Component and Interface Health	<p>Set up a CSV export of the NNM ISPi Performance for Metrics Component and Interface Health extension packs by running the following commands on the NPS Server:</p> <p>Component Health: <code><Install_Dir>/NNMPerformanceSPI/bin/configureCSVExport.ovpl -p Component_Health -a "Raw,<Target-Dir>"</code></p> <p>Interface Health: <code><Install_Dir>/NNMPerformanceSPI/bin/configureCSVExport.ovpl -p Interface_Health -a "Raw,<Target-Dir>"</code></p>
	Make the CSV files accessible on the collector host in the <code>/opt/HP/opsa/data/netcomponent</code> and <code>/opt/HP/opsa/data/netinterface</code> directories. The <code>opsa</code> user must have read/write access to these files so that they can be moved to a processed directory.

Information to Collect, continued

Collection	Actions
HP Operations Manager (OMi) Events	<p>Obtain the credentials for accessing the OMi event database. During configuration, when asked for the database instance, press return without entering an instance name to configure Operations Analytics to connect to the default database instance.</p> <p>Other information to obtain: DB port number DB user and password DB instance name (if not using the default) DB name</p>
Business Process Monitor (BPM)	<p>Obtain the credentials for accessing the BPM connection. This includes the active BSM DPS Server (DPS Hostname), the RTSM Server Port (currently the default port is 21212), and the user name (the RTSM Admin user). <i>Admin</i> is the role as appears in the RTSM console. It is important to use the right role for the integration to work correctly.</p> <p>Note: The Operations Analytics integration with BPM can connect to a BSM DPS Server configured for failover. However, if the BSM DPS Server fails, Operations Analytics does not automatically reconnect to the failover DPS server. Operations Analytics will no longer collect BPM data until the active BSM DPS Server is back online.</p> <p>Complete the following before proceeding:</p> <p>Note: For this example, the fully-qualified domain name of the BSM DPS server is <code>servername.location.domain.com</code>.</p> <p>Add an entry for the BSM DPS server to the <code>/etc/hosts</code> file in the domain in which the Operations Analytics Collector Appliance resides. For example, you would add a line for the BSM DPS server to the <code>/etc/hosts</code> file using the following format: <code>10.1.2.3 servername.location.domain.com servername</code>.</p> <p>Note: You must use the alias, <code>servername</code>, as the BSM DPS host name in the node list file.</p>

Information to Collect, continued

Collection	Actions
Custom SiteScope Collection	The fully-qualified domain name or IP address of the SiteScope server The user name of the SiteScope server The password for the SiteScope Server The port used by the SiteScope server The Single Sign-on (LWSSO) token for the SiteScope server <div style="background-color: #f0f0f0; padding: 5px;"> <p>Note: For instructions about finding the LWSSO token in the SiteScope user interface, see <i>Configuring SiteScope for Integrating Data with Operations Analytics</i> in the <i>Operations Analytics Configuration Guide</i>.</p> </div> The fully-qualified domain name of the OpsA Collector Appliance

Task 7: Configuring Collections



Note: The recommended method of configuring collections is by using the **Collections Manager** from the OpsA console. See "Collection Manager" in the OpsA Help for more information.

Operations Analytics supports additional data collections beyond those described in this document. For information about these additional collections, including more detailed information about setting up collections, see *Configuring Tenants and Collections* in the *Operations Analytics Configuration Guide*.

Operations Analytics (OpsA) is a unique platform for both simple and complex IT operational problem-solving. Use OpsA to access, combine, and compare the metric, topology, event, and log file data that your OpsA administrator configures to be collected from diverse sources in your IT environment. Because this data is collected from multiple domains, Operations Analytics enables you to identify answers to problems that are not easily solved using other methods. See the *Operations Analytics Help* for more information.

Read this guide to understand the concepts required to install, configure, and use OpsA most effectively, including helpful tips and how to set up collections after installation.

Note: Only use the `$OPSA_HOME/bin/opsa-collection-setup.sh` script to assist you when first setting up a collection. This guide explains how to use the `$OPSA_HOME/bin/opsa-`

`collection-setup.sh` script. See the *opsa-collection-setup.sh* reference page (or the Linux manpage) for more information.

Note: If you want to set up your collections manually or make changes to existing collections, use the collection configuration information in the *Operations Analytics Configuration Guide*.

- Run the `/opt/HP/opsa/bin/opsa-collection-setup.sh` script on the Operations Analytics Server Appliance.

- ▼ When prompted to enter a collector host index, enter the number that represents the collector host you plan to use.

- ▼ Enter the number for the collection you need to create for your environment on the selected collector.

Host:
Enter 1 to begin configuring an HP Operations Smart Plug-in for Oracle Collection.
Enter 2 to begin configuring an Operations Agent Collection.
Enter 3 to begin configuring an NNM ISPi Performance for Metrics Component and Interface Health Collection.
Enter 4 to begin configuring an OMi Events Collection.
Enter 8 to begin configuring a Business Process Monitor Collection.
Enter 9 to begin configuring an HP ArcSight Logger Collection.
Enter 10 to begin configuring an HP SiteScope Collection.

- Follow the prompts to enter the requested information.

- Enter *for finish* after entering all of your information for this connection.

- ◆ More Collections?

- Enter *execute all* to publish the collection configurations you just completed.

Use the following credentials when prompted for a tenant username and password:

- **User Name:** opsatenantadmin
- **Password:** opsatenantadmin

Note: While configuring the following collections, you will be prompted to enter information.

Some of the information you are prompted to enter contains default values.

→ To accept these default values, press Enter.

→ To change the default values, type in the desired value, then press Enter

Configuring Log Analytics for Logger

Note: If you do not want to configure this collection by using the Collections Manager located in the Operations Analytics console, you can configure this collection using the steps in this section.

Log Analytics is a forensic tool that scans your log messages over a given time range and generates a list of the most significant ones. See the OpsA Help for more information about using Log Analytics.

To use the Log Analytics feature with ArcSight Logger, you must complete the steps in this section. To use the Log Analytics feature with Splunk, see "[Configuring Log Analytics for Splunk](#)" on page 33

Prerequisites

- You must have the R Language Pack from Vertica installed. See *Installing and Configuring the Vertica Software* in the *Operations Analytics Installation Guide* or the *Operations Analytics Upgrade Guide* for more information.
- Use HP ArcSight Logger as the log management software, as Log Analytics does not support Splunk.
- HP ArcSight Logger must be configured and collecting data from log files. See the *HP ArcSight Logger's Administrator's Guide* for more information.

Explaining the Fields Used by Log Analytics

Log Analytics supports the following fields from HP ArcSight Logger.

Note: The following fields have to exist in HP ArcSight Logger for Log Analytics to function correctly.

- `message` (log message): If there is no message, Log Analytics attempts to obtain the message from the `name` field.
- `startTime`: The time when a specific log message was written into HP ArcSight Logger.

Note: You can configure Log Analytics to use a different time field value (instead of `startTime`) if you modify this field in the `arcsight_log_stream.xml` file before creating the collection. Look for the file in the following location: `$OPSA_HOME/conf/collection/server/config.templates/arcsight/1.0/log/stream/arcsight_log_stream.xml`

- `agentSeverity`: The severity of the log message.

Note: You can configure Log Analytics to use a different severity field value (instead of

agentSeverity) if you modify this field in the `arcsight_log_stream.xml` file before creating the collection. Look for the file in the following location: `$OPSA_HOME/conf/collection/server/config.templates/arcsight/1.0/log/stream/arcsight_log_stream.xml`

- host name: Since host name might be found in different fields of HP ArcSight Logger (depend on the log type), there are four supported fields, and Log Analytics searches for their values in the following order (ignoring null values):
 - a. `device_host_name`
 - b. `source_host_name`
 - c. `destination_host_name`
 - d. `agent_host_name`

In order to change these fields you must do the following:

- a. Enable access to the JMX console by changing the extension of the following file on the opsa collector appliance to `.txt`:

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

Wait five minutes for the changes to take effect.

- b. Open the JMX Console using the following URL:
`http://<OPSA_Collector>:29900/mbean?objectname=OPSA-Infrastructure%3AService%3DSettings`

Note: You will be prompted for authentication credentials. See the OpsA Administrator to obtain the configured authentication credentials, as the default password changed during the OpsA installation. The default user name is `opsadmin` and the default password changed during the OpsA installation.

- c. Make your changes according to the following table:

Change setSettingValuePerTenantId Values

Name	Value
<code>contextName</code>	<code>opsa-topology-settings</code>
<code>tenantId</code>	<code>opsa_default</code>
<code>settingName</code>	<code>opsa.topology.technologies.la.hosts</code>
<code>newValue</code>	

For adding a new value, as shown by `newValue` in the above table and in the bold font in the following example, you must edit the following XML and paste the new value into the `newValue` field.

Enter your preferred field for `device_host_name` as the first value of the `laHostFields` node.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<technology deviceVendor="na" deviceProduct="na"
deviceVersion="na"/><technologiesLaHosts>
<laHostFields>newValue</laHostFields>
<laHostFields>device_host_name</laHostFields>
<laHostFields>source_host_name</laHostFields>
<laHostFields>destination_host_name</laHostFields>
<laHostFields>agent_host_name</laHostFields>
</technologiesLaHosts>
</tenantTechnologiesLaHosts>
```

- d. In the command line, run the following commands:

```
Invoke /opt/HP/ops/scripts/ops-storm-kill-topology.sh
```

```
Invoke /opt/HP/ops/scripts/ops-storm-submit-topology.sh
```

Note: These new settings will affect only new messages. Messages occurring before this change are not updated.

Configuring Log Analytics Collections

Use only one of the following configuration options.

Configuration Option 1: Using One HP ArcSight Logger with Log Analytics

1. Run `$OPSA_HOME/bin/opsa/opsa-collection-setup.sh` script.

Note: You will be prompted for authentication credentials. See the OpsA Administrator to obtain the configured authentication credentials, as the default password changed during the OpsA installation. The default user name is `opsatenantadmin` and the default password changed during the OpsA installation.

2. The `opsa-collection-setup.sh` script displays a list of connected Collector Appliances. Select the Collector Appliance you want to configure.

Note: This step depends on there being at least one connected Collector Appliance.

3. Enter `9` to begin configuring an HP ArcSight Logger Collection.

4. When prompted, choose one of the following options:

5: Log Analytics-All Fields (130)

6: Log Analytics-Most used fields (43)

See "[Fields Supported for Selection Options 5 and 6](#)" on the next page for a list of the fields used for each of these selections.

Note: If you choose 5: Log Analytics-All Fields (130), Log Analytics includes all of the possible fields from HP ArcSight Logger. If you choose 6: Log Analytics-Most used fields (43), Log Analytics includes only the most significant and mandatory fields. Choosing 6: Log Analytics-Most used fields (43) decreases the load placed on HP ArcSight Logger and works better for busy HP ArcSight Logger installations.

Note: The numbers shown in this step represent the number of fields that come from HP ArcSight Logger. These fields are viewable from the Log Analytics log viewer table. See *Log Analytics* in the *Operations Analytics Help* for more information about the Log Analytics log viewer.

Note: When using multiple HP ArcSight Loggers and log configurations, all of the configurations should be of same type: **all** or **limited**.

Note: If you use multiple HP ArcSight Loggers and log configurations and want to change type from **all** to **limited** or from **limited** to **all**, do the following:

- a. Remove the collection registration using the `opsa-collection-config.sh` script without the `-purgecollection` option. See *Removing a Collection Registration for a Tenant* in the *Operations Analytics Configuration Guide* for more information.
- b. Create a node list file as shown in *Configuring a Structured Log Collection* in the *Operations Analytics Configuration Guide*.

5. Enter the HP ArcSight Logger host name from which to collect the data.

6. Enter `execute all` and wait for the setup process to complete.

Note: The setup process can take several minutes to complete.

7. Enter `exit` after the setup process completes.

8. When prompted to confirm your setup, enter `y`.

You are now ready to use the Log Analytics feature. See *Log Analytics* in the *Operations Analytics Help* for more information.

Configuration Option 2: Using Multiple HP ArcSight Loggers with Log Analytics

1. Create and prepare a node list file. Look for sample files in the following location:

```
$OPSA_HOME/conf.collection
```

Note: The node list file contains the HP ArcSight Logger host name and the query to run to collect the data. Look for the `arcsight_log_stream.properties` file for the full list of fields and the `arcsight_log_stream_common.properties` file for the common fields.

For this example, assume you created the node list file in the following location:

```
/tmp/mynodelist.properties
```

2. Run the following command from the OpsA Server Appliance to create the collector configuration:

```
$OPSA_HOME/bin/opsa-collection-config.sh -create -nodelist  
/tmp/mynodelist.properties -collectorhost <fully-qualified-domain-name of  
collector host> -source arcsight -domain log -group stream -username  
opsatenantadmin
```

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

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

3. Run the following command from the OpsA Server Appliance to publish this collection configuration to the OpsA Collector Appliance :

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

The `-publish` option uploads the collection configuration you created to the OpsA Collector Appliance. To verify that the collector configuration published successfully, look for a message stating that the publish was successful, that a table was successfully created, and that the collection was restarted.

You are now ready to use the Log Analytics feature. See *Log Analytics* in the *Operations Analytics Help* for more information.

Fields Supported for Selection Options 5 and 6

The following fields are used in the Log Analytics Collection depending on the options and fields you select during configuration:

Fields used when selecting 5: Log Analytics-All Fields (130): startTime agentAddress agentHostName agentNtDomain agentSeverity agentType agentZone agentZoneName agentZoneResource agentZoneURI applicationProtocol baseEventCount bytesIn bytesOut categoryBehavior categoryDeviceGroup categoryObject categoryOutcome categoryTechnique categorySignificance customerName destinationAddress destinationDnsDomain destinationHostName destinationMacAddress destinationNtDomain destinationPort destinationProcessName destinationServiceName destinationTranslatedAddress destinationUserId destinationUserName destinationUserPrivileges destinationZone destinationZoneName destinationZoneResource deviceAction deviceAddress deviceCustomDate1 deviceCustomDate1Label deviceCustomDate2 deviceCustomDate2Label deviceCustomNumber1 deviceCustomNumber1Label deviceCustomNumber2 deviceCustomNumber2Label deviceCustomNumber3 deviceCustomNumber3Label deviceCustomString1 deviceCustomString1Label deviceCustomString2 deviceCustomString2Label deviceCustomString3 deviceCustomString3Label deviceCustomString4 deviceCustomString4Label deviceCustomString5 deviceCustomString5Label deviceCustomString6 deviceCustomString6Label deviceEventCategory deviceEventClassId deviceExternalId deviceHostName deviceInboundInterface deviceOutboundInterface deviceProduct deviceReceiptTime deviceSeverity deviceVendor deviceVersion deviceZone deviceZoneName deviceZoneResource deviceZoneURI endTime eventId eventTime externalId fileName filePath flexDate1 flexDate1Label flexNumber1 flexNumber1Label flexNumber2 flexNumber2Label flexString1 flexString1Label flexString2 flexString2Label id message name peerName priority receiver requestClientApplication requestContext requestMethod requestUrl requestUrlFileName requestUrlQuery rowId sessionId sourceAddress sourceHostName sourceMacAddress sourceNtDomain sourcePort sourceProcessName sourceServiceName sourceTranslatedAddress sourceUserId sourceUserName sourceUserPrivileges sourceZone sourceZoneName sourceZoneResource sourceZoneURI transportProtocol type vulnerabilityExternalID vulnerabilityURI

Fields used when selecting 6: Log Analytics-Most used fields (43) agentAddress agentHostName agentNtDomain agentSeverity agentType destinationDnsDomain destinationHostName destinationMacAddress destinationNtDomain destinationPort destinationProcessName destinationUserId destinationUserName deviceAddress deviceEventCategory deviceHostName deviceProduct deviceReceiptTime deviceSeverity deviceVendor deviceVersion endTime eventId eventTime message name peerName priority requestMethod rowId sourceAddress sourceHostName sourceMacAddress sourceNtDomain sourcePort sourceProcessName startTime type

Configuring Log Analytics for Splunk

To use the Log Analytics feature with Splunk, you must complete the steps in this section. To use the Log Analytics feature with Logger, see ["Configuring Log Analytics for Logger" on page 27](#)

1. Prerequisites

- You must have the R Language Pack from Vertica installed. See *Installing and Configuring the Vertica Software* in the *Operations Analytics Installation Guide* or the *Operations Analytics Upgrade Guide* for more information.
- Make sure that you have registered splunk as specified in "Configuring and Managing Logger or Splunk for a Tenant" in the OpsA Configuration Guide.

2. Create Mapping Files

As OpsA received a raw log message from Splunk, some mapping is required to help OpsA divide the raw log messages into their components. The minimum mapping required is the message and severity fields. You can create one mapping file, or multiple for each host, source, or source type.

- To create a new mapping file, use any .properties file in the **conf/splunk/opsa_default/** directory as a template. Copy it and rename it according to the following syntax:

<source/sourcetype/host>-value for example **sourcetype-WinEventLog_System**.

- Modify the message mapping to map the message content from your data sources to OpsA.

In Splunk, use the extract field feature to mark the area of the raw log that is the message. Do this on all types of messages that will be sent to OpsA. Make the extracted field public. For details, see the Splunk documentation.

The following line takes the message from Splunk and maps it to OpsA:

```
message = <<message>>
```

- Modify the severity mappings in each mapping file to map the severities from your data sources to OpsA.

In Splunk, use the extract field feature to mark the area of the raw log that is the message severity. Do this on all types of messages that will be sent to OpsA. Make the extracted field public. For details, see the Splunk documentation.

Modify the severity mappings as seen in the following example. The Splunk values are on the right side.

```
severity = <<severity>>
```

```
very-high=fatal  
high=error,alert  
medium=warn  
low=info
```


- d. If later in this procedure, you cannot validate the collection and suspect that the data was not mapped, you can manually copy the regular expression (replacing any \ with \\) of the raw log message and copy it to the mapping file. For example:

```
splunkRegex=[^\n]*\n*\s+(?P<severity>[^\s+])(?:[^\n]* ){3}(?P<message>.+)  
severity=<<severity>>  
message=<<message>>
```

Note: If Splunk does not put the severities into the field **severity**, OpsA will import the message but will not have any data about the message severity.

- e. You can map additional fields as desired. For example, you can map the deviceVendor and deviceProduct. By default, the deviceVendor is defined as the sourcetype, but this can be changed as desired.

3. Create Splunk Collection


Log in to the OpsA user interface with a user with tenant administrator permissions. Go to Settings  button and select **Collections Manager**. Create a Log Analytics (Splunk) collection. For instructions, see "How to Configure a Log Analytics (Splunk) collection in the Operations Analytics Help.


The Log Analytics feature should now be available. It may take a few minutes for data to start coming in.

Chapter 3: Using Operations Analytics

Use the information in this section to get started using Operations Analytics (OpsA).

Getting Started

If you need to view or return to the *Welcome to Operations Analytics* Screen, click  then **Welcome**. Review the helpful information shown on this screen get started using Operations Analytics

Click  then **Help** to access the *Operations Analytics Help*.

More Information

To obtain a complete set of information about Operations Analytics (OpsA), use this guide along with other OpsA documentation. The table below shows all OpsA documents to date.

Documentation for Operations Analytics

What do you want to do?	Where to find more information
I want to install OpsA.	<i>Operations Analytics Installation Guide</i>
I want to configure and maintain OpsA	<i>Operations Analytics Configuration Guide</i>
I want to upgrade OpsA 2.10 to OpsA 2.20	<i>Operations Analytics Upgrade Guide</i>
I want to obtain help about the Operations Analytics console	<i>Operations Analytics Help</i>
I want to find the hardware and operating system requirements for OpsA	<i>Operations Analytics Support Matrix</i>
I want to read a list of the new features and review any last minute issues for OpsA	<i>Operations Analytics Release Notes</i>
I want to open a view from HP BSM to OpsA	<i>Integration with HP BSM</i>

Documentation for Operations Analytics, continued

What do you want to do?	Where to find more information
I want to view a list of software products integrated with OpsA	See the list of integrations for Operations Analytics and other HP products at http://support.openview.hp.com/sc/solutions/index.jsp#tab=tab3

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 Quick Start Guide (Operations Analytics 2.20)

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!