HP Operations Analytics

Software Version: 2.30

HP Operations Analytics Installation Guide

Document Release Date: July 2015
Software Release Date: May 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

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: About this Guide

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

Note: This manual includes examples that show script usage, command line usage, command line syntax, and file editing. If you copy and paste any examples from this manual, carefully review the results of your paste before running a command or saving a file.

For Information about Operations Analytics

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

Documentation for Operations Analytics

What do you want to do?	Where to find more information
I want to install Operations Analytics	HP Operations Analytics Installation Guide
I want to configure and maintain Operations Analytics	HP Operations Analytics Configuration Guide
I want to upgrade Operations Analytics 2.20 to Operations Analytics 2.30	HP Operations Analytics Upgrade Guide
I want to obtain help about the Operations Analytics console	*Operations Analytics Help*
I want to find the hardware and operating system requirements for Operations Analytics	HP Operations Analytics System Requirements and Sizing Guide
I want to read a list of the new features and review any last minute issues for Operations Analytics	HP Operations Analytics Release Notes
I want to open a view from HP BSM to Operations Analytics	HP Operations Analytics - BSM Integration Guide
I want to view a list of software products integrated with Operations Analytics	See the list of integrations for Operations Analytics and other HP products at Software Solutions Now

Environment Variables used in this Document

This document refers to the following environment variables and other useful directories when explaining installation and configuration instructions for the Operations Analytics Software, including the Operations Analytics Server and the Operations Analytics Collector host. The environment variables are set automatically for the opsa user who can use all Operations Analytics functionality, and has access to data at the tenant level. See *Configuring Tenants and Collections* in the Operations Analytics Configuration Guide for more information.

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

Table 1: Environment Variables

Variable Name	Path	Operations Analytics Server, Operations Analytics Collector host
OPSA_ HOME	/opt/HP/opsa	Operations Analytics Server and Collector hosts
JAVA_HOME	/opt/HP/opsa/jdk	Operations Analytics Server and Collector hosts

Table 2: Other Useful Directories

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

System Requirements

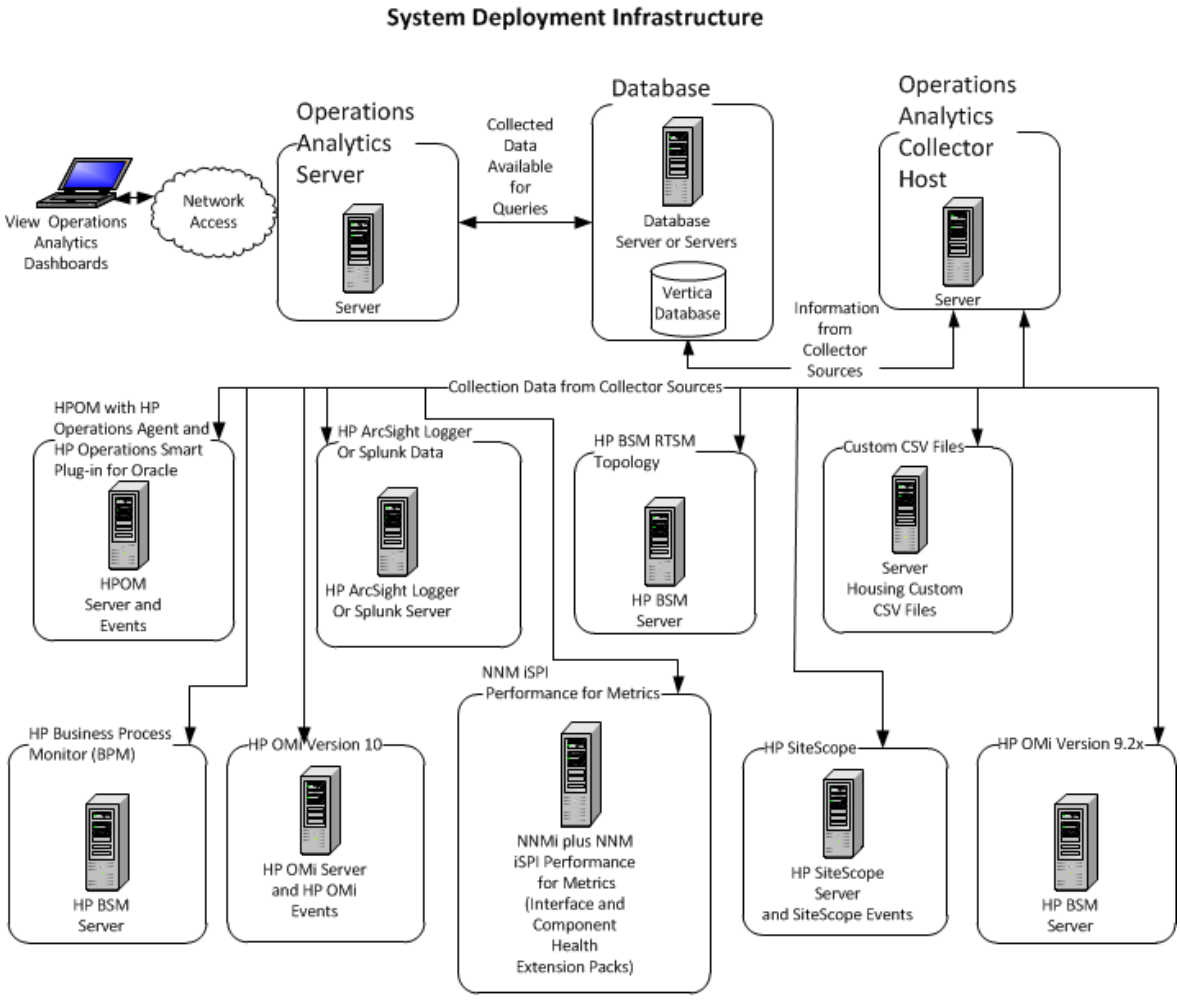
See the Operations Analytics System Requirement and Sizing Guide for the hardware and operating system requirements for Operations Analytics.

Chapter 2: Deployment Preparation

Study the information in the following section before deploying Operations Analytics.

Supported Deployments

Review the information shown in the following diagram to begin understanding the data sources supported by Operations Analytics and how they are configured together to better plan your Operations Analytics installation. After installation, add to the initial information being collected by adding more data collections. See the HP Operations Analytics Configuration Guide for more information.



Predefined User Groups

Operations Analytics provides the following predefined User Groups:

- **Super Admin**: During installation, the opsaadmin user gets created, and assigned to the Super Admin user group. **The default password for the opsaadmin user is opsaadmin**. The primary responsibility of users assigned to the Super Admin user group is to add, modify, and delete tenants and users assigned to the Tenant Admin user group. See the *opsa-tenant-manager.sh* reference page (or the Linux manpage) for information about creating and managing tenants. To view Operations Analytics reference pages, select **> Reference Pages** in the Operations Analytics console,

- **Tenant Admin**: During installation, the opsatenantadmin user gets created, and assigned to the Tenant Admin user group. opsatenantadmin is the tenant admin for the default opsa tenant. **The default password for the opsatenantadmin user is opsatenantadmin**.Only a user assigned to the Super admin user group is permitted to create a user assigned to the Tenant Admin user group. The primary responsibility of the Tenant Admin user is to add, modify, and delete users for a specific tenant. See the `opsa-tenant-manager.sh` reference page (or the Linux manpage) for information about creating and managing users for a tenant.

- **User**: During installation, the opsa user gets created, and assigned a normal user role. **The default password for the opsa user is opsa**. Only a user assigned to the Tenant admin user group is permitted to create a user having a normal user role.This role is for the normal user who can use the Operations Analytics console and has access to data for the tenant to which it is assigned. This user account must be unique across all tenants. See *Manage Users and Tenants* in the *Operations Analytics Help* for more information.

Terminology Used in this Document

Collection: Structured logs are log file data read by Operations Analytics from HP ArcSight Logger. This log information is stored (as collections) in Operations Analytics. These collections exist so that users can perform analytics on the log file contents. For example, users might want to query for all outliers by host name and application for a particular time range.

Operations Analytics Collector host: This server is the host used to manage the data collections.

Data Sources: Operations Analytics collects metrics, topology, event, and log file data from a diverse set of possible data sources.

Operations Analytics Server: This server is the host that serves Operations Analytics functions, such as integration configuration, and it is the server to which you connect your browser.

Tenant: Operations Analytics gathers metrics, topology, event, and log file data from a diverse set of possible data sources. Tenants enable you to separate information from these data sources into groups, such as collections, user accounts, and user groups. Collections can be separated by tenant and collection information cannot be shared among tenants.See *Creating Tenants* in the Operations Analytics Configuration Guide for more information.

Virtual Appliance: A virtual appliance, also referred to as **appliance** in this document, is a self-contained system that is made by combining a software application, such as Operations Analytics software, with just enough operating system for it to run optimally on industry standard hardware or a virtual machine (VMware).

Installation Overview

The following section provides an overview of the Operations Analytics installation environment.

This section includes:

- "Operations Analytics Components" below
- "Collection Sources" on the next page
- "Setting up Your Operations Analytics System" on page 12
- "Operations Analytics Port Mapping" on page 13

Operations Analytics Components

The distributed version of Operations Analytics discussed in this manual is made up of the following main components:

- **Operations Analytics Server**:
  - Provides the business logic and presentation capabilities of Operations Analytics.
  - Deployed as an OVA appliance or as a server installation.
  - Operations Analytics can have one or more Operations Analytics Servers, depending on the amount of users the system needs to support.
  - The server is JBoss-based.
- **Operations Analytics Collector Host**:
  - Connects to the different data sources and aggregates the data collected from them.
  - This data is pushed to the Operations Analytics Database.
  - Deployed as an OVA appliance or as a server installation.
  - Operations Analytics can have one or more Operations Analytics Collector hosts, depending on the data sources to which the system is connected.
- **Operations Analytics Database**:

- A Vertica database is used to support the big data analysis requirements of Operations Analytics.
- An existing Vertica database installation can be used. The Operations Analytics database (opsadb) needs to be created on it.
- A dedicated Vertica database can also be installed as part of Operations Analytics. In this case the Operations Analytics database (opsadb) will be created during the process.

> **Note:** Although this document refers to the Vertica database name for Operations Analytics as opsadb, you can choose a different name when creating this database.

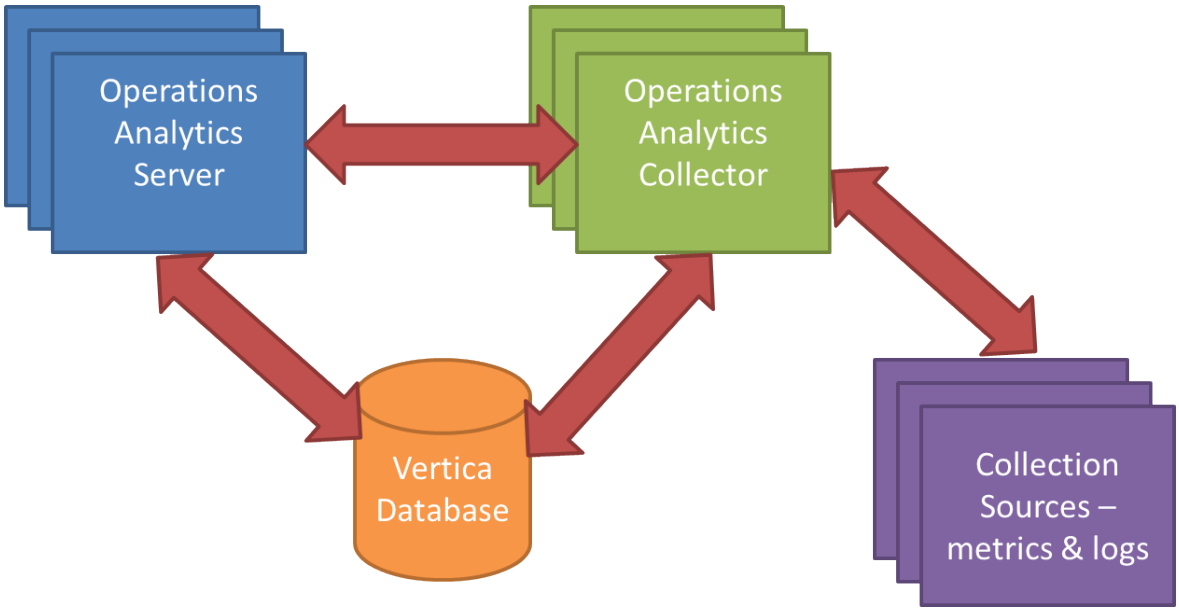
Collection Sources

Data from the collection sources is brought into Operations Analytics using the Operations Analytics Collector host.

These sources include:

- **BSM Portfolio metric collectors**: Operations Analytics supports data collection from several BSM sources. These include HP Operations Manager (OM) and HP OMi (Operations Manager i), HP Network Node Manager (NNMi), NNM iSPI Performance for Metrics, SiteScope, HP Business Process Monitor (BPM), and RTSM.
- **Log Sources**: Operations Analytics supports either one of the of the following log collectors:
  - **HP ArcSight Logger Server:**
    - An ArcSight Logger server is used to bring in log data.
    - The server retrieves data from agents that are located on different machines in the IT environment. These agents include (but are not limited to) SmartConnectors and Flex Connectors which provide access to different types of logs.
  - **Splunk**: Can also be connected to Operations Analytics as a source of log files.
- **Custom CSV files**: These can be leveraged to support data collection from additional sources.

The following is a schematic representation showing how collection sources fit into Operations Analytics:



Setting up Your Operations Analytics System

The information in this section gives you a high level overview of what will be done when setting up an Operations Analytics system.

Before beginning your Operations Analytics installation, it can save you time if you obtain the manuals shown in the following table.

Documentation Resources Referenced During the Installation Process

Integrated Product	Link to Document
Operations Analytics	Configuration Guide
Operations Analytics	System Requirements and Sizing Guide
Vertica	Installation Guide
Vertica	Administrator's Guide
Vertica	Product Documentation
Logger	Installation Guide
Logger	Administrator's Guide

System setup includes the following steps:

1. **Installation**:
   - Install the Vertica Database (*optional* - you can connect to an existing Vertica instance).
   - Install HP ArcSight Logger or Splunk to collect logs (*optional* - you can connect to an existing Logger or Splunk instance).
   - Install the Operations Analytics Server (*mandatory).*
   - Install the Operations Analytics Collector host (*mandatory).*
2. **Post-Install Configuration**
   - Connect the Operations Analytics Servers to the Vertica Database.
   - Connect the Operations Analytics Collector host to the Vertica Database.
   - Configure passwords for the default Operations Analytics users (opsatenantadmin, opsaadmin, and opsa); this is important for securing the system.
   - Configure a Logger Flex Connector on the Operations Analytics Collector host to collect system log data for self-monitoring log files from the Operations Analytics application (*optional*).
3. **Configure Collection Sources**:

   You might configure one or more of the following collection sources following a successful installation. See the Operations Analytics Configuration Guide for more information.
   - Configure the connection to several BSM data sources to collect metrics. Note that collection configuration creates a link between the Operations Analytics Server and the Operations Analytics Collector host.
   - Configure HP ArcSight Logger or Splunk to collect logs, then configure its connection to the Operations Analytics Collector host.
   - Install Logger connectors (agents) on the different IT systems so they forward log information to the Logger Server, and subsequently into Operations Analytics.
   - Configure collections from additional data sources using the custom collection capabilities.

Operations Analytics Port Mapping

The well-known network ports described in the section need to be open in a secured environment for Operations Analytics to be able to function and collect data from the data collections you configured or plan to configure.

The Operations Analytics Server and Collector hosts, as well as the other component applications used by Operations Analytics must be installed on the same subnet with full network access among them. Operations Analytics also uses a Vertica database for big data storage and HP ArcSight Logger for log collection and management. You might install and deploy these two components as part of your Operations Analytics deployment, or you might choose to connect to existing instances of these components that currently exist in your environment. If you deploy these components as part of Operations Analytics they will typically reside on the same subnet with no network restrictions between them. If you choose to leverage your existing component instances, you must enable communication between them using information from the table shown below.

Note: See the Operations Analytics Configuration Guide for detailed information about log collections as well as all other predefined and custom collections. The log collections are done by HP ArcSight Logger and the HP ArcSight Logger Syslog Connector, so any connections from ArcSight connectors or the systems sending syslog messages should be enabled to these components, respectively.

Also, you must enable communication from other collectors that communicate with the Operations Analytics Collector host.

The communication ports shown in "Well-Known Port Mapping (Sources External to Operations Analytics)" on the next page must be open on any firewall in the path between the Operations Analytics Server and Collector hosts and all of the data collectors, in the direction listed within the table. The Operations Analytics Server validates the communication to the data collectors before creating a collection. The Operations Analytics Collector host needs these open communication ports so it can collect data.

Note: In the tables shown in this section, the hosts shown in the **Open To** column listen on the port or ports shown in the **Port** column and the hosts shown in the **Open From** column initiate connections to the port or ports shown in the **Port** column.

Note: In the tables shown in this section, the listed connection type is TCP unless otherwise noted.

External traffic is the traffic coming into Operations Analytics Server and Collector hosts from a client that is not an Operations Analytics Server or an Operations Analytics Collector host. The communication ports shown in "Well-Known Port Mapping (Sources External to Operations Analytics)" on the next page lists the ports used to transmit data between non-Operations Analytics hosts to an an Operations Analytics Server or an Operations Analytics Collector host.

Well-Known Port Mapping (Sources External to Operations Analytics)

Port	Open From	Open To	Comments
80, 1098, 1099, 2506, 2507, 29602, 21212	Operations Analytics Server and Collector hosts	BSM Data Processing Server	Operations Analytics collects BPM data from the BSM Data Processing Server and not directly from BPM.
137, 138, 139, 445	Operations Analytics Collector hosts	NNM iSPI Performance for Metrics and NNMi Custom Poller	Operations Analytics uses SMB protocol to mount a CSV data directory on the NNMi system to the Operations Analytics Collector host. Because of this mounted data directory, SMB ports must be open.
381-383	Operations Analytics Server and Collector hosts	Operations Agent (OM Performance Agent and Database SPI)"	
443 or 9000	ArcSight Connectors, Operations Analytics Log File Connector for HP ArcSight Logger, Operations Analytics Server and Collector hosts	HP ArcSight Logger	You can configure this port in HP ArcSight Logger. By default, if installed as a privileged user, it is 443, otherwise, it is 9000. The Operations Analyticsdefault installation uses port 443.

Well-Known Port Mapping (Sources External to Operations Analytics), continued

Port	Open From	Open To	Comments
1433, 1521	Operations Analytics Server and Collector hosts	Database host used by OM or OMi	1443 if using MSSQL, 1521 if using Oracle. This port might have been changed by the OM or OMi database administrator.
514 UDP and 515 TCP	Managed System (the system initiating the syslog messages)	HP ArcSight Logger (Syslog Connector)	These are the default values. These values might be changed by the ArcSight administrator.
4888	ArcSight Logger	Operations Analytics Collector host	TCP Receiver: This port is used in case log data is collected from the Logger TCP forwarder and not the pull API. In this case the TCP forwarder from the ArcSight Logger source should be able to send data from the Logger server to port 4888.
5433	Operations Analytics Server and Collector hosts	Vertica	The default Vertica port is 5433. This default value can be changed by the Vertica administrator.

Well-Known Port Mapping (Sources External to Operations Analytics), continued

Port	Open From	Open To	Comments
8080	Web browsers on client devices that access the Operations Analytics console	Operations Analytics Server	Web browsers connect to the 8080 port using HTTP (non-SSL) to the Operations Analytics Server to access the Operations Analytics console. (**http://<*Operations Analytics Server*>:8080/opsa**)
8080	Operations Analytics Server and Collector hosts	SiteScope	Operations Analytics communicates with SiteScope. This port might have been configured differently by the SiteScope administrator. **Note:** Although the default port 8080 is shown here, your SiteScope application might be using some other port.

Well-Known Port Mapping (Sources External to Operations Analytics), continued

Port	Open From	Open To	Comments
8089	Operations Analytics Server and Collector hosts	Splunk	Used if Splunk is used instead of Logger.
8443 (https) 21212 (http)	Operations Analytics Server and Collector hosts	RTSM Inventory on the BSM Data Processing Server	
9443	SiteScope server	Operations Analytics Server and Collector hosts	This port is the default port of a SiteScope integration instance and can be changed by the SiteScope administrator.

Internal traffic is the traffic between Operations Analytics Servers and Operations Analytics Collector hosts. The communication ports shown in "Well-Known Port Mapping (Sources External to Operations Analytics)" on page 15 lists the ports used to transmit data among Operations Analytics Server and Collector hosts. It works better to disable any firewalls between the Operations Analytics Servers and Operations Analytics Server and Collector hosts. Each port listed in this table should be opened in both directions (send from it and receive to it).

Note: It works better to disable any firewalls between the Operations Analytics Server and Collector hosts. However, if a firewall is enabled, open the ports show in "Well-Known Port Mapping (Sources External to Operations Analytics)" on page 15.

Well-Known Port Mapping (Sources Internal to Operations Analytics)

Port	Open From	Open To	Comments
381-383	Operations Analytics Server and Collector hosts	Operations Analytics Server and Collector hosts	Used by local HPOM performance agents.
2181	Operations Analytics Server and Collector hosts	Operations Analytics Server	Any data flow that uses Apache Zookeeper within Operations Analytics.

Well-Known Port Mapping (Sources Internal to Operations Analytics), continued

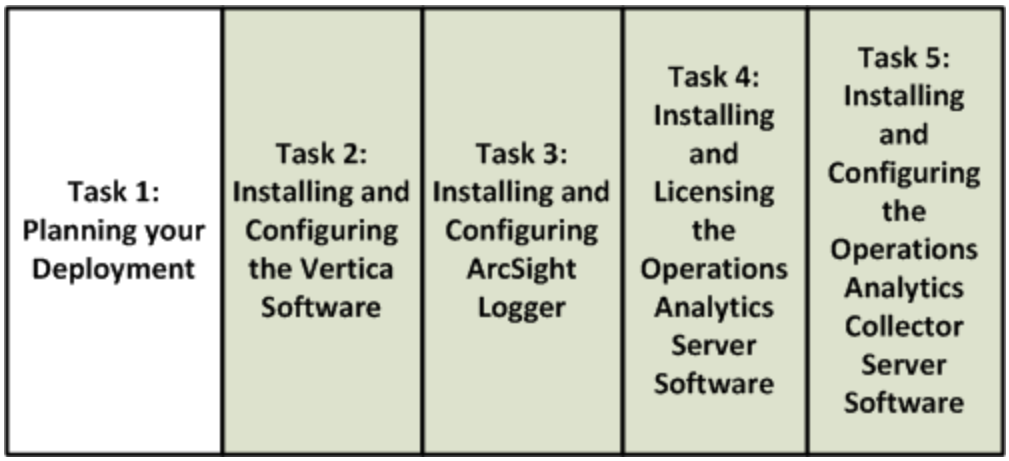
Port	Open From	Open To	Comments
2888, 3888	Operations Analytics Server and Collector hosts	Operations Analytics Server	Zookeeper leader election and peer ports.
4242	Clients connection to Apache Storm (used internally by Operations Analytics)	Operations Analytics Server	Clients connecting to Apache Storm.
6627	Operations Analytics Server and Collector hosts	Operations Analytics Server	Apache Storm Nimbus thrift port.
6700	Operations Analytics Server and Collector hosts	Operations Analytics Collector hosts	Apache Storm Nimbus worker ports.
9443	Operations Analytics Server and Collector hosts	Operations Analytics Collector hosts	Used by the Operations Analytics Server to register Operations Analytics Collector hosts.

Chapter 3: Installing Operations Analytics

This chapter guides you through the process of installing and configuring Operations Analytics. There are five main categories for the tasks to complete shown below:

1. "Task 1: Planning your Deployment" below
2. "Task 2: Installing and Configuring the Vertica Software" on the next page
3. "Task 3: Installing and Configuring HP ArcSight Logger" on page 32
4. "Task 4: Installing and Licensing the Operations Analytics Server Software" on page 34
5. "Task 5: Installing and Configuring the Operations Analytics Collector Software" on page 38

Task 1: Planning your Deployment



Use the following checklist to prepare for configuring Operations Analytics:

1. ☑ Review the following Topics:
   - "Terminology Used in this Document" on page 9
   - "Supported Deployments" on page 8
   - Operations Analytics Release Notes
   - Operations Analytics System Requirements and Sizing Guide
2. ☑ Review the information in "Operations Analytics Port Mapping" on page 13 and open the well-

known ports discussed in that section before installing Operations Analytics.

3. For the instructions in this manual, use the information in "Available Downloads for Operations Analytics 2.30 " below to obtain the installation packages.

> **Note:** All installation files must be owned by the root user.

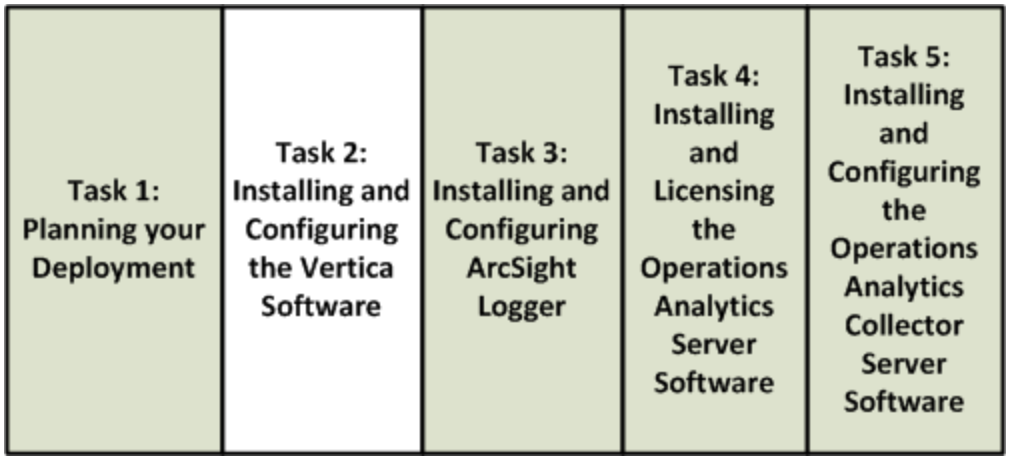
   a. Go to My software updates (use your HP Passport credentials). "Available Downloads for Operations Analytics 2.30 " below shows the available downloads for Operations Analytics.

Available Downloads for Operations Analytics 2.30

Download File Name	Purpose
HP Operations Analytics 2.30 Virtual Appliance.zip	Operations Analytics VM Installations
HP Operations Analytics 2.30 Linux Installation.zip	Operations Analytics Linux Server Installations
HP Operations Analytics 2.30 Vertica Integration.zip	Operations Analytics Vertica Installations
HP ArcSight Logger 6.0 Linux Installation.zip	Operations Analytics Logger Installations

Continue your installation at "Task 2: Installing and Configuring the Vertica Software" below

Task 2: Installing and Configuring the Vertica Software



Vertica is the database in which Operations Analytics stores configurations and collected data. The instructions in this section explain three ways to use Vertica with Operations Analytics.

Host Prerequisites and Setup

See the **Databases** section of the HP Operations Analytics System Requirements and Sizing Guide for important information about the Vertica versions and configurations supported by Operations Analytics.

Read the following if you plan to use Vertica in a virtual environment:

- Supported Platforms
- Configuring Virtual Machines for HP Vertica 7.1.x

Read the following if you plan to use Vertica installed on a physical (bare-metal) server:

Configuring the HP DL380 Gen9 24-SFF CTO Server as an HP Vertica Node

Review the *Vertica 7.1x installation Guide* and complete the following actions:

- Set the Disk Readahead to a supported value
- Disable transparent hugePages
- Set the User Max Open Files Limit to at least 65536

Installing Vertica

Download the `HP Operations Analytics 2.30 Vertica Integration` zip file and extract it to a local directory. See "Task 1: Planning your Deployment" on page 20 for more information.

Use only one of the following Vertica installation approaches:

- **Approach 1**: This is a single-node installation of the Vertica database. Use the wizard-driven installation approach shown in "Approach 1: Wizard-Driven Installation of Vertica as a Single Node" on the next page.

  Approach 2: Use an existing Vertica database and use the Operations Analytics-related extensions shown in "Approach 2: Operations Analytics-Related Extensions" on page 25.

  > **Note:** Log Analytics is a forensic tool in Operations Analytics that scans your log messages over a given time range and generates a list of the most significant ones.To use Log Analytics you must install the R Language Pack from Vertica as explained in the above link.

- **Approach 3**: Install a new Vertica database cluster with Operations Analytics-related extensions. Using this approach installs the Vertica database as a multiple node. Complete the instructions

shown in "Approach 3: Install a New Vertica Installation Cluster with Operations Analytics-Related Extensions" on page 27.

Approach 1: Wizard-Driven Installation of Vertica as a Single Node

1. From the local directory to which you downloaded and extracted the `HP Operations Analytics 2.30 Vertica Integration` zip file, navigate to the `opsa-vertica` directory.
2. Run the following command to begin the Vertica installation:
   `opsa-vertica_2.30_setup.bin`
   Follow the interactive instructions until the Vertica installation is complete.

   Note: When completing the steps in this section, ignore the warning messages regarding the existing packages.

   Note: The installation process results in the creation of the `opsadb` database.

   After the installation completes, it includes the following:

   - Vertica is installed.
   - The `opsadb` database is created.

     Note: The default username is dbadmin and the password is dbadmin.

   - The R Language Pack and MASS package is installed.
   - The Gamma distribution functions are created.
3. Optional Step: Complete the sub-steps here if you want to change the default database password, check the database status, or do both of these tasks.

   a. 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:

      i. Run the following command to log on to the `opsadb` database using the `vsql` tool:
      `/opt/vertica/bin/vsql -h hostname -p 5433 -U dbadmin -w dbadmin -d opsadb`

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

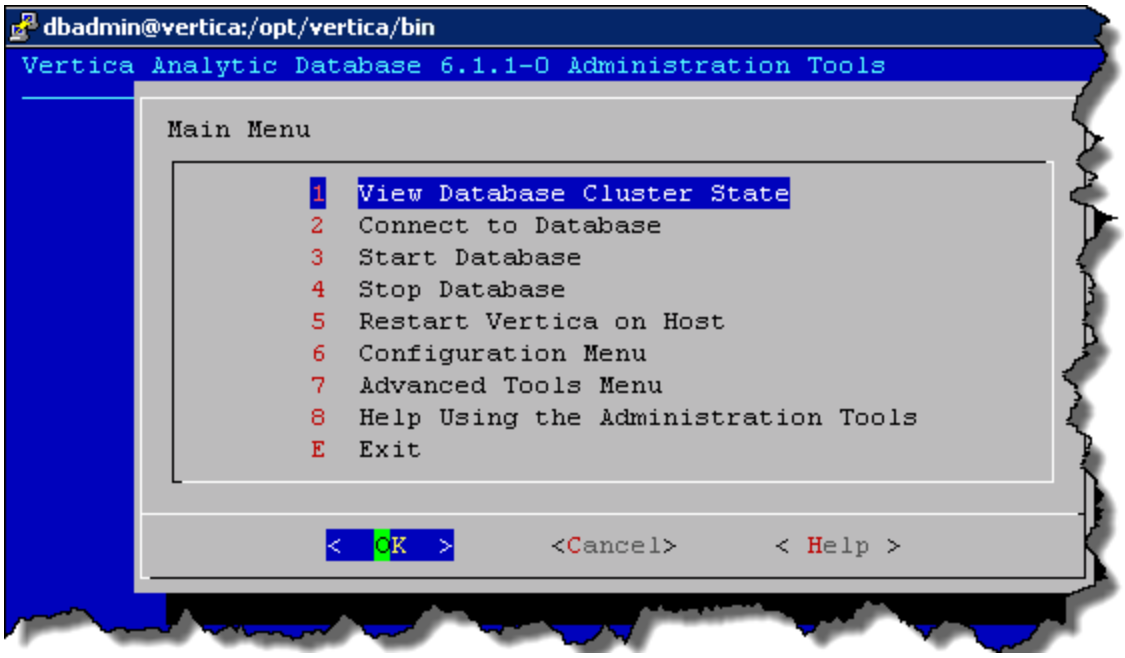
ii. Run the following command to change the password:
`alter user dbadmin identified by '<new password>';`

iii. Enter `\q` to quit the `vsql` tool.

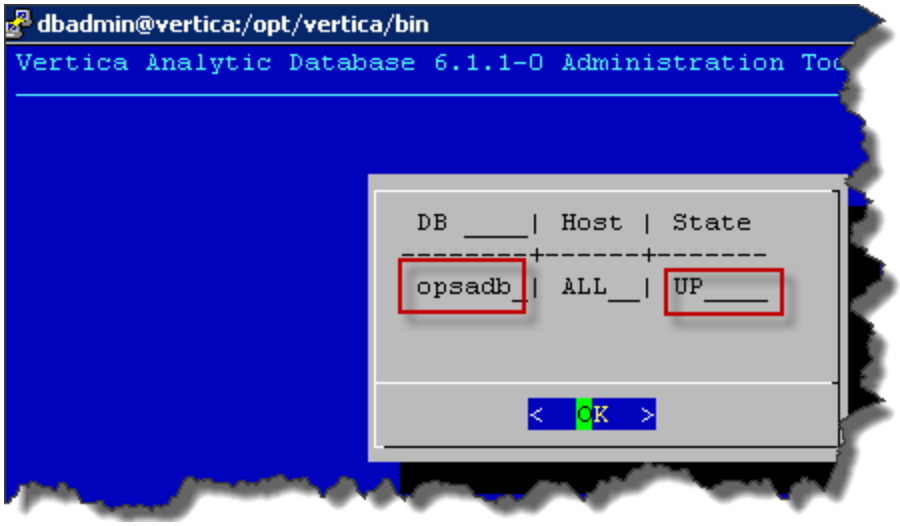
b. Do the following to check the database:

i. Run the `su -dbadmin` command.

ii. Run the `/opt/vertica/bin/adminTools` command. You should see a screen similar to the following:



iii. 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:



iv. Click **OK** twice to exit the adminTools interactive command.

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

Continue your Operations Analytics installation at "Completing other Steps after Installing Vertica" on page 31.

Approach 2: Operations Analytics-Related Extensions

If you want to use an existing Vertica installation (a Vertica that you had installed before deciding to purchase Operations Analytics, along with the R Language Pack from Vertica (to build analytics functions written in R and deploy those functions on the HP Vertica platform), use this approach.

Log Analytics is a forensic tool in Operations Analytics that scans your log messages over a given time range and generates a list of the most significant ones.To use Log Analytics you must install the R Language Pack from Vertica.

> **Note:** The R Language Pack from Vertica consumes extra disk space once you have it running. Closely monitor the consumed disk space after installing the R Language Pack from Vertica.

Do the following:

1. From the local directory to which you downloaded and extracted the `HP Operations Analytics 2.30 Vertica Integration` zip file, navigate to the `vertica` directory.
2. Log on to the server on which you are installing Vertica as a root user.
3. Run the following command to install the compat-libgfortran package from the `vertica` directory:
   `rpm -Uvh compat-libgfortran-41-4.1.2-39.el6.x86_64.rpm`
4. Install all 3 vertica-R-lang packages located in the `vertica` directory in incremental order as shown in the following example:

   ```
   rpm -Uvh vertica-R-lang-7.1.1-0.x86_64.RHEL5.rpm

   rpm -Uvh vertica-R-lang-7.1.1-3.x86_64.RHEL5.rpm

   rpm -Uvh vertica-R-lang-7.1.1-5.x86_64.RHEL5.rpm
   ```

5. Verification: To verify the R Language Pack installation, do the following:
   a. Run the following command: a. `rpm –qa | grep –i vertica-R`
   b. If you see a message similar to the following, the installation was successful:
      `vertica-R-lang-<VERSION>`
6. Complete the remaining steps in this section for each one of the Vertica cluster nodes.
   Copy the files from the `MASS` and `vertica` folders located in the local directory to which you downloaded and extracted the `HP Operations Analytics 2.30 Vertica Integration.zip` file to the `/home` directory:
7. If step 3 failed due to a connection error, run the following command: `yum install /usr/lib64/libgfortran.so.1`
8. Run the following command to create the link to the R-Vertica function: `ln -s /home/dbadmin /home_vertica`
9. Run the following command to set the correct folder permissions: `chmod 770 /home_vertica`
10. Run the following command from the `/home` directory to copy the `GammaDistribution.R` file to the `/home_vertica` directory:
    `cp GammaDistribution.R /home_vertica`
11. 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.

12. 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
    ```

13. 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`

14. Run the following command to set the correct permissions:
    `chmod 777 /home/create_R_GammaDist.sh`

15. Run the following command to switch to the dbadmin user: `su - dbadmin`

16. From the `/home` directory, run the following command: `./create_R_GammaDist.sh`

You can now use the R Language Pack along with your existing Vertica software. There is no need to install the Vertica application included with Operations Analytics.

Continue your Operations Analytics installation at "Completing other Steps after Installing Vertica" on page 31.

Approach 3: Install a New Vertica Installation Cluster with Operations Analytics-Related Extensions

To install Vertica as a multiple node cluster with Operations Analytics-related extensions, do the following for each node in the cluster:

1. Extract the contents of the `HP Operations Analytics 2.30 Vertica Integration.zip` file to a temporary location.

2. Complete the remaining steps in this section for each one of the Vertica cluster nodes.
   Copy the files from the `MASS` and `vertica` folders located in the local directory to which you downloaded and extracted the `HP Operations Analytics 2.30 Vertica Integration.zip` file to the `/home` directory:

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

4. Run the following command to set the correct folder permissions: `chmod 770 /home_vertica`

5. Run the following command from the `/home` directory to copy the `GammaDistribution.R` file to the `/home_vertica` directory:

```
cp GammaDistribution.R /home_vertica
```

6. Run the following command to install a group package to enable the MASS statistics Library to compile:

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

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

   Tip: For an alternative approach to installing development tools offline, see Unix & Linux Stack Exchange.

7. 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=<VerticaHost1>,<VerticaHost2>,<VerticaHostN> -c <catalog_path> -D <data_
   path>
   ```

   Note: Here is a practical example: `admintools -t create_db -s 10.20.100.66,10.20.100.67,10.20.100.68 -d mydb -c /catalogFs/mydb/catalog -D /DataFs/mydb/data`

8. Install all 3 vertica-R-lang packages located in the `vertica` directory in incremental order as shown in the following example:

   ```
   rpm -Uvh vertica-R-lang-7.1.1-0.x86_64.RHEL5.rpm

   rpm -Uvh vertica-R-lang-7.1.1-3.x86_64.RHEL5.rpm

   rpm -Uvh vertica-R-lang-7.1.1-5.x86_64.RHEL5.rpm
   ```

9. Verification: To verify the R Language Pack installation, do the following:

   a. Run the following command: a. `rpm –qa | grep –i vertica-R`

   b. If you see a message similar to the following, the installation was successful:
      `vertica-R-lang-<VERSION>`

10. 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`

11. Run the following command for each one of the Vertica cluster nodes to set the correct permissions:
`chmod 777 /home/create_R_GammaDist.sh`

12. Run the following command to switch to the dbadmin user: `su - dbadmin`

13. From the /home directory, run the following command: `./create_R_GammaDist.sh`

14. 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 `vsql` tool:
    `/opt/vertica/bin/vsql -h hostname -p 5433 -U dbadmin -w dbadmin -d opsadb`

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

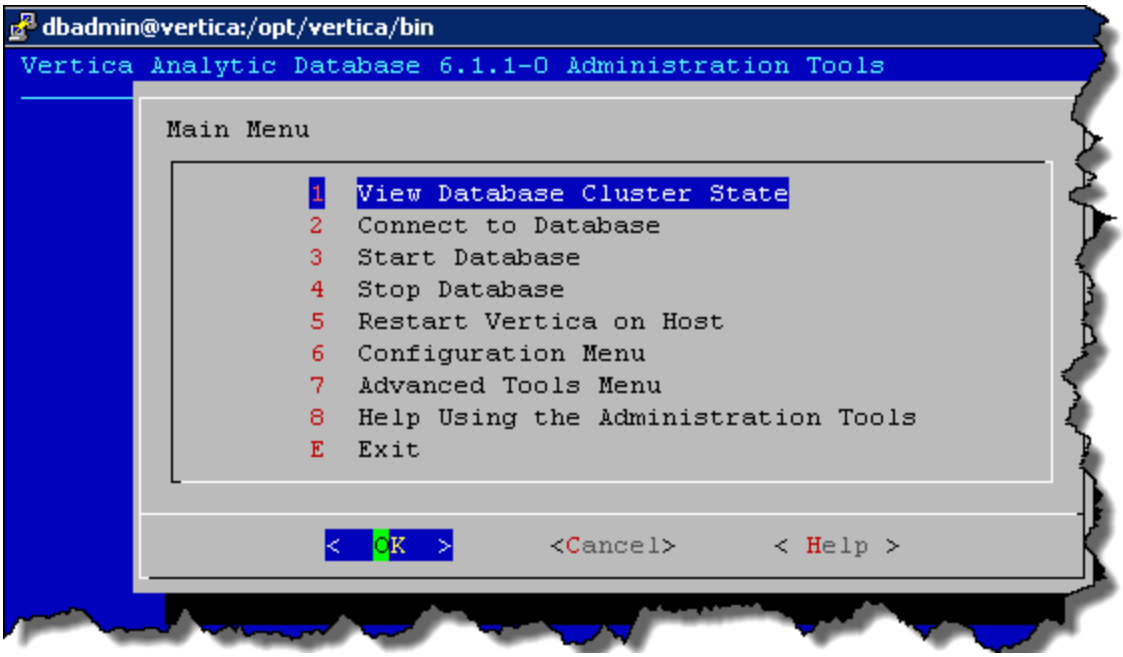
    b. Run the following command to change the password:
    `alter user dbadmin identified by '<new password>';`

    c. Enter `\q` to quit the `vsql` tool.

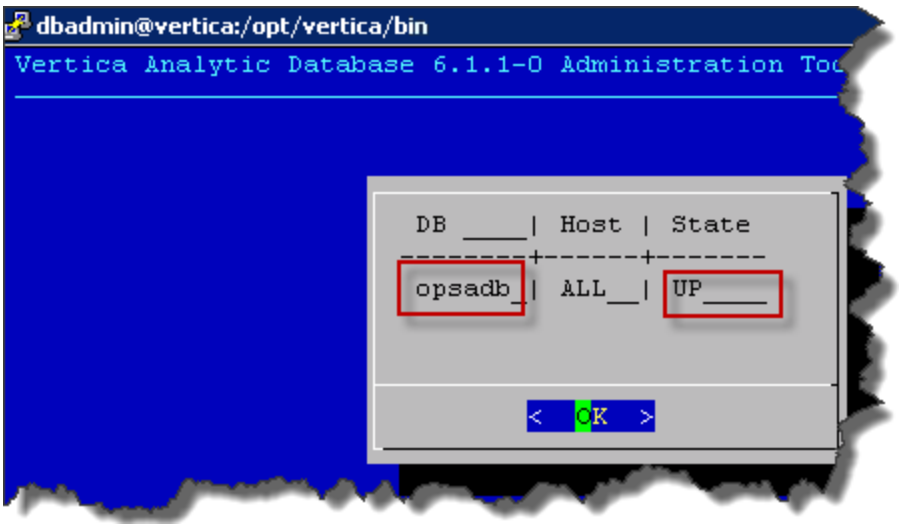
15. Do the following to check the database:

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

All of the following approaches support native resource load balancing to improve performance. To enable this native resource load balancing, run the following command: `SELECT SET_LOAD_BALANCE_POLICY('ROUNDROBIN');` after you complete

Continue your Operations Analytics installation at "Completing other Steps after Installing Vertica" below.

Completing other Steps after Installing Vertica

Stabilizing the Vertica Connection when a Firewall is Enabled

The connection between the Vertica server and the client can be prematurely terminated by a firewall timeout. Examples of these clients with regards to Operations Analytics involve any connections from either the Operations Analytics Server or the Operations Analytics Collector hosts. This could happen when a long-running query is in progress but no data is being passed back to the client, or when the Operations Analytics internal connection pool is in an idle state and the firewall timeout is less than the TCP `KEEPALIVE` setting on the database server.

> **Note:** On some Linux distributions, the default `KEEPALIVE` setting is 2 hours or 7200 seconds.

One possible solution would be to change the `KEEPALIVE` setting to a value lower than the firewall timeout. The following command is only an example of how to use the commands, so substitute different values to meet your needs. In the following example,you would run this command on each Vertica node to set the `KEEPALIVE` setting to 10 minutes (600 seconds): `echo 600 > /proc/sys/net/ipv4/tcp_keepalive_time`

Considering this example, you might do the following on the Vertica server, the Operations Analytics Server, and the Operations Analytics Collector host to save these values in the case of these servers resetting. Remember that the values used in the following steps are only there as an example. You must substitute different values to meet your needs:

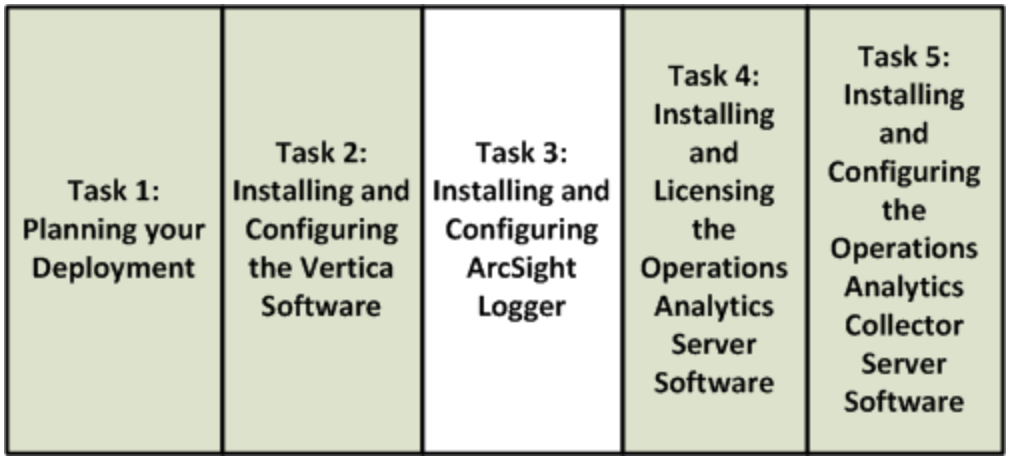
1. Edit the `/etc/sysctl.conf` file.
2. Append the following lines to the end of the file you are editing:
   ```
   net.ipv4.tcp_keepalive_time = 300
   net.ipv4.tcp_keepalive_intvl = 60
   net.ipv4.tcp_keepalive_probes=20
   ```
3. Save your work.
4. Run the following command as the root user: `sysctl -p`

Database Load Balancing

Operations Analytics supports native resource load balancing to improve performance. To enable this native resource load balancing, run the following command as the Vertica dbadmin user: `SELECT SET_LOAD_BALANCE_POLICY('ROUNDROBIN');`

Continue your Operations Analytics installation at "Task 3: Installing and Configuring HP ArcSight Logger" below.

Task 3: Installing and Configuring HP ArcSight Logger



The instructions in this section explain how to obtain the *ArcSight Logger 6.0 Installation Guide* and *ArcSight Logger 6.0 Adminstrator's Guide* to install HP ArcSight Logger and configure HP ArcSight Logger for use with Operations Analytics.

Note: If you plan to use an existing installation of HP ArcSight Logger with Operations Analytics, skip this task and continue with "Task 4: Installing and Licensing the Operations Analytics Server Software" on page 34

Note: If you plan to install and use an earlier supported version of Logger (Logger version 5.3 SP1 or 5.5) with Operations Analytics, see the *Installing and Configuring HP ArcSight Logger* section of the Operations Analytics 2.20 Installation Guide.

1. Review the *HP Operations Analytics System Requirements and Sizing Guide* for the supported platforms and browsers for HP ArcSight Logger.
2. Obtain copies of the using the ArcSight Logger 6.0 Administration Guide and ArcSight Logger 6.0 Installation Guide

Note: If you do not have authentication credentials, point your browser to HP Protect724, click the **Register** link, and follow the instructions.

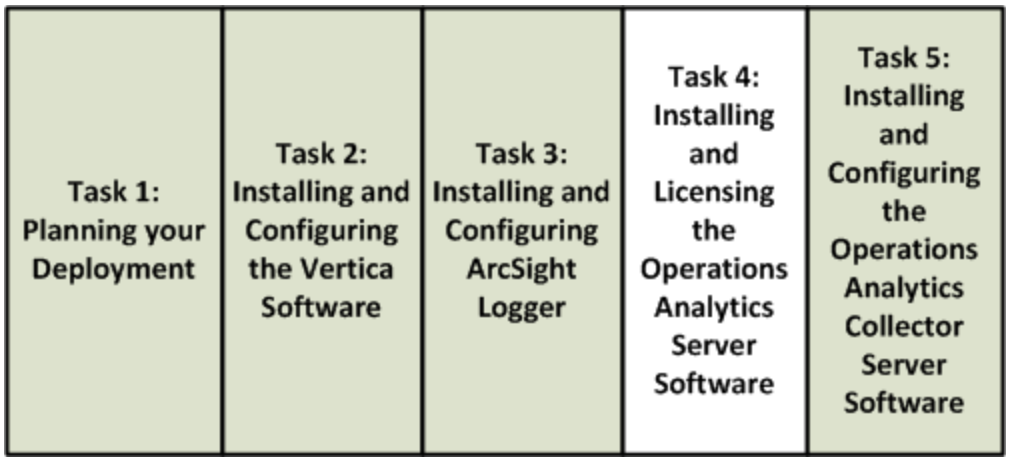
3. Download the `HP ArcSight Logger 6.0 Linux Installation` zip file from My software updates and extract the product files to a local directory. See "Task 1: Planning your Deployment" on page 20 for more information.
4. Install Logger by using information contained in the *ArcSight Logger Installation Guide*. Look in the following subsections of *Installing Software Logger on Linux* section:
   - *Prerequisites for Installation*
   - *Installing Logger*
   - *Connecting to Logger*
5. To make Logger authentication changes, see *Reset Password* in the *ArcSight Logger Administrator's Guide*.
6. Optional Step: To configure Operations Analytics to support multiple HP ArcSight Loggers, use the `$OPSA_HOME/bin/opsa-logger-config-manager.sh` script. See the *opsa-logger-config-manager.sh* reference page (or the Linux manpage) for more information. To view Operations Analytics reference pages, select **> Reference Pages** in the Operations Analytics console,

After completing this task, continue with "Task 4: Installing and Licensing the Operations Analytics Server Software" on the next page

Note: During post-installation steps explained later in "" on page 41 and "Post-Installation Steps for the Operations Analytics Collector Host" on page 47, you will be asked whether you want to automatically install the Operations Analytics Log File Connector for HP ArcSight Logger for the Operations Analytics Server and Collector hosts. Doing so enables Operations Analytics to collect Operations Analytics log events.

If you choose to install and configure the Operations Analytics Log File Connector for HP ArcSight Logger and need to make additional configuration changes later, see the *Configuring the Operations Analytics Log File Connector for HP ArcSight Logger* section of the Operations Analytics Configuration Guide.

Task 4: Installing and Licensing the Operations Analytics Server Software



You can install the Operations Analytics Server software as an appliance or on a supported server. Use one of the following options:

- "Installing the Operations Analytics Server Appliance using the VMware vSphere Client" below.
- "Installing the Operations Analytics Server Software on a Supported Server" on page 37.

Installing the Operations Analytics Server Appliance using the VMware vSphere Client

The Operations Analytics Server Appliance is installed as a virtual appliance using the `HP_Opsa_Server_OVF10.ova` file. You must deploy the `HP_Opsa_Server_OVF10.ova` file in the VMware virtual center before you can use Operations Analytics.

Note: Operations Analytics can have one or more Operations Analytics Server Appliances, depending on the amount of users the system needs to support. To add multiple Operations Analytics Server Appliances, take the following approach:

1. Install the first Operations Analytics Server Appliance and its application components as explained in this manual.
2. Install another Operations Analytics Server Appliance.
3. Run the `opsa-server-postinstall.sh -scaleout` command from the second Operations Analytics Server Appliance. See the *opsa-server-postinstall.sh* reference page (or the Linux

manpage) for more information. To view Operations Analytics reference pages, select > **Reference Pages** in the Operations Analytics console,

During the deployment process, you will be asked to specify the network parameters (IP address, network mask, gateway, DNS servers, hostname and domain name).

Complete the following tasks to deploy the Operations Analytics Server Appliance.

1. Download the `HP Operations Analytics 2.30 Virtual Appliance.zip` file and extract the product files to a local directory. See "Task 1: Planning your Deployment" on page 20 for more information.
2. Log on to the VMware vSphere Client.
3. Select **File** -> **Deploy OVF Template**.
4. Enter the URL or the file path of the `HP_Opsa_Server_OVF10.ova` file; then click **Next**.

   Note: The file path is the path to the directory in which you extracted the `HP Operations Analytics 2.30 Linux Installation.zip` file in a previous step;
5. Specify a name and location for the deployed template.
6. Follow the instructions to select the host or cluster on which you want to deploy the Server Appliance; then click **Next**.
7. Select a resource pool.
8. Select the destination storage for the Server Appliance files; then click **Next**.
9. Select the format on which you want to store the virtual disks; 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. If the User Interface does not appear, see the User's Guide to Deploying vApps and Virtual Appliances, (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.

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

Note: To log on to the Operations Analytics Server Appliance, use the following authentication credentials:
User: `opsa`
Password: `opsa`

When logging on to the Operations Analytics Server Appliance for the first time, you will be prompted to change the default password of this user. The new password should contain at least 12 characters and at least 1 lowercase character, 1 uppercase character, and 1 digit.

The `opsa` user has the privileges to switch to the root user, if necessary. You need to provide the root password (initially set to `iso*help`) to switch to the root user.

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

14. Continue with "Installing the Operations Analytics License" on the next page.

Installing the Operations Analytics Server Software on a Supported Server

Complete the following steps to deploy the Operations Analytics Server.

1. Download the `HP Operations Analytics 2.30 Linux Installation.zip` file and extract the product files to a local directory. see "Task 1: Planning your Deployment" on page 20 for more information.
2. As the root user, run `opsa_02.30_setup.bin` from the directory to which you extracted the product files.
3. When prompted, specify that you are installing the Operations Analytics Server.
4. Follow the interactive prompts to complete the installation.
5. Continue with "Installing the Operations Analytics License" below.

Installing the Operations Analytics License

Operations Analytics licensing is based on the number of Operations Analytics nodes for which data is collected. An OA node is a real or virtual computer system, or a device (for example a printer, router, or bridge) within a network.

The following types of licenses can be applied to the Operations Analytics Server:

An **Instant On** license gets applied during the Operations Analytics Server installation. This *Instant On* license is valid for 60 days and has a capacity for 500 OA nodes.

A **Permanent** license is a license that you apply after your purchase Operations Analytics, and is based on the quantity of OA nodes.

When installing the Operations Analytics license, note the following:

- You can install a *Permanent* license even though an *Instant On* license is already installed.
- Installing a *Permanent* licenses disables the *Instant On* license.
- Operations Analytics license entitlements aggregate if you apply the same kind of license in addition to the existing licenses.

  Note: For example, installing an Operations Analytics Permanent license for 100 OA nodes on top of an existing Operations Analytics Permanent license for 200 OA nodes, will aggregate the license capacity to 300 OA nodes.

- There is no license for the Operations Analytics Collector host.

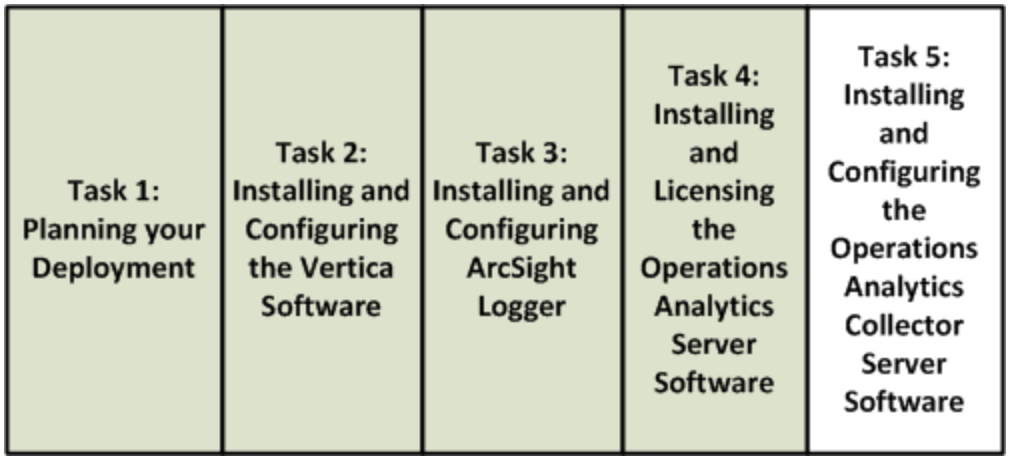
To install the Operations Analytics license, do the following:

1. Run the following command from the Operations Analytics Server to install the Operations Analytics license:
   `$OPSA_HOME/bin/opsa-license-manager.sh -add <path to license file>`
   You should see a message that, among other information, includes the following:
   `Added license from file /opt/HP/opsa/license/Neutron_License.txt successfully`

2. Run the following command to verify that the Operations Analytics license installed correctly:
   `$OPSA_HOME/bin/opsa-license-manager.sh -list`

   See the *opsa-license-manager.sh* reference page (or the Linux manpage) for more information. To view Operations Analytics reference pages, select > **Reference Pages** in the Operations Analytics console,

Task 5: Installing and Configuring the Operations Analytics Collector Software



You can install the Operations Analytics Collector software as an appliance or on a supported server. Use one of the following options:

- " Option 1: Installing and Configuring the Operations Analytics Collector Appliance using the VMware vSphere Client" on the next page.
- "Option 2: Installing the Operations Analytics Collector Software on a Supported Server" on page 40.

Option 1: Installing and Configuring the Operations Analytics Collector Appliance using the VMware vSphere Client

Complete the following configuration steps for each Operations Analytics Collector Appliance you plan to install.

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

1. Download the `HP Operations Analytics 2.30 Virtual Appliance.zip` file and extract the product files to a local directory. See "Task 1: Planning your Deployment" on page 20 for more information.
2. Log on to the VMware vCenter server or directly to the VMWARE ESX server using the VMware vSphere Client.
3. Select **File** > **Deploy OVF Template**.
4. Enter the URL or the file path of the `HP_Opsa_Collector_OVF10.ova` file; then click **Next**.

   Note: The file path is the path to the directory in which you extracted the `HP Operations Analytics 2.30 Linux Installation.zip` file in a previous step;
5. Specify a name and location for the deployed template.
6. Select the host or cluster on which you want to deploy the Operations Analytics Collector Appliance; then click **Next**.
7. Select a resource pool.
8. Select the destination storage for the Operations Analytics Collector Appliance files; then click **Next**.
9. Select the format on which you want to store the collector's virtual disks; 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.

    Note: When using DHCP, Operations Analytics uses a standard `ifcfg-eth0` file

configuration recommended by CentOS. If your network configuration is different from the standard described by CentOs, Operations Analytics might not be able to get an IP address from DHCP or access the VM using the hostname or fully-qualified domain name. See Configuring a DCHP Client in the Red Hat Enterprise Linux Deployment Guide for more information.

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**.

Note: To log on to the Operations Analytics Collector Appliance, use the following authentication credentials:
User: `opsa`
Password: `opsa`

When logging on to the Operations Analytics Collector Appliance for the first time, you will be prompted to change the default password of this user. The new password should contain at least 12 characters and at least 1 lowercase character, 1 uppercase character, and 1 digit.

The `opsa` user has the privileges to switch to the root user, if necessary. You need to provide the root password (initially set to `iso*help`) to switch to the root user.

Option 2: Installing the Operations Analytics Collector Software on a Supported Server

Complete the following steps for each Operations Analytics Collector host you plan to install.

1. Download the `HP Operations Analytics 2.30 Linux Installation.zip` file and extract the product files to a local directory. see "Task 1: Planning your Deployment" on page 20 for more information.

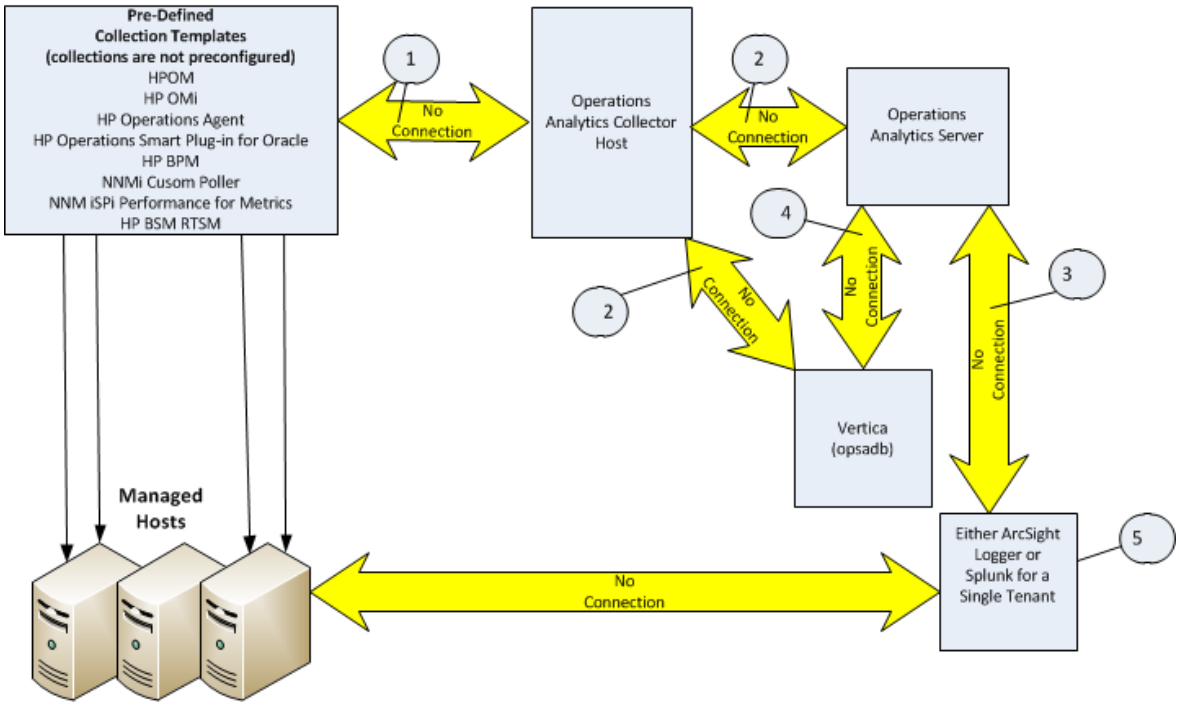
2. As the root user, run `opsa_02.30_setup.bin` from the directory to which you extracted the product files (completed in Task 1).

3. When prompted, specify that you are installing the Operations Analytics Collector host.

4. Follow the interactive prompts to complete the installation.

Post-Installation Configuration Steps for Operations Analytics

After you complete the steps in this section, common communication with the distributed components of Operations Analytics is established. The post installation script (opsa-server-postinstall.sh script) completes the final configuration steps for the different application components used by Operations Analytics. The opsa-server-postinstall.sh script configures communication among the distributed components of Operations Analytics. The following diagram shows the missing communication connections that the opsa-server-postinstall.sh script will create.



Use the following numeric references when viewing the above graphic:

1. This connection is established after a collection is created. This is also true for the connection between the Operations Analytics Collector host and Logger (or Splunk).

2. This connection is established when registering the Operations Analytics Collector host using the following command: `opsa-collection-config.sh -register -collectorhost <collector hostname>`

3. This connection is created when running the interactive `opsa-server-postinstall.sh` script if you choose to add Logger. If you do not choose to add Logger, you can establish the connection later by running the `opsa-logger-config-manager.sh -add` command.

4. This connection is established when running the `opsa-server-postinstall.sh` script.

5. Operations Analytics supports either Logger or Splunk, but not both, for a single tenant.

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

Post-Installation Steps for the Operations Analytics Server

There are four different approaches to running the `opsa-server-postinstall.sh` script:

- **Common Approach**: Use the more common approach discussed in "Option 1: Have the post-installation script prepare the database" on the next page to prepare a database that does not currently contain Operations Analytics schemas and tables. To use this option, a dbadmin database user (superuser) must have been created that has access to the Vertica database. This was accomplished if you used **Approach 1** to install Vertica in "Task 2: Installing and Configuring the Vertica Software" on page 21.

- **Manual Approach**: If you do not plan to use the information discussed in the **Common Approach**, and need the Vertica database administrator to manually prepare the database and schemas, use the approach discussed in "Option 2: Manually prepare the database:" on page 44. Using this approach, all of the database schemas would be created by the Vertica database administrator and not by the `opsa-server-postinstall.sh` script.

- **Adding more Operations Analytics Servers**: As your Operations Analytics environment expands, you might need to add more Operations Analytics Servers. To do this, you would use the `opsa-server-postinstall.sh` script with the `-scaleout` option as described in the *Adding Operations Analytics Servers* section of the Operations Analytics Configuration Guide.

  Note: Operations Analytics supports a maximum of three Operations Analytics Servers). Run the `opsa-server-postinstall.sh` script on the first Operations Analytics Server without any options as shown in the **Common Approach**. Use the instructions located the *Adding Operations Analytics Servers* section of the Operations Analytics Configuration Guide to add more Operations Analytics Servers

- **Upgrading Operations Analytics** To upgrade from the previous version of Operations Analytics use the `opsa-server-postinstall.sh` script with the `-upgrade` option as shown in the HP Operations Analytics Upgrade Guide.

Complete the following post-installation configuration steps on the Operations Analytics Server.

Note: When it runs, the opsa-server-postinstall.sh script creates tables in the database. After these tables are created, you cannot run the the opsa-server-postinstall.sh script again.

If you run the `opsa-server-postinstall.sh` script using a database that already had schemas and tables created by a previous execution of this script, 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. This issue could occur if you attempted to run the `opsa-server-postinstall.sh` script more than once create on the same Operations Analytics Server to create the Operations Analytics schemas and tables.

To run the `opsa-server-postinstall.sh` script more than once, you must drop all of the tables or you must drop the existing opsadb database and create a new one before running the `opsa-server-postinstall.sh` script again. Thethe `opsa-server-postinstall.sh` script does not support connecting to an existing database schema. See the Vertica Administrator's Guide for more information.

Note: The Vertica Installation steps explained in "Task 2: Installing and Configuring the Vertica Software" on page 21 does not create the Operations Analytics schemas and tables. It only creates the opsadb database.

Prework: Setting up the Vertica Database

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

Note: Although not mandatory, is recommended that this created database user be a superuser. If you choose not to make this created database user a superuser, the Vertica database administrator must create database schemas before configuring Operations Analytics or any Operations Analytics tenants. See **Option 2** below for more information.

Before running the `opsa-server-postinstall.sh` script, do one of the following:

- **Option 1: Have the post-installation script prepare the database**

  Verify that a dbadmin database user (superuser) exists that has access to the Vertica database. This was accomplished if you used **Approach 1** to install Vertica in "Task 2: Installing and

Configuring the Vertica Software" on page 21. Continue with "Running the Post-Installation Script" below.

- **Option 2: Manually prepare the database:**

  If the Vertica database administrator does not want Operations Analytics to automatically create an Operations Analytics dbadmin 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 the 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);`

  Note: If you use **Option 2**, you must run the `-skipSchemaCreation` option when running the `opsa-server-postinstall .sh` script in the next section.

  Continue with "Running the Post-Installation Script" below.

Running the Post-Installation Script

Complete the following post-installation configuration steps on the Operations Analytics Server:

1. Log on as an opsa user to the Operations Analytics Server (the default password is opsa).

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

2. Run only one of the following commands:

   - **If using Option 1 from the previous section**: `$OPSA_HOME/bin/opsa-server-postinstall.sh` script (interactive mode).
   - **If using Option 2 from the previous section**: `$OPSA_HOME/bin/opsa-server-postinstall.sh -skipSchemaCreation` script (interactive mode).

3. The `opsa-server-postinstall.sh` script prompts for the 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: Use either `dbadmin` or the <*newusername*> you created earlier.

- Vertica database password

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 2: Installing and Configuring the Vertica Software" on page 21 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 will not create the opsadb database on the Vertica server.

Note: If you already have the opsadb schemas and tables created on your opsadb database dur to running the `opsa-server-postinstall.sh` script more than once, you must drop all of the tables or you must drop the existing opsadb database and create a new one before running

the `opsa-server-postinstall.sh` script. The opsa-server-postinstall.sh script does not support connecting to an existing database schema. See the Vertica Administrator's Guide for more information.

Note: Although this document refers to the Vertica database name for Operations Analytics as opsadb, you can choose a different name when creating this database.

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 opsaadmin, 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 lowercase characters, and a digit character.

   Note: See "Predefined User Groups" on page 9 for more information about the predefined user groups, default user names, and passwords used by Operations Analytics.

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

     Note: Logger version 6.0 and newer supports peer Logger configurations. This means that if you plan to add a Logger host name that is configured for peer searches, you would not want to add multiple Loggers from this peer group when running this `opsa-server-postinstall.sh` script. Doing so would result in searches being initiated by multiple Loggers from the same peer group . See the ArcSight Logger Administrator's Guide for

more information about configuring Loggers for peer searching.

- Logger Webservice port
- Logger Webservice username
- Logger Webservice password

Note: These Logger details will be persisted to the database using the `opsa_default` schema. If the log management software is `arcsight`, you can configure more than one Logger using the `opsa_default` schema.

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 Operations Analytics Server.

Post-Installation Steps for the Operations Analytics Collector Host

Complete the following post-installation configuration steps on the Operations Analytics Collector host.

1. Log on as a opsa user to the Operations Analytics Collector host (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), and includes the default values shown in the following list. To accept the default value, click **Enter** for each prompt.

   Note: Although this document refers to the Vertica database name for Operations Analytics as opsadb, you can choose a different name when creating this database.

   - 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 2: Installing and Configuring the Vertica Software" on page 21 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.

Optional Step: The Operations Analytics Collector host uses a timeout and reconnect approach to connect to the Vertica database. To optimize operating system resources and reduce the operating system resources used for networking (improving operating system resource utilization), consider shortening the TCP timeout period by completing these steps:

Note: Using these steps to shorten the TCP timeout period does not only affect communication with Vertica. It also affects all TCP connections on the Operations Analytics Collector host on which you make this change.

1. As root, edit the `/etc/sysctl.conf` file on the Operations Analytics Collector host. by appending the following lines.
2. Append the following lines to the end of the`/etc/sysctl.conf` file that you are editing:

   Note: The following numbers only show how you would change the values within the`/etc/sysctl.conf` file. Substitute values that relate to the performance of the system you are using.

   ```
   net.ipv4.tcp_fin_timeout = 30
   net.ipv4.tcp_keepalive_time = 30
   ```

3. Save your work.
4. As root, run the following command on the Operations Analytics Collector host to apply the changes you made:

   ```
   sysctl -p
   ```

That completes the post-installation configuration steps for the Operations Analytics Collector host.

Note: Your next steps are to register this Operations Analytics Collector host with the Operations Analytics Server you installed, then begin configuring collections.

You must register each Operations Analytics Collector host you plan to use with the Operations Analytics Server. See *Registering Each Collector Appliance* in the *Operations Analytics Configuration Guide* for more information.

Out of the Box Log Content

"Out of the Box SmartConnector Types" on the next page provides a description of the out of the box SmartConnector types available with Operations Analytics. These SmartConnectors are automatically installed on the Operations Analytics Server and Collector hosts.

In order to see the out of the box content for non-Operations Analytics servers in Operations Analytics Dashboards, you must install SmartConnectors that are pre-configured for standard Windows, Linux, and Apache logs on each non-Operations Analytics server that you plan to use. See "Installing the Out of the Box SmartConnectors" on the next page for SmartConnector installation information.

Out of the Box SmartConnector Types

The Out of the Box SmartConnector types shown in the following table are available:

Platform	Connector Type	Description
Microsoft Windows	Microsoft Windows Event Log - Local	Monitors the following Windows logs: • Windows Application Log • Windows Security Log • Window System Event Log If required, you can configure additional logs with this connector.
Linux	Linux Audit File	Monitors the audit log.
	Linux Syslog File	Monitors predefined system files, including the following: Syslog, Cron, Mail, and Secure. **Note**: If you must monitor more than one log, for example both the Syslog and Cron logs, you must install this SmartConnector type separately for each log.
Apache	Apache HTTP Server Access File	
	Apache HTTP Server Error File	

Installing the Out of the Box SmartConnectors

Note: For general information about installing SmartConnectors, see the ArcSight Logger Configuration Guides.

You need to install the SmartConnectors on each non-Operations Analytics server that you plan to use. The Out of the Box SmartConnectors are located on the Operations Analytics Collector host in the `$OPSA_HOME/logfile` folder. You can use these files with the instructions shown in the *Configuring the Operations Analytics Log File Connector for HP ArcSight Logger* section of the Operations Analytics Configuration Guide to install the Out of the Box SmartConnectors on each computer that you want to monitor.

Accessing Operations Analytics for the First Time

To log on to Operations Analytics do the following:

1. Access the following URL: **http://*<IP Address or fully-qualified domain name of the Operations Analytics Server>*:8080/opsa**

2. After the Operations Analytics log on screen appears, use the default user credentials to log on to Operations Analytics:
   User Name: opsa
   Password: Use the password for this user that you set during installation

Click  to access the *Operations Analytics Help.*

Click the link in the upper right to **Go to Application**. Operations Analytics is not collecting data right now, but is otherwise operational.

Now you can configure your collections using information from the *Operations Analytics Configuration Guide*.

Chapter 4: Enabling the HP Operations Analytics- HP OneView Integration

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

Note: See http://www.hp.com/go/opsanalytics or http://www.hp.com/go/oneview for more information.

Licensing HP OneView

Operations Analytics comes with an Implicit node pack (Instant On) license that is valid for 60 days. You must purchase and install one of the following permanent licenses before the Instant On license expires:

- **Operations Analytics HP OneView node permanent license**: The Operations Analytics HP OneView node license enables the Operations Analytics HP OneView integration collections and features only.
- **Full Operations Analytics license (in 50 node pack) permanent license**: This license enables the full Operations Analytics collections and full features.

From the Operations Analytics console, navigate to **Help** > **About**, then click the **License** tab to view the type of license you have.

To install the Operations Analytics HP OneView node permanent license, do the following:

1. Copy the `license.dat` file issued by HP licensing service to the `/tmp` directory.
2. Run the following command as the opsa user to install the license:
   `$OPSA_HOME/bin/opsa-license-manager.sh -add /tmp/license.dat`
3. Run the following command as the opsa user and make sure the license you just installed is listed:
   `$OPSA_HOME/bin/opsa-license-manager.sh -list`

To install the 50 node pack permanent license, do the following:

1. Copy the `license.dat` file issued by HP licensing service to the `/tmp` directory.
2. Run the following command as the opsa user to install the license:
   `$OPSA_HOME/bin/opsa-license-manager.sh -add /tmp/license.dat`
3. Run the following command as the opsa user and make sure the license you just installed is listed:
   `$OPSA_HOME/bin/opsa-license-manager.sh -list`

See the *opsa-license-manager.sh* reference page (or the Linux manpage) for more information. To view Operations Analytics reference pages, select **> Reference Pages** in the Operations Analytics console,

Note: After installing a new license, from the Operations Analytics console, navigate to **Help > About**, then click the **License** tab to view the type of license you now have.

Configuring the HP Operations Analytics- HP OneView Integration

The information in this section explains how to enable and configure the Operations Analytics - HP OneView integration. Complete the work shown in each of the following notes before completing the steps shown below to enable the Operations Analytics - HP OneView integration.

Complete the following prerequisites:

- The Operations Analytics Server and the HP OneView Server must each be able to resolve each others fully-qualified domain names for the Operations Analytics - HP OneView integration to function correctly.

  Do the following before enabling the integration:

  a. Ping the fully-qualified domain name of the HP OneView server from the Operations Analytics Server.

  b. If the previous step is not successful, add the IP Address and fully-qualified domain name of the HP OneView server to the `hosts` file on the Operations Analytics Server.

- You must register the Operations Analytics Collector host you plan to use with the Operations Analytics Server. See *Registering Each Collector Appliance* in the Operations Analytics Configuration Guide for more information.

  Note: You need to know if you registered the Operations Analytics Collector host as an IP address or as a fully-qualified domain name. Write down the registration method you used for use in a later step.

- You must complete the licensing work in "Licensing HP OneView" on page 52 before completing the instructions in this section.
- You must have completed Task 1 through Task 7 as shown in "Installing Operations Analytics" on page 20.
- You must have installed the SysLog Daemon by following the instructions shown in the *Installing the Out of the Box SmartConnectors* section in "Out of the Box Log Content" on page 49. Run the installation on the SmartConnector and select the **SysLog Daemon**. You must point the SysLog Daemon to the SmartMessageReceiver.

Complete the following steps to enable and configure the Operations Analytics - HP OneView integration.

Note: When completing the following steps, if you receive a message that the HP OneView Integration failed, click **Integrate** to try configuring the integration again.

1. Install the ArcSight syslog connector on the Logger server by following the SmartConnector instructions from ArcSight.
2. Copy the `OneViewMapping.sdkrfilereader.properties` file from `/opt/HP/opsa/content-packs/oneview/logger/smart_connectors/syslog/OneViewMapping.sdkrfilereader.properties` on the Operations Analytics Server to `/opt/HP/opsa/content-packs/oneview/logger/structured_log_collection/OneViewMapping.sdkrfilereader.properties` file on the Logger server.
3. Run the following command, as root, on the Logger server to start the SysLog Daemon: `Service Arc_SysLog start`
4. Go to the Logger console and disable the UDP Receiver. Make sure that the Smart Receiver is enabled.
5. To configure the Operations Analytics - HP OneView integration, log on to Operations Analytics as the opsatenantadmin tenant administrator, then do the following:

   Note: Do not enable the Operations Analytics integration as a tenant administrator for a tenant you created. The Operations Analytics - HP OneView integration only supports the default tenant and does not support other tenants you create. The default tenant administrator is opsatenantadmin.

   a. The Operations Analytics **Welcome Page** appears.

   b. If this is the first time logging on as the opsatenantadmin tenant administrator, click the **Start Using Application** button and the HP OneView settings dialog box opens. If the HP OneView settings dialog box does not open, click **Settings** > **OneView Settings**.

c. Enter the following HP OneView setting information; then click **Integrate**.

- The fully-qualified domain name of the HP OneView server (or its IP address).
- The user name to use for the HP OneView server.
- The password for the user name you provide.
- The fully-qualified domain name (or IP address) of the Logger server.
- You will need to select one of the registered Operations Analytics Collector hosts and specify it in the same manner in which it was registered:
  - The fully-qualified domain name the Operations Analytics Collector host.
  - The IP address of the Operations Analytics Collector host.

  Note: If you do not remember the registration method you used, run the following command and determine the Operations Analytics Collector host parameter to use for this step.
  ```
  /opt/HP/opsa/bin/opsa-collection-config.sh -list –allversions –
  collectorhosts -username opsatenantadmin –password opsatenantadmin
  ```

  Note: This Operations Analytics Collector host is the one you plan to use for the Operations Analytics - HP OneView collections.
- The **Frequency** parameter adjusts how often Operations Analytics collects metric data from HP OneView. **Adjust this parameter carefully to avoid creating system resource issues**. If you leave the field for this parameter blank, Operations Analytics uses a default value of 3600 seconds (one hour). If you want to see faster results, you might set this value to 300 seconds (5 minutes).

If you encounter problems during setup, see "Troubleshooting the HP Operations Analytics- HP OneView Integration" on the next page for more information.

You can watch the integration messages as the configuration progresses. For example, you should see messages related to configuring certificates, syslog forwarding, metrics frequency, and security credentials.

Note: Assuming you used the default **Frequency** parameter shown earlier (this parameter adjusts how often Operations Analytics collects metric data), it can take up to one hour for HP OneView to forward a complete set of data to Operations Analytics.

After you finish integrating Operations Analytics with HP OneView you can view summary information for the infrastructure servers and analytics using the management data from HP OneView (log, metric, alerts, and inventory data).

Troubleshooting the HP Operations Analytics- HP OneView Integration

Use the following information to test and troubleshoot any issues with the Operations Analytics - HP OneView Integration.

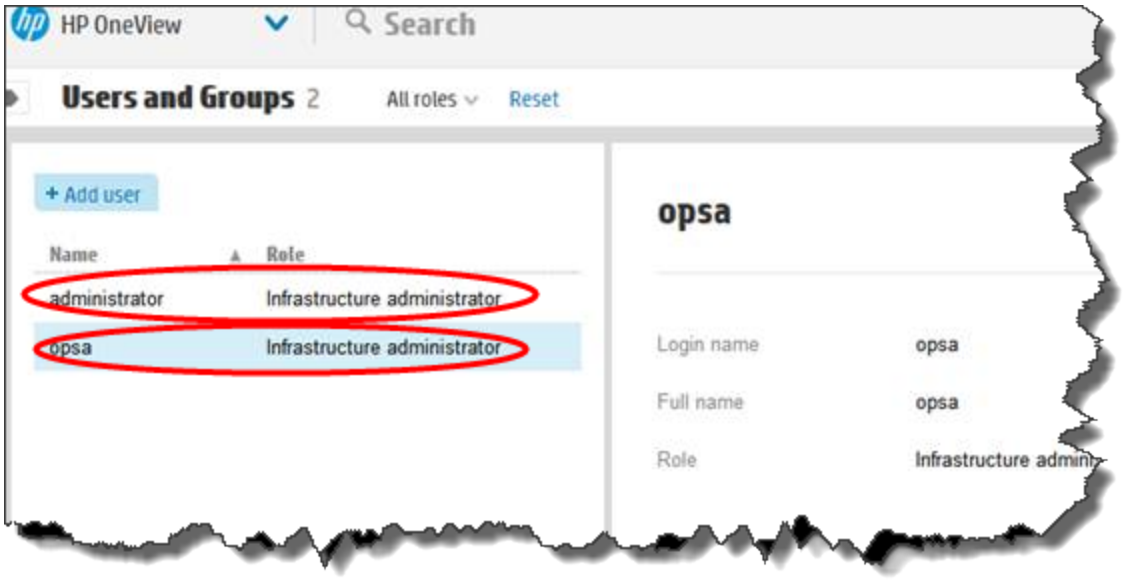
Note: It is mandatory that the Operations Analytics Server have a valid fully-qualified domain name for this integration to function successfully.

Question: When enabling the Operations Analytics - HP OneView integration, how might I avoid potential authentication problems?

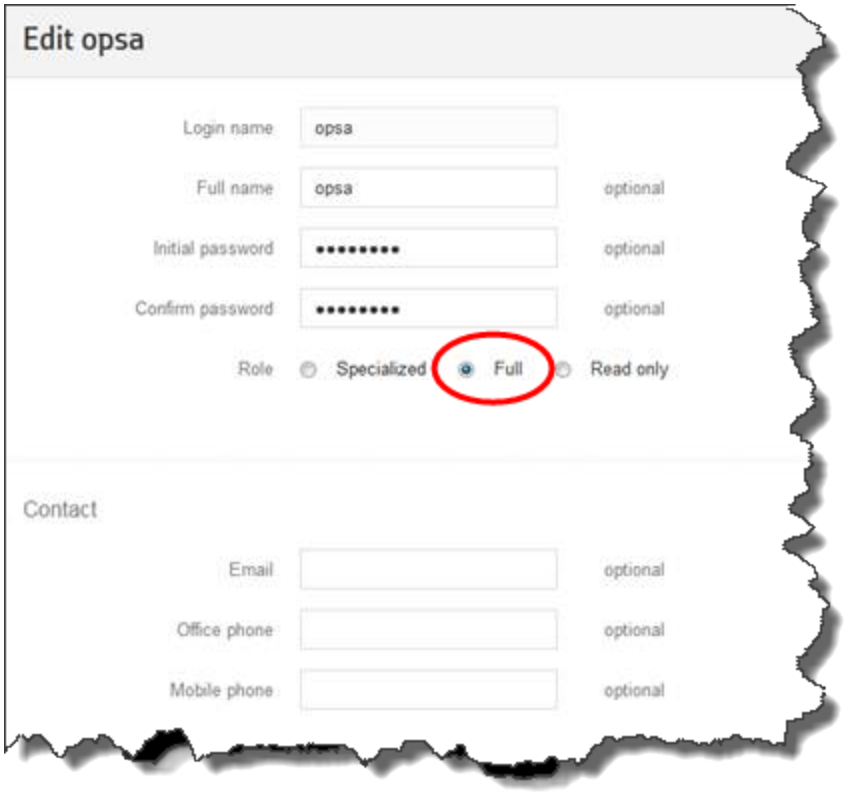
Answer: The role for the HP OneView user should have infrastructure administrator privileges.

Note: Use an existing user account or create a new user account to prevent potential authentication problems. For either approach, the user must have the infrastructure administrator role.

1. Log on to the HP OneView console.
2. Navigate to **Settings** > **users and groups**.
3. **Do only one of the following** from the HP OneView console:
   - Choose an existing infrastructure administrator for the integration like the **administrator** or **opsa** user shown below.



- Create an infrastructure administrator for the integration. Make sure to select the **Full** role when creating the infrastructure administrator.



Question: After enabling the Operations Analytics - HP OneView integration, how do I make sure that the syslog forwarding is functioning correctly?

Answer: To verify that the syslog forwarding is functioning correctly for HP Integrated Lights-Out (iLO), do the following:

1. Log on to the HP OneView server.
2. Select **Servers** > **Server Hardware** from the HP OneView console.
3. Locate the **Hardware** heading, scroll to the **iLO** row, then click the associated IP address to log on to the **Integrated Lights-Out** console.
4. Select **Administration** > **Management**.
5. Select the **Remote Syslog** tab.
6. Check that the IP address entry in the remote Syslog Server field matches the IP address of the Operations Analytics server.

Question: After enabling the Operations Analytics - HP OneView integration, how do I make sure that the metrics are functioning correctly?

Answer: You should see metrics within one hour or less. Check any of the HP OneView dashboards in Operations Analytics and verify that the metric data is appearing.

Note: You can adjust the frequency of the metrics by adjusting the `Frequency` option in the HP OneView settings.

Question: After enabling the Operations Analytics - HP OneView integration, how do I make sure that the syslog forwarding is functioning correctly for Enclosures?

Answer: To verify that the syslog forwarding is functioning correctly for Enclosures, do the following:

1. Log on to the HP Blade System Onboard Administrator (OA)
2. Select **Active Onboard Administrator**.
3. Click **System Log**.
4. Click the **Log Option** tab.
5. Check that the IP address entry in the remote Syslog Server field matches the IP address of the Operations Analytics server.

Note: If you use a hostname instead of an IP Address for these fields, and the network uses statically assigned IP addresses, you must configure a DNS server in the EBIPA settings.

Question: When setting up the integration, you see one or more integration error messages. For example, these messages might involve configuring certificates, syslog forwarding, metrics frequency, or security credentials. What should you do?

Answer: Follow any remedies included in the displayed error messages. If there are no displayed remedies, do the following:

1. Log on to Operations Analytics as a tenant administrator user.
2. Select **Settings** > **OneView Settings**
3. Configure the Operations Analytics- HP OneView integration and see if this action corrects the problem.

> **Note:** To remedy any of the problems you might encounter, complete the above steps before doing any further troubleshooting or opening a support call.

Question: When setting up the integration, where can I find relevant data?

Answer: Look for the following files in the`/opt/HP/opsa/log` directory:

- `collection_config.log` (usually the most informative)
- `collection-manager.log`
- `collection-setup.log`

About Data Collections for the HP Operations Analytics - HP OneView Integration

The following collections begin collecting data automatically after you configure the Operations Analytics - HP OneView integration:

HP OneView Data Collections

Collection Name	Source	Domain	Group
HP OneView Alerts	oneview	rabbitmq	alerts
HP OneView Interconnect Metrics	oneview	rest	Interconnect_metrics
HP OneView Inventory	oneview	rest	inventory
HP OneView Inventory Changes	oneview	rabbitmq	inventory-changes
HP OneView Metrics	oneview	rabbitmq	metrics
HP OneView Syslog	arcsight	OneView	OneViewSyslogs
HP OneView Trees	oneview	rest	topologytree

Note: The property group uid for each preconfigured Operations Analytics for HP OneView collection consists of a combination of the source, domain, and group parameters used to create the collection. For example, for the Operations Analytics for HP OneView Inventory collection, it uses a domain of rest and a group of inventory when creating the collection. The resulting property group uid is oneview_rest_inventory.

Using the HP Operations Analytics - HP OneView Integration

After you finish configuring the Operations Analytics - HP OneView integration, the Operations Analytics - HP OneView data collections begin adding data to the dashboards included with the Operations Analytics- HP OneView integration. See *Operations Analytics Integration with HP OneView* in the *Operations Analytics Help* for more information about the benefits of this integration.

HP Operations Analytics - HP OneView Integration Security Hardening

- **Authentication**: The Operations Analytics for HP OneView Inventory and Tree collections use the Rest API. This collection requires user names and passwords. The Operations Analytics for HP OneView Inventory Changes, Metrics and Alerts collections require the certificates that are stored in keystore and truststore files. These two stores require password authentication.
- **Key Management**: These keys are stored in the `/opt/HP/opsa/conf/ssl/opsa_defaults` directories.
- **Encryption**: Operations Analytics's Inventory Changes, Metrics and Alerts collections require the passwords for the keystore and truststore used by the HP OneView server. These passwords are encrypted.
- **User Permissions**: To configure the Operations Analytics - HP OneView integration, log on to Operations Analytics as a tenant administrator. See the Operations Analytics Configuration Guide for information about configuring the Operations Analytics users.
- **Certificates**: After you click the **Integrate** button, Operations Analytics sends the HP OneView host, user name, and password to the HP OneView server. The HP OneView server returns the certificate data in forms that Operations Analytics places in the `/opt/HP/opsa/conf/ssl/opsa_defaults` directories on the Operations Analytics Server. After the Operations Analytics for HP OneView collections are published (this happens automatically during the integration setup), Operations Analytics moves these files to the Operations Analytics Collector host.
- **Data being Collected**: The Operations Analytics for HP OneView collections obtain data from HP OneView, which includes logs, metrics, HP OneView alerts, and topology data.

Note: logs originate from the devices that HP OneView currently manages (they come from HP OneView-managed servers and enclosures). These logs are really syslogs.

Chapter 5: Obtaining Licenses

After purchasing Operations Analytics, you will need to download three licenses, one each for Operations Analytics, Vertica, and HP ArcSight Logger, and apply these licenses later. To obtain your licenses, do the following:

1. Using your browser, navigate to the licensing link shown in the license email you received (`www.hp.com/software/licensing`).
2. Log on using **HP Passport** credentials. You will need to register if you do not have HP Passport credentials .
3. When prompted, enter your order numbers.
4. Follow the instructions to download and apply your Operations Analytics, Vertica, and HP ArcSight Logger licenses.

Chapter 6: Maintenance Tasks

Use the information in this section to complete any necessary maintenance tasks.

Installer Troubleshooting

How to Change the Installer Working Directory

In Linux, you can change the Installer's working directory (by default `/tmp` by running the following commands:

```
export IATEMPDIR=/new/tmp/dir
export _JAVA_OPTIONS=-Djava.io.tmpdir=/new/tmp/directory
```

where `/new/temp` is the new working directory.

Restarting Operations Analytics Processes

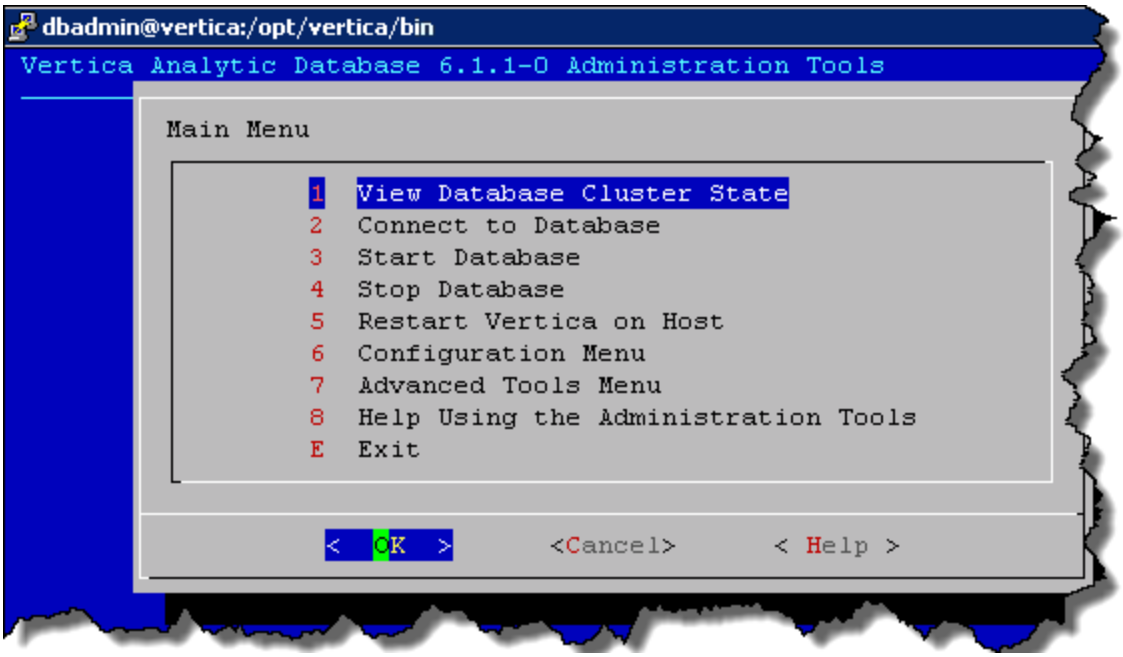
There are times when the Operations Analytics might abruptly shut down, as in during a power outage, network issue, or other unintended shutdown. For the Operations Analytics processes to function correctly, the Vertica database must completely start up before restarting the Operations Analytics processes. If the Vertica database is not available when the Operations Analytics processes start up, these processes might not function correctly.

To make sure the Operations Analytics processes start up correctly, do the following

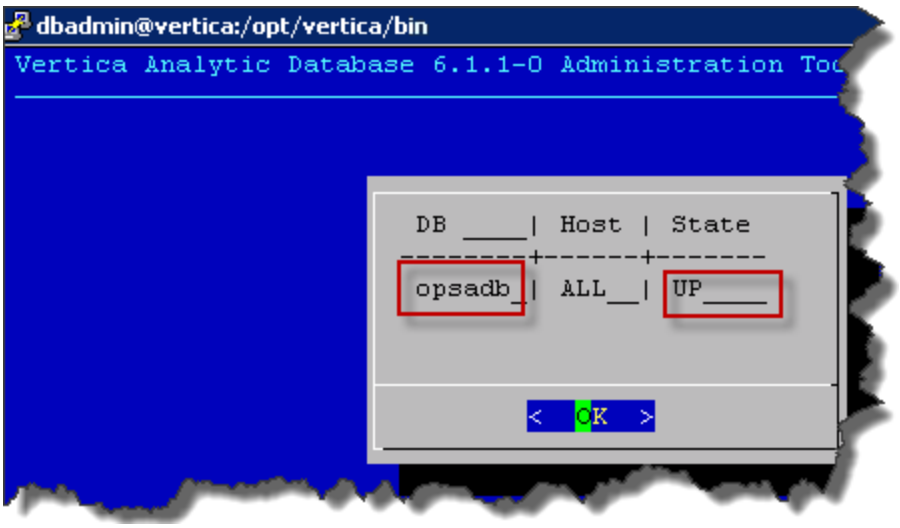
1. Do the following on the Vertica server to check the database:

   a. Run the `su -dbadmin` command.

   b. Run the `/opt/vertica/bin/adminTools` command.You should see a screen similar to the following:



   c. Enter 1 to view the state of the database; then click **OK**. You should see a screen similar to the following if the opsadb database is running:



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

e. If the database is not up, wait a few minutes, then rerun the previous steps to recheck the database.

> **Note:** Do not start the Operations Analytics processes until the Vertica database is running.

2. Run the `opsa status` command on all of the Operations Analytics Server and Collector hosts. For each server that does not have processes running, run the `opsa start` command.

3. After five minutes, check to see that you can open the Operations Analytics console .

Chapter 7: Operations Analytics Security Hardening

The following information is a summary of the security hardening recommendations for Operations Analytics.

Note: The hardening instructions shown in this section are optional. Complete the instructions in this section if you are interested in securing your Operations Analytics installation.

Disabling Unnecessary CentOS Services

Complete the following actions to make your Operations Analytics installation more secure:

- If you are not planning to use Virtual Appliance Management Infrastructure services, disable the vami-lighttp and vami-sfcbd services using the following commands:

  a. `chkconfig --level 35 vami-lighttp off`

  b. `service vami-lighttp stop`

  c. `chkconfig --level 35 vami-sfcb off`

  d. `service vami-lighttp stop`

- If you are not planning to use Network File System (NFS) mapping to the Operations Analytics Server, disable the rpcgssd, rpcsvcgssd, rpcidmapd, and nfslock services using the following commands:

  a. `chkconfig --level 345 rpcgssd off`

  b. `service rpcgssd stop`

  c. `chkconfig --level 345 rpcsvcgssd off`

  d. `service rpcsvcgssd stop`

  e. `chkconfig --level 345 rpcidmapd off`

  f. `service vami-rpcidmapd stop`

  g. `chkconfig --level 345 nfslock off`

  h. `service nfslock stop`

- SSH login for the root account is disabled by default. Operations Analytics can only be accessed by using the default user name, opsa.
- It is highly recommended that you disable the SSH weak ciphers. To do this, the configuration entries already reside in the `sshd_config` file and need to be uncommented as follows:

  Note: Not all SSH clients support the new ciphers. Make sure that your SSH client supports them.

  a. As the root user, edit the `sshd_config` file.

  b. To uncomment the following two lines, change:
  ```
  # Ciphers aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc
  # MACs hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160
  ```
  to
  ```
  Ciphers aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc
   MACs hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160
  ```

  c. Save your work.

  d. As a root user, run the following command to commit your changes: `service sshd restart`
- It is highly recommended that you use a secure protocol (HTTPS) to access Operations Analytics.
- Enable the CentOS firewall (iptables) allowing, at a minimum, the following traffic:
  - Allow all traffic from and to Loopback adapter: `iptables -A INPUT -i lo -j ACCEPT`
  - Allow traffic from anywhere to SSH port: `iptables -A INPUT -p tcp --dport ssh -j`
  - Allow traffic from and to Vertica DB: `iptables -A INPUT -s [Vertica DB IP] -j ACCEPT`
  - Allow traffic from DNS servers:
    ```
    iptables -A INPUT -p udp --sport 53 -j ACCEPT
    iptables -A INPUT -p udp --dport 53 -j ACCEPT
    ```
  - Allow traffic to Operations Analytics web server:
    HTTP: `iptables -A INPUT -p tcp --dport 8080 -j ACCEPT`
    HTTPS: `iptables -A INPUT -p tcp --dport 8080 -j ACCEPT`
  - If you do not have any other special requirements, drop all other traffic: l `iptables -A INPUT -j DROP`

Encrypting Operations Analytics

Each Operations Analytics Server uses a separate encryption key to provide secure data for each Operations Analytics deployment.

Operations Analytics provides the `opsa-key-manager.sh` script. If you want to modify the encryption password and salt for an Operations Analytics installation, do the following from the Operations Analytics Server:

1. Run the `opsa-key-manager.sh` script as a user with super-admin credentials.
2. When prompted, follow the instructions shown by the `opsa-key-manager.sh` script.
3. After the `opsa-key-manager.sh` script completes, Operations Analytics has a new encryption key and salt.

See the *opsa-key-manager.sh* reference page (or the Linux manpage), for more information. To view Operations Analytics reference pages, select  **> Reference Pages** in the Operations Analytics console,

Securing Browsers

Internet Explorer, Chrome, and Firefox do not recognize `autocomplete=off` in web forms. As a result, when you log on to Operations Analytics you might be prompted to remember your log on credentials (depending on your browser configuration).

If you are an end user of Operations Analytics, and do not want your log on credentials (user name and password) remembered,do the following:

- When prompted to store your log on credentials, acknowledge (to your browser) that you do not want your credentials saved by the browser.
- Often you can instruct your browser to stop prompting you to save credentials (for a given address).
- Often you can configure your browser to completely stop prompting you to save your passwords. If you prefer to disable this ability entirely, either configure this in the browser itself or work with your IT organization to create and deploy a corporate IT policy.

> **Note:** Refer to your browser documentation or contact your System Administrator for more details.

Other Security Considerations

Below are some other security items to consider.

- Deploy JBoss according to the security guidelines in your organization.
- Remove all external devices from your environment. These should include, but not be limited to, USB ports, CD drives, and other external media).
- Make it a regular habit to empty the temp drives on your servers.
- Keep your VMware tools updated.
- When selecting credentials to connect to the OMi database, it is recommended that you select a user with minimal credentials for reading the required information. Selecting a more powerful user could present a security vulnerability.

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 HP Operations Analytics Installation Guide (Operations Analytics 2.30)

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!