HP Operations Analytics

Software Version: 2.20

Operations Analytics Installation Guide

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

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

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.

For Information about Operations Analytics

To obtain a complete set of information about Operations Analytics (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 quickly install Operations Analytics	*Operations Analytics Quick Start Guide*
I want to install Operations Analytics	*Operations Analytics Installation Guide*
I want to configure and maintain Operations Analytics	*Operations Analytics Configuration Guide*
I want to upgrade Operations Analytics 2.10 to Operations Analytics 2.20	*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	*Operations Analytics Support Matrix*
I want to read a list of the new features and review any last minute issues for Operations Analytics	*Operations Analytics Release Notes*
I want to open a view from HP BSM to Operations Analytics	*Integration with HP BSM*

Documentation for Operations Analytics, continued

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

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 (Operations Analytics) Software, including the Operations Analytics Server Appliance and the Operations Analytics Collector Appliance. 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.

Table 1: Environment Variables

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

Table 2: Other Useful Directories

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

System Requirements

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

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

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

Known Issues and Workarounds

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

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

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

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

Terminology Used in this Document

Collection: Structured logs are fragments of log file data read by Operations Analytics (Operations Analtyics) from HP ArcSight Logger. This log information is stored (as collections) in Operations Analtyics. 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.

Collector Appliance: This virtual appliance is the server 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.

Server Appliance: This virtual appliance is the Operations Analytics Server.

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, such as VMware.

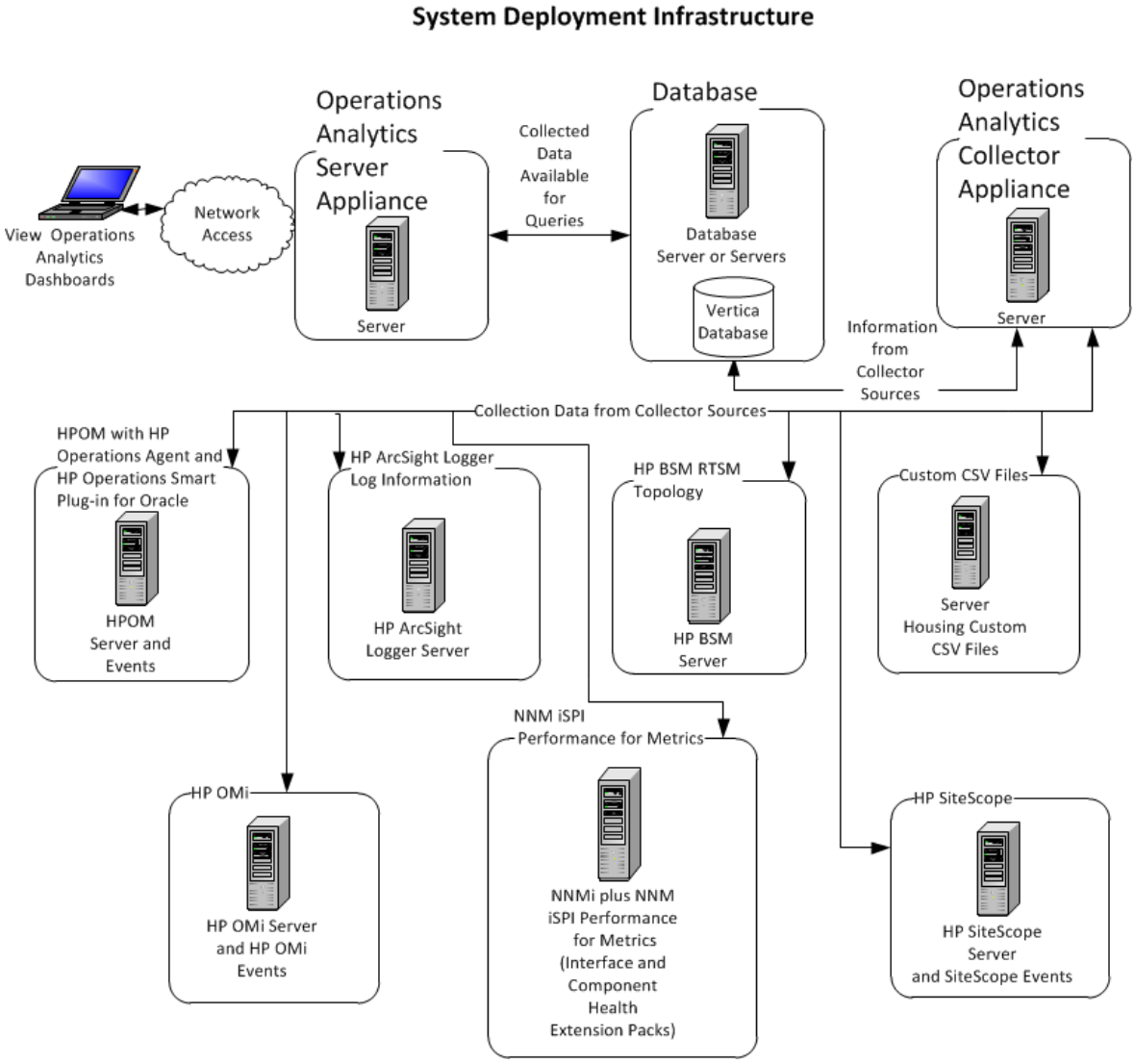
Chapter 2: Deployment Prerequisites

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 (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 *Operations Analytics Configuration Guide* for more information.

Note: For optimal results, configure the Operations Analtyics Server Appliance and the Operations Analtyics Collector Appliances to all be in UTC timezone.



Predefined User Groups

Operations Analytics (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.
- **Tenant Admin**: During installation, the opsatenantadmin user gets created, and assigned to the Tenant Admin user group. **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 user group 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.

Installation Overview

The following section provides an overview of the Operations Analytics (Operations Analytics) installation environment. Deploying Operations Analtyics is relatively easy and usually takes less than two hours to install and deploy.

This section includes:

- "Operations Analytics Components" below
- "Collection Sources" on the next page
- "Setting up Your Operations Analytics System" 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 Appliance**:
  - Provides the business logic and presentation capabilities of Operations Analytics.
  - Deployed as an OVA appliance.
  - 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 Appliance**:
  - 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.
  - Operations Analytics can have one or more Operations Analytics Collector Appliances, 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.

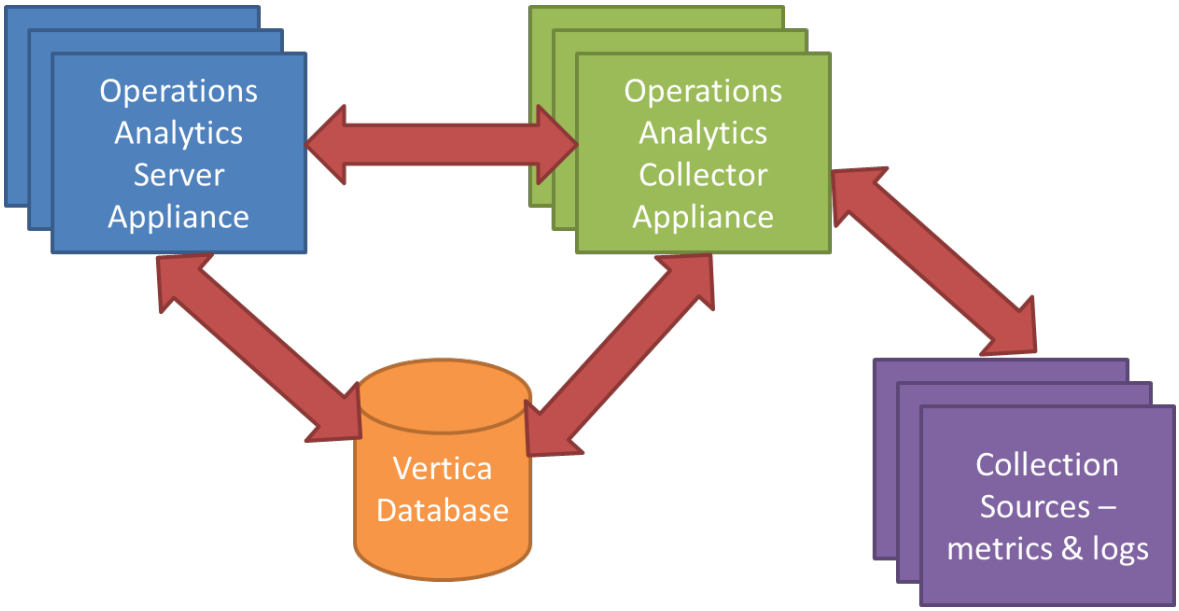
Collection Sources

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

These sources include:

- **BSM Portfolio metric collectors**. Operations Analytics supports data collection from various 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.
- **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 of Operations Analytics:



Setting up Your Operations Analytics System

System setup includes the following steps:

1. **Installation**:
   - Install the Operations Analytics Server Appliance (*mandatory).*
   - Install the Operations Analytics Collector Appliance (*mandatory).*
   - Install the Vertica Database (*optional* - you can connect to an existing Vertica instance).

   Note: If you are using an existing Vertica installation, you must manually create the opsadb database before running the post-install.

   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

2. **Post-Install Configuration**
   - This configuration step is only required if the database user is not a superuser: Unless manually created by the Vertica administrator, create the default tenant (opsa_default) and the opsa_default schemas (for the opsa_default tenant) on the opsadb database on Vertica.

   Note: If the database user is a superuser, then you only need to create the Vertica database. See "Post-Installation Configuration Steps for Operations Analytics" on page 49 for more information.

- Connect the Operations Analytics Server Appliances to the Vertica Database
- Connect the Operations Analytics Collector Appliances to the Vertica Database
- Configure the various 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 Appliance to collect system log data for self-monitoring log files from the Operations Analytics application – *optional.*

3. **Configure Collection Sources**:

   You may 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 various BSM data sources in order to collect metrics. Note that collection configuration creates a link between the Operations Analytics Server Appliance and the Operations Analytics Collector Appliance.
   - Install ArcSight Logger Server to collect logs, and then configure its connection to the Operations Analytics Collector Appliance.
   - Install Logger connectors (agents) on the different IT systems so they forward log information to the Logger Server, and subsequently into Operations Analytics.
   - Configure collection from Splunk.
   - Configure collection from additional data sources using the custom CSV 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 Appliances, 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 utilizes 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: 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 Appliance.

Well-Known Port Mapping

Port	Initiator	Sender	Receiver	Comments
383	Operations Analytics	OM Performance Agent and Database SPI	Operations Analytics Collector Appliance	
443 or 9000	ArcSight Connectors	HP ArcSight Logger, Operations Analytics Log File Connector for HP ArcSight Logger, ArcSight Connectors	HP ArcSight Logger	Can be configured in HP ArcSight Logger. By default, if installed as a privileged user it is 443, otherwise, it is 9000. Operations Analyticsdefault installation is 443
1433, 1521	Operations Analytics	OM or OMi Event	Operations Analytics Collector Appliance	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)	Syslog messages to HP ArcSight Logger Syslog Connector	HP ArcSight Logger Syslog Connector	These are the default values. These values might be changed by the ArcSight administrator.
2181 TCP	Operations Analytics Server Appliance	Twitter Storm	Operations Analytics Collector Appliance	Apache ZooKeeper connected by Twitter Storm instances running on Operations Analytics Collector Appliances.
2506, 2507	Operations Analytics	Business Process Monitor(BPM)	Operations Analytics Collector Appliance	

Well-Known Port Mapping, continued

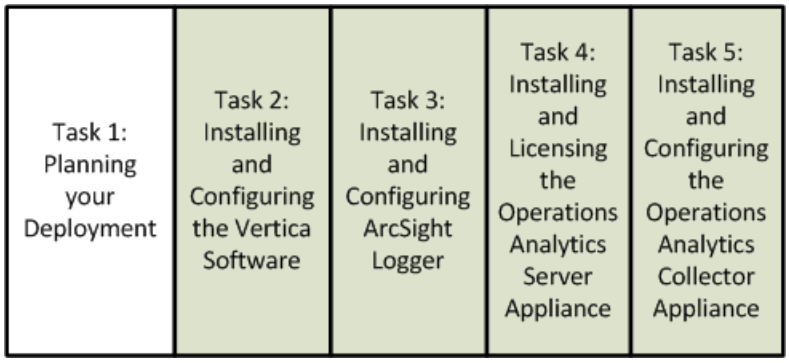
Port	Initiator	Sender	Receiver	Comments
5433	Operations Analytics	Vertica	Operations Analytics Collector and Server Appliances.	The default Vertica port is 5433. This default value can be changed by the Vertica administrator.
8080	Operations Analytics	SiteScope Collection Configuration	Operations Analytics Collector Appliance	Configuration utility communicates with Sitescope. This port might have been configured differently by Sitescope administrator. 8080 is the default port.
8089	Operations Analytics	Splunk	Operations Analytics Collector Appliance	
9443	SiteScope	SiteScope Data Collection	Operations Analytics Collector Appliance	
21212	Operations Analytics	RTSM Inventory	Operations Analytics Collector Appliance	
No Port Requirements	No Port Requirement	NNM iSPI Performance for Metrics	Operations Analytics Collector Appliance	This communication is by CSV. The requirement is for CSV files exported from NNMi to be put in a folder where Operations Analytics can obtain them.
No Port Requirement	No Port Requirement	NNMi Custom Poller	Operations Analytics Collector Appliance	This communication is by CSV. The requirement is for CSV files exported from NNMi to be put in a folder where Operations Analytics can obtain them.

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 35
4. "Task 4: Installing and Licensing the Operations Analytics Server Appliance using the VMware vSphere Client" on page 44
5. "Task 5: Installing and Configuring the Operations Analytics Collector Appliance using the VMware vSphere Client" on page 47

Task 1: Planning your Deployment

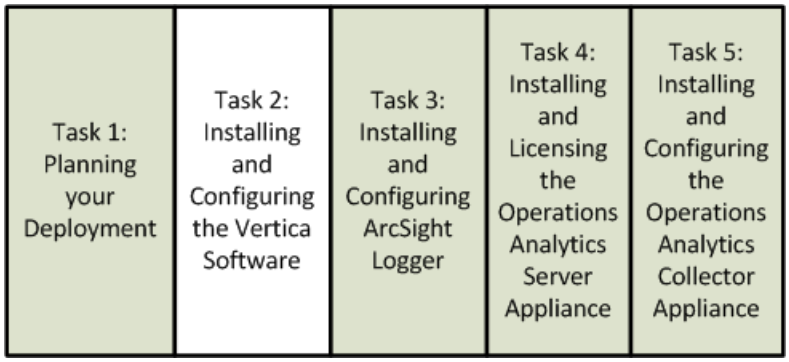


Use the following checklist to prepare for configuring Operations Analytics (Operations Analytics):

1. ☑ Review the following Topics:
   - "Terminology Used in this Document" on page 7
   - "Supported Deployments" on page 9
   - Operations Analytics Release Notes
   - Operations Analytics Support Matrix
2. ☑ Review the information in "Operations Analytics Port Mapping" on page 14 and open the well-known ports discussed in that section before installing Operations Analytics).

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 (Operations Analytics) stores configurations and collected data. The instructions in this section explain three ways to use Vertica with Operations Analytics.

Note: Operations Analytics includes the `vertica-<version>.x86_64.RHEL5.rpm` file for the Vertica installation and the `vertica-R-lang-<version>x86_64.RHEL5.rpm` for the R Language Pack from Vertica. Use these packages for optimum Vertica performance. Look for these files in the `Opsa 2.2 Integrations` directory on the product media in the `opsa-vertica-<version>.tar.gz` file.

You can also find the Vertica installation files in the `Documentation_OSRB_Third_parties.zip` file within the **Get Documentation** section of the download page.

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 "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 "Operations Analytics-Related Extensions" on page 21.

  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 "Install a New Vertica Installation Cluster with Operations Analytics-Related Extensions" on page 24.

Wizard-Driven Installation of Vertica as a Single Node

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

2. From the temporary location, extract the `opsa-vertica<version>.tar.gz` file using the following command: `tar -zxvf opsa-vertica-<version>.tar.gz`

3. From the temporary location, run the following command to begin the Vertica installation:
   `./opsa-vertica_2.00_setup.bin`
   Follow the interactive instructions until the Vertica installation is complete.

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

   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.

4. 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.

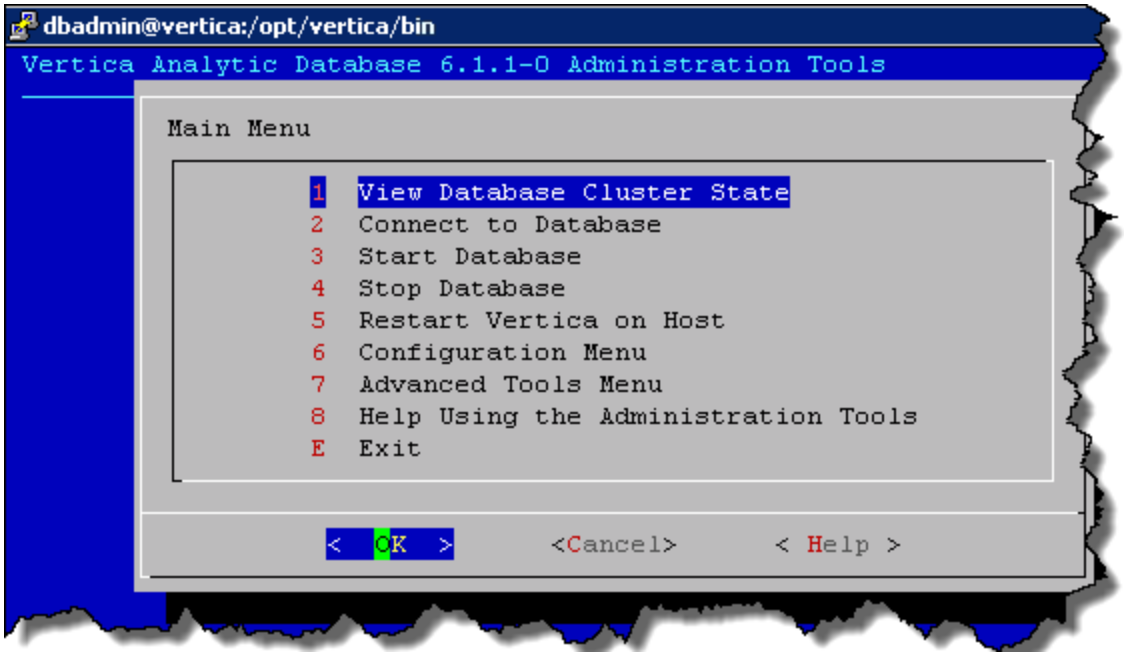
ii. Run the following command to change the password:
`alter user dbadmin identified by '<new password>';`

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

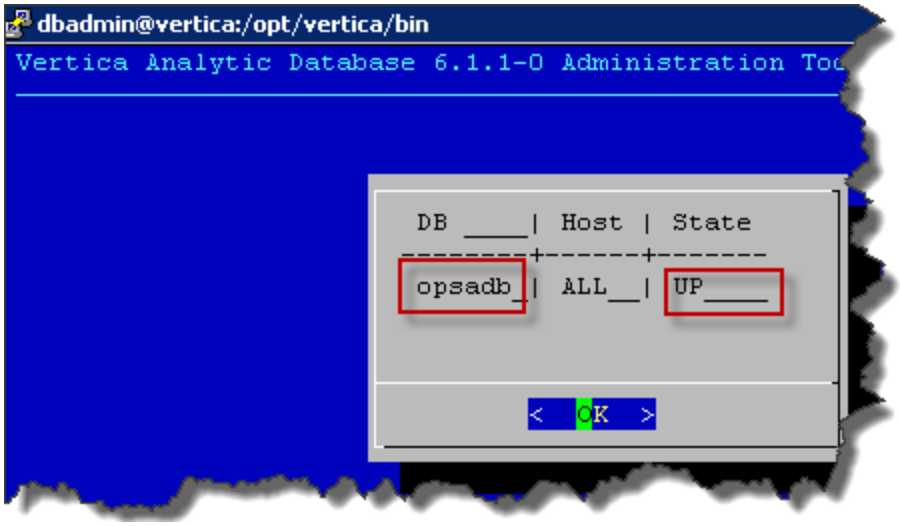
b. Do the following to check the database:

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

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 Analtyics 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.

As a possible solution to this issue, change the `KEEPALIVE` setting to a value lower than the firewall timeout using this command as an example. 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`

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), you must install the R Language Pack. Do the following:

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 a moderate amount of disk space once you have it running, so put it on a large disk.

Do the following:

1. As a root user, run the following commands to install libgfortran:

   Note: The following commands will not work without an Internet connection. Make sure you have an Internet connection before running the following commands.

   - **RHEL 6 and CentOS6**: `yum install compat-libgfortran-41`
   - **RHEL 5 and CentOS 5**: `yum install libgfortran`

2. Download the R Language Pack for Vertica. The R Language Pack must match the version of Vertica you plan to use. For example, suppose you have Vertica version 6.1.1 installed, and that Operations Analytics supports that Vertica version. You must use R Language Pack version 6.1.1, as it matches the Vertica version you are using.

   a. Using a browser, navigate to the following URL: https://my.vertica.com/download-community-edition

      Note: This URL varies depending on your Vertica account type. Use the URL for the Vertica product you purchased.

   b. Log on and download the R Language Pack.

3. Complete the remaining steps in this section for each one of the Vertica cluster nodes.
   Copy the following files from the `integrations` folder in the media to the `/home` directory:

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

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

4. If step 1 failed due to a connection error, run the following command: `yum install /usr/lib64/libgfortran.so.1`

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

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

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

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

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

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

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

9. Run the following command to start the R Language Pack installation:
   `rpm –Uvh vertica-R-lang_VERSION.rpm`
   After the installation completes, the R Language Pack installation is done.

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

    a. Run the following command: 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`

11. Complete the following steps to install the MASS package:
    a. Run the following command to set the correct permissions: `chmod 770 MASS_7.3-23.tar.gz`

    b. Copy the `/home/MASS_7.3-23.tar.gz` file to `/root/MASS_7.3-23.tar.gz`

    c. Run the following command: `/opt/vertica/R/bin/R CMD INSTALL /root/MASS_7.3-23.tar.gz`

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

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

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

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 Analtyics 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.

As a possible solution to this issue, change the `KEEPALIVE` setting to a value lower than the firewall timeout using this command as an example. 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`

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 "Task 3: Installing and Configuring HP ArcSight Logger" on page 35.

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:

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

2. From the temporary location, extract the `opsa-vertica-<version>.tar.gz` file using the following command: `tar -zxvf opsa-vertica-<version>.tar.gz`

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

3. Install Vertica as a cluster mode using the `vertica-R-lang-6.1.3-12.x86_64.RHEL5.rpm` file along with the other files extracted from the `opsa-vertica-`

<version>.tar.gz file during the previous step. For full installation details see the Vertica Installation Guide.

4. Complete the remaining steps in this section for each one of the Vertica cluster nodes.
   Copy the following files from the `integrations` folder in the media to the `/home` directory:
   - `GammaDistribution.R`
   - `MASS_7.3-23.tar.gz`
   - `libgfortran-4.1.2-52.el5_8.1.x86_64.rpm`
   - `create_R_GammaDist.sh`
   - `vertica-R-lang-6.1.3-12.x86_64.RHEL5.rpm`

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

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

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

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

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

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

9. Run the following command to start the R Language Pack installation:
   `rpm –Uvh vertica-R-lang_VERSION.rpm`
   After the installation completes, the R Language Pack installation is done.
10. Verification: To verify the R Language Pack installation, do the following:

a. Run the following command: 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`

11. Complete the following steps to install the MASS package:
    a. Run the following command to set the correct permissions: `chmod 770 MASS_7.3-23.tar.gz`

    b. Copy the `/home/MASS_7.3-23.tar.gz` file to `/root/MASS_7.3-23.tar.gz`

    c. Run the following command: `/opt/vertica/R/bin/R CMD INSTALL /root/MASS_7.3-23.tar.gz`

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

13. Run the following command as the dbadmin user to create and start opsadb:

    ```
    /opt/vertica/bin/adminTools -t create_db -d opsadb -p dbadmin --hosts=127.0.0.1
    ```

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

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

16. The Vertica database admin user is `dbadmin`, and its default password is `dbadmin`. It is recommended that you change the default password now. Do the following to change the password:

    a. Run the following command to log on to the `opsadb` database using the `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.

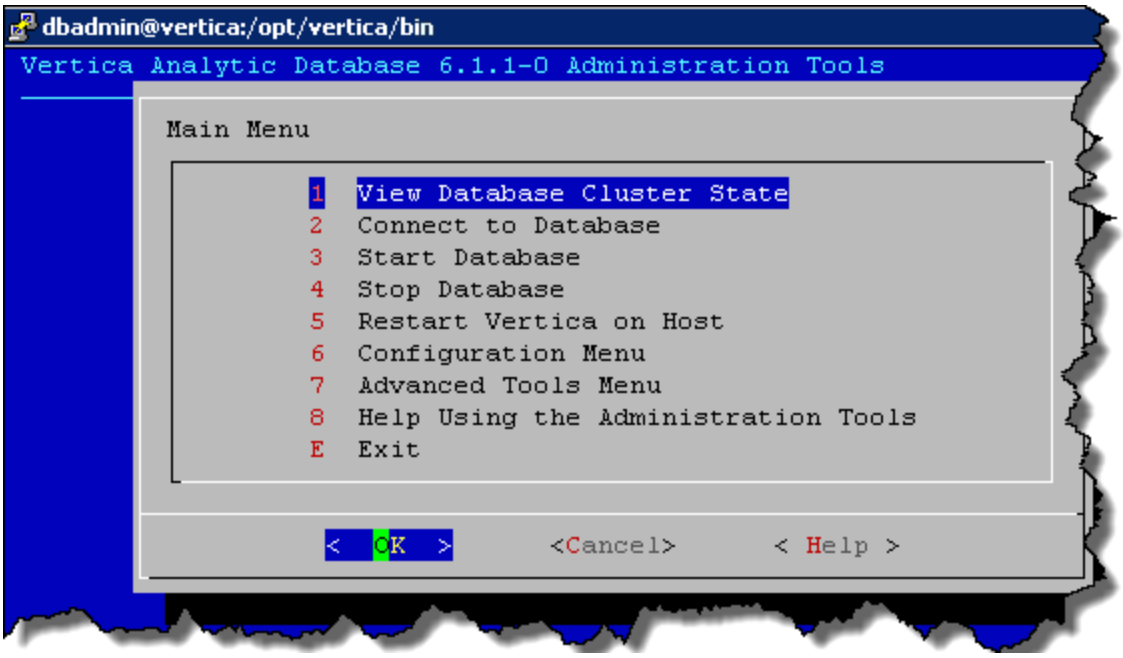
    b. Run the following command to change the password:
    `alter user dbadmin identified by '<new password>';`

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

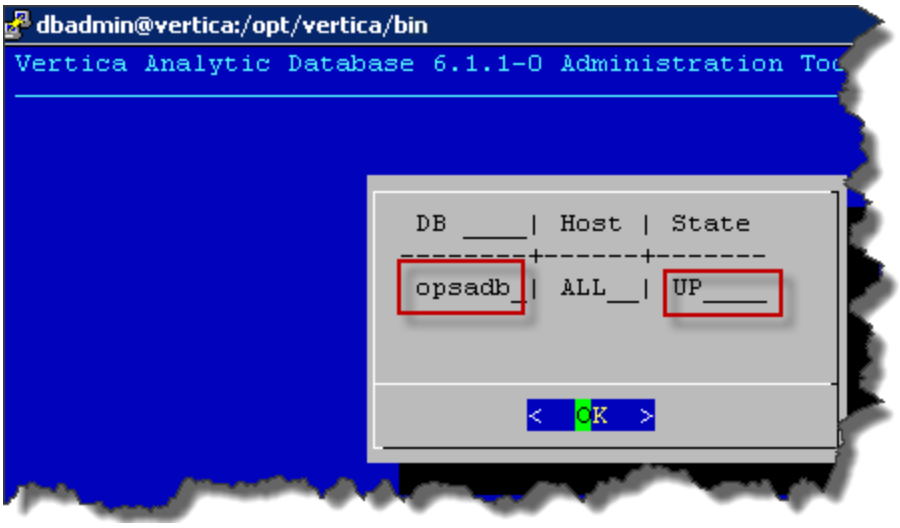
17. Do the following to check the database:

a. Run the `su -dbadmin` command.

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



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



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

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

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 Analtyics 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.

As a possible solution to this issue, change the `KEEPALIVE` setting to a value lower than the firewall timeout using this command as an example. 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`

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

If you do not plan to use the optional Vertica Load Balancer, continue your installation at "Task 3: Installing and Configuring HP ArcSight Logger" on page 35.

Optional: Installing and Configuring the Load Balancer

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

Note: See the *Vertica Enterprise Edition 6.1 Administrator's Guide* for more information about Load Balancing.

To configure the Load Balancer, use the information in the following sections:

"Configuring Vertica Nodes" on the next page

"Configuring the Directors" on page 32

"Connecting to the Virtual IP " on page 35

Configuring Vertica Nodes

This section describes how to configure a Vertica cluster of nodes for load balancing. You'll set up two directors in a master/slave configuration and include a third node for K-safety.

A Vertica cluster designed for load balancing uses the following configuration:

- **Real IP (RIP)** address is the public interface and includes:
  - The master director/node, which handles the routing of requests. The master is collocated with one of the database cluster nodes.
  - The slave director/node, which communicates with the master and takes over routing requests if a master node failure occurs. The slave is collocated with another database cluster node database cluster, such as at least one failover node to provide the minimum configuration for high availability. (K-safety).
- **Virtual IP (VIP)** address (generally assigned to eth0 in Linux) is the public network interface over which database clients connect.

> **Note:** The VIP must be public so that clients outside the cluster can contact it.

After you have set up a Vertica cluster and created a database, you can choose the nodes that will be directors. To achieve the best high-availability load balancing result when K-safety is set to 1, ensure that the IPVS master node and the slave node are located on Vertica database nodes with a buddy projections pair. (See High Availability Through Projections for information about buddy projections.)

The instructions in this section use the following node configuration:

Pre-configured IP	Node assignment	Public IPs	Private IPs
VIP	shared among all nodes	10.10.51.180	
RIP master director	node01	10.10.51.55	192.168.51.1
RIP slave director	node02	10.10.51.6	192.168.51.2
RIP failover node	node03	10.10.51.57	192.168.51.3

Notes

- In the above table, the private IPs determine which node to send a request to. They are not the same as the RIPs.
- The VIP must be on the same subnet as the nodes in the Vertica cluster.
- Both the master and slave nodes (node01 and node02 in this section) require additional installation

and configuration, as described in "Configuring the Directors" on page 32.

- Use the `cat /etc/hosts` command to display a list of all hosts in your cluster.

See Also

The following external web sites might be useful. The links worked at the last date of publication, but Vertica does not manage this content.

Linux Virtual Server Web site: **http://www.linux-vs.org/**
LVS-HOWTO Page: **http://www.austintek.com/LVS/LVS-HOWTO/HOWTO**
Keepalived.conf(5) man page: **http://linux.die.net/man/5/keepalived.conf**
ipvsadm man page:
http://at.gnucash.org/.vhost/linuxcommand.org/man_pages/ipvsadm8.html

Set Up the Loopback Interface

This procedure sets up the loopback (lo) interface with an alias on each node.

1. Log on as root on the master director (node01): `su - root`
2. Use the text editor of your choice to open `ifcfg-lo`:
   `[root@node01]# vi /etc/sysconfig/network-scripts/ifcfg-lo`
3. Set up the loopback adapter with an alias for the VIP by adding the following block to the end of the file:
   ```
   ## vip device
   DEVICE=lo:0
   IPADDR=10.10.51.180
   NETMASK=255.255.255.255
   ONBOOT=
   NAME=loopback
   ```

   Note: When you add the above block to your file, be careful not to overwrite the 127.0.0.1 parameter, which is required for proper system operations.
4. Start the device: `[root@node01]# ifup lo:0`
5. Repeat steps 1-4 on each node in the Vertica cluster.

Disable Address Resolution Protocol (ARP)

This procedure disables ARP (Address Resolution Protocol) for the VIP.

1. Log on as root on the master director (node01): `su - root`
2. Use the text editor of your choice to open the `sysctlo` configuration file:
   `[[root@node01]# vi /etc/sysctl.conf`
3. Add the following block to the end of the file:
   ```
   #LVS
   net.ipv4.conf.eth0.arp_ignore =1
   ```

```
net.ipv4.conf.eth0.arp_announce = 2
# Enables packet forwarding
net.ipv4.ip_forward =1
```

Note: For additional details,see the **LVS-HOWTO Page**:
http://www.austintek.com/LVS/LVS-HOWTO/HOWTO/.

You might also see the **Linux Virtual Server Wiki page**:
http://kb.linuxvirtualserver.org/wiki/Using_arp_announce/arp_ignore_to_disable_ARP
The **Linux Virtual Server Wiki page** provides information about using `arp_announce/arp_ignore` to disable the Address Resolution Protocol.

4. Use ifconfig to verify that the interface is on the same subnet as the VIP: `[root@node01]# /sbin/ifconfig`
In the following output, the eth0 `inet addr` is the VIP, and subnet 51 matches the private RIP under the eth1 heading:

```
eth0
Link encap:Ethernet HWaddr 84:2B:2B:55:4B:BE
inet addr:10.10.51.55 Bcast:10.10.51.255 Mask:255.255.255.0
inet6 addr: fe80::862b:2bff:fe55:4bbe/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:91694543 errors:0 dropped:0 overruns:0 frame:0
TX packets:373212 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:49294294011 (45.9 GiB) TX bytes:66149943 (63.0 MiB)
Interrupt:15 Memory:da000000-da012800

eth1
Link encap:Ethernet HWaddr 84:2B:2B:55:4B:BF
inet addr:192.168.51.55 Bcast:192.168.51.255 Mask:255.255.255.0
 inet6 addr: fe80::862b:2bff:fe55:4bbf/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:937079543 errors:0 dropped:2780 overruns:0 frame:0
TX packets:477401433 errors:0 dropped:0 overruns:0 carrier:0 collisions:0
txqueuelen:1000
 RX bytes:449050544237 (418.2 GiB) TX bytes:46302821625 (43.1 GiB)
 Interrupt:14 Memory:dc000000-dc012800

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
 inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:6604 errors:0 dropped:0 overruns:0 frame:0
TX packets:6604 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:0
 RX bytes:21956498 (20.9 MiB) TX bytes:21956498 (20.9 MiB)
```

```
 lo:0
Link encap:Local Loopback
 inet addr:10.10.51.180 Mask:255.255.255.255
UP LOOPBACK RUNNING MTU:16436 Metric:1
```

5. Use `ifconfig` to verify that the loopback interface is up:
   `[root@node01]# /sbin/ifconfig lo:0`
   You should see output similar to the following:
   ```
   lo:0 Link encap:Local Loopback
   inet addr:10.10.51.180 Mask:255.255.255.255
   UP LOOPBACK RUNNING MTU:16436 Metric:1
   ```
   If you do not see `UP LOOPBACK RUNNING`, bring up the loopback interface:
   `[root@node01]# /sbin/ifup lo`
6. Issue the following command to commit changes to the kernel from the configuration file:
   `[root@node01]# /sbin/sysctl -p`
7. Repeat steps 1-6 on all nodes in the Vertica cluster.

Configuring the Directors

Now you are ready to install the Vertica IPVS Load Balancer package and configure the master (node01) and slave (node02) directors.

1. Copy the following compressed Vertica installation file from the downloaded installation files to a temporary location:
   `opsa-vertica-1.00.tar.gz`
2. Extract the `opsa-vertica-1.00.tar.gz` file using the following command:
   `tar -zxvf opsa-vertica-1.00.tar.gz`
3. Navigate to the `packages` directory.
4. Run one of the following commands to install the Load Balancer:
   - `rpm –ivh VerticaIPVSLoadBalancer-6.1-0.RHEL6.x86_64.rpm`
   - `rpm –ivh <packages folder path>/VerticaIPVSLoadBalancer-6.1-0.RHEL6.x86_64.rpm`

Configure the Vertica IPVS Load Balancer

```
Vertica provides a script called configure-keepalived.pl in the IPVS Load Balancer
package. The script is located in /sbin, and if you run it with no options, it
prints a usage summary:
--ripips | Comma separated list of Vertica nodes; public IPs (for example,
10.10.50.116, and other addresses.)
--priv_ips | Comma separated list of Vertica nodes; private IPs (for example,
192.168.51.116, and other addresses)
--ripport | Port on which Vertica runs. Default is 5433
```

```
--iface | Public ethernet interface Vertica is configured to use (for example,
eth0)
--emailto | Address that should get alerts (for example, user@server.com)
--emailfrom | Address that mail should come from (for example, user@server.com)
--mailserver | E-mail server IP or hostname (for example, mail.server.com)
--master | If this director is the master (default), specify --master
--slave | If this director is the slave, specify --slave
--authpass | Password for keepalived
--vip | Virtual IP address (for example, 10.10.51.180)
--delayloop | Seconds keepalived waits between healthchecks. Default is 2
--algo | Sets the algorithm to use: rr, wrr, lc (default), wlc, lblc, lblcr, dh,
sh, sed, nq
--kind | Sets the routing method to use. Default is DR.
--priority | By default, master has priority of 100 and the backup (slave) has
priority of 50
```

For details about each of these parameters, see the ipvsadm(8) - Linux man page **http://at.gnucash.org/.vhost/linuxcommand.org/man_pages/ipvsadm8.html**.

Public and Private IPs

If your cluster uses private interfaces for spread cluster communication, you must use the --priv_ips switch to enter the private IP addresses that correspond to the public IP addresses (or RIPs). The IPVS keepalive daemon uses these private IPs to determine when a node has left the cluster.

The IP host ID of the RIPs must correspond to the IP host ID of the private interfaces. For example, given the following IP address mappings:
Public Private (for spread)
10.10.50.116 192.168.51.116
10.10.50.117 192.168.51.117
10.10.50.118 192.168.51.118

you must enter the IP addresses in the following order:
--ripips 10.10.50.**116**,10.10.50.**117**,10.10.50.**118**
--priv_ips 192.168.51.**116**,192.168.51.**117**,192.168.51.**118**

You must use IP addresses, not node names, or the spread.pl script could fail.

If you do not specify private interfaces, Vertica uses the public RIPs for the MISC check, as shown in step 3 below.

Set up the Vertica IPVS Load Balancer Configuration File

1. On the master director (node01), log on as root:
   ```
   $ su- root
   ```

2. Run the Vertica-supplied configuration script with the appropriate switches; for example:
   ```
   # /sbin/configure-keepalived.pl --ripips 10.10.50.116,10.10.50.117,10.10.50.118
   --priv_ips 192.168.51.116,192.168.51.117,192.168.51.118 --ripport 5433
   --iface eth0 --emailto dbadmin@companyname.com
   --emailfrom dbadmin@companyname.com --mailserver mail.server.com
   --master --authpass password --vip 10.10.51.180 --delayloop 2
   ```

```
--algo lc --kind DR --priority 100
```

Caution: The --authpass (password) switch must be the same on both the master and slave directors.

3. Check `keepalived.conf` file to verify private and public IP settings for the `--ripips` and `--priv_ips` switches, and make sure the `real_server` IP address is public.
   `# cat /etc/keepalived/keepalived.conf`
   An entry in the keepalived.conf file would resemble the following:
   ```
   real_server 10.10.50.116 5433 {
   MISC_CHECK {
   misc_path "/etc/keepalived/check.pl 192.168.51.116"
   }
   }
   ```
4. Start spread:
   `# /etc/init.d/spread.pl start`

   The `spread.pl` script writes to the `check.txt` file, which is rewritten to include only the remaining nodes if a node failure occurs. Thus, the virtual server knows to stop sending vsql requests to the failed node.
5. Start keepalived on node01:
   `# /etc/init.d/keepalived start`
6. If not already started, start sendmail to permit mail messages to be sent by the directors:
   `# /etc/init.d/sendmail start`
7. Repeat steps 1-5 on the slave director (node02), using the same switches, except (**IMPORTANT**) replace the `--master` switch with the `--slave` switch.

   Tip: Use a lower priority for the slave --priority switch. Vertica currently suggests 50.

   ```
   # /sbin/configure-keepalived.pl --ripips
   10.10.50.116,10.10.50.117,10.10.50.118
   --priv_ips 192.168.51.116,192.168.51.117,192.168.51.118 --ripport 5433
   --iface eth0 --emailto dbadmin@companyname.com
   --emailfrom dbadmin@companyname.com --mailserver mail.server.com
   --slave --authpass password --vip 10.10.51.180 --delayloop 2
   --algo lc --kind DR --priority 100
   ```

   See Also
   Keepalived.conf(5) -Linux man page **http://linux.die.net/man/5/keepalived.conf**

Connecting to the Virtual IP

To connect to the Virtual IP address using vsql, issue a command similar to the following. The IP address, which could also be a DNS address, is the VIP that is shared among all nodes in the Vertica cluster.

```
$ /opt/vertica/bin/vsql -h 10.10.51.180 -U dbadmin
```

To verify connection distribution over multiple nodes, repeat the following statement multiple times and observe connection distribution in an lc (least amount of connections) fashion.

```
$ vsql -h <VIP> -c "SELECT node_name FROM sessions"
```

Replace `<VIP>` in the above script with the IP address of your virtual server; for example:

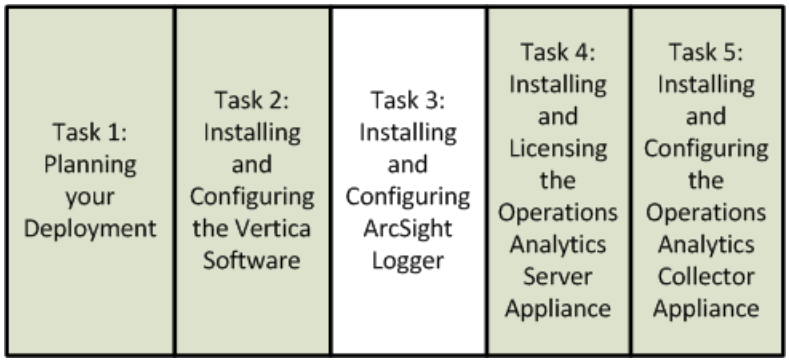
```
$ vsql -h 10.10.51.180 -c "SELECT node_name FROM sessions"
node_name
-----------------
v_ipvs_node01
v_ipvs_node02
v_ipvs_node03
(3 rows)
```

See the *Vertica Enterprise Edition 6.1 Administrator's Guide* for more information about performing other tasks related to the Load Balancer.

Task 3: Installing and Configuring HP ArcSight Logger

Follow the instructions in this section to install HP ArcSight Logger for use with Operations Analytics (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 Appliance using the VMware vSphere Client" on page 44



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

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

Prerequisites for Installation

Carefully read the following prerequisites and complete any required actions before installing HP ArcSight Logger:

- You must have downloaded the HP ArcSight Logger installation package.

  Note: See the Operations Analytics Support Matrix for a list of the supported Logger versions.

- You need a separate license file for each instance of HP ArcSight Logger. A license file is uniquely generated for each Enterprise version download.
- Make sure a non-root user account exists on the system on which you are installing HP ArcSight Logger. The non-root user must also be a non-system user with login permissions.
- Decide whether to install Logger while logged in as root or as a non-root user. Your installation options vary depending on which user you choose.
  - When you install as root, a non-root user account is still required.
  - When you install as root, you can choose to configure HP ArcSight Logger to start as a service and select the port on which HP ArcSight Logger listens for secure web connections.
  - When you install as a non-root user, HP ArcSight Logger can only listen for connections on port 9000. You cannot configure the port to a different value.
  - When upgrading, you cannot change the previous installation to a root-user installation. You will need to use the previously configured port 9000 for accessing HP ArcSight Logger software.
- The hostname of the server on which you are installing HP ArcSight Logger cannot be localhost. If it is, change the hostname before proceeding with the installation.
- **Important**: You must not have an instance of MySQL installed on the Linux server on which you will install HP ArcSight Logger. If an instance of MySQL exists on that server, uninstall it before installing HP ArcSight Logger.
- If you want to use the GUI mode of installation and will be installing HP ArcSight Logger over an SSH connection, make sure that you have enabled X window forwarding using the -X option so that you can view the screens of the installation wizard. If you will be using PuTTY, you will also need an X client on the machine from which you are connecting to the Linux machine.

- Installation on 64-bit systems requires glibc-2.12-1.25.el6.i686 and nsssoftokn- freebl-3.12.9-3.el6.i686. Install these packages if the installation fails with the following error message:
  `Installation requirements not met. Pre-install check failed: 32-bit compatibility libraries not found.`

Installation Modes

HP ArcSight Logger can be installed in the following modes:

- GUI: In this mode, a wizard steps you through the installation and configuration of HP ArcSight Logger. See "Using the GUI Mode to Install HP ArcSight Logger" below for more information.
- Console: In this mode, a command-line process steps you through the installation and configuration of HP ArcSight Logger. See "Using the Console Mode to Install HP ArcSight Logger" on page 40 for more information.

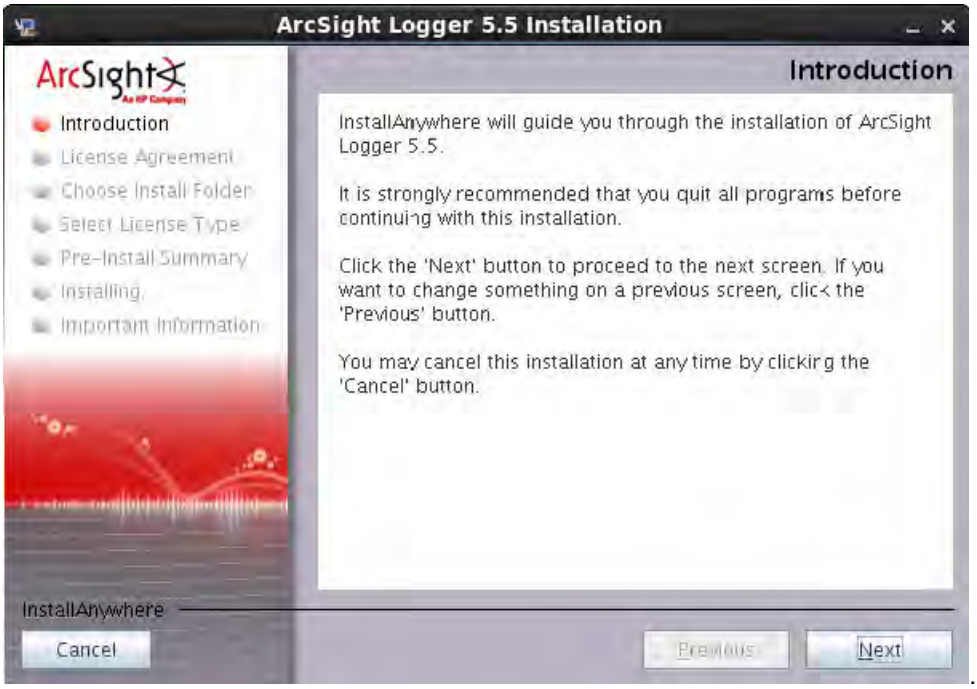
HP ArcSight Logger Installation Steps

This section describes two modes of HP ArcSight Logger installation.

Using the GUI Mode to Install HP ArcSight Logger

1. Obtain a supported copy of HP ArcSight Logger and copy the software into a separate directory.
2. Run the following two commands from the directory where you copied the HP ArcSight Logger software:
   ```
   chmod +x ArcSight-logger-5.5.0.XXXX.0.bin
   ./ArcSight-logger-5.5.0.XXXX.0.bin
   ```

3. The installation wizard launches, as shown in the following figure. Click **Next**



You can click Cancel to exit the installer at any point during the installation process.

Caution: Do not use the Ctrl+C to close the installer. If you use Ctrl+C to exit the installer and then uninstall HP ArcSight Logger, uninstallation may delete your /tmp directory.

4. The License Agreement screen is displayed. Scroll to the bottom of the license agreement to review the agreement and enable the **I accept the terms of the License Agreement** button.

5. Select **I accept the terms of the License Agreement** and click **Next**.

6. If HP ArcSight Logger is currently running on this server, an Intervention Required message is displayed. Click **Continue** to stop all current HP ArcSight Logger processes and proceed with the installation, or click or **Quit** to exit the installer.

   The installer stops the running HP ArcSight Logger processes and checks for other installation prerequisites. A message is displayed asking you to wait. Once all HP ArcSight Logger processes are stopped and the checks complete, the next screen is displayed.

7. Navigate to or specify the location where you want to install HP ArcSight Logger. By default, the /opt directory is specified.

   Note: The user as which you are installing can access the parent directory of the install directory. Otherwise, users will not be able to connect to the HP ArcSight Logger UI and will see the following error message when they try to connect, `Error 403 Forbidden. You don't have permission to access / on this server.`

8. If there is not enough space to install the software at the location you specify, a message is displayed. To proceed with the installation, specify a different location or make sufficient space at the location you specified. Click **Previous** to specify another location or **Quit** to exit the installer.

9. If HP ArcSight Logger is already installed at the location you specify, a message is displayed. Click **Upgrade** to continue or **Previous** to specify another location. For upgrade instructions and information, refer to the Release Notes for your version.

10. Indicate the type of license that you want to use.

    - To evaluate Logger using the trial license, select **No, use the trial license**, then click **Next**.

      If you start with a trial license, you can upload the license file for the Enterprise HP ArcSight Logger later. You do not need to upload a license to use the trial HP ArcSight Logger.

    - Selecting **Yes** requires that you have already purchased the Enterprise HP ArcSight Logger for a production environment and acquired a license file.

      If you have a valid license file, select **Yes**, then click **Next**.

      Click **Choose**, navigate to the license file for this HP ArcSight Logger software, then click **Next**.

11. Review the Pre-Installation Summary and click **Install**.
    Installation may take a few minutes. Please wait. Once installation is complete, the next screen is displayed.

12. If you are logged in as a root user on the system on which you are installing HP ArcSight Logger software, fill in the following fields and click **Next**.

Field	Notes
Non-root user name	This user must already exist on the system.
HTTPS port	The port number to use when accessing the HP ArcSight Logger UI. You can keep the default HTTPS port (443) or enter any other port that suits your needs. If you specify any port except 443, users will need to enter that port number in the URL they use to access the HP ArcSight Logger UI.
Configure HP ArcSight Logger as a service	Indicate whether to configure HP ArcSight Logger to run as a service. Select this option to create a service called arcsight_HP ArcSight Logger, and enable it to run at levels 2, 3, 4, and 5. If you do not enable HP ArcSight Logger to start as service during the installation process, you can still do so later. For instructions on how to enable HP ArcSight Logger to start as a service, see *System Settings* in the *ArcSight Logger Quick Start Guide*.

13. Select the locale of this installation and click **Next**.
14. Click **Next** to initialize HP ArcSight Logger components.

    Initialization may take a few minutes. Please wait. Once initialization is complete, the next screen is displayed.
15. Click **Next** to configure storage groups and storage volume and restart HP ArcSight Logger.

    Configuration may take a few minutes. Please wait. Once configuration is complete, HP ArcSight Logger starts up and the next screen is displayed.
16. Click **Done** to exit the installer.

> **Note:** Ensure that HP ArcSight Logger's publicly-accessible ports are allowed through any firewall rules that you have configured.
>
> For root installs, access to the port 443 must be allowed, plus the ports for any protocol that the logger receivers need, such as port 514 for the UDP receiver and port 515 for the TCP receiver.
>
> For non-root installs, access to port 9000 must be allowed, plus the ports for any protocol that the logger receivers need, such as port 8514 for the UDP receiver and port 8515 for the TCP receiver.
>
> The ports listed here are the default ports. Your Logger may use different ports.

Now that you are done installing and initializing HP ArcSight Logger, you can connect, log on, and start configuring HP ArcSight Logger to receive events.

Using the Console Mode to Install HP ArcSight Logger

Make sure the server on which you will be installing HP ArcSight Logger complies with the platform requirements listed in the Release Notes for your version, and that the prerequisites listed in "Prerequisites for Installation" on page 36 are met.

You can install HP ArcSight Logger as a root user or as a non-root user. See "Prerequisites for Installation" on page 36 for details and restrictions.

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

1. Run these commands from the directory where you copied the HP ArcSight Logger software:
   ```
   chmod +x ArcSight-logger-5.5.0.XXXX.0.bin
   ./ArcSight-logger-5.5.0.XXXX.0.bin -i console
   ```
2. The installation wizard launches in command-line mode, as shown below. Press **Enter** to

continue.
Introduction

InstallAnywhere will guide you through the installation of HP ArcSight Logger 5.5.

It is strongly recommended that you quit all programs before continuing with this installation.

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

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

PRESS <ENTER> TO CONTINUE:

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

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

4. Type `Y` and press `Enter` to accept the terms of the License Agreement.

5. The subsequent prompts are similar to the ones described for the GUI mode installation shown in "Using the GUI Mode to Install HP ArcSight Logger" on page 37. Follow the instructions provided for the GUI mode install to complete the installation.

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

The HP ArcSight Logger user interface is a web browser application using Secure Sockets Layer (SSL) encryption. Users must be authenticated with a name and password before they can use the interface. See the Release Notes document to find out the browsers and their versions supported for this release.

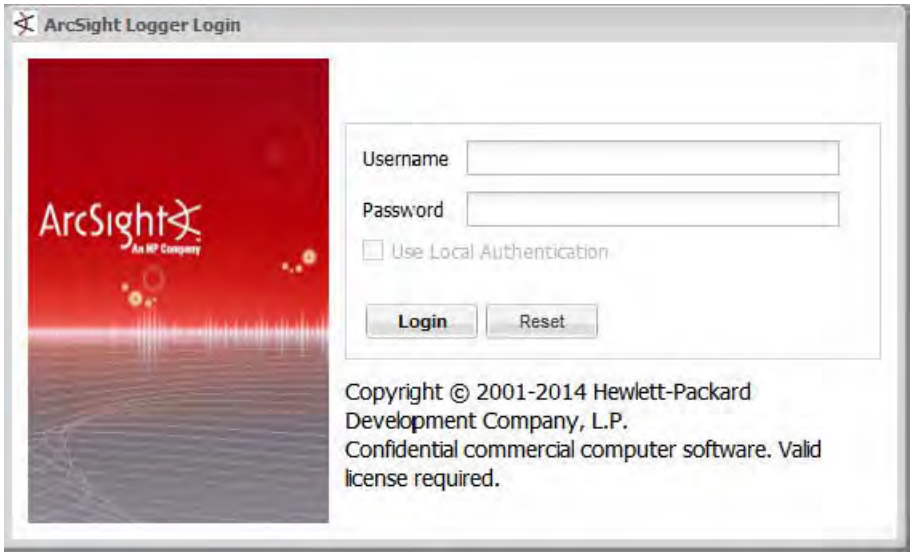
To connect and log into Logger, do the following:

1. Use the following URL to connect to Logger through a supported browser:
   `https://<hostname or IP address>:<configured_port>`

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

   After you connect, the following Log on screen is displayed.

2. Enter your user name and password, and click **Login**.



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

```
Username: admin
Password: password
```

4. After you have successfully logged in, go to the *Configuring Logger* section of the *HP ArcSight Logger Administrator's Guide* for information about how to set up Logger to start receiving events.

Note: For security reasons, be sure to change the default credentials as soon as possible after connecting to Logger for the first time. See "Changing Logger Passwords" on the next page for instructions.

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

Note: If there is an ArcSight connector available to collect the type of log file you must collect, use that connector. Only use the Operations Analytics Log File Connector for HP ArcSight Logger if an existing ArcSight connector does not meet your needs.

After you configure HP ArcSight Logger to receive the log files you are interested in, continue the installation at "Task 4: Installing and Licensing the Operations Analytics Server Appliance using the VMware vSphere Client" on page 44

Changing Logger Passwords

You can use the **Change Password** menu to change your password. This feature is available to all users for changing their passwords, unlike the **Reset Password** feature that enables a system administrator to reset the password of users without knowing the password. Passwords are subject to the password policy specified by the Admin user.

To change your password, do the following:

1. Click **System Admin** from the top-level menu bar.
2. Click **Change Password** in the Users/Groups section in the left panel to display the `Change Password for <User Name>` page.
3. Enter the `Old Password`, the `New Password`, and enter the `New Password` a second time to confirm.
4. Click **Change Password**.

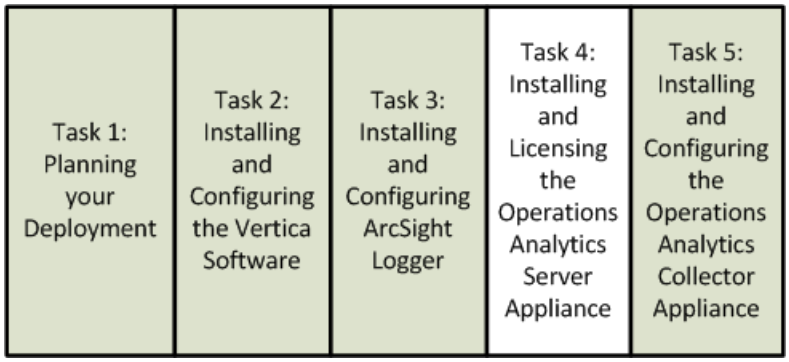
Configuring Multiple HP ArcSight Loggers

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.

Understanding the Operations Analytics Log File Connector for HP ArcSight Logger

During installation, the Operations Analytics Log File Connector for HP ArcSight Logger is installed automatically. It is also automatically configured for the Operations Analytics Collector and Server Appliances to collect Operations Analytics log events. If you want to make additional configuration changes for the Operations Analytics Log File Connector for HP ArcSight Logger, 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 Appliance using the VMware vSphere Client



The Operations Analytics (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.

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. Log on to the VMware vSphere Client.
2. Select **File** -> **Deploy OVF Template**.
3. Enter the URL or the file path of the `HP_Opsa_Server_OVF10.ova` file, based on where the OVA file is located; then click **Next**.

4. Specify a name and location for the deployed template.
5. Follow the instructions to select the host or cluster on which you want to deploy the Server Appliance; then click **Next**.
6. Select a resource pool.
7. Select the destination storage for the Server Appliance files; then click **Next**.
8. Select the format on which you want to store the virtual disks; then click **Next**.
9. Enter the network properties by specifying the field values shown in the following table.

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

Network Properties

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

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

Note: When logging on to the Operations Analytics Server Appliance for the first time, use one of the following authentication credentials:
User: `opsa`
Password: `opsa`

User: `root`
Password: `iso*help`

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

Installing the Operations Analytics License

Operations Analytics licensing is based on the number of Operations Analytics (OA) 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.

Note: To view the existing Operations Analytics license, navigate to **Help** > **About**> **License** from the Operations Analytics console.

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

An *Instant On* license gets applied during the Operations Analytics Server Appliance 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 either an *Evaluation* or *Permanent* license even though an Instant On license is already installed.
- Installing either of these 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 Appliance.

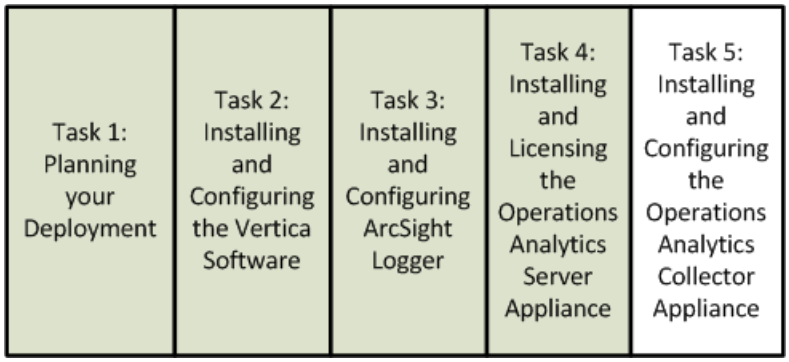
To install the Operations Analytics license, do the following:

1. Run the following command from the Operations Analytics Server Appliance 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.

Task 5: Installing and Configuring the Operations Analytics Collector Appliance using the VMware vSphere Client



Complete the following configuration steps for each Operations Analytics (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. Log on to the VMware vCenter server or directly to the VMWARE ESX server using the VMware vSphere Client.

2. Select **File** -> **Deploy OVF Template**.

3. Point your web browser to the following location: `http://<path to file>/HP_Opsa_Collector_OVF10.ova`; then click **Next**.

4. Specify a name and location for the deployed template.

5. Select the host or cluster on which you want to deploy the Operations Analytics Collector Appliance; then click **Next**.

6. Select a resource pool.
7. Select the destination storage for the Operations Analytics Collector Appliance files; then click **Next**.
8. Select the format on which you want to store the collector's virtual disks; then click **Next**.
9. 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 https://www.centos.org/docs/5/html/Deployment_Guide-en-US/s1-dhcp-configuring-client.html 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.

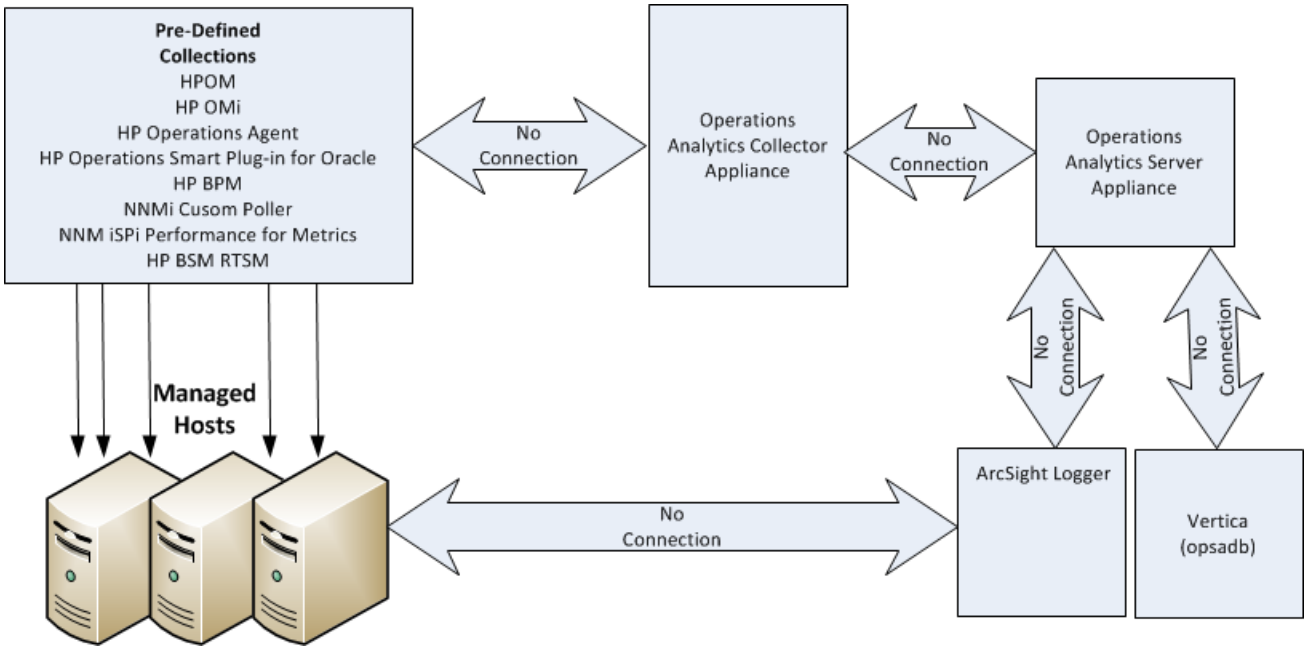
10. Specify the VA Host Name and Timezone settings; then click **Next**.
11. Select the **Power on after deployment** option; then click **Finish**.

Note: When logging on to the Operations Analytics Collector Appliance for the first time, use one of the following authentication credentials:
User: `opsa`
Password: `opsa`
User: `root`

Password: `iso*help`

Post-Installation Configuration Steps for Operations Analytics

The post installation script (opsa-server-postinstall.sh script) completes the final configuration steps for the different application components used by Operations Analytics (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 soon create.



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 Appliance

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

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

explaining how to run the `opsa-server-postinstall.sh` script to remedy an already configured Vertica database.

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

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

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

  Continue with "Running the Post-Installation Script" on the next page.

Running the Post-Installation Script

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

1. Log on as an opsa user to the 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 the `$OPSA_HOME/bin/opsa-server-postinstall.sh` script (interactive mode).

3. The `opsa-server-postinstall.sh` script prompts for following information, and includes a default value surrounded by brackets. To accept the default value, click **Enter** for each prompt.

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

     Note: 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 18 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 schema installed from a previous installation, you must delete it. The opsa-server-postinstall.sh script does not support connection to an existing database schema. You must drop the old opsadb database and create a new one before running the opsa-server-postinstall.sh script. See the *Vertica Enterprise Edition 6.1 Administrator's Guide* for more information

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 lower case characters, and a digit character.

   Note: See "Predefined User Groups" on page 10 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
- 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. The `opsa-server-postinstall.sh` script prompts you 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.
>
> 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 Appliance.

Post-Installation Steps for the Operations Analytics Collector Appliance

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

1. Log on as a opsa user to the Operations Analytics Collector Appliance (the default password is opsa).
2. Run the `$OPSA_HOME/bin/opsa-collector-postinstall.sh` script (interactive mode).
3. The `opsa-collector-postinstall.sh` script prompts for following Vertica database host details (where the `opsadb` database is created), 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 18 for more information.

4. The `opsa-collector-postinstall.sh` script prompts you to decide if you want to `Configure the OPSA Flex connector for ArcSight Logger [yes/no]`. For the remainder of these instructions the name for the OPSA Flex connector will be the Operations Analytics Log File Connector for HP ArcSight Logger. If you enter `no`, that completes the installation. If you enter `yes`, do the following:

a. Review the list of Logger hosts already configured for the opsa_default tenant.

b. Enter the serial number of the Logger host for which you want to configure the Operations Analytics Log File Connector for HP ArcSight Logger.

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

Out of the Box Log Content

In order to see the out of the box content in Operations Analytics (Operations Analytics) Dashboards, you need to install SmartConnectors that are pre-configured for standard Windows, Linux, and Apache logs.

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.

Platform	Connector Type	Description
	Linux Syslog File	Monitors predefined system files, including the following: Syslog, Cron, Mail, and Secure. **Note**: If you need to monitor more than one log, for example both the Syslog and Cron logs, you need to 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

You need to install the SmartConnectors on each computer that you want to monitor.

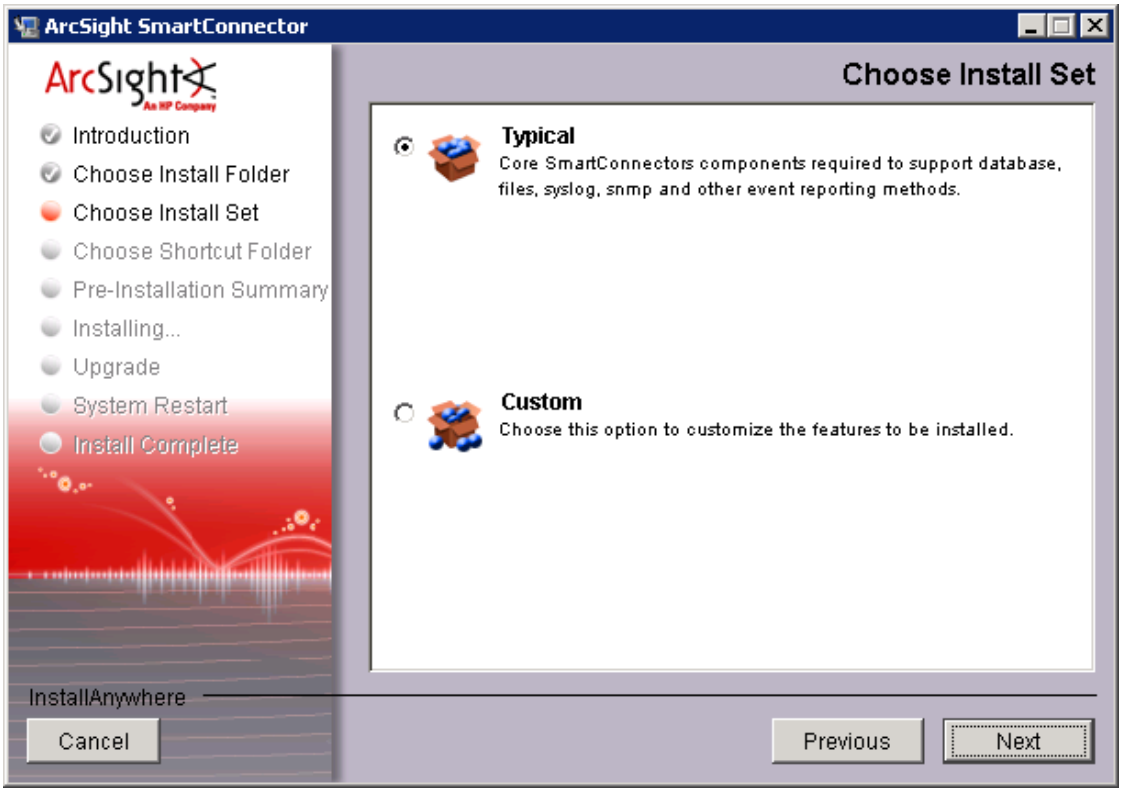
Note: For general information about installing SmartConnectors, see the ArcSight Logger Configuration Guides.

Note: The Out of the Box SmartConnectors are located on the Operations Analtyics Collector Appliance in the `$OPSA_HOME/logfile` folder.

1. Open the ArcSight Logger Smart Connector Installation wizard.
2. In the Choose Install Folder window, navigate to or specify the location where you want to install the SmartConnector and click **Next**.

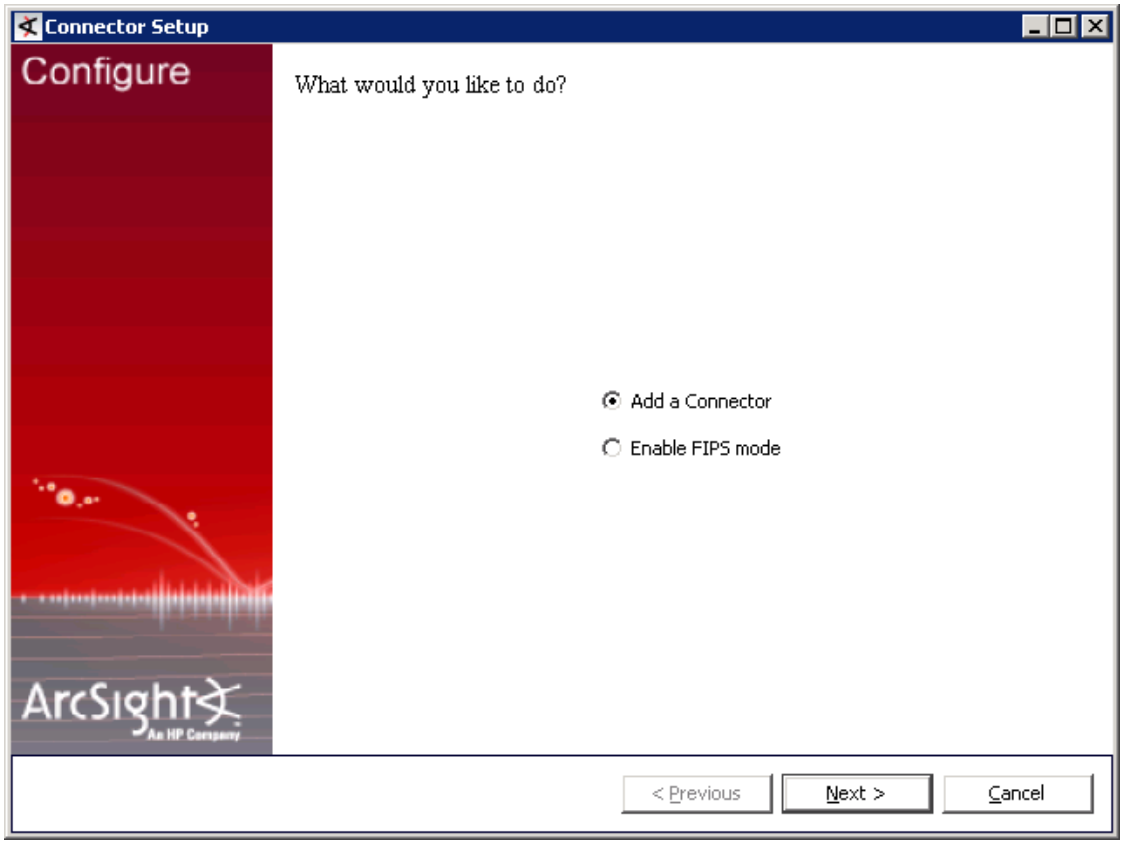
   Note: If you need to install more than one SmartConnector, each SmartConnector must be installed in a different folder.

   The Choose Install Set window opens.



3. Select **Typical** and click **Next**. The Choose Shortcut Folder window opens.
4. Select the required locations for the ArcSight icons, and click **Next**. The Pre-Install Summary window opens.

5. Click **Install** to open the Connector Setup wizard.

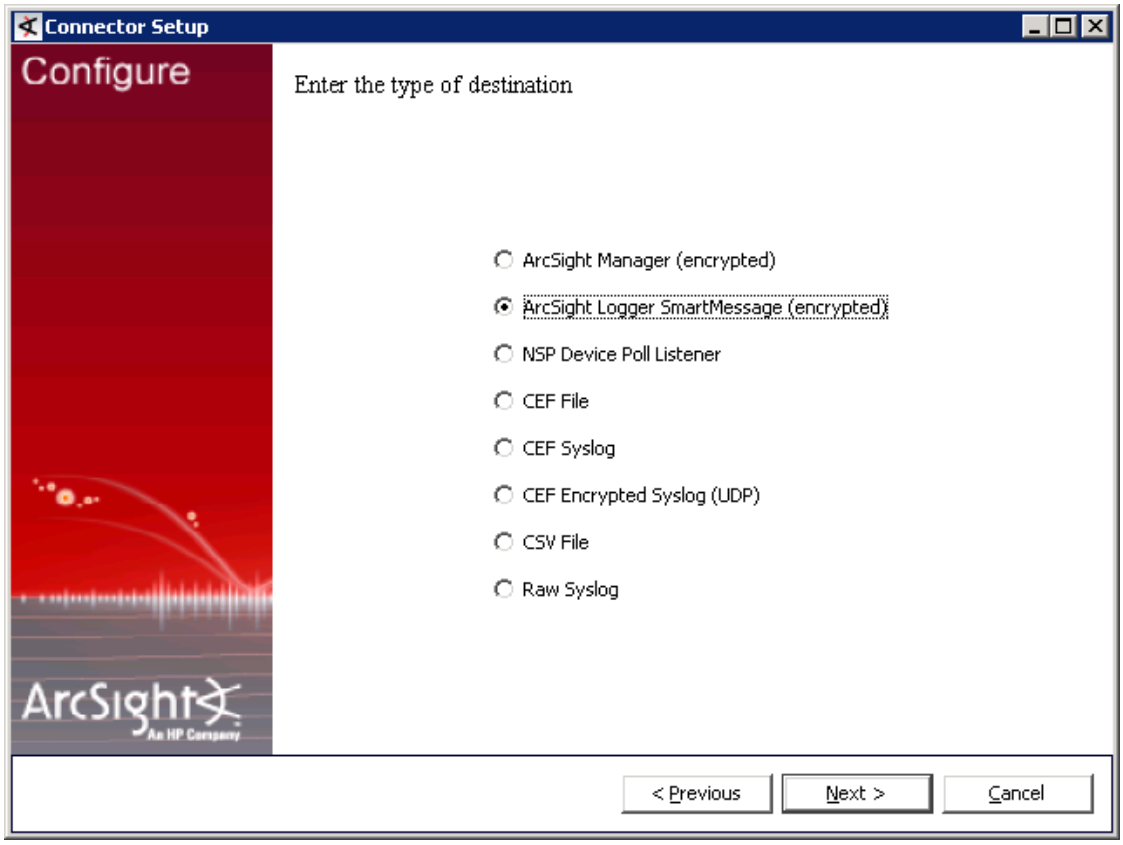


6. Select **Add a Connector** and click **Next**.
7. Select the required SmartConnector type. The following pre-configured types are available:
   - **Microsoft Windows Event Log - Local** (monitors the following Windows logs: Windows Application Log, Windows Security Log, Window System Event Log.)
   - **Linux Audit File** (monitors the audit log)
   - **Linux Syslog File** (monitors predefined system files, including the following: Syslog, Cron, Mail, Secure.If you need to monitor more than one log, you need to install this SmartConnector type separately for each log.)
   - **Apache HTTP Server Access File**
   - **Apache HTTP Server Error File**
8. Click **Next**.
   - If you are installing a Linux connector, enter the required path and log. Following are typical paths for the supported logs:

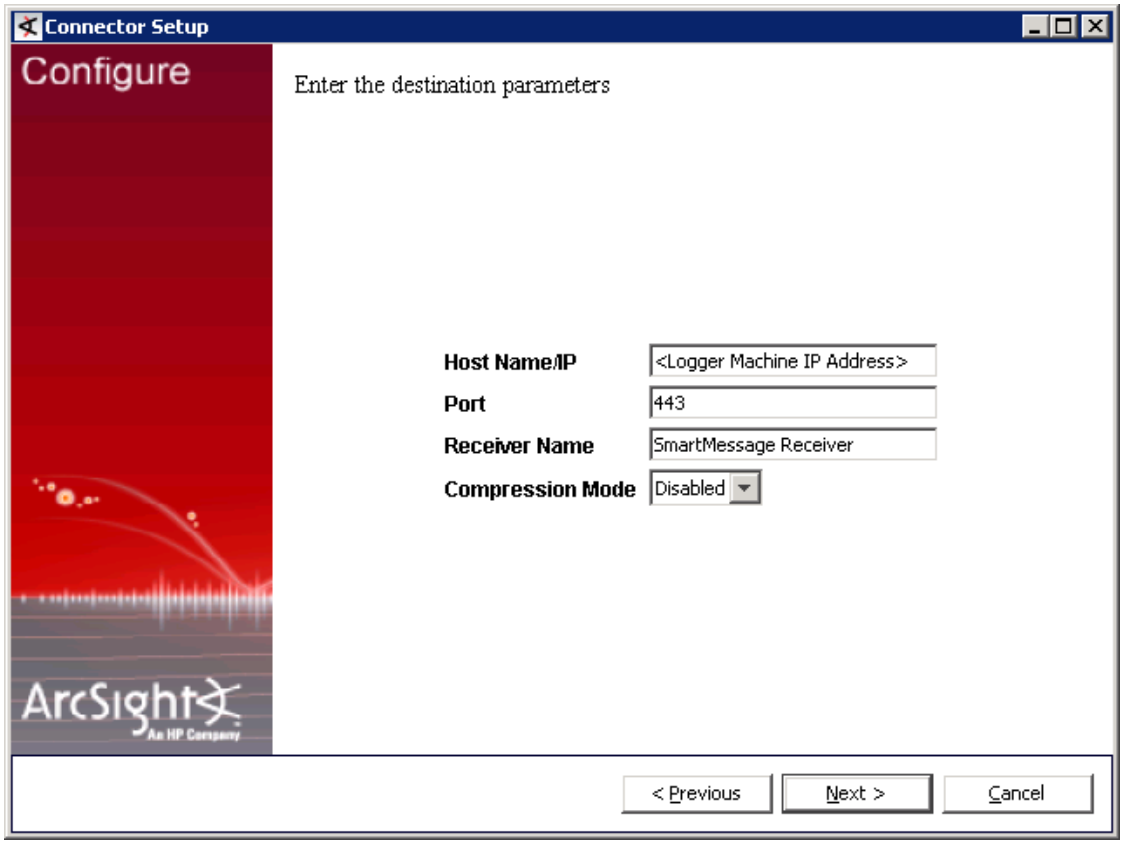
- /var/log/audit/audit.log
- /var/log/messages
- /var/log/cron
- /var/log/maillog
- /var/log/secure

- If you are installing an Apache connector, the wizard prompts you for the Log File Name.
- If you are installing the Windows Event Log connector, the wizard prompts you for the Event Log Types and Batch Query Buffer Size.

9. Enter the required information and click **Next**. The Type of Destination window opens.



10. Select **ArcSight Logger SmartMessage (encrypted)** and click **Next**. The Destination Parameters window opens.



11. Enter the following information:

    - **Host Name/IP** - The Host Name or IP address of the logger machine.
    - **Port** - 443
    - **Receiver Name** - SmartMessage Receiver

    Note: *SmartMessage Receiver* is the default receiver name for this receiver type. If this default name does not work, you can check the correct receiver name:

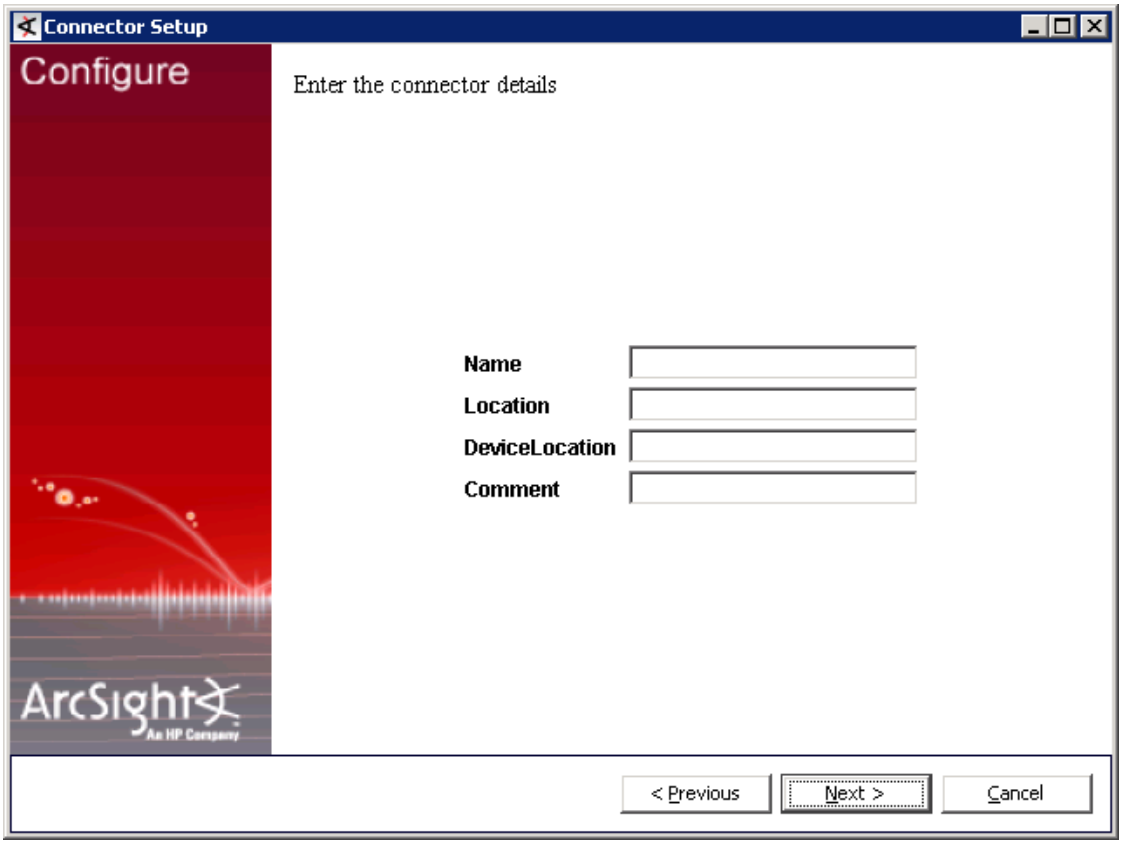
    i. In ArcSight Logger, select **Configuration > Event Input**.

    ii. On the **Receivers** tab, identify the name of the receiver of type **SmartMessage Receiver**.

The SmartMessage receiver is configured to work with these SmartConnectors. If required, you can create a different receiver in ArcSight Logger. For details, see the ArcSight Logger documentation.

- **Compression Mode** - Disabled

12. Click **Next**. The Connector Details window opens.



13. Enter the following information:

- **Name** - Name of the host monitor
- **Location** - The location of the host monitor
- **Device Location** - The host name or IP address
- **Comment**

The above information will be displayed in ArcSight Logger. For details of how this information will be displayed in ArcSight Logger, see the relevant Smart Connector ArcSight Logger document.

14. Click **Next** to register the connector and complete the installation process.
15. After the installation process is complete, you need to manually start the service.
    a. Click the Windows Start button and in the Start Search field type **Services** and press enter.
    b. Right-click on the required service and select **Start**.

After installing the SmartConnector, you will need to manually configure and publish it. For details, see *Configuring ArcSight Logger Out of the Box Smart Connector Collections* in the *Operations Analytics Configuration Guide.*

Accessing Operations Analytics for the First Time

To log on to Operations Analytics (Operations Analytics):

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 **Continue Using 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*.

Obtaining Licenses

After purchasing Operations Analytics, you will need to download three licenses, one each for Operations Analytics (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.

Operations Analytics Security Hardening

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

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 Appliance, 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`

- It is highly recommended that you disable the SSH login for the root account. Before doing that, you must add the Operations Analytics default user name, opsa, to the sudoers file using the following commands:

  a. `vi /etc/sudoers`

  b. Add the following line to the file (just as an example): `opsa ALL=(ALL) ALL`.

c. Save your changes.

d. `vi /etc/ssh/sshd_config`

e. Add the following line to the file: `PermitRootLogin no`

f. Save your changes.

g. `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 Analtyics 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 Appliance 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 Appliance:

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.

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 Operations Analytics Installation Guide (Operations Analytics 2.20)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to sw-doc@hp.com.

We appreciate your feedback!