HP Operations Analytics

For the Linux Operating System

Software Version: 2.00

Operations Analytics Installation and Configuration Guide

Document Release Date: December 2013

Software Release Date: December 2013

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®, Windows®, Windows NT®, Windows 8®, and Windows 9® are U.S. registered 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: **http://h20230.www2.hp.com/selfsolve/manuals**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: **http://h20229.www2.hp.com/passport-registration.html**

Or click the **New users - please register** link on the HP Passport login page.

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

Support

Visit the HP Software Support Online web site at: **http://www.hp.com/go/hpsoftwaresupport**

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

HP Software online 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:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

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 More Information about Operations Analytics

To obtain a complete set of information about Operations Analytics, use this guide along with other Operations Analyticsdocumentation. 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 obtain help about the Operations Analytics console.	See theOperations Analytics Help.
I want to find the hardware and operating system requirements for Operations Analytics.	See the Operations Analytics Support Matrix.
I want to find additional information about Operations Analytics.	See the Operations Analytics Release Notes.
I want to open a view from HP OMi to Operations Analytics.	See the *Integration with HP Operations Manager i: HP Operations Analytics 2.0* White Paper

Environment Variables used in this Document

This document refers to the following environment variables and other useful directories when explaining installation and configuration instructions for the Operations Analytics Software, including the Operations Analytics Server 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 "Environment Variables used in this Document" 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.

Terminology Used in this Document

Analytic Query Language (AQL): The more advanced offering of two query languages supported by Operations Analytics. Use AQL when the Phrased Query Language (PQL) syntax is not specific enough to return the data you need. When using AQL, it is helpful if you have programming or scripting skills as well as some knowledge of databases. See *About Analytics Query Language (AQL) Functions* in the Operations Analytics help for more information.

Collection: A collection defines the data to be collected and corresponds to a database table in which the Operations Analytics Collector Appliance stores the data.

Custom Collections The list of collections supported by the Operations Analytics Server Appliance that do not have predefined templates.

Collector Appliance: This virtual appliance is the Operations Analytics 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.

HP Service Health Analyzer (SHA): HP Service Health Analyzer analyzes abnormal service behavior and alerts IT managers of service degradation before an issue affects their business.

Link Tags: Special tags used to relate collection information. Create the same link tag for each collection you want to link together.

Meta Model: A way to describe the data to collect for analysis; it includes the construction and development of the frames, rules, constraints, models and theories applicable and useful for modeling a predefined class of problems.

Metrics: Structured data that is typically collected from HP's existing management products, other data files or from other 3rd party management software. A metric is a measurement of one attribute at specific point in time for a specified sub-entity or resource (such as CPU utilization). A metric is based on the most recent user-initiated search query.

Outlier or **Outliers**: Data that is outside of the normal range based on the data collected to date.

predefined Collection Templates: The list of predefined collection templates that reside on the Operations Analytics server appliance for the collections Operations Analytics supports by default.

Phrased Query Language (PQL) : The less advanced offering of two query languages supported by Operations Analytics. Use PQL in the early stages of troubleshooting a problem. With this approach, type a word or phrase that begins to describe the type of problem you want to resolve and then select from the list of suggestions provided by Operations Analytics. See *About the Phrased Query Language* in the Operations Analytics help for more information.

Raw Logs: These are log messages as they appear from the log management application with which Operations Analytics is integrated. These log files must be configured using the log file management software supported by Operations Analytics. See theOperations Analytics *Support Matrix* for more information.

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

Structured Logs: These are fragments of log file data that are stored as collections in Operations Analytics. These collections exist so that users can perform analytics on the log file contents. For example, users might want to query for all outliers by host name and application for a particular time range.

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. See "Terminology Used in this Document" 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.

Data Sources used in Operations Analytics

In today's complex data center environments, the source of a problem is not always easy to detect using traditional management and troubleshooting tools that look only for predetermined solutions to known potential problems. For example, many management and troubleshooting tools are designed to provide analytics for a specific problem context, such as root cause isolation, outlier detection, and service level agreement violation. They provide these services by using a specific data set and analytics technique.

With Operations Analytics you generate insights from the IT data in your environment that you, the Operations Analytics administrator, chooses to collect in your network. And because identifying the most useful analytics to derive from the data generally depends on the problem context, the user community provides each data request.

As the Operations Analytics administrator, you configure collections from a diverse set of possible sources. For example, if you have HP Network Node Manager (NNMi) or HP Operations Manager (HPOM), you can configure collections to gather NNMi topology or HPOM events occurring within your network.

See "Table 2: Predefined Data Collection Sources by Collection Type""Data Sources used in Operations Analytics "and "Table 3: Custom Data Collection Sources by Collection Type" for the list of supported data sources.

> **Note**: Operations Analytics requires that you use a configuration template to configure each collection. See "Table 2: Predefined Data Collection Sources by Collection Type" to determine the data sources that have predefined configuration templates. You create Custom Collections for any supported data source that does not have a configuration template provided by Operations Analytics.

Operations Analytics provides predefined collection templates for the data sources shown in the following table:

Table 2: Predefined Data Collection Sources by Collection Type

Predefined Data Collection Sources	Metrics Collection Type	Events Collection Type	Topology Collection Type	Inventory Collection Type
HP BSM RTSM (Configuration Item Inventory)	no	no	no	yes
HP Business Process Monitor (BPM)	yes	no	no	no
HP NNMi Custom Poller	yes	no	no	no

Table 2: Predefined Data Collection Sources by Collection Type, continued

Predefined Data Collection Sources	Metrics Collection Type	Events Collection Type	Topology Collection Type	Inventory Collection Type
HP Network Node Manager iSPI Performance for Metrics Component Health	yes	no	no	no
HP Network Node Manager iSPI Performance for Metrics Interface Health	yes	no	no	no
HP Operations Agent	yes	no	no	no
HP Operations Smart Plug-in for Oracle	yes	no	no	no
HP OMi (Operations Manager i) Events	no	yes	no	no
HP Operations Manager (OM) Events	no	yes	no	no

Operations Analytics supports, but does not provide predefined collection templates for the data sources shown in the following table:

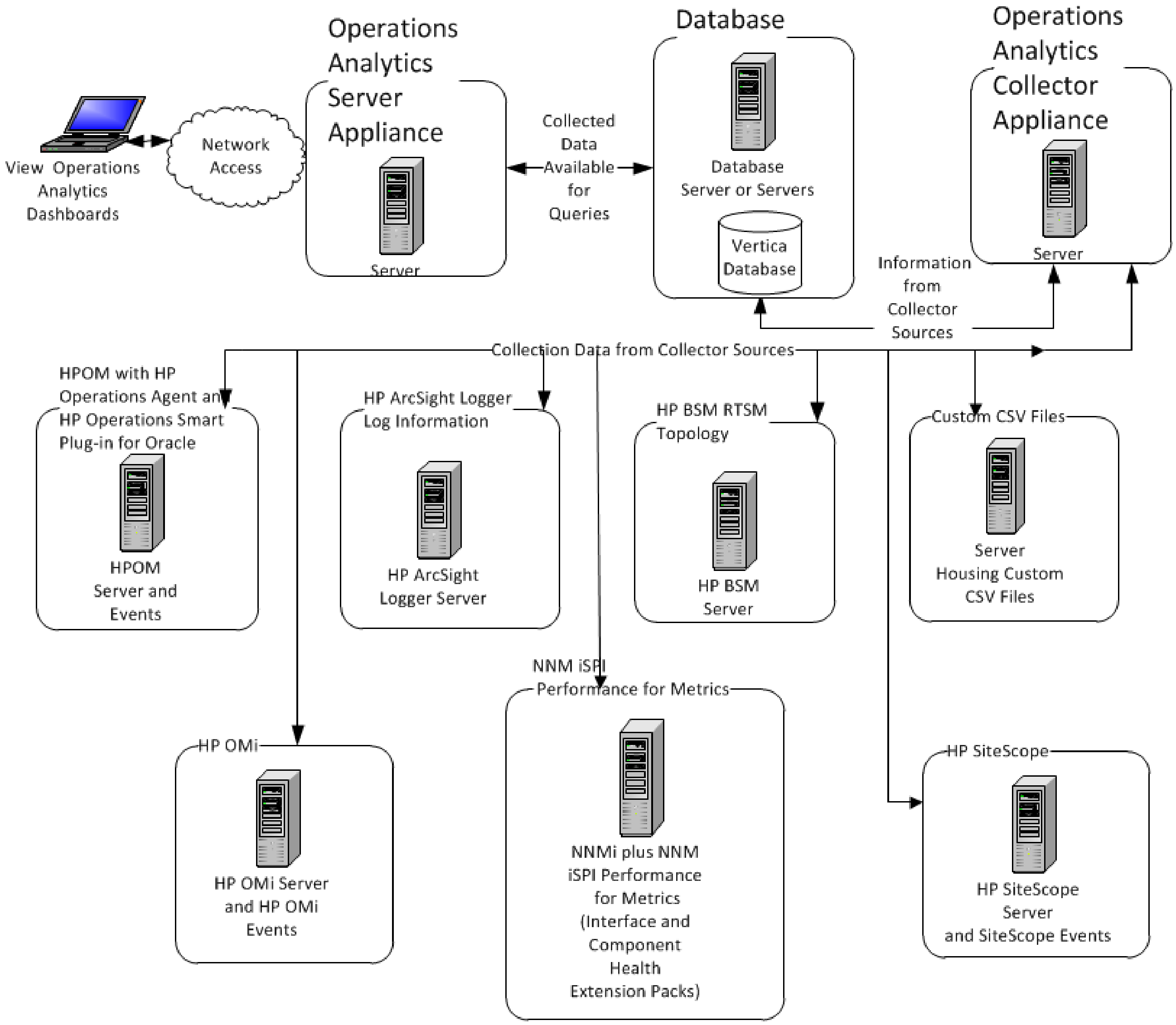
Table 3: Custom Data Collection Sources by Collection Type

Custom Collection Data Source	Topology Collection Type	Metrics Collection Type	Structured Logs Collection Type	Undefined Collection Type
HP SiteScope	no	yes	no	no
Structured Logs	no	no	yes	no
Custom CSV Files	no	no	no	yes

Supported Deployments

Review the information shown in the following diagram to begin understanding the data sources used by Operations Analytics and how they are configured together to better plan your Operations Analytics installation.

System Deployment Considerations


View Operations Analytics Dashboards
Network Access
Operations Analytics Server Appliance
Server
Collected Data Available for Queries
Database
Database Server or Servers
Vertica Database
Operations Analytics Collector Appliance
Server
Information from Collector Sources
Collection Data from Collector Sources
HPOM with HP Operations Agent and HP Operations Smart Plug-in for Oracle
HPOM Server and Events
HP ArcSight Logger Log Information
HP ArcSight Logger Server
HP BSM RTSM Topology
HP BSM Server
Custom CSV Files
Server Housing Custom CSV Files
NNM iSPI Performance for Metrics
NNMi plus NNM iSPI Performance for Metrics (Interface and Component Health Extension Packs)
HP OMi
HP OMi Server and HP OMi Events
HP SiteScope
HP SiteScope Server and SiteScope Events

Operations Analytics supports the deployments described in this chapter.

Installation Overview

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

This section includes:

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

Operations Analytics Components

Operations Analytics is made up of the following main components:

- **Operations Analytics Server**:
  - Provides the business logic and presentation capabilities of Operations Analytics.
  - Deployed as an OVA appliance.
  - 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 Collectors 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.

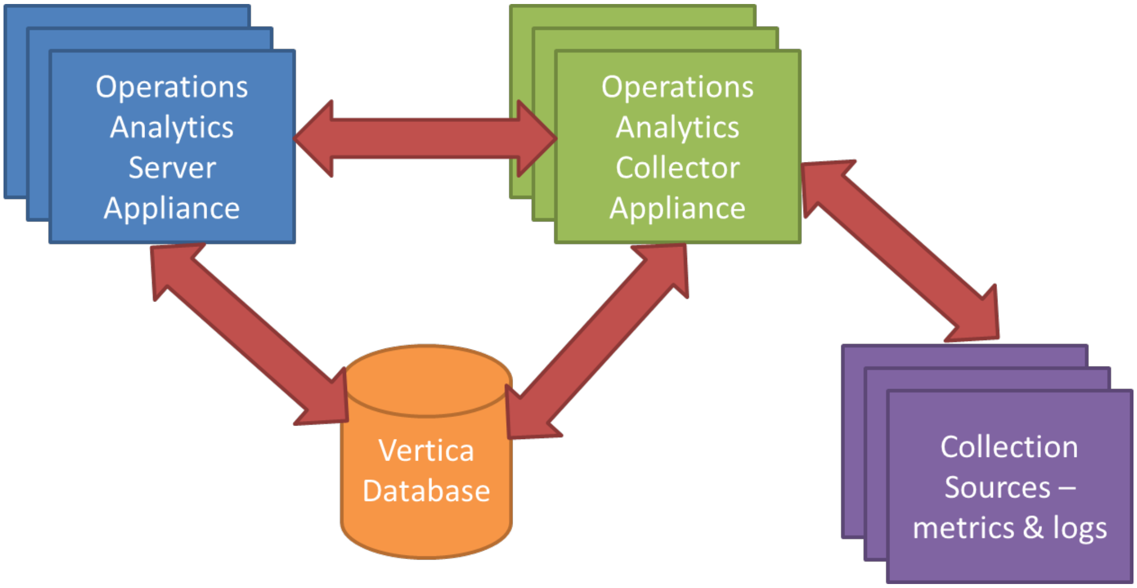
Collection Sources

Data from the collection sources is brought into Operations Analytics via 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 (NNM) and NNMi, 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:


Operations Analytics Server Appliance
Operations Analytics Collector Appliance
Vertica Database
Collection Sources – metrics & logs

Setting up Your Operations Analytics System

System setup includes the following steps:

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

     Note that if you are using an existing Vertica installation, you must manually create the OPSADB database before running the post-install.
2. **Post-Install Configuration**:
   - Create the opsa_default schema (for the default tenant) on the OPSADB database on Vertica.
   - Connect the Operations Analytics Server Appliance/s to the Vertica Database
   - Connect the Operations Analytics Collector Appliance/s to the Vertica Database
   - Configure the various passwords for the default Operations Analytics users; this is important for securing the system
   - Configure a Logger Flex Connector (e.g. agent) on the Operations Analytics Server Appliance to collect system log data for self-monitoring (Operations Analytics logs are collected) – *optional.*
3. **Configure Collection Sources**:

   You may configure one or more of the following collection sources:
   - 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.

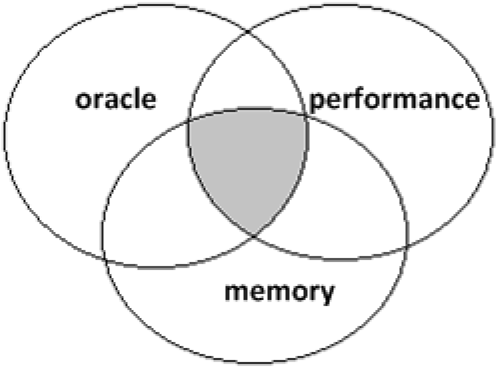
How Tags are Used in Operations Analytics

A tag is a word or phrase that is associated with a metric, topology, event, or log file attribute that is stored as part of a collection in Operations Analytics. Tags are provided by Operations Analytics.

Tags are used in the Operations Analytics Phrased Query Language or Analytics Query Language to create an Operations Analytics dashboard. They help to define the following:

- Entity class names for which you want information, such as a database collection tagged with **database** or a metric collection with transaction rates tagged with **transaction** and **performance**.
- Hardware and software components, such as **cpu**, **memory**, **disk**, **interface**, **tablespace**, **process**, and **threads**.
- Metrics or problem areas, such as **utilization**, **availability**, **performance**, and **change**.

Operations Analytics creates an intersection of the tags used to query for a Guided Troubleshooting Dashboard. For example, the query **oracle memory performance** returns only the metrics that are associated with all three tags (**oracle memory performance**) as represented in the following diagram:



The purpose of tagging is to find a suitable set of metrics and logs that relate to a specific question a user might pursue using Operations Analytics query languages. The Operations Analytics administrator defines tags before configuring an Operations Analytics collection or after configuring a collection using the `$OPSA_HOME/bin/opsa-tag-manager.sh` script. See *Creating and Applying Tags* in this document for more information.

Use the following guidelines when configuring tags:

- Collections should only be assigned tags that describe the purpose of the whole domain.
- Typically these tags are the entity class that is associated with a domain.

- Examples of these tags are as follows:
  - Oracle
  - performance
  - memory
- Always use a tag for the most specific entity type that describes the whole collection within which you want to search.

If you add tags to a metric in a collection, tag it as follows:

- Use entity elements that describe the metric or text variable (such as tablespace, process, cpu, or disk).
- Use tags that depict the purpose of the metric (such as performance, availability, error, security, change).
- Use tags that depict a search focus. This tag should only be applied to important metrics that either are prototypical for a set of metrics (cpu) or gives important information about the health of an entity (like error rate for a database).
- Keep the tag length short, but descriptive enough to meet your needs. Tags are limited to 256 characters.

To configure tags when configuring collections, see the *Configuring Tags, Tenants, and Collections* section in this document.

Obtaining Licenses

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

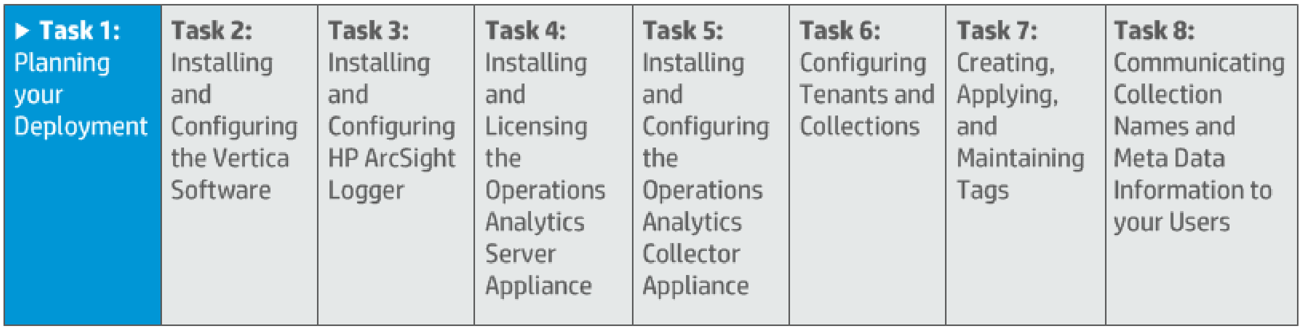
1. Using your browser, navigate to the licensing link shown in the license email you received (`www.hp.com/software/licensing`).
2. Log on using **HP Passport** credentials. You will need to register if you do not have HP Passport credentials .
3. When prompted, enter your order number.
4. Follow the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

Chapter 3: Installing Operations Analytics

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

1. "Task 1: Planning your Deployment"
2. "Task 2: Installing and Configuring the Vertica Software"
3. "Task 3: Installing and Configuring HP ArcSight Logger"
4. "Task 4: Installing and Licensing the Operations Analytics Server Appliance using the VMware vSphere Client"
5. "Task 5: Installing and Configuring the Operations Analytics Collector Appliance using the VMware vSphere Client"
6. " Configuring Tenants and Collections (Task 6)"
7. "Creating, Applying, and Maintaining Tags (Task 7)"
8. " Communicating Collection Names and Meta Data Information to your Users (Task 8)"

Task 1: Planning your Deployment



▶ **Task 1:** Planning your Deployment	**Task 2:** Installing and Configuring the Vertica Software	**Task 3:** Installing and Configuring HP ArcSight Logger	**Task 4:** Installing and Licensing the Operations Analytics Server Appliance	**Task 5:** Installing and Configuring the Operations Analytics Collector Appliance	**Task 6:** Configuring Tenants and Collections	**Task 7:** Creating, Applying, and Maintaining Tags	**Task 8:** Communicating Collection Names and Meta Data Information to your Users

Use the following checklist to prepare for configuring Operations Analytics:

1. ☑ Review the following Topics:
   - "Terminology Used in this Document"
   - "Data Sources used in Operations Analytics "
   - "Supported Deployments"

2. ☑ Review the information in "Operations Analytics Port Mapping" and open the well-known ports discussed in that section before installing Operations Analytics.

3. ☑ List the data sources, including the event, metrics, and structured log sources, from which you want Operations Analytics to collect information. You will need to configure a data collection for each data source on your list. See "Data Sources used in Operations Analytics " for more information.

4. ☑ List the data sources for which Operations Analytics provides configuration templates. This can be a subset of your list of data sources from which you want Operations Analytics to collect information. See "Supported Deployments" for more information.

5. ☑ List the custom data sources for which Operations Analytics does not provide configuration templates. This should be a subset of your list of data sources from which you want Operations Analytics to collect information. See "Supported Deployments" for more information.

   > **Tip**: You will need to follow a different procedure for those collections that do not have a configuration template provided.

6. ☑ Collectors can support multiple collections. Using the lists you created earlier, decide on the number of collectors and the number of servers you will need to support your desired collections.

7. ☑ A tag is a word or phrase that is associated with a metric, topology, event, or log file attribute that is stored as part of a collection in Operations Analytics. Based on the lists you created earlier, list the tags you might need to create to differentiate the data you plan to collect.

8. ☑ Considering the aggregate list of data you plan to collect, and the collections you plan to create, list the potential data queries you might use (by collection) when considering this diverse set of data.

9. ☑ Optional: Using a tenant model, you can separate the information you plan to collect, referred to as a collection, among groups of users. If this applies to your networked environment, make a list of the user groups for which you must separate the information.

10. ☑ Optional: If you use a tenant model you will need to assign user groups. User Groups are predefined in Operations Analytics and determine which tasks each User Account that is assigned to the User Group can perform. See the following predefined User Groups table for more information.

    Note the following:

    - User Accounts must be unique across all Tenants.

    - All User Groups can access the Operations Analytics console.

    - You cannot add a new User Group to Operations Analytics.

- A User Account was assigned to the Super Admin User Group when you installed Operations Analytics.

Predefined User Groups

User Group	Description	Supported Tasks
Super Admin	User accounts assigned to this User Group can access the following information for each tenant defined: ○ Collectors ○ Collections ○ Meta Data ○ Tags ○ User Accounts ○ User Groups	Add, modify, and delete tenants.
Tenant Admin	User accounts assigned to this User Group can access the following information only for the tenant to which they are assigned: ○ Collectors ○ Collections ○ Meta Data ○ Tags ○ User Accounts ○ User Groups	Add, modify, and delete user accounts. Manage the collectors, collections, meta data, and tags for a specified tenant.
User	User accounts assigned to this User Group can access the Operations Analytics console..	Access and perform tasks using the Operations Analytics Home Page and Guided Troubleshooting Dashboards.

Make a list of the Operations Analytics personnel you might have and the roles you might assign them.

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

Task 2: Installing and Configuring the Vertica Software

Task 1: Planning your Deployment	▶ **Task 2:** Installing and Configuring the Vertica Software	**Task 3:** Installing and Configuring HP ArcSight Logger	**Task 4:** Installing and Licensing the Operations Analytics Server Appliance	**Task 5:** Installing and Configuring the Operations Analytics Collector Appliance	**Task 6:** Configuring Tenants and Collections	**Task 7:** Creating, Applying, and Maintaining Tags	**Task 8:** Communicating Collection Names and Meta Data Information to your Users

1. Copy the following compressed Vertica installation file from the downloaded installation files to a temporary location:

   ```
   opsa-vertica-1.00.tar.gz
   ```

2. From the temporary location, extract the opsa-vertica-1.00.tar.gz file using the following command:

   ```
   tar -zxvf opsa-vertica-1.00.tar.gz
   ```

3. From the temporary location, run the following command to begin the Vertica installation:

   ```
   ./opsa-vertica_1.00_setup.bin
   ```

   Follow the interactive instructions until the Vertica installation is complete.

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

4. 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.

   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".

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"

"Configuring the Directors"

"Connecting to the Virtual IP "

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".
- 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 pagehttp://kb.linuxvirtualserver.org/wiki/Using_arp_announce/arp_ignore_to_disable_ARP** for 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:

   > **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.

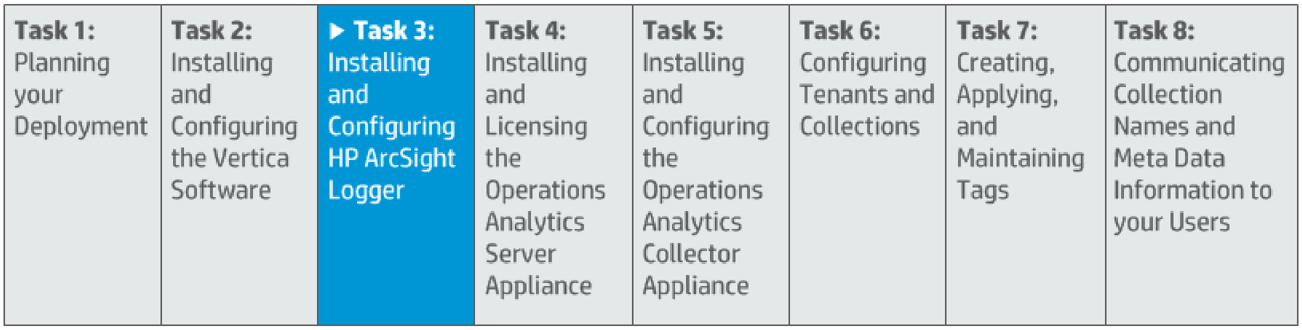
```
$ vsql -h <VIP> -c "SELECT node_name FROM sessions"
```

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



Task 1: Planning your Deployment	**Task 2:** Installing and Configuring the Vertica Software	**▶ Task 3:** Installing and Configuring HP ArcSight Logger	**Task 4:** Installing and Licensing the Operations Analytics Server Appliance	**Task 5:** Installing and Configuring the Operations Analytics Collector Appliance	**Task 6:** Configuring Tenants and Collections	**Task 7:** Creating, Applying, and Maintaining Tags	**Task 8:** Communicating Collection Names and Meta Data Information to your Users

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

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

Prerequisites for Installation

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

- You need a separate license file for each instance of HP ArcSight Logger. A license file is uniquely generated for each Enterprise version download.

- Make sure a non-root user account exists on the system on which you are installing HP ArcSight Logger. The non-root user must also be a non-system user with login permissions.
  You can be logged in as a root user or a non-root user on the server on which you are installing the software. Your installation options vary depending on which you choose.

  - When you install as a root user, a non-root user account is still required.

  - When you install as a root user, 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.

  - If you are upgrading from a version before 5.1, you cannot change the previous installation to a root-user installation. You will need to use the previously configured port 9000 for accessing HP ArcSight Logger software.

- The hostname of the server on which you are installing HP ArcSight Logger cannot be localhost. If it is, change the hostname before proceeding with the installation.

- You must not have an instance of MySQL installed on the Linux server on which you will install HP ArcSight Logger. If an instance of MySQL exists on that server, uninstall it before installing HP ArcSight Logger.
- If you want to use the GUI mode of installation and will be installing HP ArcSight Logger over an SSH connection, make sure that you have enabled X window forwarding using the -X option so that you can view the screens of the installation wizard. If you will be using PuTTY, you will also need an X client on the machine from which you are connecting to the Linux machine.
- Installation on 64-bit systems requires glibc-2.12-1.25.el6.i686 and nsssoftokn- freebl-3.12.9-3.el6.i686. Install these packages if the installation fails with the following error message: Installation requirements not met. Pre-install check failed: 32-bit compatibility libraries not found.

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" 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" for more information.

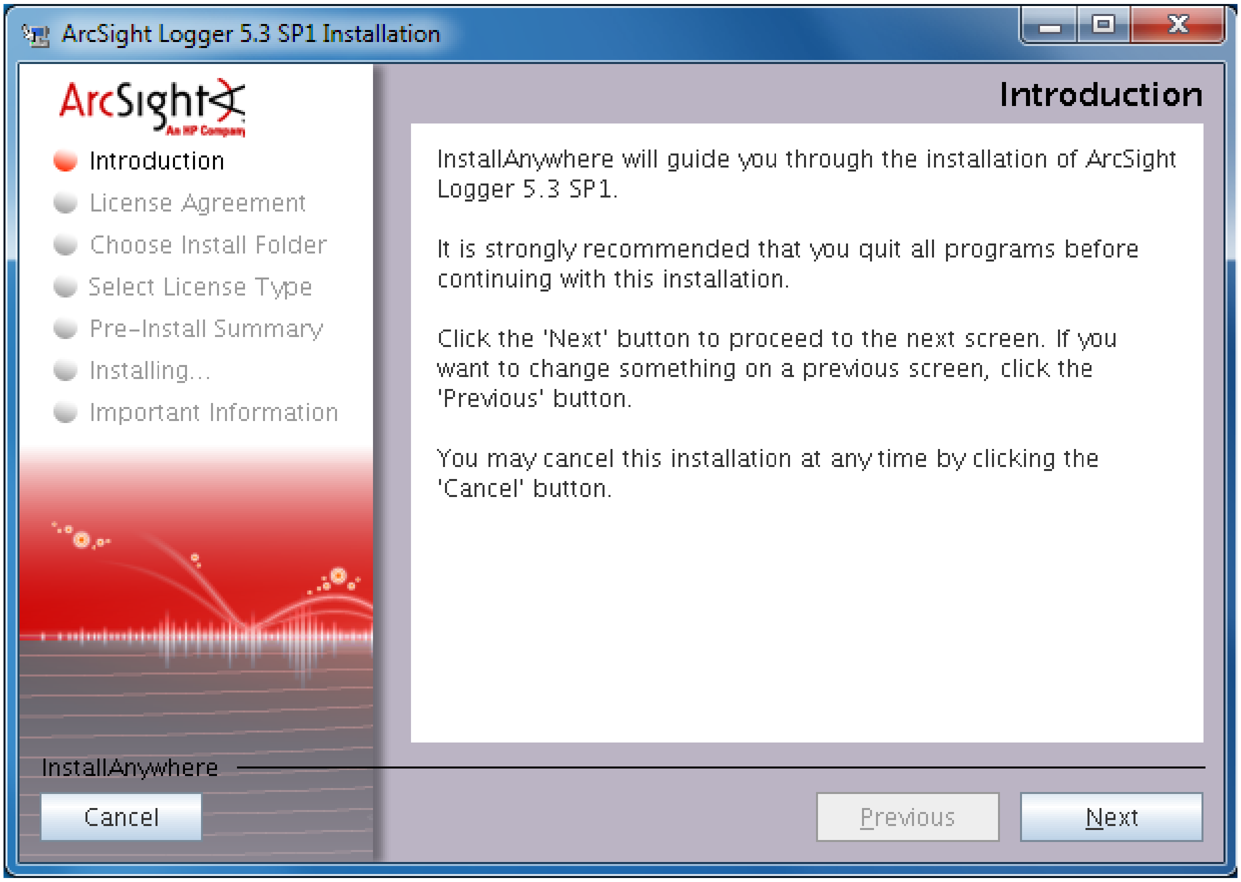
HP ArcSight Logger Installation Steps

This section describes two modes of HP ArcSight Logger installation.

Using the GUI Mode to Install HP ArcSight Logger

1. Obtain a copy of HP ArcSight Logger version 5.3 SP1 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-5.3.1.XXXX.0.bin
   ./ArcSight-logger-5.3.1.XXXX.0.bin
   ```

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



ArcSight Logger 5.3 SP1 Installation

Introduction

InstallAnywhere will guide you through the installation of ArcSight Logger 5.3 SP1.

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

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

.
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. Select whether to use the trial License or a license file. If you start with a trial license, you can upgrade to use a license file later.

   - If you have a valid license file, select **Yes** and then click **Next**.
   Click **Choose**, navigate to the license file for HP ArcSight Logger, and then click **Next**.
   If the license file is uploaded successfully, the License Status section (below the Upload License button) indicates that status.
   - To evaluate HP ArcSight Logger using the trial license, select **No, use the trial license**, and then click **Next**.

10. Review the Pre-Installation Summary and click **Install**.

11. 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 the port you specify is already in use, you will be asked to select a different port. If you specify any port except 443, users will need to enter that port number in the URL they use to access the HP ArcSight Logger UI.
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*.

12. Select the locale of this installation and click **Next**.

13. 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.

14. 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.

15. Click **Done** to exit the installer.

16. Now that you are done installing and initializing HP ArcSight Logger, you can connect, log in, 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" are met.

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

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

1. Run these commands from the directory where you copied the HP ArcSight Logger software:
   ```
   chmod +x ArcSight-logger-5.3.1.XXXX.0.bin
   ./ArcSight-logger-5.3.1.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 5.3 SP1.
   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 5.3 SP1 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". 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.

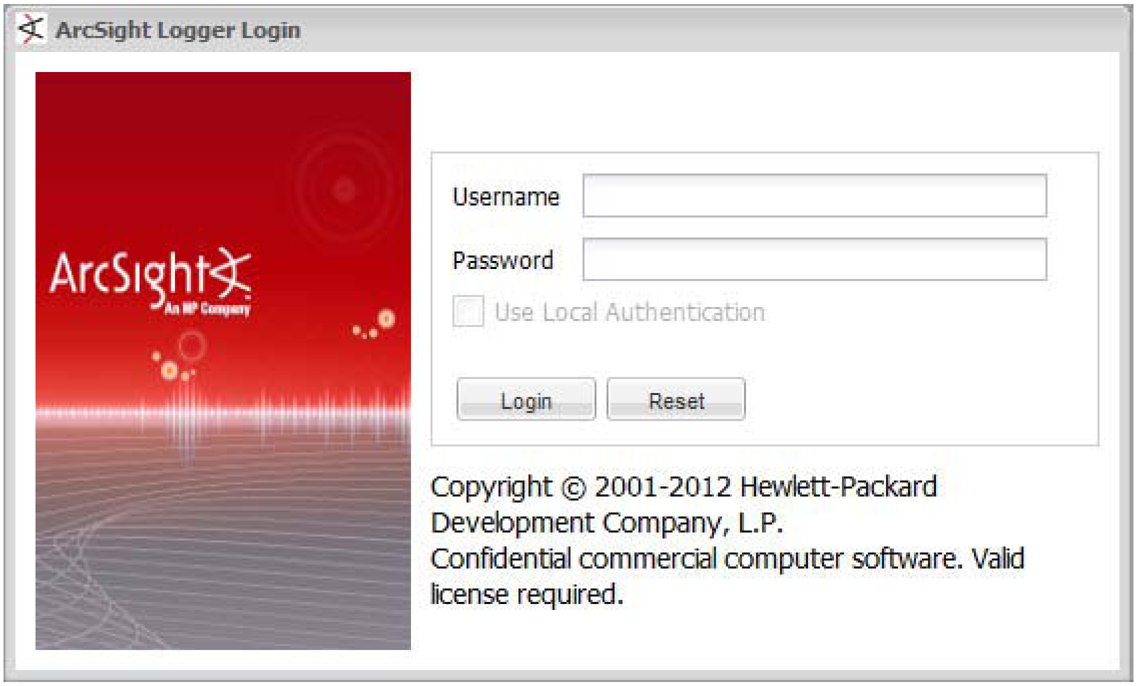
To connect and log into Logger, do the following:

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 Logger installation.

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

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



Copyright © 2001-2012 Hewlett-Packard Development Company, L.P.
Confidential commercial computer software. Valid license required.

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" for instructions.

> Note: You will need to configure Logger to collect the log files you are interested in. 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 "Installing and Configuring the Operations Analytics Log File Connector for HP ArcSight Logger" 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"

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.

Installing and Configuring the Operations Analytics Log File Connector for HP ArcSight Logger

The Operations Analytics Log File Connector for HP ArcSight Logger collects raw log files and tags them with some important information, such as hostname and process name. Operations Analytics uses the Operations Analytics Log File Connector for HP ArcSight Logger to create a generic application log file connector that collects all of the log information needed by Operations Analytics.

Note: The Operations Analytics Log File Connector for HP ArcSight Logger is supported on the Windows and Linux platforms operating system.

Purpose : Use the installation instructions in this section if you must configure Operations Analytics to collect raw log files and tag them with some important information. You also might need to install the Operations Analytics Log File Connector for HP ArcSight Logger to collect application logs.

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.

All other ArcSight connectors, such as the **SmartConnector for Apache HTTP Server Access File**, should be installed and configured using the ArcSight installation packages and documentation for any specific ArcSight connector.

Note: For the best results, use existing ArcSight connectors to collect log data, since they will do extensive parsing of the log message. The Operations Analytics Log File Connector for HP ArcSight Logger does not do any parsing of the log message.

If there is not a specific ArcSight connector available for the log collection you need, then use the Operations Analytics Log File Connector for HP ArcSight Logger. To install and configure the Operations Analytics Log File Connector for HP ArcSight Logger, follow the instructions at "Installing and Configuring the Operations Analytics Log File Connector for HP ArcSight Logger".

There are several out-of-the-box connectors available which let you connect to standard Windows, Linux, or Apache logs. For details, see "Task 3: Installing and Configuring HP ArcSight Logger" on page 30.

For Operations Analytics to better utilize the raw log data from HP ArcSight Logger, use the fields shown in the following table.

Mandatory Fields to use for Arcsight Logger Collections

Field	Field Definition
Timestamp	The timestamp of the log message. For HP ArcSight Logger this is the receipt time that shows when the connector read the log message from the log file.

Mandatory Fields to use for Arcsight Logger Collections, continued

Field	Field Definition
Hostname	The hostname of the system on which the log file resides. The Operations Analytics Log File Connector for HP ArcSight Logger sets the `Common Event Format (CEF)` field, `sourceHostName`, with the configured hostname for a log folder.

It is helpful to know the name of the process (for example: Apache Web Server) that created the log file along with the name of the application (such as Acme Order Application). The Operations Analytics Log File Connector for HP ArcSight Logger sets the `sourceProcessName` CEF field with the configured process name and the `sourceServiceName` CEF field with the configured application name for a log folder.

Installing 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. Use these instructions to manually install the Operations Analytics Log File Connector for HP ArcSight Logger on other non-Operations Analytics servers that need to send log events to HP ArcSight Logger.

Look for the following installation package on any Operations Analytics Collector Appliance:
`$OPSA_HOME/logfile/opsa-arcsight-connector-dist-linux.zip`

Do not install the Operations Analytics Log File Connector for HP ArcSight Logger before deciding how you want to collect application logs in your environment. Select from the following deployment methods:

1. **Central Log File Management**: To use this method, install the Operations Analytics Log File Connector for HP ArcSight Logger on a central server. Using this approach, all of your application logs are stored using one of the following methods:

   - The application log files are copied to the central log server in their own directory.

   - The log file directories are shared, then mounted on the central server.

   This method enables you to use one central log server to administer the Operations Analytics Log File Connector for HP ArcSight Logger, but introduces extra work to get the application log files located on the central log server.

   When using this method, the Operations Analytics Log File Connector for HP ArcSight Logger is already installed in the `/opt/HP/opsa/arcsight` folder and configured for collecting log files from the Collector Appliance. That means you can use the Operations Analytics Collector Appliance as a central log file server.

2. **Local Log File Management**: To use this method, install the Operations Analytics Log File Connector for HP ArcSight Logger on the same system that is running the application, and on which the log files are being created. This type of deployment eliminates the need to export or

copy log files to a central server, but requires more effort to manage and maintain a larger quantity of Operations Analytics Log File Connector for HP ArcSight Loggers.

After selecting the deployment method you plan to use, complete the following steps:

1. Extract the install package in the desired installation directory (for example, you might run the following command: `unzip opsa-arcsight-connector-dist-linux.zip`).

2. Open the directory containing the extracted the zip files.

3. Run the following command to install the Operations Analytics Log File Connector for HP ArcSight Logger:
   - **Windows**: `opsa-logfile-flexconnector-config.bat`
   - **Linux**: `sh opsa-logfile-flexconnector-config.sh`

4. During installation, the script prompts you for the information shown in the following table:
   Parameters for the opsa_logfile_flexconnector_config Script

Parameter	Parameter Description
ArcSight Logger Hostname	Hostname or IP address of the HP ArcSight Logger server to which you want this connector to send log messages.
ArcSight Logger Port (443)	The Smart Message Receiver port to which you want the Operations Analytics Log File Connector for HP ArcSight Logger to connect. By default HP ArcSight Logger uses port 443.
Name of Smart Message Receiver	The name of the Smart Message Receiver that receives messages from this Operations Analytics Log File Connector for HP ArcSight Logger. By default, HP ArcSight Logger defines a Smart Message Receiver called **SmartMessage Receiver**. You must enable this Smart Message Receiver name on the HP ArcSight Logger server.
Connector Name	The unique name for this installation of the Operations Analytics Log File Connector for HP ArcSight Logger.
Connector Location	This is an optional configuration for specifying the location of the Operations Analytics Log File Connector for HP ArcSight Logger.

5. After the installation completes, you will be prompted to configure the Operations Analytics Log File Connector for HP ArcSight Logger. To configure the Operations Analytics Log File Connector for HP ArcSight Logger, complete the steps shown in "Configuring the Operations Analytics Log File Connector for HP ArcSight Logger".

Configuring 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. Use the following instructions to make additional configuration changes for the Operations Analytics Log File Connector for HP ArcSight Logger.

Unless specifically noted in these instructions, always use the $OPSA_HOME/bin/opsa-logfile-flexconnector-config.sh or $OPSA_HOME/bin/opsa-logfile-flexconnector-config.bat script to configure the Operations Analytics Log File Connector for HP ArcSight Logger.

> Configuring the Operations Analytics Log File Connector for HP ArcSight Logger using different methods than described in this documentation is not supported.

1. Stop the Operations Analytics Log File Connector for HP ArcSight Logger before configuring it. See "Manually Starting and Stopping the Operations Analytics Log File Connector for HP ArcSight Logger " for more information.

   > **Note**: You must restart the Operations Analytics Log File Connector for HP ArcSight Logger after configuring it.

2. Navigate to the root installation directory.

   > This is the folder in which you copied, then unzipped, the `opsa-arcsight-connector-dist-windows.zip` or `opsa-arcsight-connector-dist-linux.zip` file.

3. Run the following command to configure the Operations Analytics Log File Connector for HP ArcSight Logger:

   - **Windows**: `$OPSA_HOME/bin/opsa-logfile-flexconnector-config.bat`
   - **Linux**: `sh $OPSA_HOME/bin/opsa-logfile-flexconnector-config.sh`

4. The configuration menu appears, showing the following options:

   - "Option 1) Change Logger Server"
   - "Option 2) List Log Folders"
   - "Option 3) Add Log Folder"
   - "Option 4): Edit Log Folder"

- "Option 5): Delete Log Folder"
- "Option 6): Test Log Folders"
- "Option 7): Exit"

Select the option for the configuration task you want to complete.

Option 1) Change Logger Server

Use the **Change Logger Server** option to change the configuration associated with the connection between the Operations Analytics log file connector and the HP ArcSight Logger server.

After selecting this option, the configuration script prompts you for the parameters shown in the next table.

HP ArcSight Logger Server Parameters

Parameter	Description
HP ArcSight Logger Hostname	The hostname or IP address of the HP ArcSight Logger server to which you want the Operations Analytics Log File Connector for HP ArcSight Logger to send log messages.
HP ArcSight Logger Port (443)	The Smart Message Receiver port to which you want HP ArcSight Logger to connect. HP ArcSight Logger uses port 443 by default.
Name of Smart Message Receiver	The name of the Smart Message Receiver that you want to receive the log messages from the Operations Analytics Log File Connector for HP ArcSight Logger. By default, HP ArcSight Logger defines a Smart Message Receiver called **SmartMessage Receiver**. The Smart Message Receiver name you provide must be enabled on the HP ArcSight Logger server.

Option 2) List Log Folders

Use the **List Log Folder** option to display the current list of configured log folders and associated configuration parameters within the Operations Analytics Log File Connector for HP ArcSight Logger.

Option 3) Add Log Folder

Use the **Add Log Folder** option to add a log folder to the Operations Analytics Log File Connector for HP ArcSight Logger.

After selecting this option, the configuration script prompts you for the following configuration parameters associated with adding a log folder.

Log Folder Parameters

Parameter	Description
Log Folder Path	The full directory path in which the log files reside.
Log File Name Wildcard	The wildcard filter used to select which files to process in the log folder path.
Process Name	The name of the process that creates the log files in the log folder path.
Application Name	The name of the application to which the log files are associated.
Hostname	The hostname of the server from which the log files originated. If the log files originate from the server on which the Operations Analytics Log File Connector for HP ArcSight Logger is installed, this would be the hostname of the local server. If the log files originate from a remote server, specify the hostname of the server from which the log files originated.
Multiline Regular Expression	If the log files being collected in a log folder span more than one line, you must provide a regular expression that is used to match the beginning of a line. A frequently used example of this would be to create a regular expression to match a time stamp that is located at the beginning of a line.

Option 4): Edit Log Folder

Use the **Edit log Folder** option to list the current configured log folders. To edit a specific log folder, enter the number assigned to that log folder. After selecting this option, the configuration script prompts you for the following configuration parameters associated with editing that log folder. The configuration script shows the current configured values, as shown in the following table (the values between the parentheses).

After selecting this option, the configuration script prompts you for the following configuration parameters associated with editing the specified log folder.

Configured Log Folder Parameters

Parameter	Description
Log Folder Path (<*current configure value*>)	The full directory path in which the log files reside.

Configured Log Folder Parameters, continued

Parameter	Description
Log File Name Wildcard (<*current configure value*>)	The wildcard filter used to select which files to process in the log folder path.
Process Name (<*current configure value*>)	The name of the process that creates the log files in the log folder path.
Application Name (<*current configure value*>)	The name of the application to which the log files are associated.
Hostname (<*current configure value*>):	The hostname of the server from which the log files originated. If the log files originate from the server on which the Operations Analytics Log File Connector for HP ArcSight Logger is installed, this would be the hostname of the local server. If the log files originate from a remote server, specify the hostname of the server from which the log files originated.
Multiline Regular Expression (<*current configure value*>)	If the log files being collected in a log folder span more than one line, you must provide a regular expression that is used to match the beginning of a line. A frequently used example of this would be to create a regular expression to match a time stamp that is located at the beginning of a line.

Option 5): Delete Log Folder

Use the **Delete Log Folder** option to list the configured log folders. To delete a specific log folder, enter the number assigned to that log folder.

Option 6): Test Log Folders

Use the **Test Log Folders** option to run a test against all of the configured log folders. This test checks to see that the file name pattern and multiline regular expression are working as configured. It is highly recommended that you run this test to ensure that your configuration works before starting the Operations Analytics Log File Connector for HP ArcSight Logger.

The test does the following:

- For each configured log folder, the test script reads the first file that matches the file name pattern and parses that file using the multiline regular expression for that folder.
- The test script shows the first 3 messages of the file for each configured log folder.
- The test script only shows the first 40 characters of a line.

Option 7): Exit

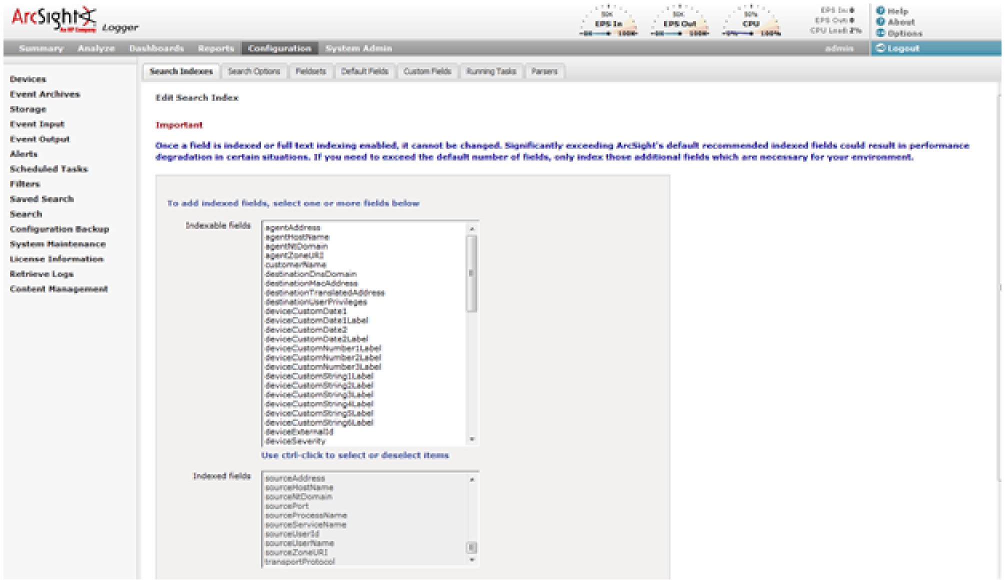
Use the **Exit** option to exit the Operations Analytics Log File Connector for HP ArcSight Logger configuration script .

Filtering HP ArcSight Logger Queries

You can use the `sourceHostName`, `sourceProcessName`, and `sourceServiceName` CEF fields to filter log messages to just those for a particular application and process. For example, suppose you want to query only **Collector** related log files for Operations Analytics. To do this, you might run the following HP ArcSight Logger query: `sourceProcessName = “OPSA Collector” AND sourceServiceName = “OPSA”`

If any CEF fields you are trying to use as search filters are not working, do the following for each of those CEF fields to add them as search fields:

1. From the HP ArcSight Logger UI, Navigate to the **Configuration**->**Search**->**Search Indexes** TAB
2. Add the CEF fields to HP ArcSight Logger you want to use in your HP ArcSight Logger search queries.



Edit Search Index

Important

Once a field is indexed or full text indexing enabled, it cannot be changed. Significantly exceeding ArcSight's default recommended indexed fields could result in performance degradation in certain situations. If you need to exceed the default number of fields, only index those additional fields which are necessary for your environment.

To add indexed fields, select one or more fields below

Indexable fields:
agentAddress
agentHostName
agentNtDomain
agentZoneURI
customerName
destinationDnsDomain
destinationMacAddress
destinationTranslatedAddress
destinationUserPrivileges
deviceCustomDate1
deviceCustomDate1Label
deviceCustomDate2
deviceCustomDate2Label
deviceCustomNumber1Label
deviceCustomNumber2Label
deviceCustomNumber3Label
deviceCustomString1Label
deviceCustomString2Label
deviceCustomString3Label
deviceCustomString4Label
deviceCustomString5Label
deviceCustomString6Label
deviceExternalId
deviceSeverity

Use ctrl-click to select or deselect items

Indexed fields:
sourceAddress
sourceHostName
sourceNtDomain
sourcePort
sourceProcessName
sourceServiceName
sourceUserId
sourceUserName
sourceZoneURI
transportProtocol

Manually Starting and Stopping the Operations Analytics Log File Connector for HP ArcSight Logger

Starting the Operations Analytics Log File Connector for HP ArcSight Logger : Navigate to the root installation directory; then run the following command to start the Operations Analytics Log File Connector for HP ArcSight Logger:

- **Windows**: `".\bin\arcsight.bat agents"`
- **Linux**: `./bin/arcsight agents`

Stopping the Operations Analytics Log File Connector for HP ArcSight Logger: Type `control-C` to stop the Operations Analytics Log File Connector for HP ArcSight Logger.

To make it easier to start and stop the Operations Analytics Log File Connector for HP ArcSight Logger, follow the instructions shown in "Configuring the Operations Analytics Log File Connector for HP ArcSight Logger to Run as a Service".

Configuring the Operations Analytics Log File Connector for HP ArcSight Logger to Run as a Service

It is recommended that you configure the Operations Analytics Log File Connector for HP ArcSight Logger to run as a service so that it automatically starts when rebooting the server on which the connector is running. Use one of the following methods to run the Operations Analytics Log File Connector for HP ArcSight Logger as a service.

Method 1 (Command Line):

> **Note**: You must run the `arcsight.bat` (Windows) and `arcsight` (Linux) scripts shown in this section as a user that has permission to add a service to the server on which you run the command. It is recommended that the user the service is run as is the same user that installed the Operations Analytics Log File Connector for HP ArcSight Logger.

1. From the server on which you installed the Operations Analytics Log File Connector for HP ArcSight Logger, navigate to the root installation directory.

   > This is the folder in which you copied, then unzipped, the `opsa-arcsight-connector-dist-windows.zip` or `opsa-arcsight-connector-dist-linux.zip` file.

2. Run the following command to configure the Operations Analytics Log File Connector for HP ArcSight Logger to run as a service.

   - **Windows**: `current\bin\arcsight.bat agentsvc -i -u` *`<user that installed the Operations Analytics Log File Connector for`*

HP ArcSight Logger>

- **Linux**: `current/bin/arcsight agentsvc -i -u` *<user that installed the Operations Analytics Log File Connector for HP ArcSight Logger>*

3. Complete the following steps to adjust the amount of memory used by the Operations Analytics Log File Connector for HP ArcSight Logger service:
   a. Edit the `<InstallDir>/current/user/agent/agent.wrapper.conf` file.

   b. Set the `wrapper.java.initmemory` property value to a larger value. For example, if the value is set to 256 (MB), you might double the value to 512 (MB).

   c. Set the `wrapper.java.maxmemory` property value to a larger value. For example, if the value is set to 512 (MB), you might double the value to 1024 (MB).

   > **Note**: The `wrapper.java.maxmemory` property value must be equal to or greater than the `wrapper.java.initmemory` property value.

   d. Save your work.

Method 2: User Interface

1. Navigate to the root installation directory.

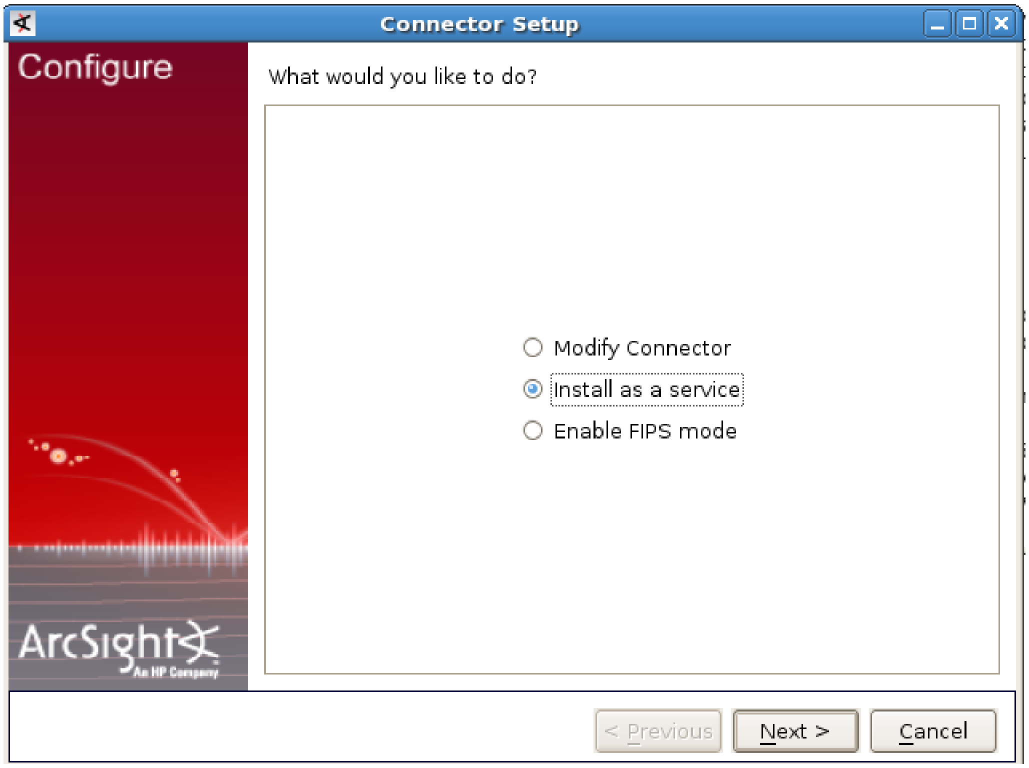
   > This is the folder in which you copied, then unzipped, the `opsa-arcsight-connector-dist-windows.zip` or `opsa-arcsight-connector-dist-linux.zip` file.

2. Run the following command to configure the Operations Analytics Log File Connector for HP ArcSight Logger to run as a service.

   - **Windows**: `".\bin\arcsight agentsetup.bat -c"`

   - **Linux**: `./bin/arcsight agentsetup –c`

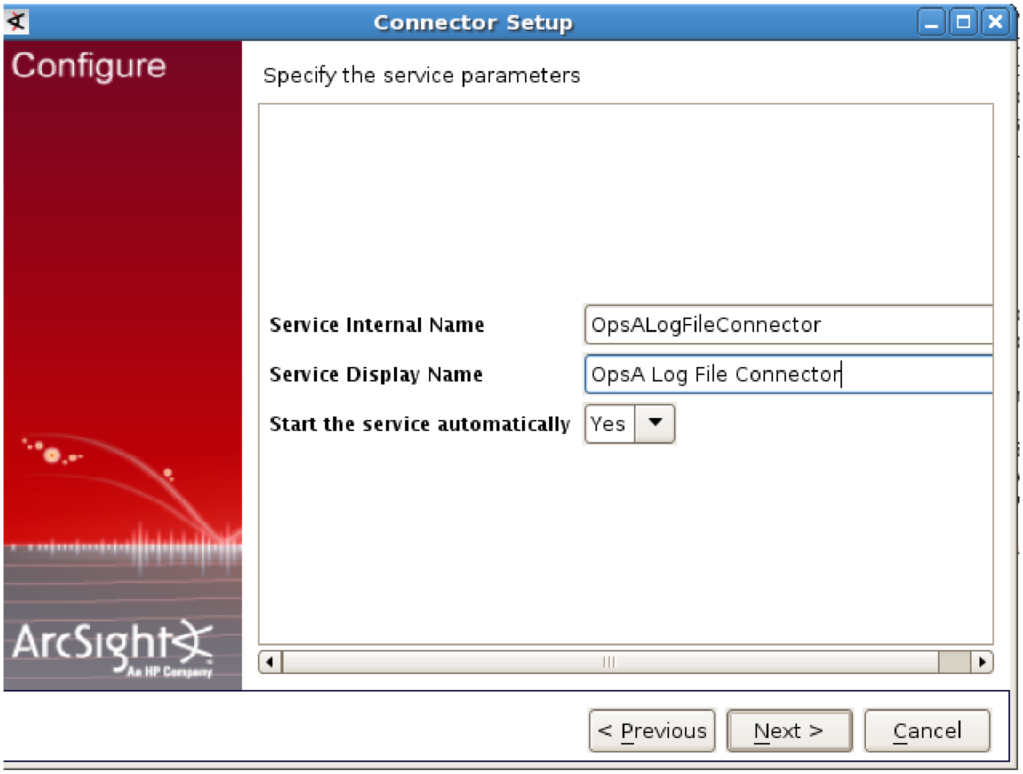
3. Select **Install as a service**; then click **Next**.



What would you like to do?

○ Modify Connector
● Install as a service
○ Enable FIPS mode

4. Enter the service name details. You must set **Start the service automatically** to **Yes**. Click **Next** after you finish.



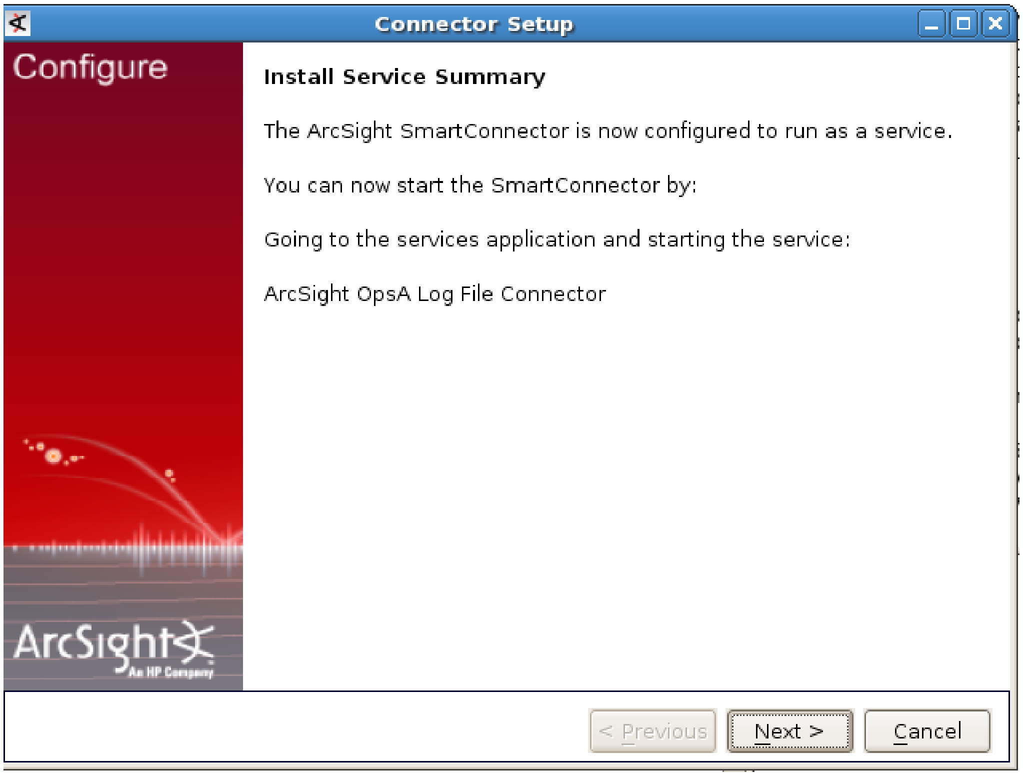
Specify the service parameters

Service Internal Name: OpsALogFileConnector

Service Display Name: OpsA Log File Connector

Start the service automatically: Yes

5. After the installation completes successfully, you should see the following message:



Install Service Summary

The ArcSight SmartConnector is now configured to run as a service.

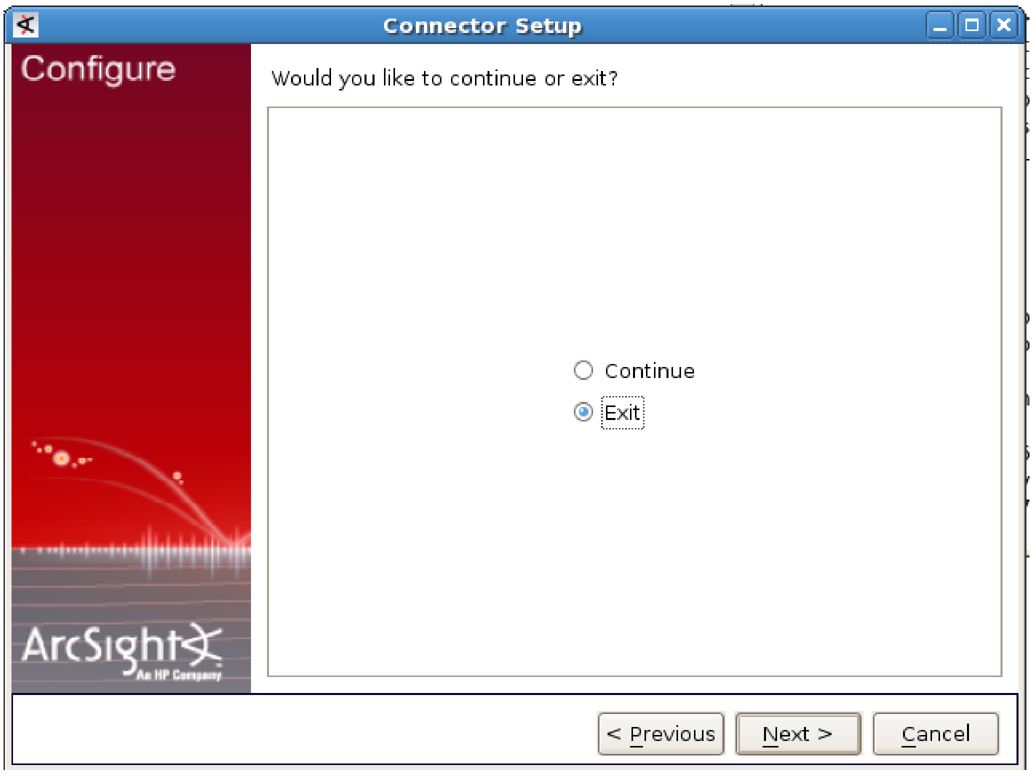
You can now start the SmartConnector by:

Going to the services application and starting the service:

ArcSight OpsA Log File Connector

Click **Next** to continue.

6. Select **Exit** ; then click **Next** to complete the installation.



Would you like to continue or exit?

○ Continue

● Exit

7. Complete the following steps to adjust the amount of memory used by the Operations Analytics Log File Connector for HP ArcSight Logger service:
   a. Edit the `<InstallDir>/current/user/agent/agent.wrapper.conf` file.

   b. Set the `wrapper.java.initmemory` property value to a larger value. For example, if the value is set to 256 (MB), you might double the value to 512 (MB).

   c. Set the `wrapper.java.maxmemory` property value to a larger value. For example, if the value is set to 512 (MB), you might double the value to 1024 (MB).

   > **Note**: The `wrapper.java.maxmemory` property value must be equal to or greater than the `wrapper.java.initmemory` property value.

   d. Save your work.

Stopping the Operations Analytics Log File Connector for HP ArcSight Logger from Running as a Service

If you have a need to stop Operations Analytics Log File Connector for HP ArcSight Logger from running as a service, use one of the following methods to run the Operations Analytics Log File Connector for HP ArcSight Logger as a service.:

Method 1 (Command Line):

> **Note**: You must run the `arcsight.bat` (Windows) and `arcsight` (Linux) scripts shown in this section as a user that has permission to remove a service from the server on which you run the command.

1. Navigate to the root installation directory.

   > **Note**: This is the folder in which you copied, then unzipped, the `opsa-arcsight-connector-dist-windows.zip` or `opsa-arcsight-connector-dist-linux.zip` file.

2. Run the following command to stop Operations Analytics Log File Connector for HP ArcSight Logger from running a service.

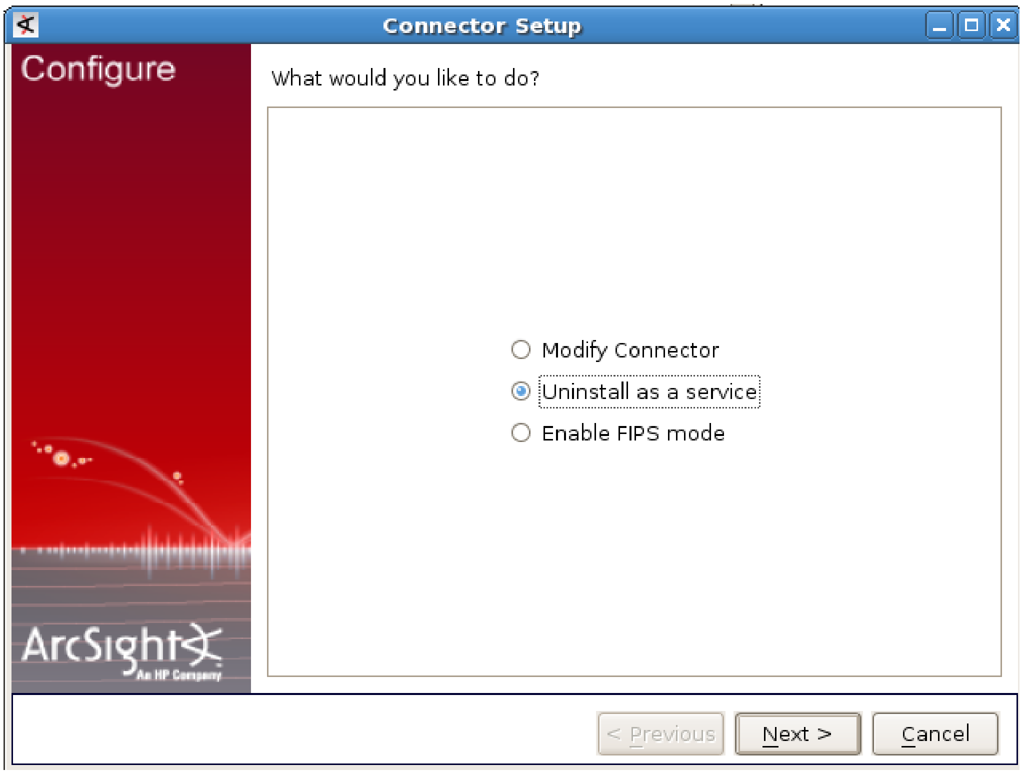
   - **Windows**: `current\bin\arcsight.bat agentsvc -r`
   - **Linux**: `current/bin/arcsight agentsvc -r`

Method 2 (User Interface):

1. Navigate to the root installation directory. Run the following command to stop Operations Analytics Log File Connector for HP ArcSight Logger from running a service.

   - **Windows**: `".\bin\arcsight agentsetup.bat -c"`
   - **Linux**: `./bin/arcsight agentsetup –c`

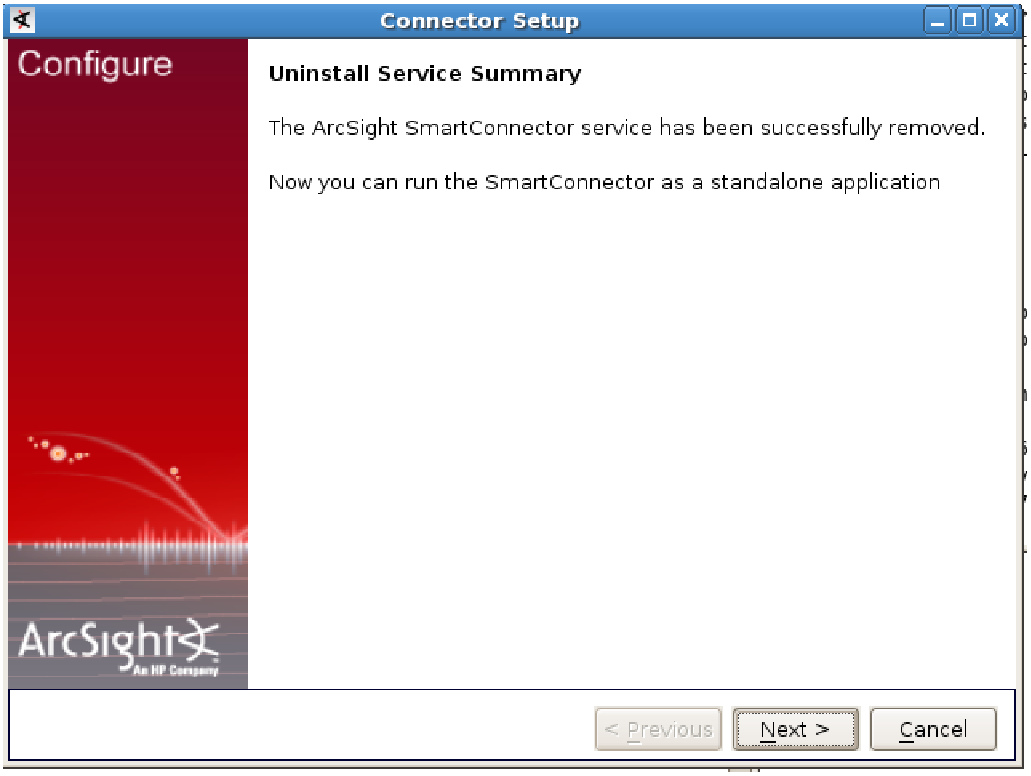
2. Select **Uninstall as a service**; then click **Next**.



What would you like to do?

○ Modify Connector
● Uninstall as a service
○ Enable FIPS mode

3. After the service is successfully uninstalled, you should see the following message:

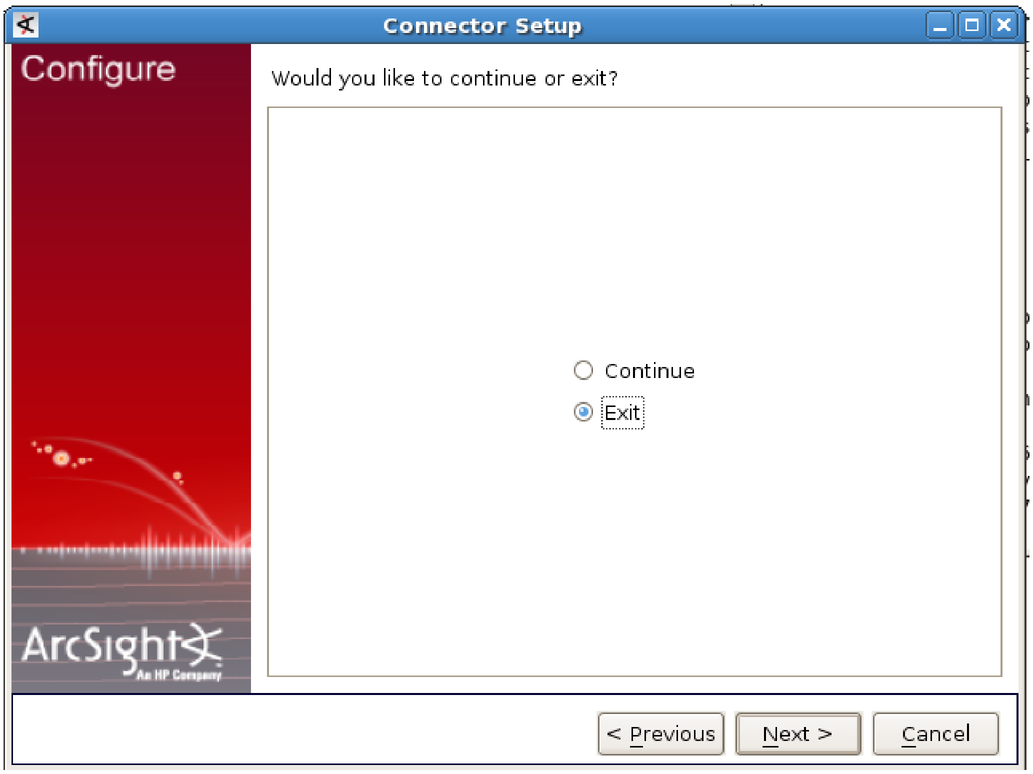


Uninstall Service Summary

The ArcSight SmartConnector service has been successfully removed.

Now you can run the SmartConnector as a standalone application

4. Select **Exit** ; then click **Next** to complete the installation.



Would you like to continue or exit?

○ Continue

● Exit

Troubleshooting the Operations Analytics Log File Connector for HP ArcSight Logger

When troubleshooting the Operations Analytics Log File Connector for HP ArcSight Logger, look in the `[<InstallDir>]/current/logs` directory for log files associated with the connector's directory. Look for log entries that contain `WARN` or `ERROR`.

Problem: You do not see any log messages appearing in the HP ArcSight Logger UI from the Operations Analytics Log File Connector for HP ArcSight Logger.

Solution: This problem could be caused by a connection error between the Operations Analytics Log File Connector for HP ArcSight Logger and the server. Check for log entries containing `AgentLoggerSecureEventTransport` in the `[<InstallDir>]/current/logs/agent.log` file. If you see an entry similar to the following, there are connection issues between the connector and the HP ArcSight Logger server:

```
[2013-07-05 09:18:03,449][ERROR]
[default.com.arcsight.agent.loadable.transport.event._
AgentLoggerSecureEventTransport][openConnection] Connection to
[10.10.10.155] port 443 and receiver [My Smart Receiver] failed 0-
event message test
```

Problem: Log messages appear in the HP ArcSight Logger server, but some of the CEF fields are wrong or missing.

Solution: Make sure that the data you entered is valid by checking the `[<InstallDir>]/current/logs/agent.log` file for log entries containing `AgentSanityVerifier`. The following log entry shows an example involving `sourceHostName` not appearing in the HP ArcSight Logger server due to an invalid host name being entered when configuring the Operations Analytics Log File Connector for HP ArcSight Logger:

```
[2013-07-08 13:46:26,271][WARN ][default.com.arcsight.agent.loadable._
AgentSanityVerifier][checkHostNames] Invalid device host name
encountered[my Hostname]
```

> As a best practice, always run the **Test Log Folders** option after configuring the Operations Analytics Log File Connector for HP ArcSight Logger.

Using Other ArcSight Connectors

Raw Log Message

For Operations Analytics to display a user friendly log message, it is recommended that you configure all ArcSight connectors to preserve the raw log message. If you prefer not to do this because of the extra cost of storing the raw message, then Operations Analytics uses the Raw CEF string when it displays the log message.

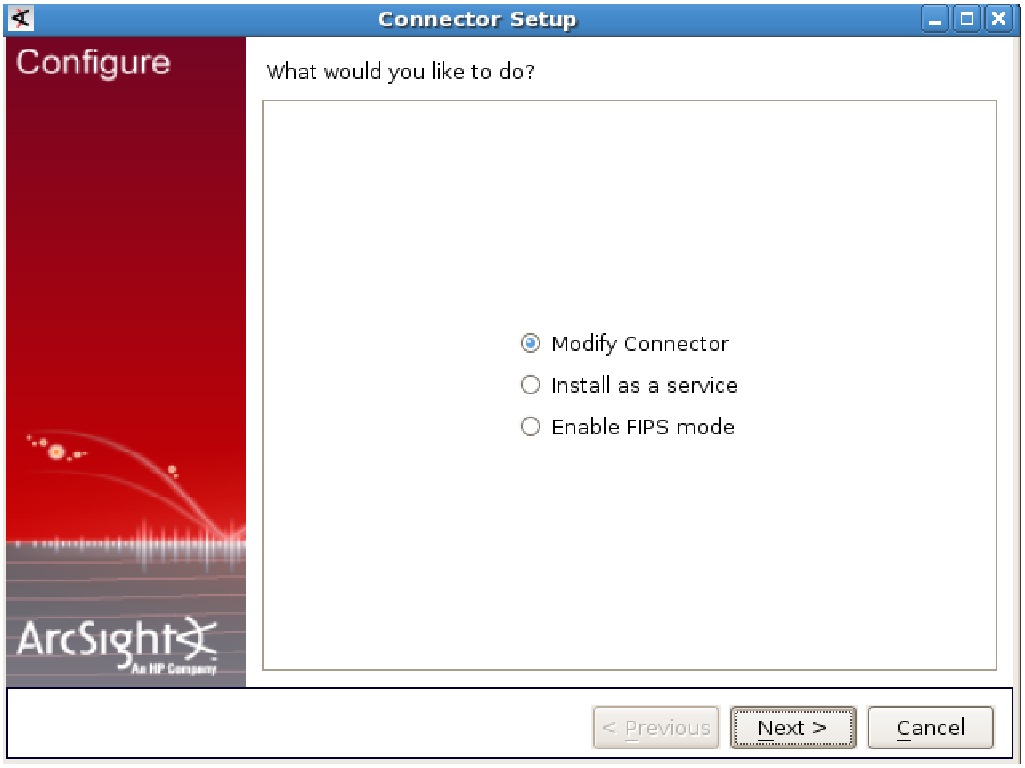
Do the following to set up the ArcSight connector to preserve the raw event:

1. Run the following command to start the setup script:

   - **Windows**: `<Connector Install Directory>/current/bin/runagentsetup.bat`

   - **Linux**: `<Connector Install Directory>/current/bin/runagentsetup.sh`

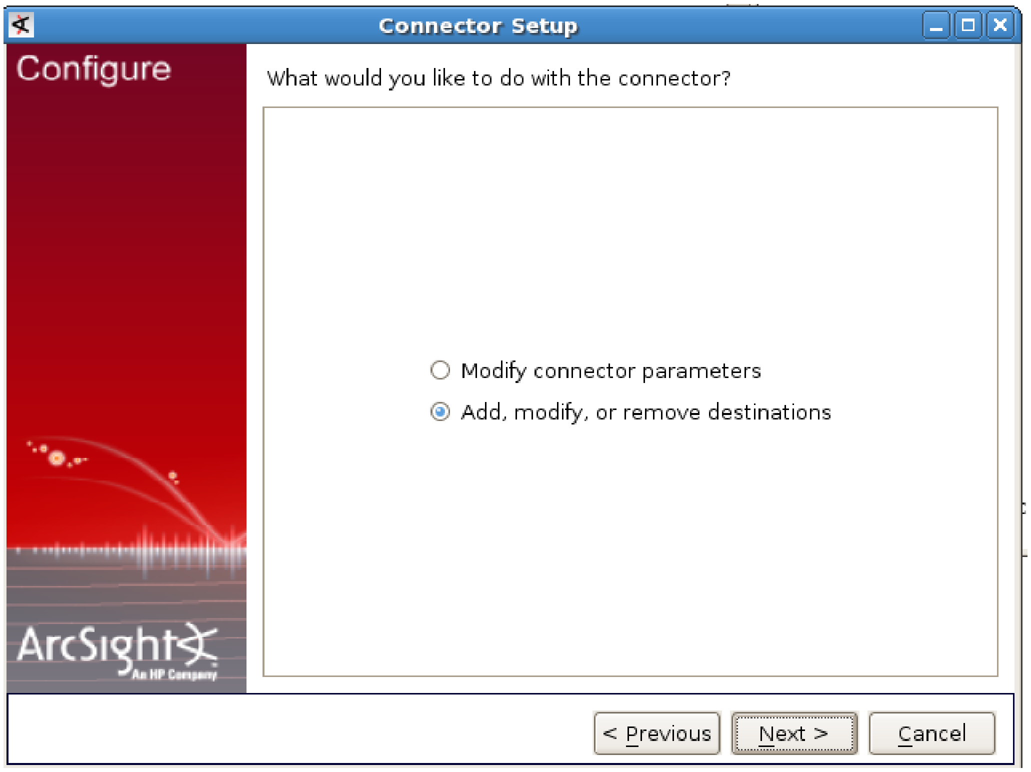
2. Select **Modify Connector**; then click **Next**.



What would you like to do?

● Modify Connector
○ Install as a service
○ Enable FIPS mode

3. Select **Add, modify, or remove destinations**; then click **Next**.

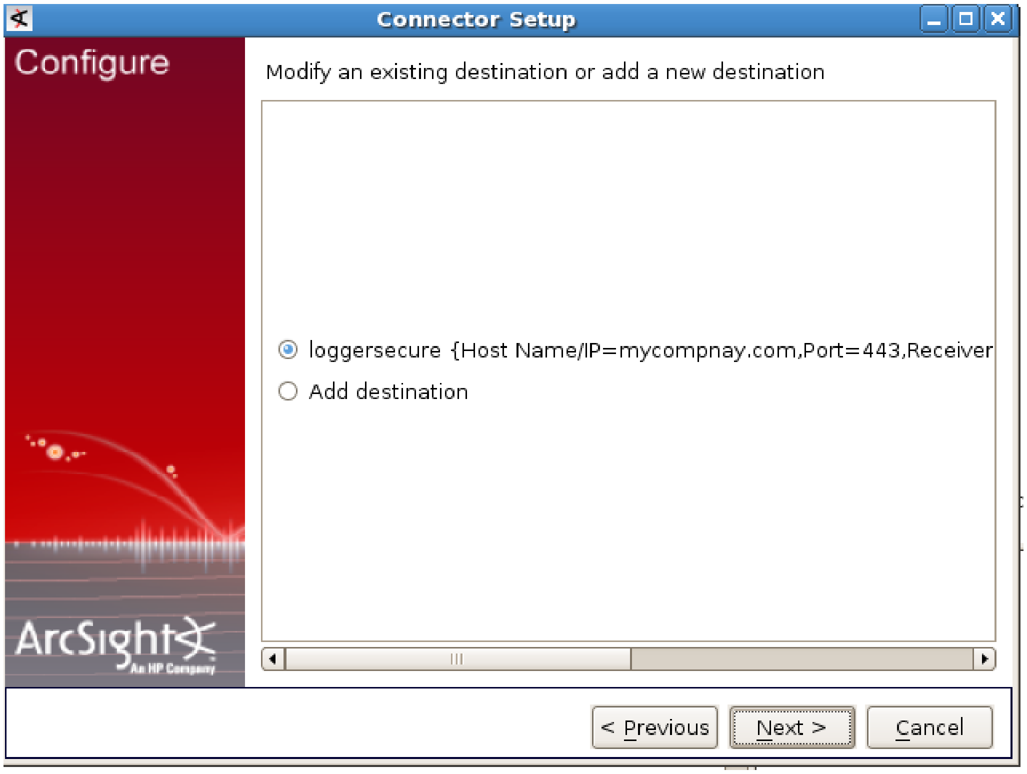


What would you like to do with the connector?

○ Modify connector parameters

● Add, modify, or remove destinations

4. Select the destination to modify; then click **Next**.

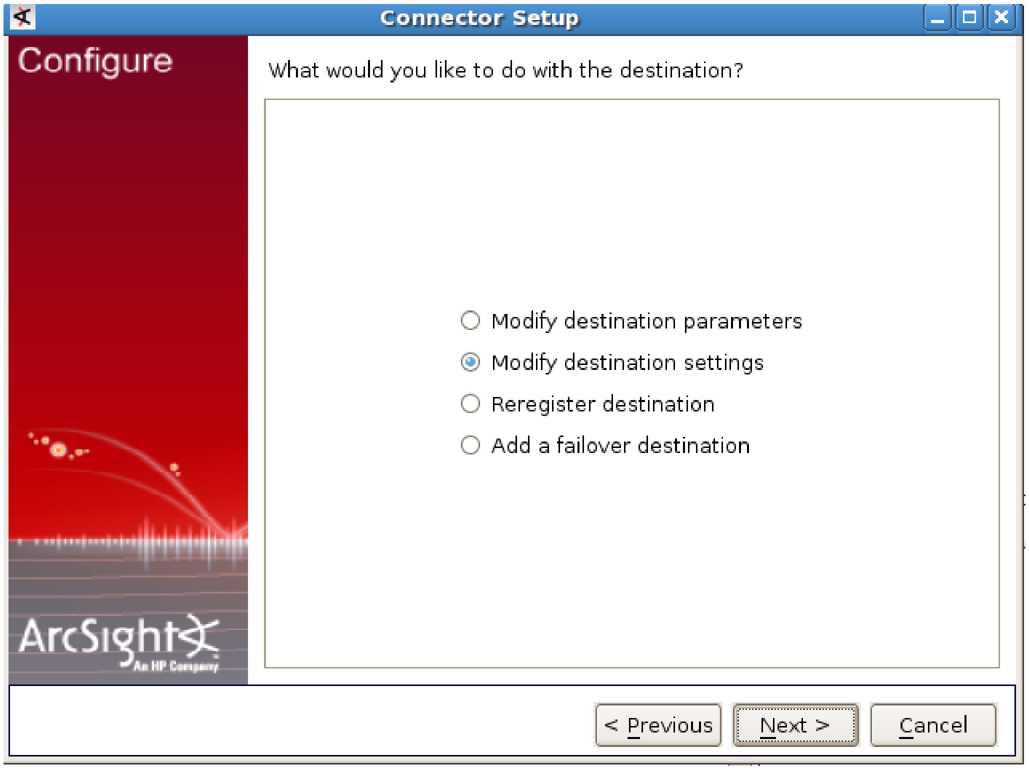


Modify an existing destination or add a new destination

● loggersecure {Host Name/IP=mycompnay.com,Port=443,Receiver

○ Add destination

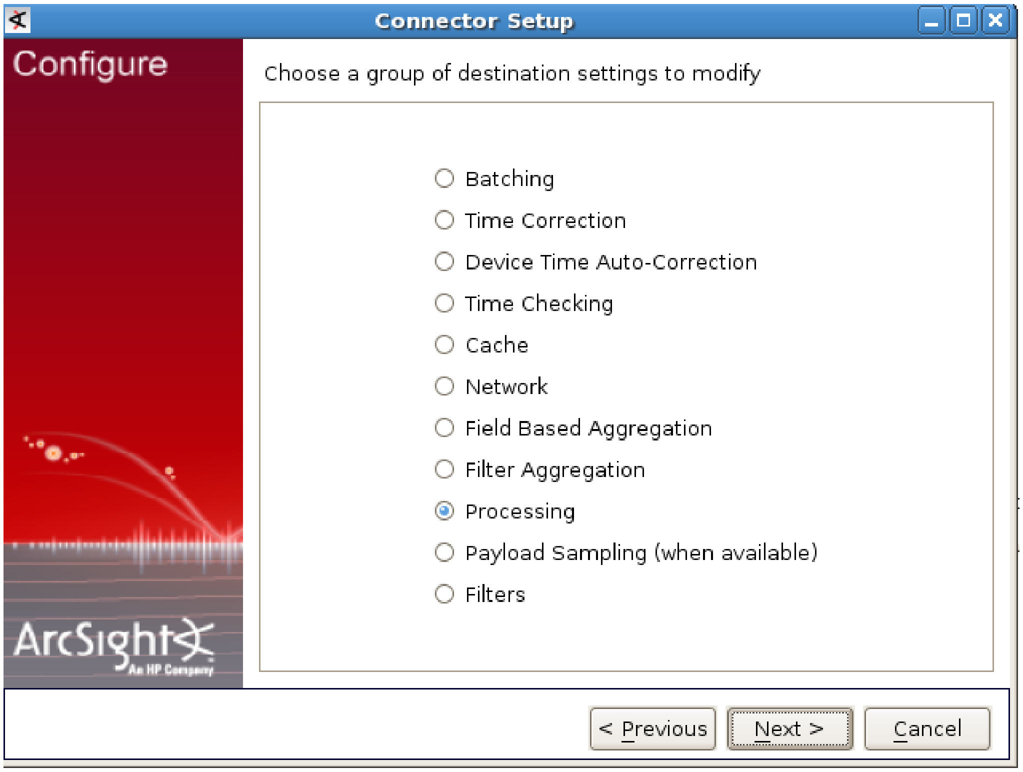
5. Select **Modify destination settings**; then click **Next**.



What would you like to do with the destination?

○ Modify destination parameters
● Modify destination settings
○ Reregister destination
○ Add a failover destination

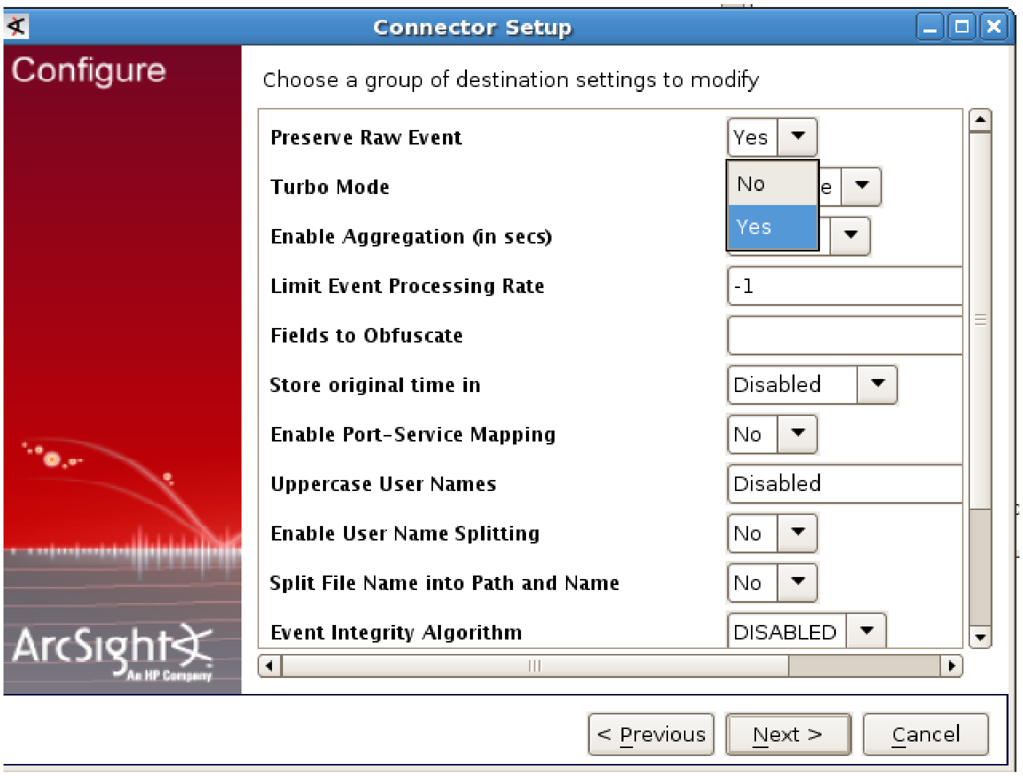
6. Select **Processing**; then click **Next**.



Choose a group of destination settings to modify

○ Batching
○ Time Correction
○ Device Time Auto-Correction
○ Time Checking
○ Cache
○ Network
○ Field Based Aggregation
○ Filter Aggregation
● Processing
○ Payload Sampling (when available)
○ Filters

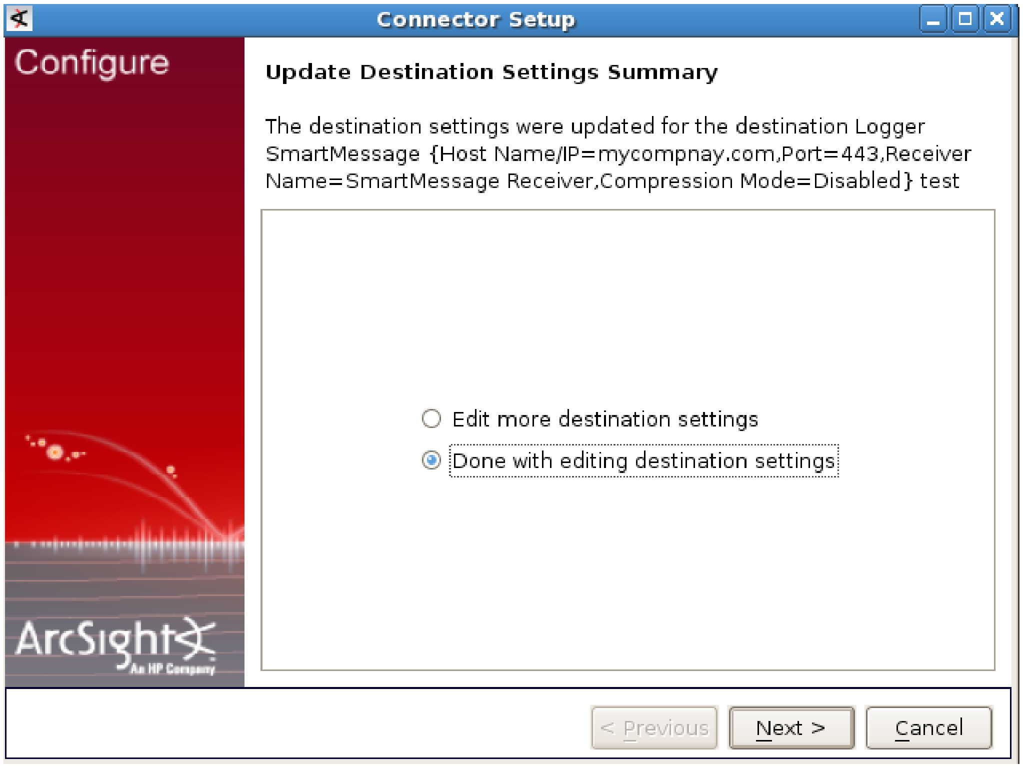
7. Set **Preserve Raw Event** to **Yes**; then click **Next**.



Choose a group of destination settings to modify

Preserve Raw Event	Yes
Turbo Mode	e
Enable Aggregation (in secs)	
Limit Event Processing Rate	-1
Fields to Obfuscate	
Store original time in	Disabled
Enable Port-Service Mapping	No
Uppercase User Names	Disabled
Enable User Name Splitting	No
Split File Name into Path and Name	No
Event Integrity Algorithm	DISABLED

8. Click **Done with editing destination settings**; then click **Next**.



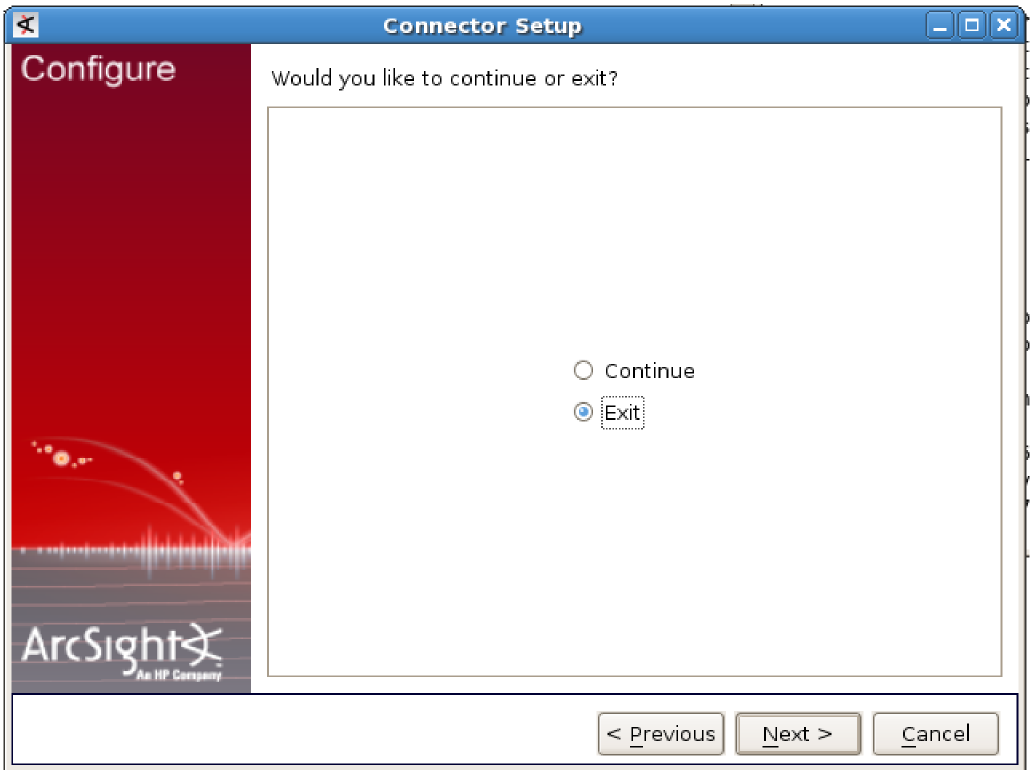
Update Destination Settings Summary

The destination settings were updated for the destination Logger SmartMessage {Host Name/IP=mycompnay.com,Port=443,Receiver Name=SmartMessage Receiver,Compression Mode=Disabled} test

○ Edit more destination settings

● Done with editing destination settings

9. Select **Exit**; then click **Next**.



Would you like to continue or exit?

○ Continue

● Exit

Setting Hostname, Application, and Process Names

If the ArcSight connector is not currently setting the `sourceHostName`, `sourceProcessName`, or `sourceServiceName` CEF fields, you can set these to the name of the process and application using the following steps:

If the ArcSight connector is not setting the CEF fields to store a process name, application name, or host name, you can correct this issue using the following steps:

1. Navigate to the `<`*`Connector Install Director`*`/current/user/agent/map` directory.

2. Identify all of the map property files in this directory (`map*.properties`), then identify the next available number that can be used. For example if the map property files listed were `map.0.properties map.1.properties` the next available number would be 2 (as in `map.2.properties`). This (next available) number is used to define the order in which the map files are processed by the ArcSight connector.

3. Create a file called `map.<`*`next available number`*`>.properties`.

4. Insert the following entries into the `map.<`*`next available number`*`>.properties` file:

a. Add the CEF fields you want to set as the first line in the file. For example, to set all three of the CEF fields (`set.event.sourceProcessName`, `set.event.sourceHostName`, and `set.event.sourceServiceName`), add the following line as the first line in the file:

   ```
   set.event.sourceProcessName, set.event.sourceHostName,
   set.event.sourceServiceName.
   ```

b. The second line contains the static values to be set for the CEF fields you just defined in the first line. For example, add the following line to the file to set the `sourceProcessName`, `sourceHostName`, and `sourceServiceName` CEF fields to `MyHostname`, `MyProcess`, and `MyApplication` respectively: `MyProcess, MyHostname.com, MyApplication`

   > **Example**:
   > ```
   > set.event.sourceProcessName,set.event.sourceHostName,set.event.sourceServiceName
   > MyProcess,MyHostname.com,MyApplication
   > ```

Uninstalling the Operations Analytics Log File Connector for HP ArcSight Logger

To uninstall the Operations Analytics Log File Connector for HP ArcSight Logger, do the following:

1. Stop the Operations Analytics Log File Connector for HP ArcSight Logger before continuing. See "Manually Starting and Stopping the Operations Analytics Log File Connector for HP ArcSight Logger " for more information.

2. If you configured the Operations Analytics Log File Connector for HP ArcSight Logger to run as a service then remove that service. See "Stopping the Operations Analytics Log File Connector for HP ArcSight Logger from Running as a Service " for more information.

3. Remove the root installation directory.

   > This is the folder in which you copied, then unzipped, the `opsa-arcsight-connector-dist-windows.zip` or `opsa-arcsight-connector-dist-linux.zip` file.

Task 4: Installing and Licensing the Operations Analytics Server Appliance using the VMware vSphere Client

Task 1: Planning your Deployment	**Task 2:** Installing and Configuring the Vertica Software	**Task 3:** Installing and Configuring HP ArcSight Logger	▶ **Task 4:** Installing and Licensing the Operations Analytics Server Appliance	**Task 5:** Installing and Configuring the Operations Analytics Collector Appliance	**Task 6:** Configuring Tenants and Collections	**Task 7:** Creating, Applying, and Maintaining Tags	**Task 8:** Communicating Collection Names and Meta Data Information to your Users

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. Select the **Power on after deployment** option; then click **Finish**.

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.

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.

> 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:

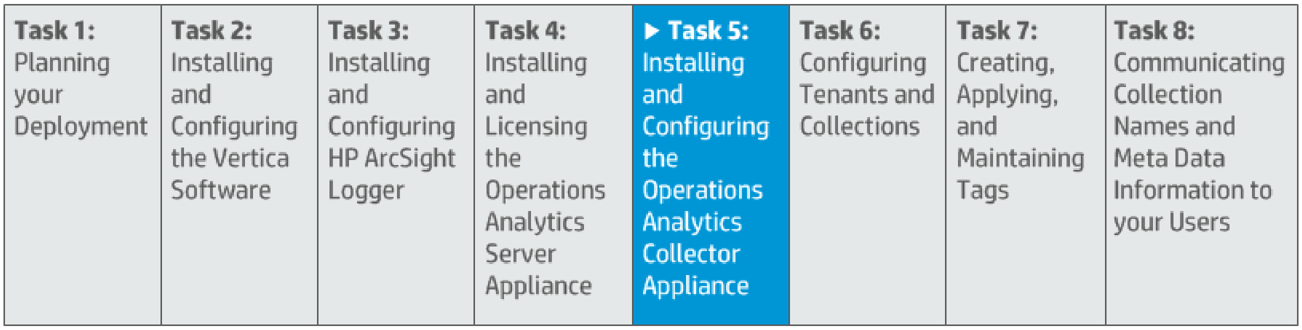
1. Run the following command from the Operations Analytics Server Appliance to install the Operations Analytics license:
   `$OPSA_HOME/bin/opsa-license-manager.sh -add <path to license file>`
   You should see a message that, among other information, includes the following:

   ```
   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



Task 1: Planning your Deployment	**Task 2:** Installing and Configuring the Vertica Software	**Task 3:** Installing and Configuring HP ArcSight Logger	**Task 4:** Installing and Licensing the Operations Analytics Server Appliance	▶ **Task 5:** Installing and Configuring the Operations Analytics Collector Appliance	**Task 6:** Configuring Tenants and Collections	**Task 7:** Creating, Applying, and Maintaining Tags	**Task 8:** Communicating Collection Names and Meta Data Information to your Users

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

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

1. 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 Collector Appliance; then click **Next**.

6. Select a resource pool.

7. Select the destination storage for the Collector Appliance files; then click **Next**.

8. Select the format on which you want to store the collector's virtual disks; then click **Next**.

9. Enter the network properties by specifying the field values shown in the following table.

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

   Network Properties

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

10. Specify the VA Host Name and Timezone settings; then click **Next**.

11. Select the **Power on after deployment** option; then click **Finish**.

Post-Installation Configuration Steps for Operations Analytics

The post installation script completes the final configuration steps for the different application components used by Operations Analytics. To finish the post-installation configuration steps 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.

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 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.

   - Host name of Vertica database (if it exists)
   - Port number of Vertica database
   - Database user name
   - Database password

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

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

5. The `opsa-server-postinstall.sh` script prompts you to change the passwords for the opsaadmin, opsatenantadmin, and opsa default application users. Follow the interactive instructions carefully to reset these passwords.

   > **Note**: See "Creating Tenants " 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].

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` does not prompt you for more than one set of Splunk configuration details.

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 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 information, and includes the default values shown in the following list. To accept the default value, click **Enter** for each prompt.

   - Host name of Vertica database (localhost)
   - Port number of Vertica database (5433)

- User name for the Vertica database (dbadmin)
- Password for the Vertica database

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.

Accessing Operations Analytics for the First Time

To log on to Operations Analytics:

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

2. After the Operations Analytics login screen appears, use the default user credentials to log on to Operations Analytics:
   User Name: opsa
   Password: opsa

Click ? to access the Operations Analytics online help.

Now you can configure your collections at " Configuring Tenants and Collections (Task 6)".

Chapter 4: Configuring Tenants and Collections (Task 6)

Task 1: Planning your Deployment	**Task 2:** Installing and Configuring the Vertica Software	**Task 3:** Installing and Configuring HP ArcSight Logger	**Task 4:** Installing and Licensing the Operations Analytics Server Appliance	**Task 5:** Installing and Configuring the Operations Analytics Collector Appliance	**▶ Task 6:** Configuring Tenants and Collections	**Task 7:** Creating, Applying, and Maintaining Tags	**Task 8:** Communicating Collection Names and Meta Data Information to your Users

A collection defines the data to be collected and corresponds to a database table in which the Operations Analytics Collector Appliance stores the data. To populate the Operations Analytics database with useful information you must configure collections using the information in this section. The instructions cover the following:

1. Registering your collector appliances.

2. Identifying the collections for which you want to collect data.

3. For any of the custom collections you must create a collection template that describes what is being collected.

4. Specifying what nodes to collect against in a node properties file.

5. Creating a collector for the each of the collections and assigning those collectors to a specific collector appliance.

"Terminology Used in this Document" and "Supported Deployments" for more information about data sources from which Operations Analytics can collect data.

You configure collections through command line interaction using the `opsa-collection-config.sh` script. Operations Analytics stores configurations on its file system and not in the Operations Analytics database. If you have multiple Operations Analytics Server Appliances installed, you must designate one of them from which to complete collection configuration. You should back up these files as part of your company's server backup strategy. All collection configuration files are stored in the `/opt/HP/opsa/conf/collection` directory.

For best results, configure your collections in the following order (from less complex to more complex collection configurations):

1. HPOM Events Collection

2. OMi Events Collection

3. HP Operations Agent Collection
4. HP Operations Smart Plug-in for Oracle Collection
5. HP Business Process Monitor Collection
6. NNMi Custom Poller Collection
7. NNM iSPi Performance for Metrics Component Health Collection
8. NNM iSPi Performance for Metrics Interface Health Collection
9. HP BSM RTSM NNMi Configuration Item Collection
10. ArcSight Logger Collection
11. Custom CSV Collection
12. Custom SiteScope Collection
13. Structured Log Collection

Registering Collector Appliances and Preparing for Collector Configuration

Operations Analytics relies on collected metrics, topology, event, and log file data from a diverse set of possible data sources. An Operations Analytics Collector Appliance contains the software that listens for data coming from a device. Each server that is running the Operations Analytics Collector software must be registered as a Collector Appliance. Customers can register a collector, then use that registered collector for multiple collections.

During the process of collector configurations, you must complete the steps in this section before configuring either custom or predefined collections. After you complete the steps in this section continue to "Configuring Collections using Predefined Templates " and "Configuring Collections for Custom Data Sources " to finish configuring your collections.

Registering a collector appliance is a two-step process:

1. "Creating Tenants "
2. "Registering Each Collector Appliance"

Creating Tenants

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. For each collection you define for the data sources supported by Operations Analytics, you must define a corresponding Tenant Admin.

Before creating collections, you can create a new tenant and the corresponding Tenant Admin, decide on which existing tenant to use, or use the default Tenant, opsatenantadmin, before proceeding with collection configuration. A collection is automatically associated with a tenant depending on the Tenant Admin user that the Operations Analytics administrator provides as input when running the `$OPSA_HOME/bin/opsa-collection-config.sh` script.

When using the `$OPSA_HOME/bin/opsa-collection-config.sh` script, some examples in this document use a predefined Tenant Admin user, opsatenantadmin, for the predefined opsa_ default tenant. When defining collections, replace the opsatenantadmin shown in the example with the Tenant Admin user for the collection you are creating.

Note: You can configure a collector to collect data from a data source for only one tenant. So a single collector cannot be used to collect data from a single data source for multiple tenants.

Note: There might be tenant limitations when configuring collections for products that support multiple tenants. Each collector you configure for a collection supports a single tenant, so the data source from which it is collecting must also be for a single tenant. See the *Operations Analytics Support Matrix* for a list of these limitations.

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* in the Operations Analytics help for more information.

You can create a tenant from the Operations Analytics console or by using the `$OPSA_HOME/bin/opsa-tenant-manager.sh` script. See *Add a Tenant* in the Operations Analytics help for more information about creating a tenant using the Operations Analytics console. To create a tenant and a Tenant admin user for a collection by using the `opsa-tenant-manager.sh` script, do the following:

1. Run the `$OPSA_HOME/bin/opsa-tenant-manager.sh` command from the Operations Analytics Server Appliance as a user assigned to the Super Admin User Group. See the *opsa-tenant-manager.sh* reference page (or the Linux manpage) for information about managing tenants.

2. Enter **Add a new tenant** and follow the interactive commands to add the new tenant.

3. Run the `$OPSA_HOME/bin/opsa-tenant-manager.sh` command as a user assigned to the Super Admin User Group. .

4. Enter **Add a new user** and follow the interactive commands to add a user assigned to the Tenant Admin user group for the newly created tenant.
   See the *opsa-tenant-manager.sh* reference page (or the Linux manpage) or *Manage Users* in the Operations Analytics help for information about managing users.

See the *opsa-tenant-manager.sh* reference page (or the Linux manpage) or *Manage Users* in the Operations Analytics help for information about managing users.

If you do not create a Tenant Admin user while adding a new tenant (as shown above in steps 3 and 4), add the Tenant Admin user for the new tenant later using the `$OPSA_HOME/bin/opsa-user-manager.sh` script. Do the following:

1. Run the `$OPSA_HOME/bin/opsa-user-manager.sh` command.

2. Enter **Add a new user** option.

3. Enter the Super Admin username and password.

4. Enter the Tenant Name for which you must add the Tenant Admin user.

5. Enter the new Tenant Admin user name.

6. Enter the new password for the new Tenant Admin user name.

7. Confirm the password.

The newly added Tenant Admin user is now available to add, modify, and delete users for its specified tenant. See the *opsa-user-manager.sh* reference page (or the Linux manpage) for more information.

Configuring and Managing Logger or Splunk for a Tenant

Use the information in this section to configure and manage Logger or Splunk configurations for a tenant.

> **Note**: If the log management software is Logger, you can configure more than one Logger for a tenant. If the log management software is Splunk, you can configure only one Logger for a tenant.

> **Note**: For this release, Operations Analytics supports Splunk version 5.0.2.

> **Note**: When running the following command, use port 443 for Logger and port 8089 for Splunk.

To add an HP ArcSight Logger or Splunk configuration for a tenant, run the following command:

```
opsa-logger-config-manager.sh -loginUser <Tenant Admin User> -
loginPassword <password> -add -loggerType (arcsight | splunk) -host
<hostname> -port <port> -sslEnabled (true | false) -username <user> -
password <password>
```

To delete an HP ArcSight Logger or Splunk configuration for a tenant, run the following command:

```
opsa-logger-config-manager.sh -loginUser <Tenant Admin User> -
loginPassword <password> -delete -host <hostname>
```

To list existing HP ArcSight Logger or Splunk configurations for a tenant, run the following command: `opsa-logger-config-manager.sh -loginUser <Tenant Admin User> - loginPassword <password> -list`

To update an existing HP ArcSight Logger or Splunk configuration for a tenant, run the following command: `opsa-logger-config-manager.sh -loginUser <Tenant Admin User> - loginPassword <password> -update -host <hostname> -port <port> - password <password>`

See the *opsa-logger-config-manager.sh* reference page (or the Linux manpage) for more information.

Registering Each Collector Appliance

You must register each Operations Analytics Collector Appliance you plan to use with the Operations Analytics Server Appliance. If you plan to use Tenants, you must use the `-tenant` option with the `opsa-collection-config.sh`command. See the *opsa-collection-config.sh* reference page (or the Linux manpage) for more information.

To register an Operations Analytics Collector Appliance with the Operations Analytics Server Appliance, do the following:

1. Run the following command on the Operations Analytics Collector Appliance to make sure the opsa-collector process is running:

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

   Look for a message stating the `opsa-collector` process is running. If the message states that the `opsa-collector` process is stopped, restart the process using the following command: `$OPSA_HOME/bin/opsa-collector start`.

2. Run the following command from the Operations Analytics Server Appliance:

   ```
   $OPSA_HOME/bin/opsa-collection-config.sh -register -collectorhost
   <fully-qualified domain name of the collector appliance host> -port
   9443 -username <tenant admin user>
   ```

> **Note**: If you have the collector appliance configured to use SSL for data communications, use the `-ssl` option in this command. If you have changed the HTTP user name or password on the Operations Analytics collector appliance, use the `-coluser` and `-colpass` option in this command. You must also use the fully-qualified domain name of the collector appliance host when using this command. See the *opsa-collection-config.sh* reference page (or the Linux manpage) for more information.

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

> **Note**: The default port to which Operations Analytics listens is 9443. You can modify this port in cases of port conflicts. See "Configuring the HTTPS and HTTPS Port for the Operations Analytics Collector Appliance" for more information.

If the script communicates successfully with the Operations Analytics Collector Appliance, it registers it in the Operations Analytics Server Appliance database and displays a success message.

Configuring Collections using Predefined Templates

Operations Analytics supports several predefined collection templates. See "Supported Deployments" for a list of predefined collection templates.

To configure Operations Analytics to collect data from the supported data sources you plan to use, you must configure collections using a list of predefined collection templates that reside on the Operations Analytics Server Appliance. These predefined collection templates are defined in advance so that administrators only have to configure Operations Analytics collectors to collect data using those predefined collection templates.

You can use the `$OPSA_HOME/bin/opsa-collection-setup.sh` script to assist you when configuring collections that use predefined templates. See the *opsa-collection-setup.sh* reference page (or the Linux manpage) for more information.

> **Note**: Use the `$OPSA_HOME/bin/opsa-collection-setup.sh` script to assist you when first setting up a collection. See the *Operations Analytics Quick Start Guide* for information about how to use the `$OPSA_HOME/bin/opsa-collection-setup.sh` script.
>
> To obtain a copy of the *Operations Analytics Quick Start Guide*, go to: **http://h20230.www2.hp.com/selfsolve/manuals**
>
> This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html
Or click the **New users - please register** link on the HP Passport login page.

Note: If you want to set up your collections manually or make changes to existing collections, use the collection configuration information in this document. Only use the `$OPSA_HOME/bin/opsa-collection-setup.sh` script to assist you when first setting up a collection.

Before creating collections, you can create a new tenant and the corresponding Tenant Admin, decide on which existing tenant to use, or use the default Tenant, opsatenantadmin, before proceeding with collection configuration. A collection is automatically associated with a tenant depending on the Tenant Admin user that the Operations Analytics administrator provides as input when running the `$OPSA_HOME/bin/opsa-collection-config.sh` script.

When using the `$OPSA_HOME/bin/opsa-collection-config.sh` script, some examples in this document use a predefined Tenant Admin user, opsatenantadmin, for the predefined opsa_default tenant. When defining collections, replace the opsatenantadmin shown in the example with the Tenant Admin user for the collection you are creating.

Complete the following configuration steps for the predefined data collection templates that reside on the Operations Analytics Server Appliance:

- "Configuring an HP Operations Manager (HPOM) Events Collection"
- "Configuring an HP Operations Manager (OMi) Events Collection"
- "Configuring an HP Operations Agent Collection"
- "Configuring an HP Operations Smart Plug-in for Oracle Collection"
- "Configuring an HP Business Process Monitor Collection"
- "Configuring an NNMi Custom Poller Collection"
- "Configuring an NNM ISPi Performance for Metrics Component Health Collection"
- "Configuring an NNM ISPi Performance for Metrics Interface Health Collection"
- "Configuring an HP BSM RTSM Configuration Item (CI) Collection"

Configuring an HP Operations Manager (HPOM) Events Collection

For special circumstances related to how Microsoft SQL Server is set up in the HPOM environment, see "Configuring HP Operations Manager (HPOM) (Creating a Database User Account on an HPOM Database Server)"

Setting the Correct Time Zone

An Operations Analytics Collector Appliance uses the GMT time zone for the HPOM event source. If the HPOM server is in a different time zone, you must specify that time zone in the collection template file before configuring the HPOM collection.

Do the following if you want to specify a time zone other than GMT:

1. Edit the following collection template file:
   `/opt/HP/opsa/conf/collection/server/config.templates/om/<`*`template version`*`>/events/omevents`
   The default <*template version*> is 1.0. Specify the version as appropriate.

2. Specify the time zone offset from GMT by editing the `timezone` attribute of the following column element names: `timestamp`, `TimeReceivedTimeStamp`, and `TimeCreatedTimeStamp`.

   For example, to specify a timezone that is 3.5 hours ahead of GMT the `timezone` attribute's value needs to be `GMT+3:30`

   ```
   <column name="timestamp" position="2" datatype="datetime"
   length="0" datetype="date" format="MM/dd/yyyy HH:mm:ss"
   timezone="GMT+3:30" key="no" mapsto="TimeOfStateChangeTimeStamp"
   value="" label="Timestamp" columnname="timestamp" unit="" tags=""
   type="attribute" />
   ```

3. You must complete this change for both of the following `collection` elements:
   - The element with the `sourcegroup` attribute set to `mssql`.

   - The element with the `sourcegroup` attribute set to `oracle`.

After you complete the above steps to specify your time zone in the collection template file, you can use the instructions in the remainder of this section to configure the HPOM collection.

Configuration Steps

After you complete the steps in this section, the HP Operations Manager Events Collection collects events every 15 minutes, and collects all OM events that occurred since the last poll.

> **Note**: An Operations Analytics Collector Appliance can only collect data for a single HPOM or OMi event source. If you configure more than one HPOM or OMi event source for an Operations Analytics Collector Appliance, it collects the events from only one of the event sources at every collection interval. It cannot be determined from which event source data collection occurs for a given collection interval. To remedy this, configure a separate Operations Analytics Collector appliance for each HPOM or OMi event source.

There are two methods of configuring Operations Analytics for the HPOM events collection, the **Automated Configuration Method** and the **Manual Configuration Method**. You must select one of these methods to configure Operations Analytics for the HPOM events collection. Do not attempt to use both the Automated Configuration Method and the Manual Configuration Method.

Automated Configuration Method: This approach is more automated than the Manual Configuration Method, making configuration easier. Do the following to use the Automated Configuration Method:

1. The Automated Configuration Method provides the sample collection template, `$OPSA_HOME/conf/collection/sample/sample_auto_config_node.properties`, located on the Operations Analytics server appliance. Copy the `sample_auto_config_node.properties` file to a separate location, then edit the `sample_om_node.properties` file and add, among other information, the following Operations Manager information:

   - For an OMW host (HP Operations Manager on a Windows server), the Automated Configuration Method includes the OMW host's fully-qualified domain name and its database details.

   - For an OMU host (HP Operations Manager on a UNIX or Linux server), the Automated Configuration Method includes the OMU host's fully-qualified domain name and its database details.

2. Save your work.

3. Encrypt the passwords in the node properties file by running the following command from the Operations Analytics Server Appliance:
   ```
   $OPSA_HOME/bin/opsa-collection-config.sh –encrypt <path>/sample_auto_config_node.properties
   ```

4. Run the following command from the Operations Analytics Server Appliance to configure the collector hosts and publish the collection information:

   ```
   $OPSA_HOME/bin/opsa-collector-auto-conf.sh <path>/<sample_om_node.properties> -collectevents -configuredomain [Oracle|System] -username <tenant admin user>
   ```

   Note: The `opsa-collector-auto-conf.sh` script sets up HP Operations Agent, HP Operations Smart Plug-in for Oracle, and OM event collection using only one command.

   Note: The command output shows the list of registered collectors and distributes the list of nodes providing system performance metrics, Oracle performance metrics, or both among the registered collectors.

   Note: The `opsa-collector-auto-conf.sh` script prompts you for the Tenant Admin password for the username you use in the commands shown in this section. See the opsa-collector-auto-conf.*sh* reference page (or the Linux manpage) for more information.

Manual Configuration Method: Do the following for a more manual approach to configuring Operations Analytics for the HPOM events collection:

1. A node list file contains details about the sources from which you plan to collect information. There are sample nodelist files located in the `$OPSA_HOME/conf/collection/sample` directory. Operations Analytics administrators can use these sample files to publish the node list file. There are two sample node list files for the HPOM Events collection: `sample_OMW_node.properties` (for HP Operations Manager for Windows) and `sample_OMU_node.properties` (for HP Operations Manager for UNIX and Linux). For HPOM events, the node list files contain, among other information, a list of servers that have HPOM installed.

   The node list file for HP Operations Manager for Windows must include the information shown in the following table:

   Node List File Fields and Values

Field	Value
omwdbserver.hostdnsname	The fully-qualified domain name of the HPOM server.
omwdbserver.port	`1433`: The port used to connect to the HPOM server.
omwdbserver.username	The user name to use for connecting to the HPOM server. See "Configuring HP Operations Manager (HPOM) (Creating a Database User Account on an HPOM Database Server)" for instructions about creating this user.
omwdbserver.instanceName	`OVOPS`
omwdbserver.datasource_type	`OM`
omwdbserver.database_type	`MSSQL`
omwdbserver.database_name	`openview`

   The node list file for HP Operations Manager for UNIX and Linux must include the information shown in the following table:

Field	Value
omudbserver.hostdnsname	The fully-qualified domain name of the HPOM server.
omudbserver.port	`1521`: The port used to connect to the HPOM server.
omudbserver.username	`opc_op`: The user name to use for connecting to the HPOM server.
omudbserver.database_	`null`

Field	Value
name	
omudbserver.instance_ name	openview
omudbserver.datasource_ type	OM
omudbserver.database_ type	ORACLE

To edit the node list file, do the following from the Operations Analytics Server Appliance:

a. Copy the `sample_OMW_node.properties` or `sample_OMU_node.properties` file from the `$OPSA_HOME/conf/collection/sample` directory to some location, such as `/tmp/mynodelist.properties`.

b. Edit the `/tmp/mynodelist.properties` file, adding the appropriate information; then save your work.

2. Run the following command from the Operations Analytics Server Appliance to encrypt the password:

```
$OPSA_HOME/bin/opsa-collection-config.sh -encrypt
/tmp/mynodelists.properties
```

3. Run the following command from the Operations Analytics Server Appliance to create the collector configuration:

```
$OPSA_HOME/bin/opsa-collection-config.sh -create -nodelist
/tmp/mynodelist.properties -collectorhost <fully-qualified-domain-
name of collector host> -source om -domain events -group omevents -
username <tenant admin user>
```

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

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

4. Run the following command from the Operations Analytics Server Appliance to validate the collection configuration you just created:

```
$OPSA_HOME/bin/opsa-collection-config.sh -list -allversions -
```

```
collectorhosts -username <tenant admin user>
```

To verify a successful collection configuration creation, look for a message showing the expected collector host name, tenant name, and tenant version. The message should also include the source template details such as its `version`, `domain`, and `group`.

5. Run the following command from the Operations Analytics Server Appliance to publish this collection configuration to the Operations Analytics Collector Appliance :

   ```
   $OPSA_HOME/bin/opsa-collection-config.sh -publish -collectorhost fully-
   qualified domain name of the collector host> –username <tenant admin user>
   ```

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

Configuring an HP Operations Manager (OMi) Events Collection

After you complete the steps in this section, the HP OMi Events Collection collects events every 15 minutes, and collects all OMi events that occurred since the last poll.

> **Note**: The OMi collection is also able to accept events from HP Service Health Analyzer (SHA), a component of Business Service Management (BSM). If you have installed SHA on a BSM server and have configured the OMi collection, the OMi collection automatically accepts SHA events. You can then use the collected SHA event data to anticipate and predict IT problems. The following is a short description of SHA.

HP Service Health Analyzer (SHA): HP Service Health Analyzer analyzes abnormal service behavior and alerts IT managers of service degradation before an issue affects their business.

> **Note**: An Operations Analytics Collector Appliance can only collect data for a single HPOM or OMi event source. If you configure more than one HPOM or OMi event source for an Operations Analytics Collector Appliance, it collects the events from only one of the event sources at every collection interval. It cannot be determined from which event source data collection occurs for a given collection interval. To remedy this, configure a separate Operations Analytics Collector appliance for each HPOM or OMi event source.

You must complete the following steps for the OMi collection events:

1. A node list file contains details about the sources from which you plan to collect information. There are sample nodelist files located in the `$OPSA_HOME/conf/collection/sample` directory. Operations Analytics administrators can use these sample files to publish the node list file. Choose the sample node list file based on the database used by your HP OMi

application: `sample_OMi_MSSQL_node.properties` or `sample_OMi_ORACLE_node.properties`. The node list file for the HP OMi Event collection must include the information shown in the following table:

Node List File Fields and Values

Field	Value
omidbserver.hostdnsname	The fully-qualified domain name of the OMi server.
omidbserver.port	`1433`: The port used to connect to the OMi server.
omidbserver.username	`USERNAME`: The user name to use for connecting to the OMi server.
omidbserver.instanceName	`INSTANCE_NAME`
omidbserver.datasource_type	`OMI`
omidbserver.database_type	`ORACLE`
omidbserver.database_name	`DATABASE_NAME`

To edit the node list file, do the following from the Operations Analytics Server Appliance:

a. Copy the `sample_OMi_MSSQL_node.properties` or `sample_OMi_ORACLE_node.properties` file from the `$OPSA_HOME/conf/collection/sample` directory to some location, such as `/tmp/mynodelist.properties`.

> **Note**: Choose the sample node list file based on the database used by your HP OMi application.

b. Edit the `/tmp/mynodelist.properties` file, adding the appropriate information; then save your work.

2. Run the following command from the Operations Analytics Server Appliance to encrypt the password:

```
$OPSA_HOME/bin/opsa-collection-config.sh -encrypt
/tmp/mynodelists.properties
```

3. Run the following command from the Operations Analytics Server Appliance to create the collector configuration:

```
$OPSA_HOME/bin/opsa-collection-config.sh -create -nodelist
/tmp/mynodelist.properties -collectorhost <fully-qualified-domain-
name of collector host> -source omi -domain events -group omievents
-username <tenant admin user>
```

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

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

4. Run the following command from the Operations Analytics Server Appliance to validate the collection configuration you just created:

   ```
   $OPSA_HOME/bin/opsa-collection-config.sh -list -allversions -
   collectorhosts -username <tenant admin user>
   ```

   To verify a successful collection configuration creation, look for a message showing the expected collector host name, tenant name, and tenant version. The message should also include the source template details such as its `version`, `domain`, and `group`.

5. Run the following command from the Operations Analytics Server Appliance to publish this collection configuration to the Operations Analytics Collector Appliance :

   ```
   $OPSA_HOME/bin/opsa-collection-config.sh -publish -collectorhost
   <fully-qualified domain name of the collector host> –username
   <tenant admin user>
   ```

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

Configuring an HP Operations Agent Collection

There are two methods of configuring Operations Analytics for HP Operations Agent, the **Automated Configuration Method** and the **Manual Configuration Method**. You must select one of these methods to configure Operations Analytics for HP Operations Agent. Do not attempt to use both the Automated Configuration Method and the Manual Configuration Method.

The HP Operations Agent Collection collects global system information on the host that is running the HP Operations Agent. After you complete the steps in this section, the HP Operations Agent Collection collects raw metrics every 15 minutes, with 5 minute data granularity.

Automated Configuration Method: This approach is more automated than the Manual Configuration Method, making configuration easier. Do the following to use the Automated Configuration Method:

1. The Automated Configuration Method provides the sample collection template, `$OPSA_HOME/conf/collection/sample/sample_auto-config-node.properties`, located on the Operations Analytics server appliance. Copy the `sample-auto-config-node.properties` file to a separate location, then edit the `sample-auto-config-node.properties` file and add, among other information, the following Operations Manager information:

   - For an OMW host (HP Operations Manager on a Windows server), the Automated Configuration Method includes the OMW host's fully-qualified domain name and its database details.

   - For an OMU host (HP Operations Manager on a UNIX or Linux server), the Automated Configuration Method includes the OMU host's fully-qualified domain name and its database details.

2. Save your work.

3. Run the following command from the Operations Analytics Server Appliance to encrypt the passwords in the `mynodelists.properties` file:

   ```
   $OPSA_HOME/bin/opsa-collection-config.sh -encrypt <path>/sample-auto-config-node.properties
   ```

4. Run the following command from the Operations Analytics Server Appliance to configure the collector hosts and publish the collection information:

   ```
   $OPSA_HOME/bin/opsa-collector-auto-conf.sh <path>/<sample-auto-config-node.properties> -collectevents -configuredomain [Oracle|System] -username <tenant admin user>
   ```

   Note: The `opsa-collector-auto-conf.sh` script sets up HP Operations Agent, HP Operations Smart Plug-in for Oracle, and OM event collection using only one command.

   Note: The command output shows the list of registered collectors and distributes the list of nodes providing system performance metrics, Oracle performance metrics, or both among the registered collectors.

   Note: The `opsa-collector-auto-conf.sh` script prompts you for the Tenant Admin password for the username you use in the commands shown in this section. See the opsa-collector-auto-conf.*sh* reference page (or the Linux manpage) for more information.

Manual Configuration Method: Do the following for a more manual approach to configuring Operations Analytics for HP Operations Agent:

1. A node list file contains details about the sources from which you plan to collect information. There are sample nodelist files located in the `$OPSA_HOME/conf/collection/sample`

directory. Operations Analytics administrators can use these sample files to publish the node list file. The sample node list file for the HP Operations Agent collection is `sample_oa_pa_node.properties`. The node list file for the Operations Agent collection must contain a list of servers that have the HP Operations Agent installed. The node list file for the Operations Agent collection must include the information shown in the following table:

Node List File Fields and Values

Field	Value
panode1.somedomain.com	The fully-qualified domain name of a server that has the HP Operations Agent installed.
panode2.somedomain.com	The fully-qualified domain name of a server that has the HP Operations Agent installed.
Add more servers that have the HP Operations Agent installed	The fully-qualified domain name of a server that has the HP Operations Agent installed.

To edit the node list file, do the following from the Operations Analytics Server Appliance:

a. Copy the `sample_OA_PA_node.properties` file from the `$OPSA_HOME/conf/collection/sample` directory to some location, such as `/tmp/mynodelist.properties`.

b. Edit the `/tmp/mynodelist.properties` file, adding the appropriate information; then save your work.

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

```
$OPSA_HOME/bin/opsa-collection-config.sh -create -nodelist
/tmp/mynodelist.properties -collectorhost <fully-qualified domain
name of the collector host> -source oa -domain sysperf -group
global
 -username <tenant admin user>
```

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

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

3. Run the following command from the Operations Analytics Server Appliance to validate the collection configuration you just created:

```
$OPSA_HOME/bin/opsa-collection-config.sh -list -allversions -
collectorhosts -username <tenant admin user>
```

To verify a successful collection configuration creation, look for a message showing the expected collector host name, tenant name, and tenant version. The message should also include the source template details such as its `version`, `domain`, and `group`.

4. Run the following command from the Operations Analytics Server Appliance to publish this collection configuration to the Operations Analytics Collector Appliance :

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

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

To remove nodes from an HP Operations Agent Collection follow these steps:

1. Copy the node list file to a temporary location. For example, you might run the following command:
```
cp
/opt/HP/opsa/conf/collection/config.files/<collectorhost>/<tenant>
/1.0/oa/1.0/sysperf/global/nodelist /tmp
```

2. Edit the node list file. For example, you might edit the `tmp/nodelist` file, then remove the `HP Operations Agent Collection` nodes.

3. For this example, you might run the following command:
```
opsa-collection-config.sh -nodelist /tmp/nodelist -collectorhost
<fully-qualified domain name of the collector host> -source oa -
domain sysperf -group global -username opsatenantadmin.
```
Enter `yes`when prompted with, "`Do you want to overwrite the existing node list (instead of appending to it) (Y/N) ?`"

4. For this example, you might run the following command to publish these changes:
```
 opsa-collection-config.sh -publish -collectorhost <collectorhost> -
username opsatenantadmin
```

Configuring an HP Operations Smart Plug-in for Oracle Collection

There are two methods of configuring Operations Analytics for HP Operations Smart Plug-in for Oracle, the **Automated Configuration Method** and the **Manual Configuration Method**. You must select one of these methods to configure Operations Analytics for HP Operations Smart Plug-in for Oracle. Do not attempt to use both the Automated Configuration Method and the Manual Configuration Method.

After you complete the steps in this section, the HP Operations Smart Plug-in for Oracle Collection collects metrics every 15 minutes, with 5 minute data granularity.

Automated Configuration Method: This approach is more automated than the Manual Configuration Method, making configuration easier. Do the following to use the Automated Configuration Method:

1. The Automated Configuration Method provides the sample collection template, `$OPSA_HOME/conf/collection/sample/sample_auto-config-node.properties`, located on the Operations Analytics server appliance. Copy the `sample-auto-config-node.properties` file to a separate location, then edit the `sample-auto-config-node.properties` file and add, among other information, the following Operations Manager information:

   - For an OMW host (HP Operations Manager on a Windows server), the Automated Configuration Method includes the OMW host's fully-qualified domain name and its database details.

   - For an OMU host (HP Operations Manager on a UNIX or Linux server), the Automated Configuration Method includes the OMU host's fully-qualified domain name and its database details.

2. Save your work.

3. Run the following command from the Operations Analytics Server Appliance to encrypt the passwords in the `mynodelists.properties` file:
   ```
   $OPSA_HOME/bin/opsa-collection-config.sh -encrypt <path>/sample-auto-config-node.properties
   ```

4. Run the following command from the Operations Analytics Server Appliance to configure the collector hosts and publish the collection information:

   ```
   $OPSA_HOME/bin/opsa-collector-auto-conf.sh <path>/<sample-auto-config-node.properties> -collectevents -configuredomain
   [Oracle|System] -username <tenant admin user>
   ```

   Note: The `opsa-collector-auto-conf.sh` script sets up HP Operations Agent, HP Operations Smart Plug-in for Oracle, and OM event collection using only one command.

   Note: The command output shows the list of registered collectors and distributes the list of nodes providing system performance metrics, Oracle performance metrics, or both among the registered collectors.

> **Note**: The `opsa-collector-auto-conf.sh` script prompts you for the Tenant Admin password for the username you use in the commands shown in this section. See the opsa-collector-auto-conf.*sh* reference page (or the Linux manpage) for more information.

Manual Configuration Method: Do the following for a more manual approach to configuring Operations Analytics for HP Operations Smart Plug-in for Oracle:

1. A node list file contains details about the sources from which you plan to collect information. There are sample nodelist files located in the `$OPSA_HOME/conf/collection/sample` directory. Operations Analytics administrators can use these sample files to publish the node list file. The sample node list file for the HP Operations Agent Smart Plug-in for Oracle collection is `sample_oa_pa_node.properties`. The node list file for the HP Operations Agent Smart Plug-in for Oracle collection must contain a list of servers that have the HP Operations Agent and the HP Operations Smart Plug-in for Oracle installed. The node list file for the HP Operations Agent Smart Plug-in for Oracle collection must include the information shown in the following table:

   Node List File Fields and Values

Field	Value
oanode1.somedomain.com	The fully-qualified domain name of a server that has the HP Operations Agent and the HP Operations Smart Plug-in for Oracle installed.
oanode2.somedomain.com	The fully-qualified domain name of a server that has the HP Operations Agent and the HP Operations Smart Plug-in for Oracle installed.
Add more servers that have the HP Operations Agent and the HP Operations Smart Plug-in for Oracle installed.	The fully-qualified domain name of a server that has the HP Operations Agent and the HP Operations Smart Plug-in for Oracle installed.

   To edit the node list file, do the following from the Operations Analytics Server Appliance:

   a. Copy the `sample_OA_PA_node.properties` file from the `$OPSA_HOME/conf/collection/sample` directory to some location, such as `/tmp/mynodelist.properties`.

   b. Edit the `/tmp/mynodelist.properties` file, adding the appropriate information; then save your work.

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

   ```
   $OPSA_HOME/bin/opsa-collection-config.sh -create -nodelist
   /tmp/mynodelist.properties -collectorhost <fully-qualified domain
   ```

```
name of the collector host> -source oa -domain oraperf -group graph
-username <tenant admin user>
```

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

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

3. Run the following command from the Operations Analytics Server Appliance to validate the collection configuration you just created:

   ```
   $OPSA_HOME/bin/opsa-collection-config.sh -list -allversions -
   collectorhosts -username <tenant admin user>
   ```

   To verify a successful collection configuration creation, look for a message showing the expected collector host name, tenant name, and tenant version. The message should also include the source template details such as its `version`, `domain`, and `group`.

4. Run the following command from the Operations Analytics Server Appliance to publish this collection configuration to the Operations Analytics Collector Appliance :

   ```
   $OPSA_HOME/bin/opsa-collection-config.sh -publish -collectorhost
   <fully-qualified domain name of the collector host> –username
   <tenant admin user>
   ```

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

To remove nodes from an HP Operations Smart Plug-in for Oracle Collection follow these steps:

1. Copy the node list file to a temporary location. For example, you might run the following command:

   ```
   cp
   /opt/HP/opsa/conf/collection/config.files/<collectorhost>/<tenant>/
   1.0/oa/1.0/oraperf/graph/nodelist /tmp
   ```

2. Edit the node list file. For example, you might edit the `tmp/nodelist` file, then remove the `HP Operations Smart Plug-in for Oracle Collection` nodes.

3. For this example, you might run the following command:

   ```
   opsa-collection-config.sh -nodelist /tmp/nodelist -collectorhost
   ```

```
<fully-qualified domain name of the collector host> -source oa -
domain oraperf -group graph -username opsatenantadmin.
```

Enter `yes`when prompted with, "`Do you want to overwrite the existing node list (instead of appending to it) (Y/N) ?`"

4. For this example, you might run the following command to publish these changes:

```
opsa-collection-config.sh -publish -collectorhost <collectorhost> -
username opsatenantadmin
```

Configuring an HP Business Process Monitor Collection

After you complete the steps in this section, HP BPM starts sending data to the HP Business Process Monitor Collection. The HP Business Process Monitor Collection collects metrics related to application transaction response times. The HP Business Process Monitor Collection collects data as it arrives from BPM.

Connecting two or more Operations Analytics Collector Appliances to the same BSM server host is not a supported configuration.

Complete the following before proceeding:

> **Note**: For this example, the fully-qualified domain name of the BSM DPS server is `servername.location.domain.com`.

Add an entry for the BSM DPS server to the `/etc/hosts` file in the domain in which the Operations Analytics Collector Appliance resides. For example, you would add a line for the BSM DPS server to the `/etc/hosts` file using the following format:

```
10.1.2.3 servername.location.domain.com servername.
```

> **Note**: You must use the alias, *servername*, as the BSM DPS host name in the node list file.

To configure a Business Process Monitor (BPM) collection, do the following:

1. A node list file contains details about the sources from which you plan to collect information. There are sample nodelist files located in the `$OPSA_HOME/conf/collection/sample` directory. Operations Analytics administrators can use these sample files to publish the node list file. The sample node list file for the BPM collection is `sample_BPM_node.properties`. The node list file for the BPM collection needs to include a single node from the BSM cluster. This node must be a DPS node. Operations Analytics uses this node to extract BPM data from the BSM cluster. Operations Analytics also uses this node to obtain the BSM location name from BSM's RTSM. The node list file for the BSM BPM collection must include the information shown in the following table:

Node List File Fields and Values

Field	Value
bpmserver.hostdnsname	The fully-qualified domain name of the RTSM DPS server.
bpmserver.port	`21212`: The port used to connect to the RTSM DPS server.
bpmserver.username	`admin`: The user name to use for connecting to the RTSM DPS server.

To edit the node list file, do the following from the Operations Analytics Server Appliance:

a. Copy the `sample_BPM_node.properties` file from the `$OPSA_HOME/conf/collection/sample` directory to some location, such as `/tmp/mynodelist.properties`.

b. Edit the `/tmp/mynodelist.properties` file, adding the appropriate information; then save your work.

2. Run the following command from the Operations Analytics Server Appliance to encrypt the password:

```
$OPSA_HOME/bin/opsa-collection-config.sh -encrypt
/tmp/mynodelist.properties
```

3. Run the following command from the Operations Analytics Server Appliance to create the collector configuration:

```
$OPSA_HOME/bin/opsa-collection-config.sh -create -nodelist
/tmp/mynodelist.properties -collectorhost <fully-qualified-domain-
name of collector host> -source bpm -domain application -group
performance -username <tenant admin user>
```

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

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

4. Run the following command from the Operations Analytics Server Appliance to validate the collection configuration you just created:

```
$OPSA_HOME/bin/opsa-collection-config.sh -list -allversions -
collectorhosts -username <tenant admin user>
```

To verify a successful collection configuration creation, look for a message showing the expected collector host name, tenant name, and tenant version. The message should also include the source template details such as its `version`, `domain`, and `group`.

5. Run the following command from the Operations Analytics Server Appliance to publish this collection configuration to the Operations Analytics Collector Appliance :

   ```
   $OPSA_HOME/bin/opsa-collection-config.sh -publish -collectorhost
   <fully-qualified domain name of the collector host> -username
   <tenant admin user>
   ```

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

Configuring an NNMi Custom Poller Collection

After you complete the steps in this section, the NNMi Custom Poller Collection reads data from the CSV files within 60 seconds of the file being placed in the source directory. You can use an NNMi Custom Poller Collection to collect numeric metrics from any NNMi Custom Poller MIB expression.

The NNMi Custom Poller collection template is generic, as it stores a MIB instance and a MIB value. This MIB value id defined as a `float` data type. Since Custom Poller can poll any type of MIB value, you must only send Custom Poller CSV files that contain numeric MIB values to this collection .

If you must create an Operations Analytics collection that matches what is being collected, you must create a custom CSV collection template. For example, you might have a Custom Poller Collection for network interface errors. To use this Custom Poller Collection, create a Custom CSV Collection, adding the appropriate tags and labels to identify the data for that collection. See "Configuring a Custom CSV Collection" for more information.

1. To enable NNMi to export Custom Poller collections, do the following:

   a. Using the NNMi console, enable NNMi to export custom poller collections to make the metrics from your collections available for Operations Analytics. Configuring NNMi to export custom poller collections enables NNMi to export metrics, such as CSV files, into the following directory:

      - *Windows*:
        ```
        <Install_Dir>\ProgramData\HP\HP BTO
        Software\shared\nnm\databases\custompoller\export\final
        ```
      - *UNIX*:
        ```
        /var/opt/OV/shared/nnm/databases/custompoller/export/final
        ```

      See the *HP Network Node Manager i Deployment Reference*, the *HP NNMi Help*, or the *HP Network Node Manager i Software Step-by-Step Guide to Custom Poller White Paper* for more information.

b. The default configuration for the custom poller collection template is for Operations Analytics to read all of the files having file names that match the `*.csv*` or `*.gz*` pattern. If you need the collector to read a different set of files, the Operations Analytics administrator must edit the appropriate custom poller collector template file and specify a different file pattern. To change the pattern, edit the custom poller collection template and make the value changes you must make to the `filepattern=` tag.

Note: You must make the files exported from the `/var/opt/OV/shared/nnm/databases/custompoller/export/final` directory on NNMI available on the Operations Analytics Collector Appliance in the `/opt/HP/opsa/data/nnm` directory.

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

a. Edit the following collection template:
`/opt/HP/opsa/conf/collection/server/config.templates/nnm/1.0/netperf/mib/nnm_netperf_mib_collection.xml`.

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

Note: The `opsa` user on the Operations Analytics Collector Appliance must have read and write access to the NNMi files on the Operations Analytics Collector Appliance to move them to the processed directory. The default process directory is `/opt/HP/opsa/data/nnm_processed`.

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

```
$OPSA_HOME/bin/opsa-collection-config.sh -create -collectorhost
<fully-qualified domain name of the collector host> -source nnm -
domain netperf -group mib -username <tenant admin user>
```

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

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

3. Run the following command from the Operations Analytics Server Appliance to validate the collection configuration you just created:

   ```
   $OPSA_HOME/bin/opsa-collection-config.sh -list -allversions -
   collectorhosts -username <tenant admin user>
   ```

   To verify a successful collection configuration creation, look for a message showing the expected collector host name, tenant name, and tenant version. The message should also include the source template details such as its version, domain, and group.

4. Run the following command from the Operations Analytics Server Appliance to publish this collection configuration to the Operations Analytics Collector Appliance:

   ```
   $OPSA_HOME/bin/opsa-collection-config.sh -publish -collectorhost
   <fully-qualified domain name of the collector host> –username
   <tenant admin user>
   ```

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

Configuring an NNM ISPi Performance for Metrics Component Health Collection

After you complete the steps in this section, the NNMi ISPi Performance for Metrics Component Health Collection reads data from the CSV files within 60 seconds of the file being placed in the source directory.

1. For the Collector Appliance to access raw metric information from the NNM iSPI Performance for Metric's component health extension pack, you must export these metrics to CSV files. Run the following command on the NNM iSPI Performance for Metric server to export these metrics to CSV files in the `/csvexports` directory:
   - *Windows (Raw Information)*:

     ```
     <Install_Dir>\NNMPerformanceSPI\bin\configureCsvExport.ovpl -p
     Component_Health -a "Raw,<Target-Dir>"
     ```

   - *UNIX: (Raw Information)*:

     ```
     /opt/OV/NNMPerformanceSPI/bin/configureCsvExport.ovpl -p
     Component_Health -a "Raw,<Target-Dir>"
     ```

   Note: you must make the exported component health metrics available on the Operations Analytics Collector Appliance in the `/opt/HP/opsa/data/netcomponent` directory.

   If you want to use a different directory than `/opt/HP/opsa/data/netcomponent`, do

> the following:
>
> a. Edit the following collection template:
>
> ```
> /opt/HP/opsa/conf/collection/server/config.templates/nnmispi/
> 1.0/
> netcomponent/component/nnmispi_netcomponent_component_
> collection.xml.
> ```
>
> b. Specify a different directory for the `sourcedir` attribute.

> **Note**: The `opsa` user on the Operations Analytics Collector Appliance must have read and write access to the component health metric files in the Operations Analytics Collector Appliance to move them to the processed directory. The default process directory is `/opt/HP/opsa/data/netcomponent_processed`.

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

   ```
   $OPSA_HOME/bin/opsa-collection-config.sh -create -collectorhost
   <fully-qualified domain name of the collector host> -source nnmispi
   -domain netcomponent -group component -username <tenant admin user>
   ```

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

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

3. Run the following command from the Operations Analytics Server Appliance to validate the collection configuration you just created:

   ```
   $OPSA_HOME/bin/opsa-collection-config.sh -list -allversions -
   collectorhosts -username <tenant admin user>
   ```

   To verify a successful collection configuration creation, look for a message showing the expected collector host name, tenant name, and tenant version. The message should also include the source template details such as its `version`, `domain`, and `group`.

4. Run the following command from the Operations Analytics Server Appliance to publish this collection configuration to the Operations Analytics Collector Appliance :

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

<tenant admin user>

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

Configuring an NNM ISPi Performance for Metrics Interface Health Collection

After you complete the steps in this section, the NNMi ISPi Performance for Metrics Interface Health Collection reads data from the CSV files within 60 seconds of the file being placed in the source directory.

1. For the Collector Appliance to access live metric information from the NNM iSPI Performance for Metric's interface health extension pack, you must export these metrics to CSV files. Run the following command on the NNM iSPI Performance for Metric server to export these metrics to CSV files in the `/csvexports` directory:
   - *Windows (Raw Information)*:

     ```
     <Install_Dir>\NNMPerformanceSPI\bin\configureCsvExport.ovpl -p
     Interface_Health -a "Raw,<Target_Directory">
     ```

   - *UNIX (Raw Information)*:

     ```
     /opt/OV/NNMPerformanceSPI/bin/configureCsvExport.ovpl -p
     Interface_Health -a "Raw,<Target_Directory">
     ```

   > **Note**: you must make the exported interface health metrics available on the Operations Analytics Collector Appliance in the `/opt/HP/opsa/data/netinterface` directory. If you want to use a different directory than `/opt/HP/opsa/data/netinterface`, do the following:
   >
   > a. Edit the following collection template:
   >
   > ```
   > /opt/HP/opsa/conf/collection/server/config.templates/nnmispi/
   > 1.0/
   > netinterface/interface/nnmispi_netinterface_interface_
   > collection.xml.
   > ```
   >
   > b. Specify a different directory for the `sourcedir` attribute.

   > **Note**: The `opsa` user on the Operations Analytics Collector Appliance must have read and write access to the interface health metric files on the Operations Analytics Collector Appliance to move them to the processed directory. The default process directory is `/opt/HP/opsa/data/netinterface_processed`.

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

   ```
   $OPSA_HOME/bin/opsa-collection-config.sh -create -collectorhost
   <fully-qualified domain name of the collector host> -source nnmispi
   -domain netinterface -group interface -username <tenant admin user>
   ```

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

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

3. Run the following command from the Operations Analytics Server Appliance to validate the collection configuration you just created:

   ```
   $OPSA_HOME/bin/opsa-collection-config.sh -list -allversions -
   collectorhosts -username <tenant admin user>
   ```

   To verify a successful collection configuration creation, look for a message showing the expected collector host name, tenant name, and tenant version. The message should also include the source template details such as its version, domain, and group.

4. Run the following command from the Operations Analytics Server Appliance to publish this collection configuration to the Operations Analytics Collector Appliance :

   ```
   $OPSA_HOME/bin/opsa-collection-config.sh -publish -collectorhost
   <fully-qualified domain name of the collector host> –username
   <tenant admin user>
   ```

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

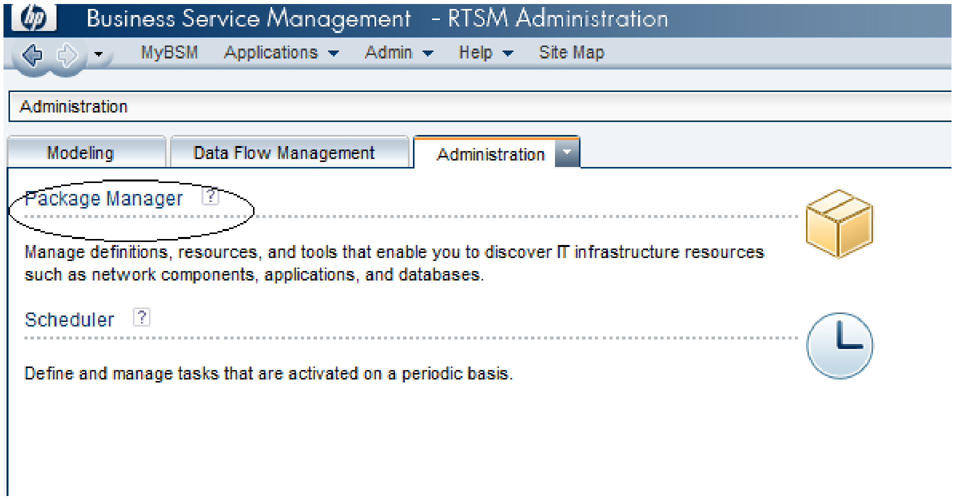
Configuring an HP BSM RTSM Configuration Item (CI) Collection

After you complete the steps in this section, the HP BSM RTSM CI Collection collects data every 6 hours

1. Before configuring any of the HP BSM RTSM collections, you must deploy OPSA views on the BSM Server. Do the following:

a. Copy the `$OPSA_HOME/conf/collection/rtsm_views/OPSA_Views.zip` file to the local server from where the BSM UI is launched.

b. Access the **Package Manager** module through the BSM UI:



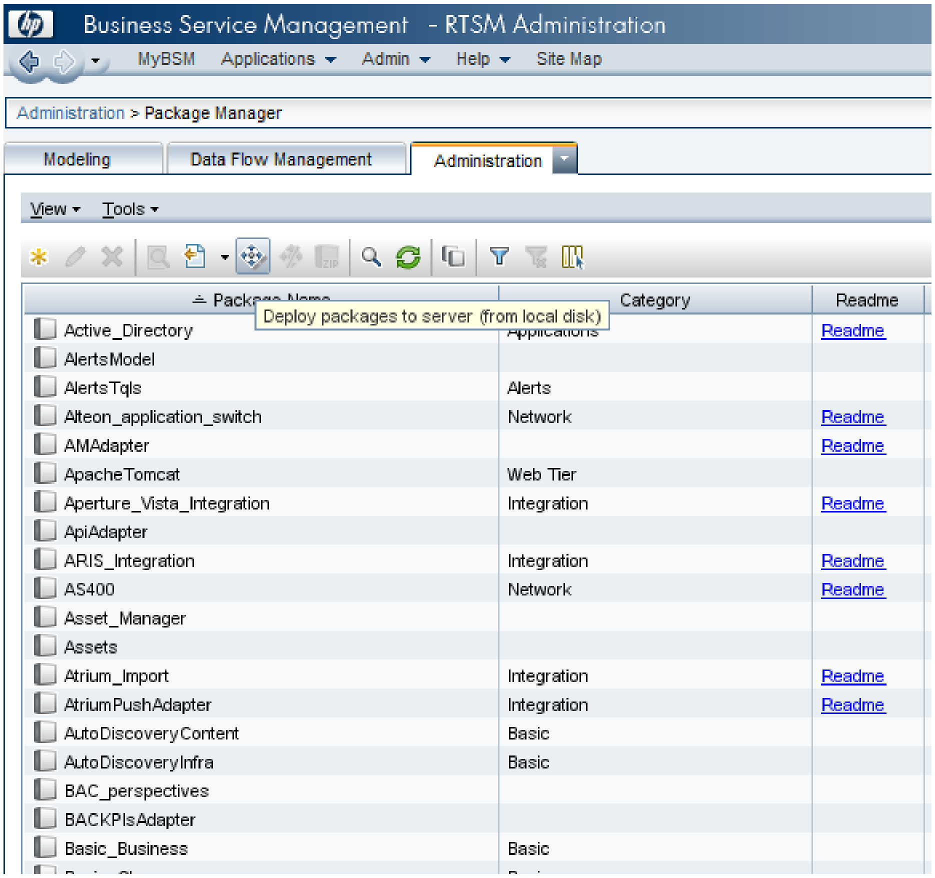
Package Manager

Manage definitions, resources, and tools that enable you to discover IT infrastructure resources such as network components, applications, and databases.

Scheduler

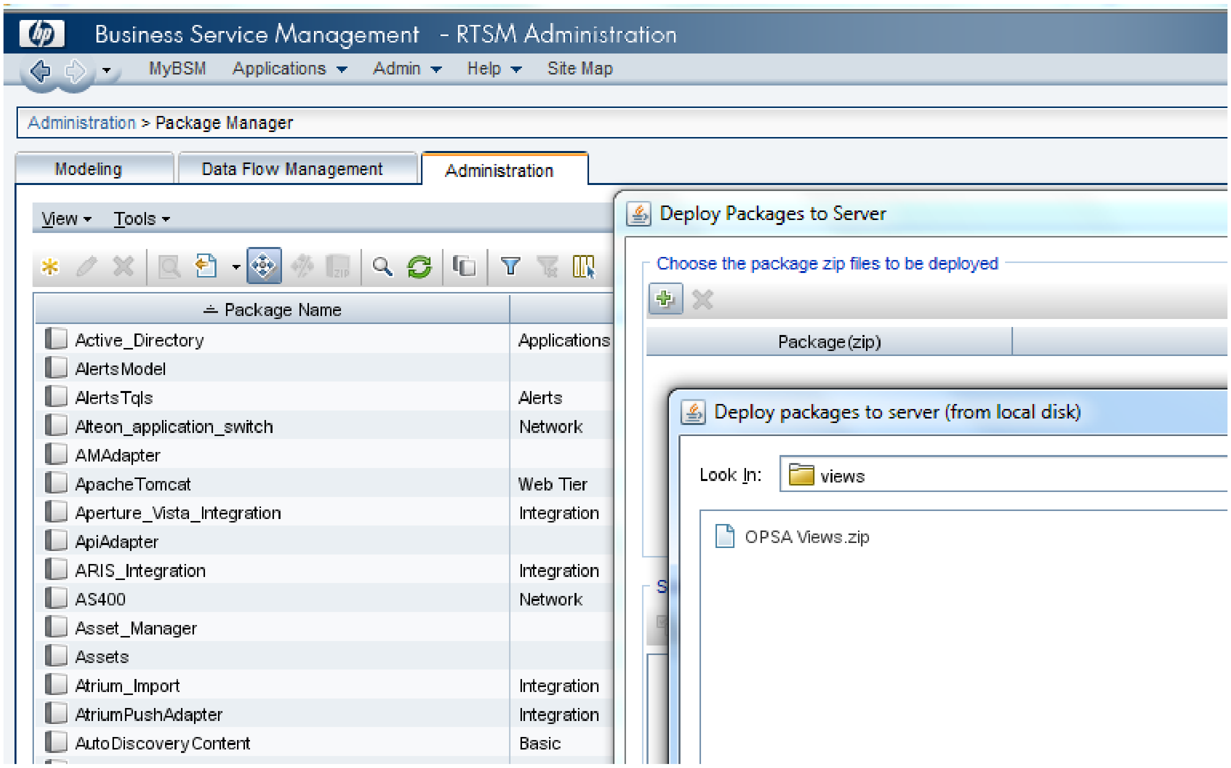
Define and manage tasks that are activated on a periodic basis.

c. Select the **Deploy packages to server (from local disk)** option.


Business Service Management - RTSM Administration
MyBSM
Applications
Admin
Help
Site Map
Administration > Package Manager
Modeling
Data Flow Management
Administration
View
Tools
Deploy packages to server (from local disk)

Package Name	Category	Readme
Active_Directory	Applications	Readme
AlertsModel		
AlertsTqls	Alerts	
Alteon_application_switch	Network	Readme
AMAdapter		Readme
ApacheTomcat	Web Tier	
Aperture_Vista_Integration	Integration	Readme
ApiAdapter		
ARIS_Integration	Integration	Readme
AS400	Network	Readme
Asset_Manager		
Assets		
Atrium_Import	Integration	Readme
AtriumPushAdapter	Integration	Readme
AutoDiscoveryContent	Basic	
AutoDiscoveryInfra	Basic	
BAC_perspectives		
BACKPIsAdapter		
Basic_Business	Basic	

d. Select the **OPSA_Views.zip** file from the local disk as shown in the following screen shot:

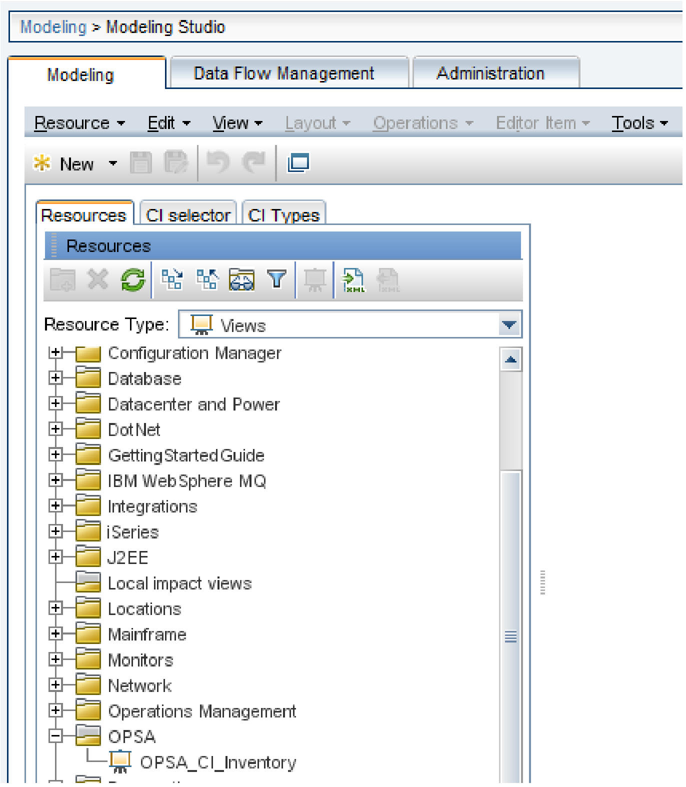

Business Service Management - RTSM Administration
MyBSM
Applications
Admin
Help
Site Map
Administration > Package Manager
Modeling
Data Flow Management
Administration
View
Tools
Deploy Packages to Server
Choose the package zip files to be deployed
Package (zip)
Deploy packages to server (from local disk)

Package Name	
Active_Directory	Applications
AlertsModel	
AlertsTqls	Alerts
Alteon_application_switch	Network
AMAdapter	
ApacheTomcat	Web Tier
Aperture_Vista_Integration	Integration
ApiAdapter	
ARIS_Integration	Integration
AS400	Network
Asset_Manager	
Assets	
Atrium_Import	Integration
AtriumPushAdapter	Integration
AutoDiscoveryContent	Basic

Look In: views

OPSA Views.zip

e. Once deployed, the views should be visible in the Modeling studio as shown in the following screen shot:



Resource Type: Views

2. A node list file contains details about the sources from which you plan to collect information. There are sample nodelist files located in the `$OPSA_HOME/conf/collection/sample` directory. Operations Analytics administrators can use these sample files to publish the node list file. The sample node list file for the BSM RTSM CI collection is `sample_RTSM_node.properties`.

Operations Analytics administrators can use this sample file to publish the node list file.

The node list file for the BSM RTSM CI collection must include the information shown in the following table:

Node List File Fields and Values

Field	Value
rtsmserver.hostdnsname	The fully-qualified domain name of the RTSM DPS server.
rtsmserver.port	`21212`: The port used to connect to the RTSM DPS server.
rtsmserver.username	`admin`: The user name to use for connecting to the RTSM DPS server.

Node List File Fields and Values, continued

Field	Value
rtsmserver.datasource_type	`rtsm`

To edit the node list file, do the following from the Operations Analytics Server Appliance:

a. Copy the `sample_RTSM_node.properties` file from the `$OPSA_HOME/conf/collection/sample` directory to some location, such as `/tmp/mynodelist.properties`:

b. Edit the `/tmp/mynodelist.properties` file, adding the appropriate information; then save your work.

3. Run the following command from the Operations Analytics Server Appliance to encrypt the password:

```
$OPSA_HOME/bin/opsa-collection-config.sh -encrypt
/tmp/mynodelist.properties
```

4. Run the following command from the Operations Analytics Server Appliance to create the collector configuration:

```
$OPSA_HOME/bin/opsa-collection-config.sh
-create -nodelist /tmp/mynodelist.properties
-collectorhost <fully-qualified domain name of the collector host>
-source rtsm
-domain ci -group inventory -username <tenant admin user>
```

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

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

5. Run the following command from the Operations Analytics Server Appliance to validate the collection configuration you just created:

```
$OPSA_HOME/bin/opsa-collection-config.sh
-list -collectorhosts -allversions -username <tenant admin user>
```

To verify a successful collection configuration creation, look for a message showing the expected collector host name, tenant name, and tenant version. The message should also include the source template details such as its `version`, `domain`, and `group`.

6. Run the following command from the Operations Analytics Server Appliance to publish this collection configuration to the Operations Analytics collector appliance:

   ```
   $OPSA_HOME/bin/opsa-collection-config.sh -publish -collectorhost
   <fully-qualified domain name of the collector host> –username
   <tenant admin user>
   ```

   The `-publish` option uploads the collection configuration you created to the Operations Analytics collector appliance.

   To verify that the collector configuration published successfully, look for a message stating that the publish was successful, that a table was successfully created, and that the collection was restarted.

Configuring HP Operations Manager (HPOM) (Creating a Database User Account on an HPOM Database Server)

Performing this task depends on how Microsoft SQL Server is set up in the HPOM environment and how you can configure the HP Embedded Collector to communicate with the HPOM database server. There are two possible scenarios:

- **Scenario 1**: HPOM for Windows 8.x/9.x is installed on one system with Microsoft SQL Server 2005 or Microsoft SQL Server 2008 installed on the same system or a remote system. The HP Embedded Collector, which is installed on another system, can be configured to connect to SQL Server either through Windows authentication or SQL Server authentication (mixed-mode authentication). The authentication method defined in SQL Server can be used in the HP Embedded Collector to configure the HPOM database connection.

- **Scenario 2**: HPOM for Windows 8.x uses Microsoft SQL Server 2005 Express Edition that is embedded with it by default. Similarly, HPOM for Windows 9.x uses the embedded Microsoft SQL Server 2008 Express Edition by default. The authentication mode in this scenario is Windows NT authentication. However, in this case, a remote connection between SQL Server and the HP Embedded Collector is not possible. Therefore, you must create a user account for the HP Embedded Collector so that mixed-mode authentication is possible in this scenario.

Before creating the user account, you must first enable mixed-mode authentication. For the steps, see the Enable Mixed Mode authentication after installation section in the Microsoft Support KB article at the following URL: **http://support.microsoft.com/kb/319930**

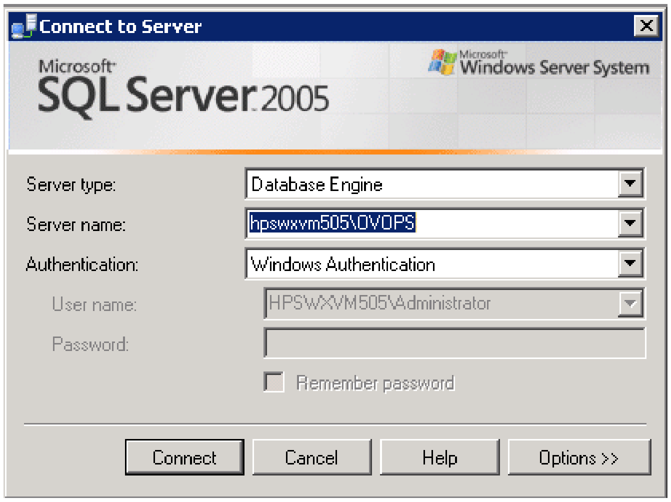
To create a user name and password for authentication purposes, perform the following steps. If you are using Microsoft SQL Server 2008, the steps are similar to the following steps performed in SQL Server 2005:

1. Create a user name and password:

   a. Log on to the HPOM system with embedded Microsoft SQL Server 2005.

   b. The Microsoft SQL Server Management Studio window opens. Click **Start** > **Programs** >**Microsoft SQL Server 2005** > **SQL Server Management Studio**. If SQL Server Management Studio is not installed on your system, you can download it from the Microsoft web site using the following URL:
   `http://www.microsoft.com/downloads/en/details.aspx?FamilyID=c243a5ae-4bd1-4e3d-94b8-5a0f62bf7796.`

   c. In the **Connect to Server** dialog box, select **NT Authentication** in the **Authentication** list, then click **Connect**.



Server type: Database Engine

Server name: hpswxvm505\OVOPS

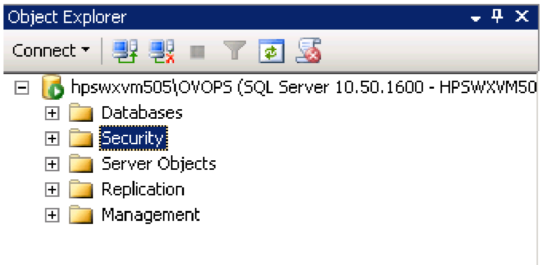
Authentication: Windows Authentication

User name: HPSWXVM505\Administrator

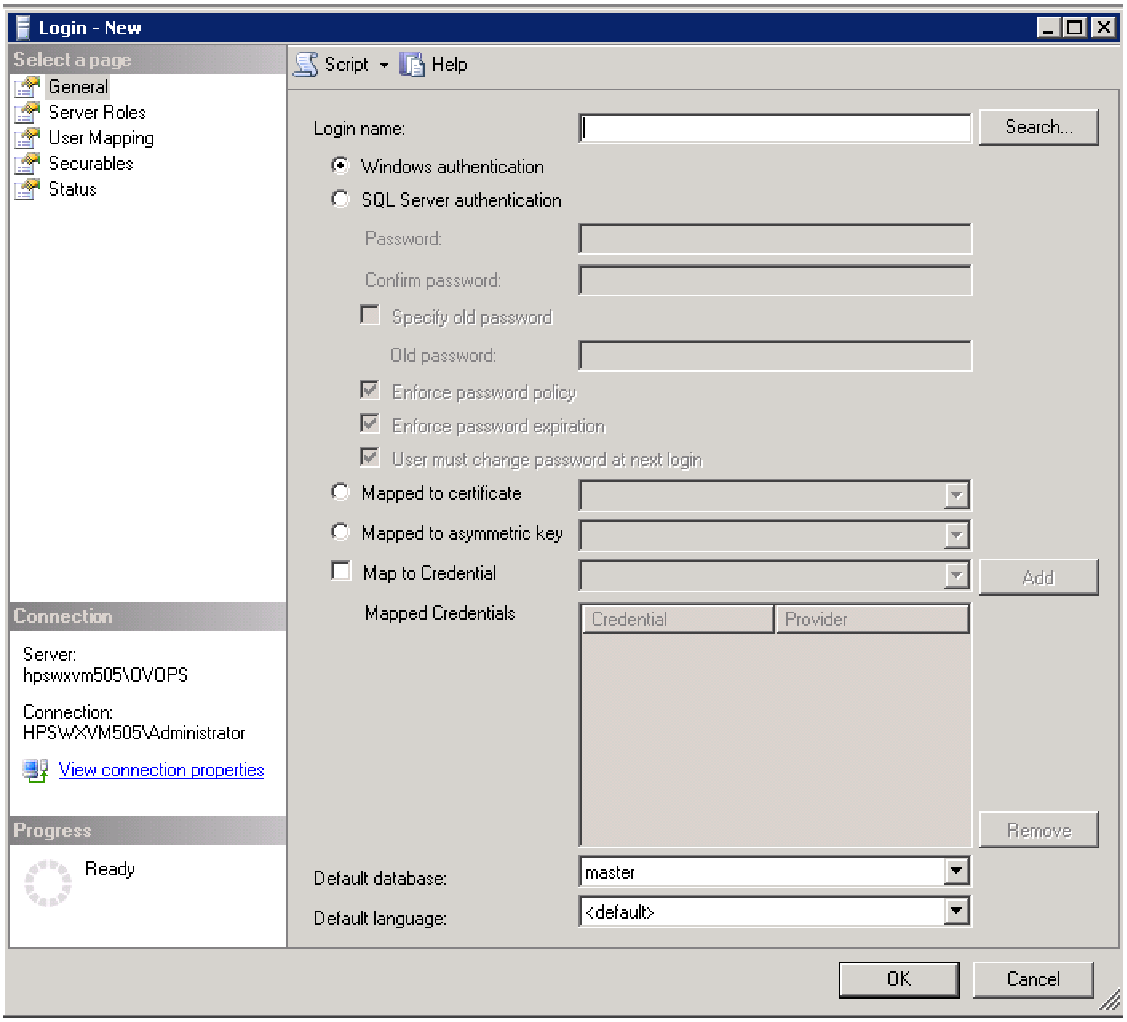
Password:

□ Remember password

   d. In the **Object Explorer** pane, expand **Security**.



e. Right-click **Logins** and click **New Login**. The Login - New dialog box opens.



Login name:

● Windows authentication

○ SQL Server authentication

Password:

Confirm password:

□ Specify old password

Old password:

☑ Enforce password policy

☑ Enforce password expiration

☑ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

□ Map to Credential

Default database: master

Default language: <default>

Server:
hpswxvm505\OVOPS

Connection:
HPSWXVM505\Administrator

f. In the **Login** name field, type a user name. Specify the other necessary details.

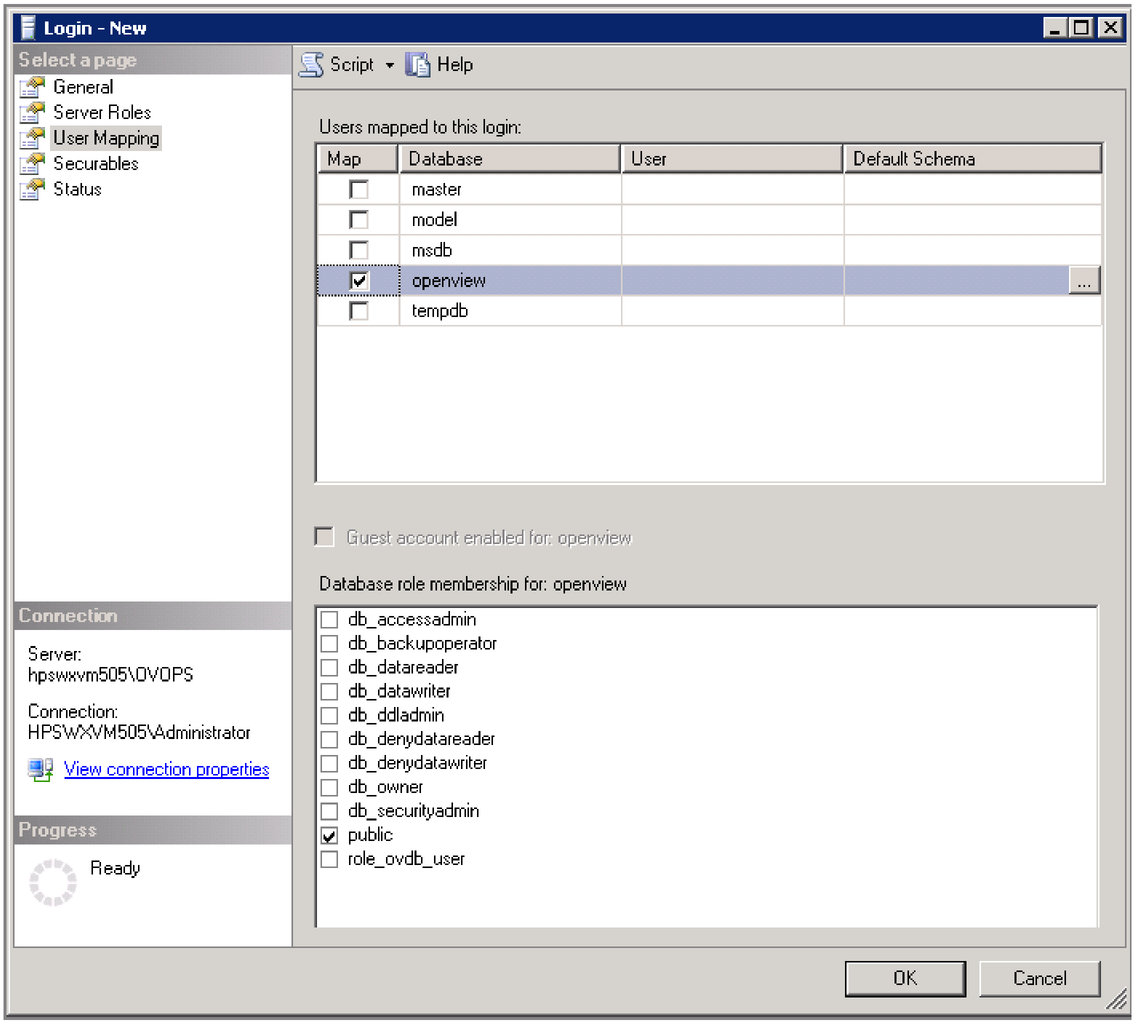
g. Select the **SQL Server authentication** radio button.

h. In the **Password** field, type the password.

i. In the **Confirm password** field, retype the password. You might want to disable the password enforcement rules to create a simple password.

j. Click **User Mapping**.

k. Under **Users mapped to this login**, select the check box next to **openview**.



Users mapped to this login:

Map	Database	User	Default Schema
☐	master		
☐	model		
☐	msdb		
☑	openview		
☐	tempdb		

☐ Guest account enabled for: openview

Database role membership for: openview

☐ db_accessadmin
☐ db_backupoperator
☐ db_datareader
☐ db_datawriter
☐ db_ddladmin
☐ db_denydatareader
☐ db_denydatawriter
☐ db_owner
☐ db_securityadmin
☑ public
☐ role_ovdb_user

Server:
hpswxvm505\OVOPS

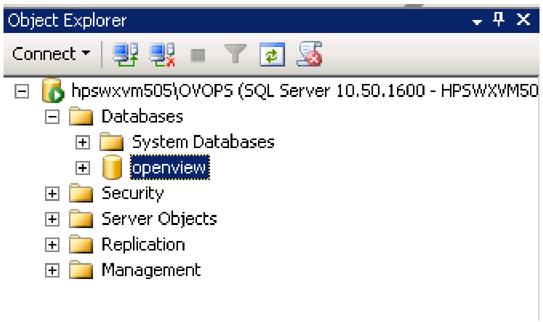
Connection:
HPSWXVM505\Administrator

Ready

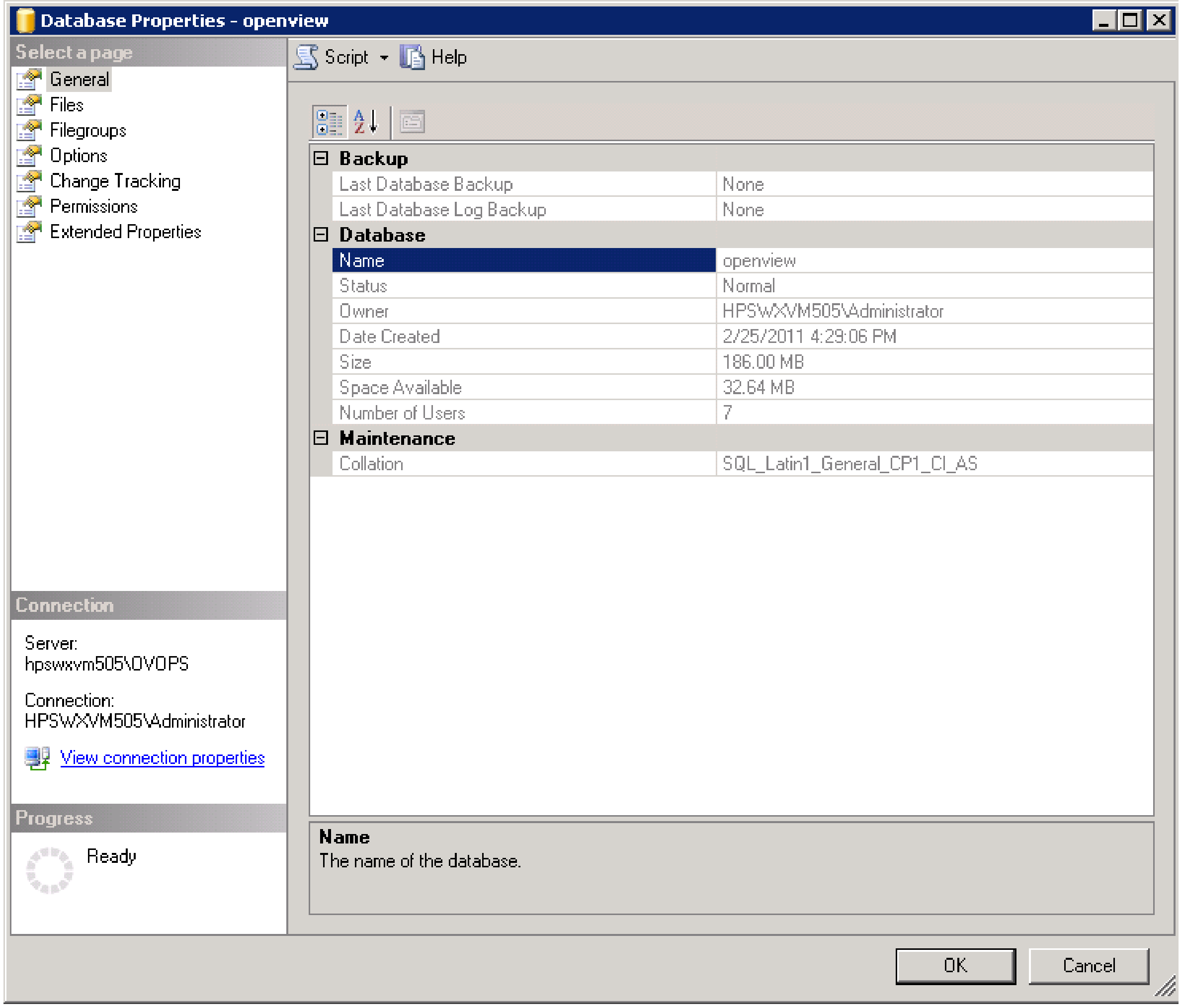
l. Click **OK** to create the user name and password.

2. The database user must have at least the **Connect** and **Select** permissions. To enable the **Connect** and **Select** permissions for the newly created user account, follow these steps:

a. In the **Object Explorer** pane, expand **Databases**.



b. Right-click **openview** , then click **Properties**. The Database Properties - openview dialog box opens.



Server:
hpswxvm505\OVOPS

Connection:
HPSWXVM505\Administrator

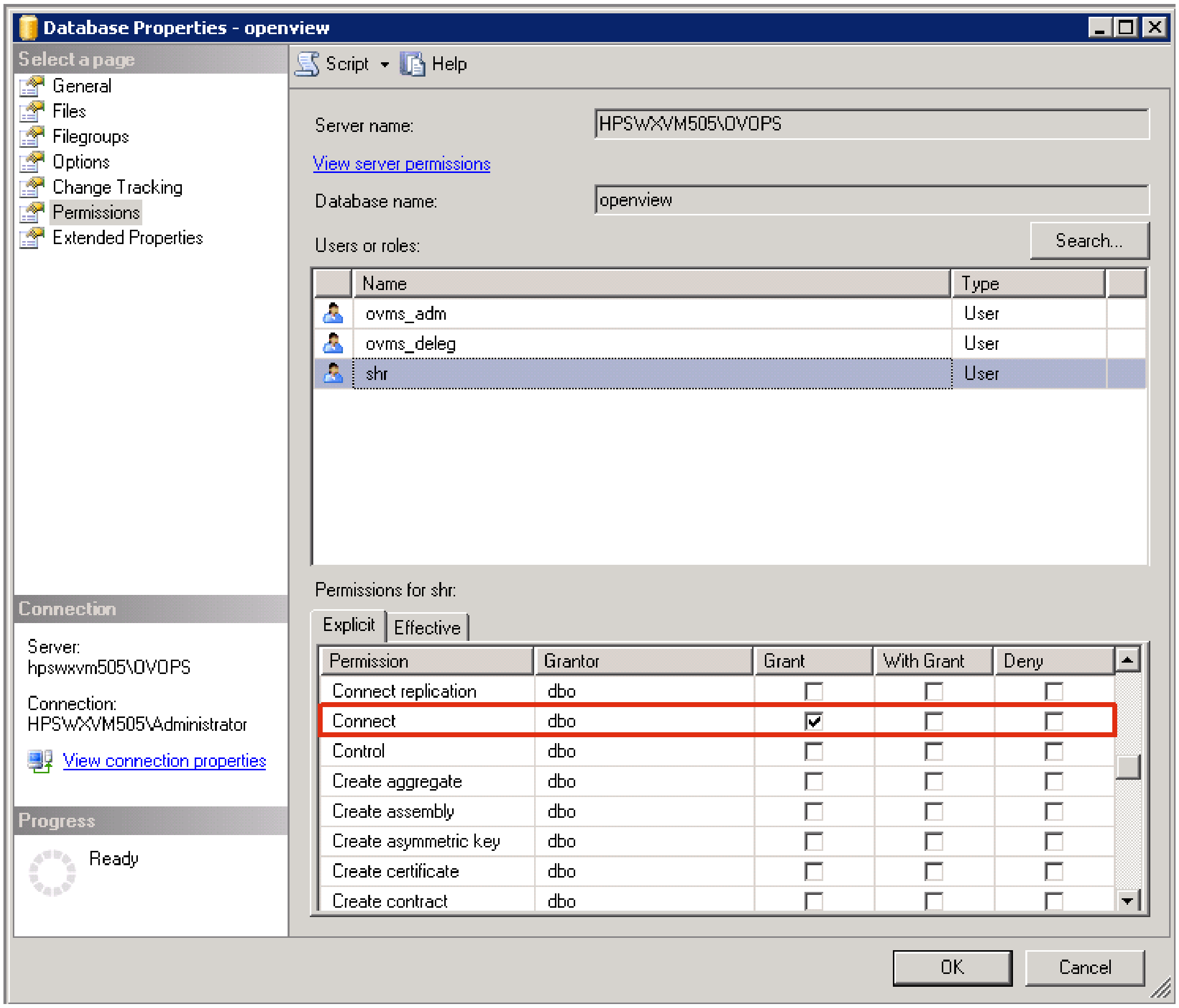
Backup	
Last Database Backup	None
Last Database Log Backup	None
Database	
Name	openview
Status	Normal
Owner	HPSWXVM505\Administrator
Date Created	2/25/2011 4:29:06 PM
Size	186.00 MB
Space Available	32.64 MB
Number of Users	7
Maintenance	
Collation	SQL_Latin1_General_CP1_CI_AS

Name
The name of the database.

c. Under the **Select a page** pane, click **Permissions**.

d. Under **Users or roles**, click the newly created user account.

e. Under **Explicit permissions for test**, scroll down to the **Connect** permission, then select the **Grant** check box for this permission.



Server name: HPSWXVM505\OVOPS

Database name: openview

Users or roles:

Name	Type
ovms_adm	User
ovms_deleg	User
shr	User

Permissions for shr:

Permission	Grantor	Grant	With Grant	Deny
Connect replication	dbo	□	□	□
Connect	dbo	☑	□	□
Control	dbo	□	□	□
Create aggregate	dbo	□	□	□
Create assembly	dbo	□	□	□
Create asymmetric key	dbo	□	□	□
Create certificate	dbo	□	□	□
Create contract	dbo	□	□	□

Connection

Server:
hpswxvm505\OVOPS

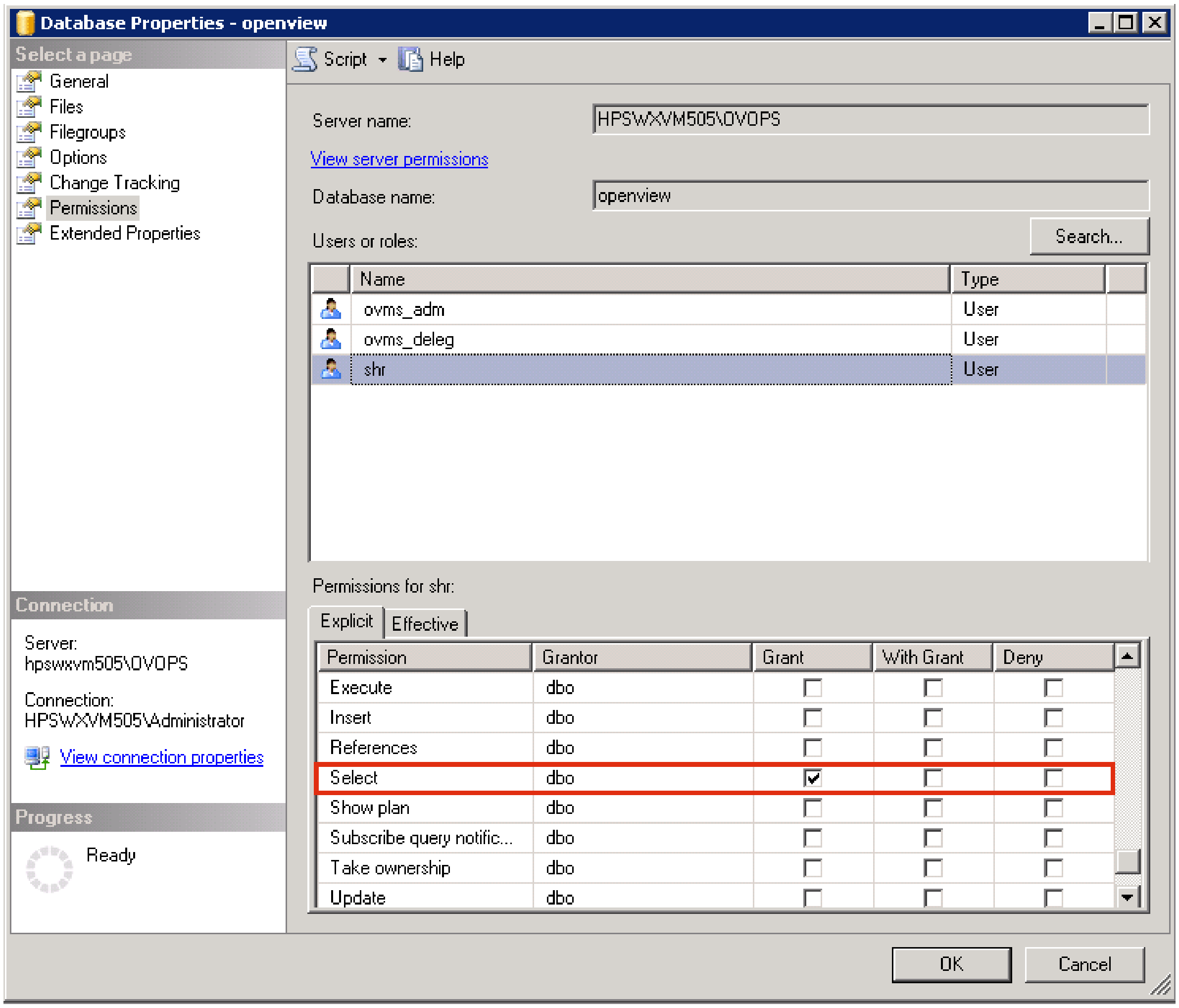
Connection:
HPSWXVM505\Administrator

View connection properties

Progress

Ready

f. Scroll down to the **Select** permission and select the **Grant** check box for this permission.



Server name: HPSWXVM505\OVOPS

Database name: openview

Users or roles:

Name	Type
ovms_adm	User
ovms_deleg	User
shr	User

Permissions for shr:

Permission	Grantor	Grant	With Grant	Deny
Execute	dbo	□	□	□
Insert	dbo	□	□	□
References	dbo	□	□	□
Select	dbo	☑	□	□
Show plan	dbo	□	□	□
Subscribe query notific...	dbo	□	□	□
Take ownership	dbo	□	□	□
Update	dbo	□	□	□

Connection

Server:
hpswxvm505\OVOPS

Connection:
HPSWXVM505\Administrator

View connection properties

Progress

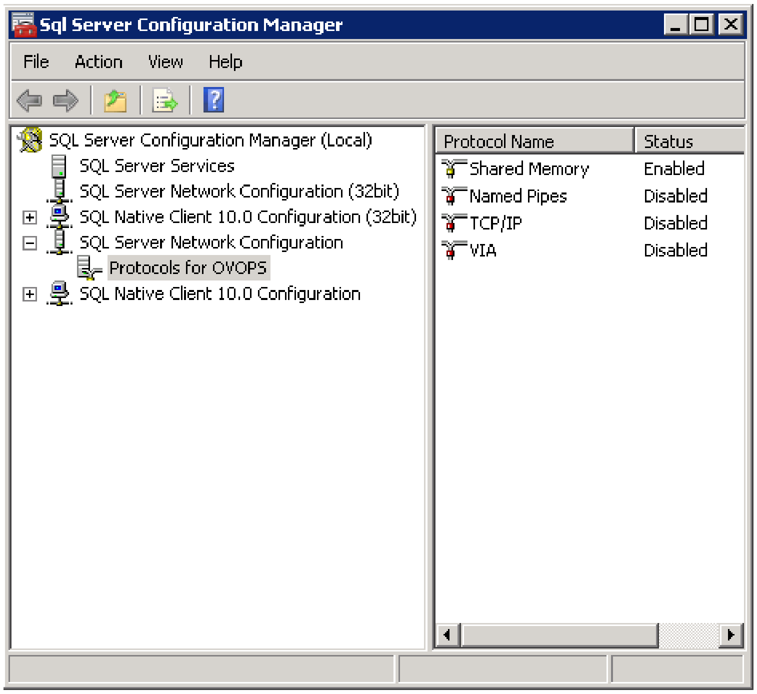
Ready

g. Click **OK**.

3. Check for the HPOM server port number:

   a. Click **Start** > **Programs** > **Microsoft SQL Server 2005** > **Configuration Tools** > **SQL Server Configuration Manager**. The SQL Server Configuration Manager window opens.

b. Expand **SQL Server Network Configuration** and select **Protocols for OVOPS**. If the instance name has been changed, select the appropriate instance name.

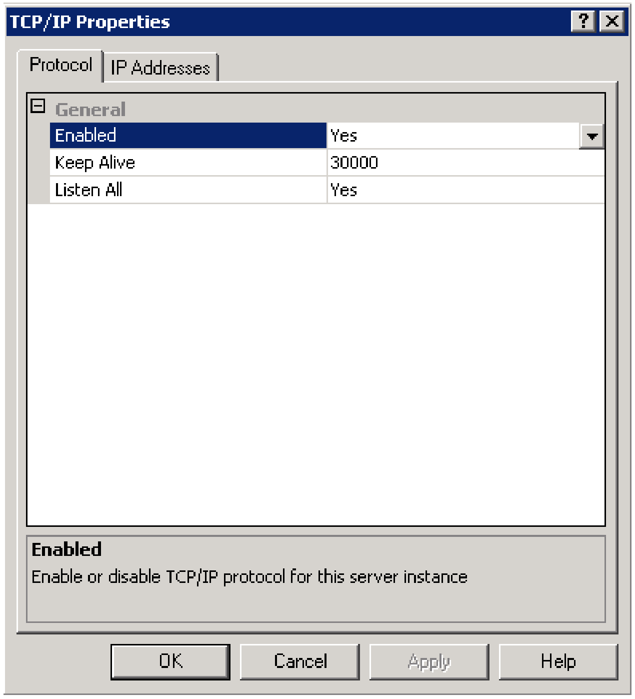


SQL Server Configuration Manager (Local)
- SQL Server Services
- SQL Server Network Configuration (32bit)
- SQL Native Client 10.0 Configuration (32bit)
- SQL Server Network Configuration
  - Protocols for OVOPS
- SQL Native Client 10.0 Configuration

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Disabled
TCP/IP	Disabled
VIA	Disabled

c. On the right pane, right-click **TCP/IP**, then click **Enable**.

d. Right-click **TCP/IP** again, then click **Properties**. The TCP/IP Properties dialog box opens.



General

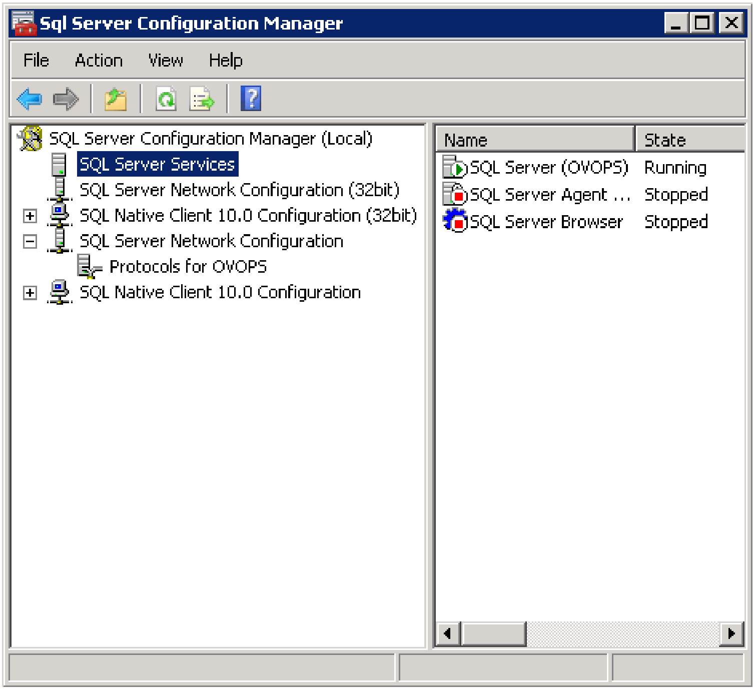
Enabled	Yes
Keep Alive	30000
Listen All	Yes

Enabled
Enable or disable TCP/IP protocol for this server instance

   e. On the **IP Addresses** tab, under the **IPAll**, note the port number.

4. Restart the HPOM database server:

   a. In the SQL Server Configuration Manager window, click **SQL Server Services**.



SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit)
SQL Native Client 10.0 Configuration (32bit)
SQL Server Network Configuration
Protocols for OVOPS
SQL Native Client 10.0 Configuration

Name	State
SQL Server (OVOPS)	Running
SQL Server Agent ...	Stopped
SQL Server Browser	Stopped

   b. On the right pane, right-click **SQL Server (OVOPS)**, then click **Restart**.

You can use the newly created user name, password, and the observed instance name and port number when configuring the HPOM data source connection in the Administration Console.

> **Note**: You can perform these steps by using the command prompt utility, osql. For more information, see the Microsoft Support KB article at the following URL: http://support.microsoft.com/kb/325003

Configuring Collections for Custom Data Sources

Operations Analytics relies on collected metrics, topology, event, and log file data from a diverse set of possible data sources. An Operations AnalyticsCollector Appliance contains the software that listens for data coming from a device. Each server that is running the Operations Analytics Collector software is configured as a Collector Appliance.

To configure Operations Analytics to collect data from the supported custom data sources you plan to use, you must configure collections by creating collection templates that reside on the Operations Analytics Server Appliance. The instructions in this section explain how to configure Operations Analytics to begin collecting data for the custom data sources you plan to use.

Navigate to the instructions for the custom data source or sources you plan to use:

- "Configuring a Custom CSV Collection"
- "Configuring a Custom SiteScope Collection"
- "Configuring a Structured Log Collection"

Configuring a Custom CSV Collection

After you complete the steps in this section, the Custom CSV Collection reads data from the CSV files within 60 seconds of the file being placed in the source directory.

1. Choose the `<filename>.csv` file you want to load into the Operations Analytics database. For Operations Analytics, consider that most `<filename>.csv` files for a CSV collection will have a CSV file with a header and at least one row of data. For this example, assume this file name is `your_file.csv`.

2. For this example, suppose you run the following command from the Operations Analytics Server Appliance to create the custom CSV template:

   ```
    $OPSA_HOME/bin/opsa-csv-template-gen.sh -inputfile your_file.csv -
   name <your_template_name> -domain <testDomain> -group <testGroup>
   -sourcedir /opt/HP/opsa/data/<mySourceDirectory> -datecolumn Time -
   dateformat MM/dd/yyyy hh:mm:ss -timezone GMT+0 -filepattern *.csv -
   grouptype metrics -key Time, Usage in MHz
   ```

   See the *opsa-csv-template-gen.sh* reference page (or the Linux manpage) for more information.

   Look for a message similar to the following:

   ```
   Generated the Custom CSV collection template
   /opt/HP/opsa/conf/collection/server/config.templates/custom/1.0/tes
   tDomain/testGroup/<your_template_name>.xml
   ```

   Use the following pattern letters when configuring the date format to use when parsing date strings:

Letter	Date or Time Component	Presentation	Examples
G	Era designator	Text	AD
Y	Year	Year	1996; 96
M	Month in Year	Month	July; Jul; 07
w	Week in Year	Number	27

Letter	Date or Time Component	Presentation	Examples
W	Week in month	Number	2
D	Day in year	Number	189
d	Day in month	Number	10
F	Day of week in month	Number	2
E	Day in week	Text	Tuesday; Tue
a	Am/Pm marker	Text	PM
H	Hour in day (0-23)	Number	0
k	Hour in day (1-24)	Number	24
K	Hour in am/pm (0-11)	Number	0
h	Hour in am/pm (1-12)	Number	12
m	Minute in hour	Number	30
s	Second in minute	Number	55
S	Millisecond	Number	978
z	Time zone	General time zone	Pacific Standard Time; PST; GMT-08:00
Z	Time zone	RFC 822 time zone	-0800

The following examples show how to interpret date and time patterns in the U.S. locale. The given date and time are 2001-07-04 12:08:56 local time in the U.S. Pacific Time time zone.

Date and Time Pattern	Result
"yyyy.MM.dd G 'at' HH:mm:ss z"	2001.07.04 AD at 12:08:56 PDT
"EEE, MMM d, ''yy"	Wed, Jul 4, '01
"h:mm a"	12:08 PM
"hh 'o''clock' a, zzzz"	12 o'clock PM, Pacific Daylight Time
"K:mm a, z"	0:08 PM, PDT

Date and Time Pattern	Result
"yyyyy.MMMMM.dd GGG hh:mm aaa"	02001.July.04 AD 12:08 PM
"EEE, d MMM yyyy HH:mm:ss Z"	Wed, 4 Jul 2001 12:08:56 -0700
"yyMMddHHmmssZ"	010704120856-0700
"yyyy-MM-dd'T'HH:mm:ss.SSSZ"	2001-07-04T12:08:56.235-0700

3. For this example, the result of running this command is the `<your_template_name>.xml` file, and is a collection template for the `your_file.csv` file.

   > The purpose of the `-datecolumn`, `dateformat`, and `-timezone` options is to identify one column from the `your_file.csv` file as the `timestamp` column for the database table. This column selection is mandatory for Operations Analytics collections using metric tables. These options are provided to help you, as the Operations Analytics administrator, to identify the correct column.

4. For this example, run the following command from the Operations Analytics Server Appliance to create the collector configuration:

   ```
   $OPSA_HOME/bin/opsa-collection-config.sh -create -collectorhost
   <fully-qualified domain name of the collector host> -source custom
   -domain <testDomain> -group <testGroup> -username <tenant admin
   user>
   ```

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

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

5. Run the following command from the Operations Analytics Server Appliance to validate the collection configuration you just created:

   ```
   $OPSA_HOME/bin/opsa-collection-config.sh -list -allversions -
   collectorhosts -username <tenant admin user>
   ```

   To verify a successful collection configuration creation, look for a message showing the expected collector host name, tenant name, and tenant version. The message should also include the source template details such as its version, domain, and group.

6. Run the following command from the Operations Analytics Server Appliance to publish this

collection configuration to the Operations Analytics Collector Appliance :

```
$OPSA_HOME/bin/opsa-collection-config.sh -publish -collectorhost
<fully-qualified domain name of the collector host> -username
<tenant admin user>
```

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

If you want to add tags to a Custom CSV Collection, use the `opsa-tag-manager.sh` command . See "Configuring a Custom CSV Collection" and the *opsa-tag-manager.sh* reference page (or the Linux manpage) for more information.

Configuring a Custom SiteScope Collection

After you complete the steps in this section, SiteScope starts sending data to the Custom SiteScope Collection. The Custom SiteScope Collection collects data as it arrives from SiteScope.

Configuring a Collector Appliance by creating custom collector templates is a two-step process:

1. "Generating and Configuring Templates (Custom SiteScope Collection)"
2. "Configuring SiteScope for Integrating Data with Operations Analytics (Automated Method)"

> **Note**: If you prefer to use a manual method to configure SiteScope for Integrating data with Operations Analytics, see "Configuring SiteScope for Integrating Data with Operations Analytics (Manual Method)".

> **Note**: The automated method supports SiteScope version 11.10 or newer.

Generating and Configuring Templates (Custom SiteScope Collection)

To configure a Custom SiteScope Collection, you must use SiteScope Unit Of Measurement (UOM) files as an input for the opsa-sis-collector-auto-conf.sh script. If you are using Operations Analytics for SiteScope version 11.22IP or newer, skip this step and go directly to "Configuring SiteScope for Integrating Data with Operations Analytics (Automated Method)".

If you are using an earlier version of SiteScope, you have two options:

- Option 1: Use the opsa-sis-collector-auto-conf.sh script with the default UOM file. The default UOM file is located at `$OPSA_HOME/conf/collection/sitescope_configuration/uom/data_integration_uom.xml`. Using the default UOM file, follow the instructions at "Configuring SiteScope for Integrating Data with Operations Analytics (Automated Method)".

> **Note**: Operations Analytics includes a default UOM file, `$OPSA_HOME/conf/collection/sitescope_configuration/uom/data_integration_uom.xml`, which supports many of the metrics supported by Operations Analytics. Use the `-uomfiles` option to optionally define a UOM folder path containing UOM files you manually extracted.

- Option 2: To use metrics that are not supported by the default UOM file complete the steps shown below, then follow the instructions at "Configuring SiteScope for Integrating Data with Operations Analytics (Automated Method)"". After following the steps below, then selecting the link, use the `-uomfiles` option to define a UOM folder path containing UOM files you manually extracted.

1. Using the SiteScope UI, navigate to the **Diagnostics Integration Preferences** page (**Using SiteScope** > **Preferences** > **Integration Preferences** > **Diagnostics Integration Preferences**)

2. Click **Generate UOM XML**. Doing so creates the UOM XML file on the HP SiteScope server in the following location: `%SITESCOPE_HOME%\conf\integration\data_integration_uom.xml`.

3. Complete steps 1 and 2 for each SiteScope server from which you plan to collect data.

4. Create an empty directory on the Operations Analytics Server Appliance; then copy the generated UOM files to this newly created directory.

   > **Note**: Rename the UOM files before you copy them to the newly created directory, as many of the generated UOM files might have the same name (`data_integration_uom.xml`).

   > **Note**: When creating SiteScope collection templates, only place valid UOM files in the directory. Do not place any other files in that directory.

5. Optional: You can use the `opsa-sis-collector-auto-conf` script to create complete collection templates for most of the monitor types shown in "Supported Monitor Types". However, there are few created templates you might need to customize after you create them. For example, you might need to customize the template contents of the following SiteScope monitor types, as you should vary the template content to match the data you configure the monitor to collect:
   - JMXMonitor
   - XMLMetrics

   There are two tasks you might need to complete when customizing the creation of a SiteScope collection template for a particular monitor type:

a. **Parsing the counter names to separate out metric names from instance attributes**: Create a regular expression definition in the `/opt/HP/opsa/conf/collection/sitescope_measure_regex_patterns/custom` directory. See the `/opt/HP/opsa/conf/collection/sitescope_measure_regex_patterns/custom/README_BEFORE_CREATING_PATTERNS.txt` file for specific instructions about creating regular expressions to parse the counter names for a SiteScope monitor type.

b. **Defining the data type, tags and units for a parsed metric**: Create a regular expression definition in the `/opt/HP/opsa/conf/collection/sitescope_metadata_patterns/custom` directory. See the `/opt/HP/opsa/conf/collection/sitescope_measure_regex_patterns/custom/README_BEFORE_CREATING_PATTERNS.txt` file for specific instructions about creating regular expression definitions for assigning data types, tags, and units to metrics for a SiteScope monitor type.

Supported Monitor Types

The following list shows the monitor types currently supported by the Custom SiteScope Collection:

Apache
BACIntegrationConfiguration
BACIntegrationStatistics
Composite
ConnectionStatisticsMonitor
CPU
DatabaseCounter
DHCP
Directory
DiskSpace
DNS
DynamicDiskSpace
File
FTPMonitor
HealthServerLoadMonitor
HyperVMonitor
JMXMonitor
LDAPMonitor
LogEventHealthMonitor
LogMonitor
Memory
MicrosoftWindowsEventLog
MQStatusMonitor
MSActiveServerPages
MSIISServer
MSSQLServer
MSWinodwsMediaServer
NetworkBandwidthMonitor

Oracle
Ping
Port
SAPPerformance
Script
Service
SiebelApplicationServer
SolarisZones
SQLQuery
SSLCertificatesStatus
Sybase
UnixResources
URLContent
URLMonitor
URLSequenceMonitor
VMware
VMwareHostCPUMonitor
VMwareHostMemoryMonitor
VMwareHostStateMonitor
VMwareHostStorageMonitor
WebServer
WebService
WebSphere
WindowsPerformance
WindowsResources
WindowsServicesState
XMLMetrics

Configuring SiteScope for Integrating Data with Operations Analytics (Automated Method)

Complete the following tasks to configuring HP SiteScope to forward data to an Operations Analytics Collector Appliance.

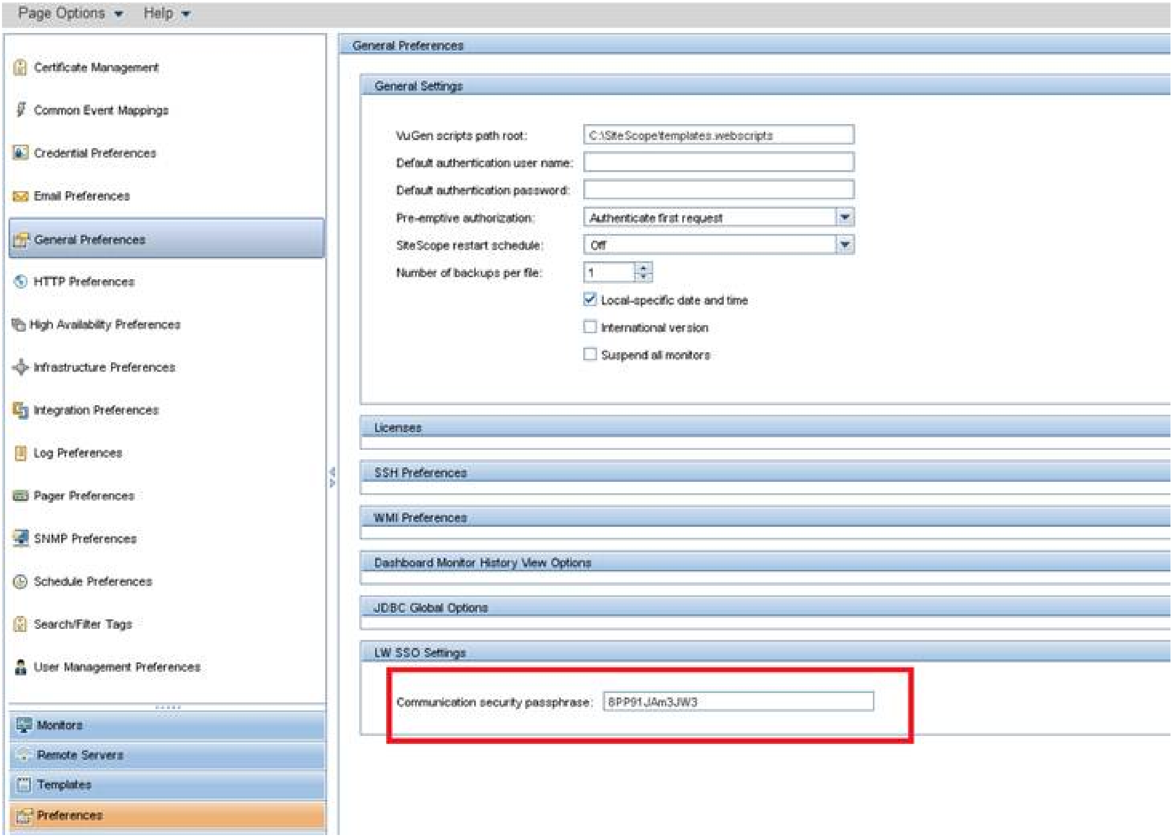
1. A node list file contains details about the sources from which you plan to collect information. The node list file for the Custom SiteScope Collections must include the information shown in the following table.

   > **Note**: Each of the following settings could be configured for a specific SiteScope server, such as `server1`. If the SiteScope server value is missing, the default setting is used. For example, if the `"<`*`server1`*`>.port = "` string does not exist in the node list file, Operations Analytics uses the value of the `"default.port = "` setting for `server1`.

Node List Fields and Values

Field	Value
server.names	The aliases of the SiteScope server names, delimited by commas. These are the servers from which you plan to collect SiteScope information.
<*server* >.hostdnsname	IP Address or fully-qualified domain name of the SiteScope servers for which you are configuring collections. If you need to support failover for the SiteScope servers, specify all the SiteScope servers included in the failover configuration.
.port	The port used to connect to the SiteScope server. Set this if a server does not use the default.port value. The `server.port` setting could be configured for a specific server, such as `server1`. If the server value is missing, the default setting is used. For example if the "`<server1>.port =`" string does not exist in the node list file, Operations Analytics uses the value of the "`default.port =`" setting for `server1`.
.username	The default user name used to connect to the SiteScope server. This is typically `admin`. This field might be set to empty (no value).
.initString	The default value of the initstring used for SSL communication with the SiteScope server. **You can obtain this initString from the SiteScope screen shown below this table.**
.use_ssl	Set this field to `true` to enable SSL communication with the SiteScope server. The default setting is `false`. If you set `default.use_ssl=true`, you need to export the certificate from the Operations Analytics Collector Appliance and import this certificate on each SiteScope server. See *Configuring SiteScope to Use SSL* in the *HP SiteScope Deployment Guide* and the *opsa-collector-manager.sh* reference page for more information.
.opsa_collector	The fully-qualified domain name or the IP address of the common collector that collects data from the SiteScope servers. Do not use `localhost` or `127.0.0.1`.

Finding the initstring in SiteScope



VuGen scripts path root: C:\SiteScope\templates.webscripts
Default authentication user name:
Default authentication password:
Pre-emptive authorization: Authenticate first request
SiteScope restart schedule: Off
Number of backups per file: 1
☑ Local-specific date and time
□ International version
□ Suspend all monitors

Communication security passphrase: 8PP91JAm3JW3

View the sample node list file shown below:

```
server.names=sis01313,sis01388

#properties for sis01313 servers

sis01313.hostdnsname=sis1.somedomain.com

#properties for sis01388 server

sis01388.hostdnsname=sis2.somedomain.com

sis01388.port=18080

#common properties for sis servers

default.port=8080

default.username=admin

default.initString=8PP91JAm3JW3
default.use_ssl=false

default.opsa_collector=opsac
```

To edit the node list file, do the following from the Operations Analytics Server Appliance:

Edit the `$OPSA_HOME/conf/collection/sitescope_configuration/sample_SiteScope_node.properties` file, adding the appropriate information from the examples shown above, then save your work.

2. Run the following command from the Operations Analytics Server Appliance to encrypt the password:

```
$OPSA_HOME/bin/opsa-collection-config.sh -encrypt $OPSA_
HOME/conf/collection/sitescope_configuration/sample_SiteScope_
node.properties
```

> **Note**: If the SiteScope password is empty, edit the nodelist file and remove the value from the appropriate `<server>.password` setting. For example, you might change the value to `sis01.password =`.

3. Run the following command from the Operations Analytics Server Appliance to create the collector configuration.

```
$OPSA_HOME/bin/opsa-sis-collector-auto-conf.sh -nodelist $OPSA_
HOME/conf/collection/sitescope_configuration/sample_SiteScope_
node.properties -username opsatenantadmin -password opsatenantadmin
[-ignoretag] [-forceupdate] [-forcedelete] [-skipcontent] [-
uomfiles] <path to directory containing UOM files>]
```

> **Note**: When running the `opsa-sis-collector-auto-conf.sh` script, you might see an error similar to the following :
>
> `No implementation defined for org.apache.commons.logging.LogFactory.`
>
> If this happens, run the command in this step from the `/opt/HP/opsa/bin/support/` directory.

.

Use the following option definitions for this command:

- The -nodelist options points to the node list file created earlier.
- opsatenantadmin is the default predefined Tenant Admin user for the predefined opsa_default tenant. If you are not using the default tenant, use the Tenant Admin user and password for the tenant you defined for your collections.
- opsatenantadmin is the password for the default predefined Tenant Admin user (for the predefined opsa_default tenant). If you are not using the default tenant, use the Tenant Admin user and password for the tenant you defined for your collections.

- Use the `ignoretag` option to ignore the step of tagging the monitors within SiteScope. The opsa-sis-collector-auto-conf.sh script creates a tag named `opsa_<tenant-name>` and associates it with the root SiteScope group, which means that all monitors will be recursively tagged automatically and dynamically. In some cases, you might want to configure only a subset of the monitors. In those situations, use the `ignoretag` option to manually handle the tagging.

- Use the `–forceupdate` option if you did not make any changes since the last time you ran the opsa-sis-collector-auto-conf.sh script, and still want to **force** the script to make changes in already saved SiteScope profiles. If you use the `–forceupdate` option when running the opsa-sis-collector-auto-conf.sh script, it deletes the old integration configuration and replaces it with the new configuration. For example, if you made some manual changes on the SiteScope profile side and want to return to the original configuration, use the `–forceupdate` option.

- Use the `–forcedelete` option if you want to remove SiteScope configurations made since you last ran the `$OPSA_HOME/bin/opsa-sis-collector-auto-conf.sh` script. To do this, remove the corresponding alias from the `server.names=` setting in the nodelist file, then run the `$OPSA_HOME/bin/opsa-sis-collector-auto-conf.sh` script using the `–forcedelete` option.

- As mentioned in the note beneath "Configuring a Custom SiteScope Collection"Operations Analytics includes a default UOM file, `$OPSA_HOME/conf/collection/sitescope_configuration/uom/data_integration_uom.xml`, which supports many of the metrics supported by Operations Analytics. Use the `–uomfiles` option to optionally define a UOM folder path containing UOM files you manually extracted.

After completing the configuration steps in this section, SiteScope begins forwarding data to the Operations Analytics Collector Appliance based on the configuration choices you made.

Configuring SiteScope for Integrating Data with Operations Analytics (Manual Method)

The following tasks, showing steps and diagrams, explain an example of configuring HP SiteScope to forward data to an Operations Analytics Collector Appliance.

> **Note**: You must complete the step in "Configuring a Custom SiteScope Collection" before completing the configuration steps in this section.

To configure SiteScope to send data to Operations Analytics, you must complete 3 tasks:

- "Task 1: Creating a SiteScope Tag"
- "Task 2: Using the New SiteScope Tag to Mark the Monitor or Monitor Groups"
- "Task 3: Creating a New Data Integration Preference"

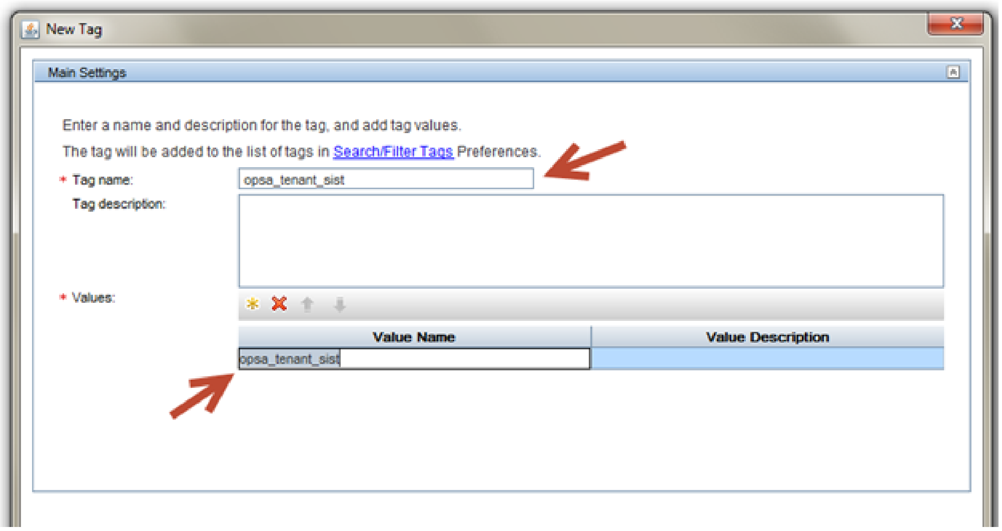
Task 1: Creating a SiteScope Tag

To create a SiteScope tag, do the following:

1. Log on to SiteScope as an **Admin** user.

2. Navigate to **Preferences** > **Search/Filter Tags**

3. Click the **New Tag icon** (the gold-colored star) to create a new tag.
   The following shows the window that should open:



Enter a name and description for the tag, and add tag values.

The tag will be added to the list of tags in Search/Filter Tags Preferences.

* Tag name: opsa_tenant_sist

Tag description:

* Values:

Value Name	Value Description
opsa_tenant_sist	

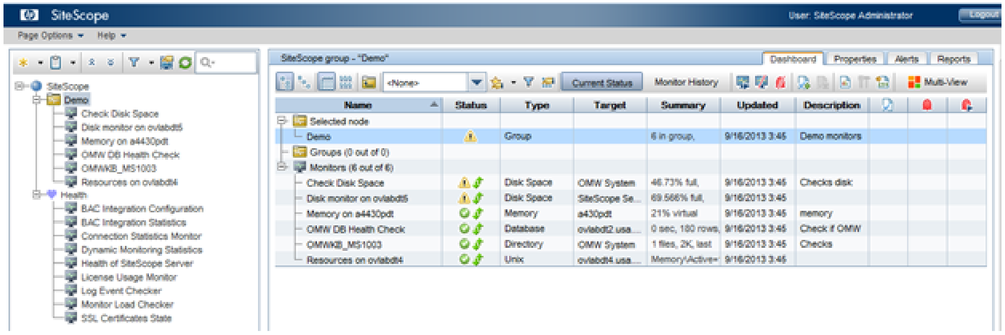
For the **Tag Name** value, enter the name of your choice. For example, you might enter `opsa_tenant_sist`. Click the gold-colored star in the **Values**area, then enter a **Value Name** using the identical string that you used for the **Tag Name** value (`opsa_tenant_sist` for this example).

4. Click **OK** to save the tag definition.

Task 2: Using the New SiteScope Tag to Mark the Monitor or Monitor Groups

To use the tag you just created to mark the Monitor Groups, individual Monitors, or both, from which you want metrics sent to Operations Analytics, do the following:

1. Navigate to the Monitors panel in SiteScope. This is normally the main screen you see when you first log on to SiteScope. The following shows an example system:



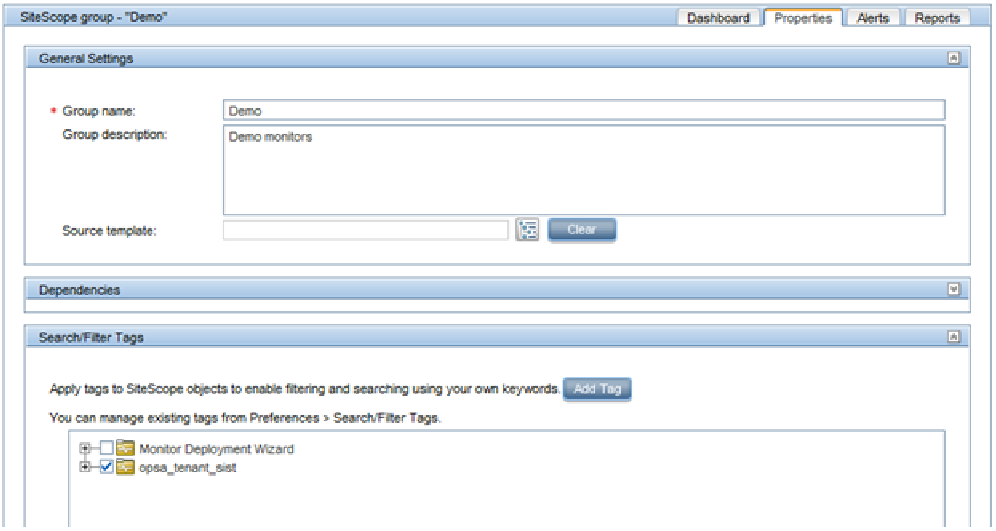
SiteScope group - "Demo"

Name	Status	Type	Target	Summary	Updated	Description
Selected node						
Demo	⚠	Group		6 in group,	9/16/2013 3:45	Demo monitors
Groups (0 out of 0)						
Monitors (6 out of 6)						
Check Disk Space	⚠	Disk Space	OMW System	46.73% full,	9/16/2013 3:45	Checks disk
Disk monitor on ovlabdt5	⚠	Disk Space	SiteScope Se...	69.566% full,	9/16/2013 3:45	
Memory on a4430pdt	✓	Memory	a430pdt	21% virtual	9/16/2013 3:45	memory
OMW DB Health Check	✓	Database	ovlabdt2.usa....	0 sec, 180 rows,	9/16/2013 3:45	Check if OMW
OMWKB_MS1003	✓	Directory	OMW System	1 files, 2K, last	9/16/2013 3:45	Checks
Resources on ovlabdt4	✓	Unix	ovlabdt4.usa....	Memory\Active=	9/16/2013 3:45	

2. For each Monitor Group or individual Monitorfrom which you want metrics sent to Operations Analytics, mark the Group or Monitor with the tag you created in "Task 1: Creating a SiteScope Tag". For example, to mark the entire **Demo** Monitor Group (as in sending metrics from all of the monitors in the group), follow these steps:

   a. Select the **Monitor Group** name in the hierarchy list on the left of the screen.

   b. Click the **Properties** tab. For a Monitor Group, the following window opens:



SiteScope group - "Demo"

* Group name: Demo

Group description: Demo monitors

Source template:

Apply tags to SiteScope objects to enable filtering and searching using your own keywords.

You can manage existing tags from Preferences > Search/Filter Tags.

☐ Monitor Deployment Wizard
☑ opsa_tenant_sist

   c. In the **Search/Filter Tags** configuration panel, select the checkbox for the tag you created in "Task 1: Creating a SiteScope Tag".

   d. Click **Save** to save your changes to the Monitor Group configuration.

> **Note**: If you do not want to send metrics **from all of the monitors within a group**, you must mark each desired monitor individually. The steps are the same as :
>
> i. Select the **Monitor Group** name in the hierarchy list on the left of the screen.
>
> ii. Click the **Properties**tab and a window opens.
>
> iii. Navigate to the **Search/Filter Tags** panel.

iv. Select the checkbox for the tag you created in "Task 1: Creating a SiteScope Tag".

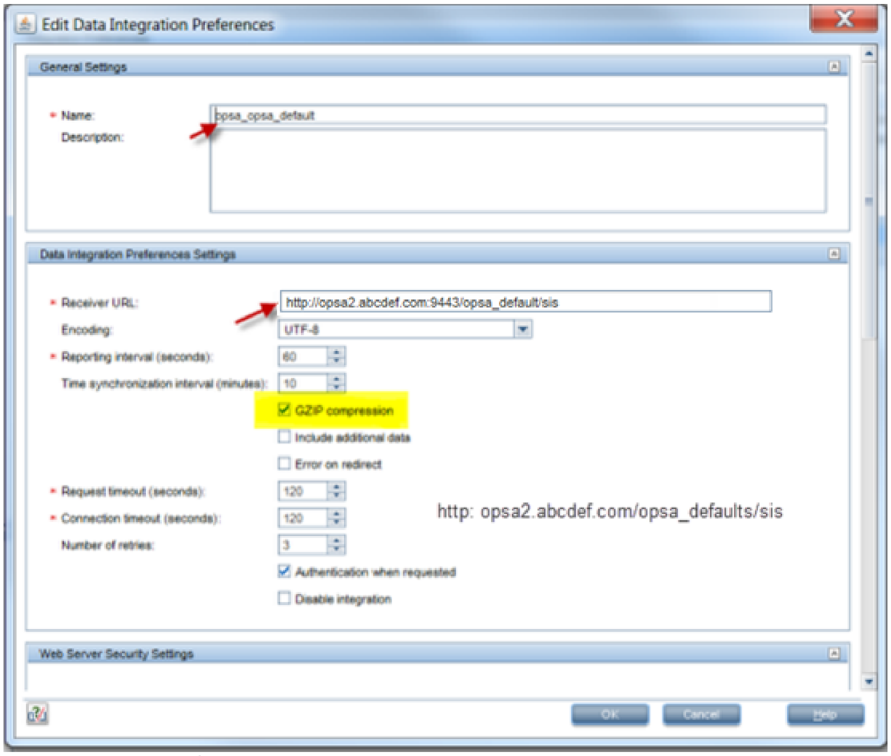
v. Click **Save** to save your changes to the Monitor Group configuration.

Task 3: Creating a New Data Integration Preference

In this final task, configure a new `Data Integration` preference that tells SiteScope where to send the marked data metrics:

1. From SiteScope, Navigate to **Preferences** > **Integration Preferences**.

2. Click the gold-colored star (the New Integration icon), then select the **Data Integration** link in the pop-up window. The following configuration window should appear:



Edit Data Integration Preferences
General Settings
Data Integration Preferences Settings
Web Server Security Settings
OK
Cancel
Help

* Name: opsa_opsa_default
Description:
* Receiver URL: http://opsa2.abcdef.com:9443/opsa_default/sis
Encoding: UTF-8
* Reporting interval (seconds): 60
Time synchronization interval (minutes): 10
☑ GZIP compression
☐ Include additional data
☐ Error on redirect
* Request timeout (seconds): 120
* Connection timeout (seconds): 120
Number of retries: 3
☑ Authentication when requested
☐ Disable integration

http: opsa2.abcdef.com/opsa_defaults/sis

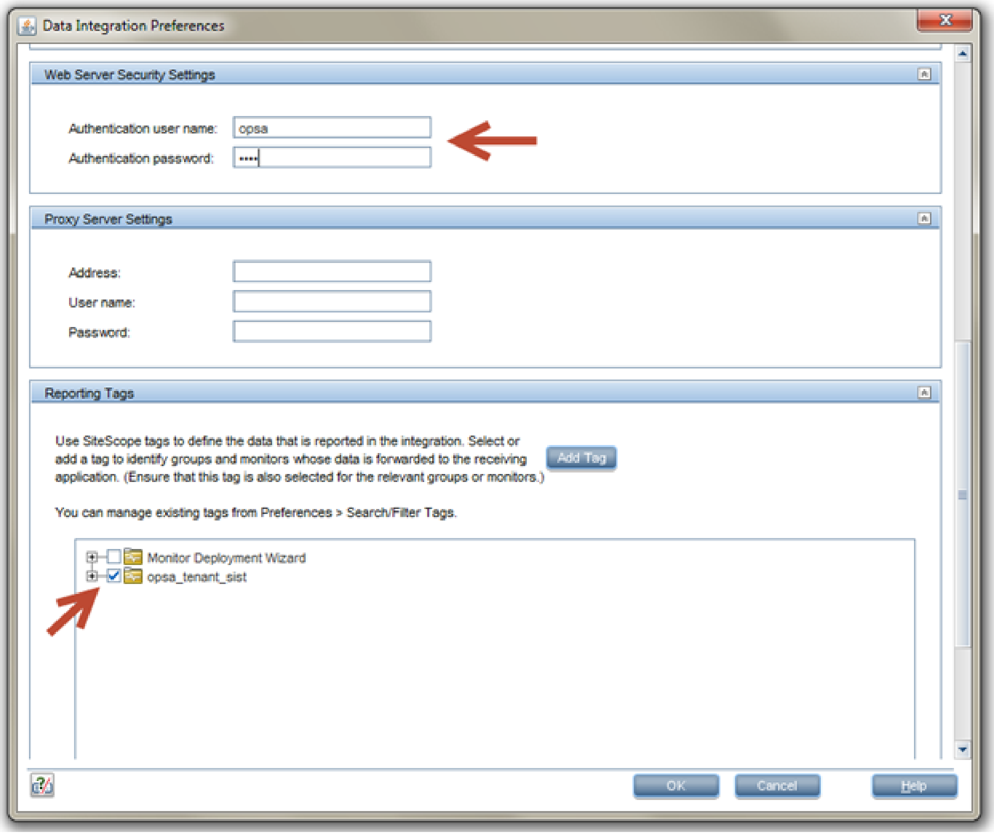
Provide a Name for this Data Integration, then provide the Receiver URL using the following format: `http://`*`<fully-qualified domain name or ip address of the Operations Analytics Collector>`*`:9443/<tenant_name>/sis`

Select the **GZIP compression** option.

In this example, the target Operations Analytics Collector is `opsa2.abcdef.com` and the target Operations Analytics tenant is `opsa_default` (the default tenant). You do not need to change any other settings, as shown in the configuration window above.

3. Scroll down in the configuration window. In the **Web Server Security Settings** panel, authenticate using the credentials for the tenant being configured, which is `opsa` in this example.

   > **Note**: These credentials are the same as those you would use to log on to the Operations Analytics Console for a given tenant. For the example , the credentials are `opsa` (user name) and `opsa` (password).



Data Integration Preferences

Web Server Security Settings

Authentication user name: opsa

Authentication password: ••••

Proxy Server Settings

Address:

User name:

Password:

Reporting Tags

Use SiteScope tags to define the data that is reported in the integration. Select or add a tag to identify groups and monitors whose data is forwarded to the receiving application. (Ensure that this tag is also selected for the relevant groups or monitors.)

You can manage existing tags from Preferences > Search/Filter Tags.

□ Monitor Deployment Wizard

☑ opsa_tenant_sist

4. Finally, check the box for the tag that you created earlier in "Task 1: Creating a SiteScope Tag". Selecting this tag is the most important setting, as it connects the previously marked **Monitor Groups** and **Monitors** to the Data Integration being configured.

5. Click **OK** to create the new SiteScope Data Integration.

After completing the configuration steps in this section, SiteScope begins forwarding data to the Operations Analytics Collector Appliance based on the configuration choices you made.

Configuring a Structured Log Collection

After you complete the steps in this section, the Structured Log Collection collects data every 5 minutes.

By default the `logger.max.sessions` property is set to a value of 5 in an Operations Analytics Collector Appliance and 25 for an Operations Analytics Server Appliance . This means there can be a maximum of 5 Logger session per Logger host in an Operations Analytics Collector Appliance and 25 Logger sessions per Logger host in an Operations Analytics Server Appliance.

To set the maximum number of Logger sessions for the Operations Analytics Collector and Server Appliances, do the following on both the Operations Analytics Collector Appliance and the Operations Analytics Server Appliance:

1. Edit the `$OPSA_HOME/conf/opsa-config.properties` file.
2. Set the `logger.max.sessions` property to the desired value.

   > **Note**: The sum of the values you set in the Operations Analytics Collector and Server Appliances must not exceed 30.

3. Save your work.
4. If you changed the `logger.max.sessions` property on the Operations Analytics Server Appliance, restart the `opsa-server` service by running the following commands from the Operations Analytics Server Appliance:
   a. `$OPSA_HOME/bin/opsa-server stop`

   b. `$OPSA_HOME/bin/opsa-server start`

   See the *opsa-server* reference page (or the Linux manpage) for more information.
5. If you changed the `logger.max.sessions` property on the Operations Analytics Collector Appliance, restart the `opsa-collector` service by running the following commands from the Operations Analytics Collector Appliance:
   a. `$OPSA_HOME/bin/opsa-collector stop`

   b. `$OPSA_HOME/bin/opsa-collector start`

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

If you have two or more Operations Analytics Server Appliances configured in a distributed environment, you must spread the 25 Logger sessions across both Operations Analytics Server Appliances. If you do not configure these session values correctly, one appliance might control all of the sessions, while the remaining appliance cannot control any sessions.

> **Note**: If you are not planning to configure structured log collections, then set the `logger.max.sessions` property on the Operations Analytics Server Appliance to 30. Doing so enables Operations Analytics to use all of the Logger sessions for rawlog searches in the Operations Analytics console.

> **Note**: As mentioned above, from a resource perspective, there is a limit to the number of Logger sessions supported by HP Operations Analytics Software. HP strongly recommends that, when you configure Logger collections, you assign those Logger collections to one common Operations Analytics collector. Doing so reduces the number of Logger sessions.

To configure an Operations Analytics Structured Log Collection, do the following:

1. Run the following command from the Operations Analytics Server Appliance if you think there might be an existing structured log collection template you can use. Running this command shows you the available predefined templates: `$OPSA_HOME/bin/opsa-collection-config.sh -list -templates -username <tenant admin user>`

2. If there is no existing structured log collection template do the following from the Operations Analytics Server Appliance to create one:

   a. Review the following two HP ArcSight Logger collection templates:

      ```
      /opt/HP/opsa/conf/collection/sample/config.templates/arcsight/1.0
      /apache/access/apache_access.xml
      /opt/HP/opsa/conf/collection/sample/config.templates/arcsight/1.0
      /log/structuredlog/arcsight_collection.xml
      /opt/HP/opsa/conf/collection/sample/config.templates/splunk/1.0/l
      og/structuredlog/splunk_collection.xml
      ```

   b. Copy one of these templates to a temporary location; then edit the file to create the collection template you need for your structured log collection. Suppose that, for this example, we call this file `mystructuredlog.xml`.

   c. Edit the `mystructuredlog.xml` file:

      i. Change the `domain`, `tags`, `group`, and `label` attributes for the `collectiongroup` element.

      ii. Configure the columns to be collected.

      iii. Save your work.

   d. Copy the `mystructuredlog.xml` file to

      ```
      /opt/HP/opsa/conf/collection/server/config.templates/<arcsight |
      splunk>/<domain from template files>/<group from template
      files/mystructuredlog.xml
      ```

3. A node list file contains details about the sources from which you plan to collect information. There are sample nodelist files located in the `$OPSA_HOME/conf/collection/sample` directory. Operations Analytics administrators can use these sample files to publish the node list file. The sample node list file for the Structured Log collection is either `sample_ArcSight_node.properties` or `sample_Splunk_node.properties`.

   Complete the following steps from the Operations Analytics Server Appliance for the Structured Log collection :

   a. Copy the appropriate node list file from the `$OPSA_HOME/conf/collection/sample` directory to some location, such as `/tmp/mynodelist.properties`:

      > **Note**: Select the template file pertaining to the type of collection you are configuring.

b. Edit the `/tmp/mynodelist.properties` file; add information according to what is written in the sample file; then save your work.

4. Run the following command from the Operations Analytics Server Appliance to create the collector configuration:

```
$OPSA_HOME/bin/opsa-collection-config.sh -create -nodelist
/tmp/mynodelist.properties -collectorhost <fully-qualified-domain-
name of collector host> -source splunk|arcSight -domain <domain
from template files> -group <domain from template files> -username
<tenant admin user>
```

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

5. Run the following command from the Operations Analytics Server Appliance to validate the collection configuration you just created:

```
$OPSA_HOME/bin/opsa-collection-config.sh -list
-allversions -collectorhosts -username <tenant admin user>
```

To verify a successful collection configuration creation, look for a message showing the expected collector host name, tenant name, and tenant version. The message should also include the source template details such as its version, domain, and group.

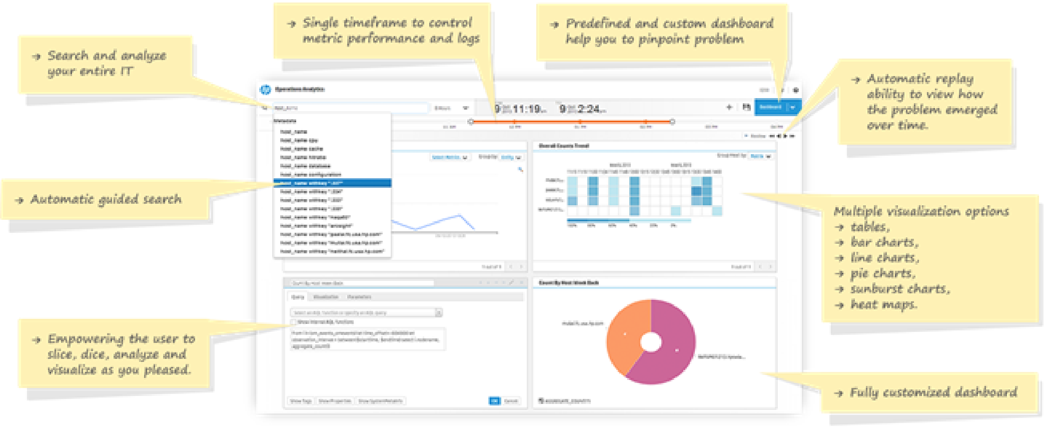
6. Run the following command from the Operations Analytics Server Appliance to publish this collection configuration to the Operations Analytics Collector Appliance:

```
$OPSA_HOME/bin/opsa-collection-config.sh -publish -collectorhost
<fully-qualified domain name of the collector host> –username
<tenant admin user>
```

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

Getting Started with Operations Analytics

The following graphic provides a brief overview of the Operations Analytics Console.



→ Search and analyze your entire IT

→ Single timeframe to control metric performance and logs

→ Predefined and custom dashboard help you to pinpoint problem

→ Automatic replay ability to view how the problem emerged over time.

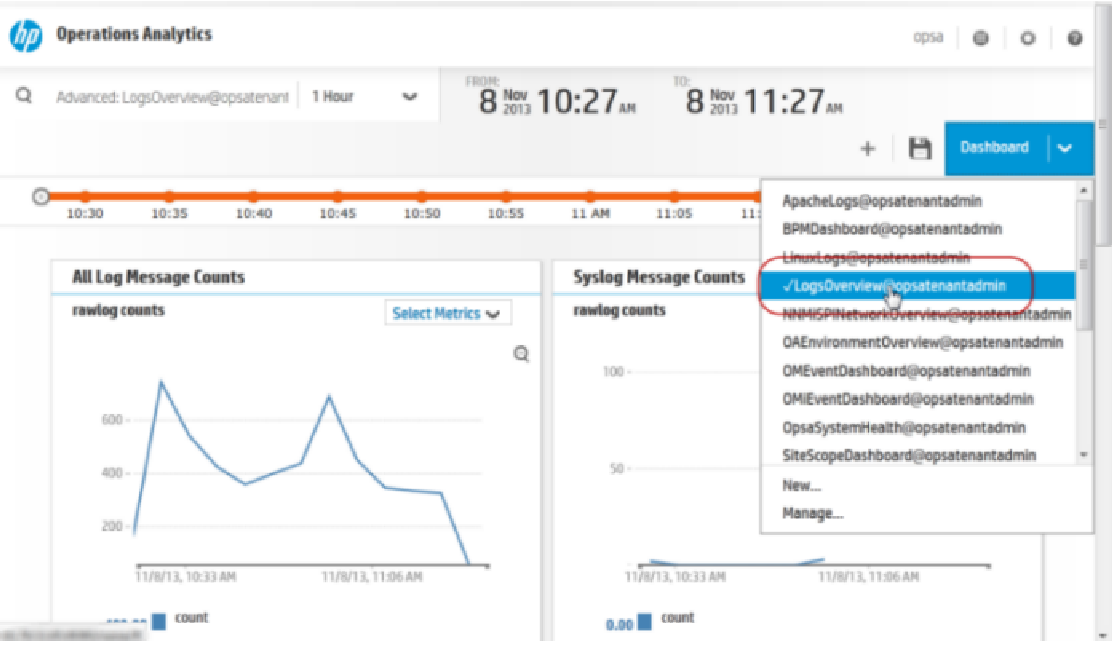
→ Automatic guided search

Multiple visualization options
→ tables,
→ bar charts,
→ line charts,
→ pie charts,
→ sunburst charts,
→ heat maps.

→ Empowering the user to slice, dice, analyze and visualize as you pleased.

→ Fully customized dashboard

Click **LogsOverview** to see the Logs Overview dashboard, which provides an overview of information for the log messages in your IT environment. See the Operations Analytics online help for more information about dashboards.


Operations Analytics
opsa
Advanced: LogsOverview@opsatenant
1 Hour
FROM:
8 Nov 2013 10:27 AM
TO:
8 Nov 2013 11:27 AM
Dashboard
10:30
10:35
10:40
10:45
10:50
10:55
11 AM
11:05
All Log Message Counts
rawlog counts
Select Metrics
600
400
200
11/8/13, 10:33 AM
11/8/13, 11:06 AM
count
Syslog Message Counts
rawlog counts
100
50
0.00
ApacheLogs@opsatenantadmin
BPMDashboard@opsatenantadmin
LinuxLogs@opsatenantadmin
✓LogsOverview@opsatenantadmin
NNMiSPINetworkOverview@opsatenantadmin
OAEnvironmentOverview@opsatenantadmin
OMEventDashboard@opsatenantadmin
OMiEventDashboard@opsatenantadmin
OpsaSystemHealth@opsatenantadmin
SiteScopeDashboard@opsatenantadmin
New...
Manage...

For more information about getting started with Operations Analytics, see *Getting Started with HP Operations Analytics* in the *Operations Analytics help*.

Chapter 5: Creating, Applying, and Maintaining Tags (Task 7)

Task 1:	**Task 2:**	**Task 3:**	**Task 4:**	**Task 5:**	**Task 6:**	**▶ Task 7:**	**Task 8:**
Planning your Deployment	Installing and Configuring the Vertica Software	Installing and Configuring HP ArcSight Logger	Installing and Licensing the Operations Analytics Server Appliance	Installing and Configuring the Operations Analytics Collector Appliance	Configuring Tenants and Collections	Creating, Applying, and Maintaining Tags	Communicating Collection Names and Meta Data Information to your Users

Operations Analytics supports three types of tags:

- Property Group Tags: Operations Analytics administrators add these tags to an entire collection.
- Link Tags: Link Tags are special tags used to relate collection information. Operations Analytics administrators add these tags to define a link between collections, creating the same link tag for each collection they want to link together.
- Property Tags: Operations Analytics administrators add these link tags to one or more properties (or database columns) for a specific collection.

To manage tags, use the opsa-tag-manager.sh script. See the `opsa-tag-manager.sh` reference page (or the Linux manpage) for more information.

Note: Tags, property uids, and property group uids are not case sensitive. They are always converted into lowercase.

Adding Tags

Use the following command to add tags:

- **Property Tags**: `$OPSA_HOME/bin/opsa-tag-manager.sh -add_tags -type property_group -file /opt/HP/opsa/tmp/property_tags.csv -username <`*`username`*`>`
- **Property Group Tags**: `$OPSA_HOME/bin/opsa-tag-manager.sh -add_tags -type property_group -file /opt/HP/opsa/tmp/property_group_tags.csv -username <`*`username`*`>`
- **Link Tags**: `$OPSA_HOME/bin/opsa-tag-manager.sh -add_tags -type link -file /opt/HP/opsa/tmp/link_tags.csv -username <`*`username`*`>`

Listing Tags

Use the following command to list tags:

- **Property Tags**: `$OPSA_HOME/bin/opsa-tag-manager.sh -list_tags -type property [-propertygroup_id` *`ID`*`] [-property_id ID] -username <`*`username`*`>`
- **Property Group Tags**: `$OPSA_HOME/bin/opsa-tag-manager.sh -list_tags -type property_group [-propertygroup_id` *`ID`*`] -username <`*`username`*`>`
- **Link Tags**: `$OPSA_HOME/bin/opsa-tag-manager.sh -list_tags -type link -username <`*`username`*`>`

Deleting Tags

Do not delete any pre-existing tags used for pre-defined collection templates, as that might disrupt these collections.

Use the following command to delete tags:

- **Property Tags**: `$OPSA_HOME/bin/opsa-tag-manager.sh -delete_tags -type property -propertygroup_id <property group id> -tag_name <`*`list of comma-separated tags`*`> -username <`*`username`*`>`
- **Property Group Tags**: `$OPSA_HOME/bin/opsa-tag-manager.sh -delete_tags -type property_group -propertygroup_id <property group id> -tag_name <`*`list of comma-separated tags`*`> -username <`*`username`*`>`
- **Link Tags**: `$OPSA_HOME/bin/opsa-tag-manager.sh -delete_tags -type link -propertygroup_id <property group id> -rel_propertygroup_id <`*`property group uid of source`*`> -username <`*`username`*`>`

Chapter 6: Communicating Collection Names and Meta Data Information to your Users (Task 8)

Task 1:	**Task 2:**	**Task 3:**	**Task 4:**	**Task 5:**	**Task 6:**	**Task 7:**	▶ **Task 8:**
Planning your Deployment	Installing and Configuring the Vertica Software	Installing and Configuring HP ArcSight Logger	Installing and Licensing the Operations Analytics Server Appliance	Installing and Configuring the Operations Analytics Collector Appliance	Configuring Tenants and Collections	Creating, Applying, and Maintaining Tags	Communicating Collection Names and Meta Data Information to your Users

On way for operators to view the tags and property groups available to them is to View the **SystemMetaInfo** dashboard, which displays all of the active collections and the tags being used. The information in this dashboard provides operators with a lot of the information they need for more effective queries. See *Dashboards Provided by Operations Analytics* in the *Operations Analytics Help* for more information.

To create a list of the collections and tags your users will be interested in, you can also do the following:

1. To list all of the tenants configured for an Operations Analytics Server Appliance, run the `$OPSA_HOME/bin/opsa-tenant-manager.sh -list -loginUser [Super Admin User] -loginPassword [Super Admin User Password]` command from the Operations Analytics Server Appliance. Make a list of the tenants shown in the command output for your users. See the *opsa-tenant-manager.sh* reference page (or the Linux manpage) for more information.

2. To list all of the published collectors and collections for a tenant, run the `$OPSA_HOME/bin/opsa-collection-config.sh -list -collectorhosts -username <Tenant Admin User>` command from the Operations Analytics Server Appliance. Make a list of the published collectors and collections shown in the command output for your users. See the *opsa-collection-config.sh* reference page (or the Linux manpage) for more information.

3. Use the `$OPSA_HOME/bin/opsa-tag-manager.sh` script from the Operations Analytics Server Appliance to view and identify the tags in which your users are interested. Experiment with the options available with the `opsa-tag-manager.sh` script to identify the tags you must communicate to your users. . See the *opsa-tag-manager* reference page (or the Linux manpage) for more information. Make a list of these tags

4. Combine the information from these steps and distribute this information to your Operations Analytics users.

Chapter 7: Accessing Operations Analytics

There are several security methods you can configure for user access and authentication for Operations Analytics.

Configuring SSL for the Operations Analytics Server Appliance

One-way SSL provides secure communication between the client and the Operations Analytics server. During an SSL session creation, the server sends a digital certificate (self-signed or CA signed) containing information about the server. This information, such as domain, organization, and location, helps the client verify the server’s identity. SSL is disabled by default.

It is recommended that customers enable SSL communication for those environments where security is a concern. When you configure a Collector Appliance for SSL communication, you must export the client certificate from the Collector Appliance, then import that certificate into the trust store on the Operations Analytics Server Appliance using the `$OPSA_HOME/bin/opsa-server-manager.sh` script. See "Configuring SSL for the Operations Analytics Collector Appliance" for more information about configuring SSL for the Operations Analytics Collector Appliance.

Use the information in this section to manage SSL on the Operations Analytics Server Appliance.

Configuring SSL with a Certificate Authority (CA) Signed Certificate for the Operations Analytics Server Appliance

Complete the following steps to enable SSL communication to the Operations Analytics Server Appliance using a CA signed certificate:

1. Before enabling SSL to the Operations Analytics Server Appliance, complete this step to create a user in JBoss **Management Realm**. do the following:
   a. Run the `$OPSA_HOME/jboss/bin/add-user.sh` script.

   b. For the first question, answer **"a" - Management User (mgmt-users.properties)**, then follow the instructions.

      > **Note**: You will need to provide the JBoss management realm credentials when enabling SSL later in these instructions.

2. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script, and log on with **super-admin** credentials. See the *opsa-server-managersh* reference page (or the Linux manpage), for more information.

3. Select the **Configure SSL** option.

4. Select the **Import CA certificate to OPSA server keystore** option to import a CA signed certificate to OPSA server keystore. The `opsa-server-manager.sh` script prompts you for the certificate alias name and lists a set of used aliases.. Enter a unique alias name that has not been used.

   Note: The administrator can get a CA signed certificate by generating a Certificate Signing Request file using the self-signed certificate stored in OPSA keystore. Submit this Certificate Signing Request to a certificate authority. To generate a Certificate Signing Request from a self-signed certificate, select the **Generate certificate signing request option** .The `opsa-server-manager.sh` script prompts you for the alias of the self-signed certificate. Enter `opsa_server` from the list of aliases to generate Certificate Signing Request for a self-signed certificate.

5. Optional: Select the **Import trusted certificate to OPSA server truststore** option to import trusted certificates (if any). For example, you can add HP ArcSight Logger's server certificate to the OPSA truststore file.

6. Select the **Enable/Disable SSL** option to enable SSL. You will need to enter the JBoss **Management Realm** user and password you created in the first step.The `opsa-server-manager.sh` script prompts you for the certificate alias to be used for SSL communication. Enter one of the aliases from the listed aliases.

7. Select the **Go back to main menu** option; then select the **Restart OPSA server** option to restart the Operations Analytics Server Appliance.

   Note: Your configuration changes will not occur unless the server is restarted.

8. Operations Analytics users can access the Operations Analytics Console using HTTP or HTTPS.

   Note: If a user attempts to use HTTP when HTTPS is configured, the user will automatically be redirected using HTTPS.

Configuring SSL with a Self-Signed Certificate for the Operations Analytics Server Appliance

Complete the following steps to enable SSL communication to the Operations Analytics Server Appliance using a self-signed certificate:

1. Before enabling SSL to the Operations Analytics Server Appliance, complete this step to create a user in JBoss **Management Realm**. Do the following:
   a. Run the `$OPSA_HOME/jboss/bin/add-user.sh` script.

   b. For the first question, answer **"a" - Management User (mgmt-users.properties)**, then follow the instructions.

> **Note**: You will need to provide the JBoss management realm credentials when enabling SSL later in these instructions.

2. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script, and log on with **super-admin** credentials. See the *opsa-server-manager.sh* reference page (or the Linux manpage), for more information.

3. Select the **Configure SSL** option.

4. Select the **Generate self-signed certificate for OPSA server** option to generate a self-signed certificate and add the certificate to the Operations Analytics server keystore.

   > **Note**: The `opsa-server-manager.sh` script stores the self-signed certificate in the `keystore` file with the `opsa_server` alias name.

   > **Note**: Set the self-signed certificate attributes, such as `common name`, `country`, and `validity` by editing the `/opt/HP/opsa/conf/ssl/cert/opsa-self-signed-cert.template` file.

5. Optional: Select the **Import trusted certificate to OPSA server truststore** option to import trusted certificates (if any). For example, you can add HP ArcSight Logger's server certificate to the OPSA truststore file.

6. Select the **Enable/Disable SSL** option to enable SSL. You will need to enter the JBoss **Management Realm** user and password you created in the first step.The `opsa-server-manager.sh` script prompts you for the certificate alias to be used for SSL communication. Enter one of the aliases from the listed aliases.

7. Select the **Enable/Disable SSL** option to enable SSL. The `opsa-server-manager.sh` script prompts you for the certificate alias to be used for SSL communication. Enter `opsa-server`.

   > `opsa_server` is one of the aliases shown by the script.

8. Select the **Go back to main menu** option; then select the **Restart OPSA server** option to restart the Operations Analytics Server Appliance..

   > **Note**: Your configuration changes will not occur unless the server is restarted.

9. Operations Analytics users can access the Operations Analytics Console using HTTP or HTTPS.

   > **Note**: If a user attempts to use HTTP when HTTPS is configured, the user will automatically be redirected using HTTPS.

Editing the SSL Configuration for the Operations Analytics Server Appliance

To change the certificate alias used for SSL communication, do the following:

1. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script, and log on with **super-admin** credentials. See the *opsa-server-managersh* reference page (or the Linux manpage), for more information.

2. Select the **Configure SSL** option.

3. Select the **Change key alias to be used for SSL communication** option.

4. The `$OPSA_HOME/bin/opsa-server-manager.sh` script prompts you for the alias name, and lists the existing set of aliases from the OPSA keystore. Enter the desired alias name from the list.

5. Select the **Go back to main menu** option, then select the **Restart OPSA server** option to restart the Operations Analytics Server Appliance.

   > **Note**: Your configuration changes will not occur unless the server is restarted.

Disabling the SSL Configuration for the Operations Analytics Server Appliance

To disable the SSL communication, do the following:

1. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script, and log on with **super-admin** credentials. See the *opsa-server-managersh* reference page (or the Linux manpage), for more information.

2. Select the **Configure SSL** option.

3. Select the **Enable/Disable SSL** option.

4. The `$OPSA_HOME/bin/opsa-server-manager.sh` script prompts you for a confirmation. Enter `yes` to disable the SSL communication.

5. Select the **Go back to main menu** option, then select the **Restart OPSA server** option to restart the Operations Analytics Server Appliance.

Managing the OPSA Keystore and Truststore for the Operations Analytics Server Appliance

To modify the OPSA keystore and truststore password, do the following:

1. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script, and log on with **super-admin** credentials. See the `opsa-server-manager.sh` reference page (or the Linux manpage) for more information.

2. Select the **Configure SSL** option.

3. Select the **Modify OPSA keystore/truststore password** option.

4. The `$OPSA_HOME/bin/opsa-server-manager.sh` script prompts you for the new password for the keystore and truststore. Enter the new passwords.

5. Select the **Go back to main menu** option, then select the **Restart OPSA server** option to restart the Operations Analytics Server Appliance.

To delete a certificate from the OPSA keystore and truststore, do the following:

1. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script, and log on with **super-admin** credentials. See the `opsa-server-manager.sh` reference page (or the Linux manpage) for more information.

2. Select the **Configure SSL** option.

3. Select the **Delete certificate from OPSA server keystore** or **Delete certificate from OPSA server truststore** option.

4. The `$OPSA_HOME/bin/opsa-server-manager.sh` script prompts you for the alias name, listing the existing set of aliases from the OPSA keystore/truststore. Enter the alias name to be deleted from the list.

5. Select the **Go back to main menu** option, then select the **Restart OPSA server** option to restart the Operations Analytics Server Appliance.

> The certificate delete will fail if the certificate is in use.

To export a certificate from the OPSA keystore, do the following:

1. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script, and log on with **super-admin** credentials. See the `opsa-server-manager.sh` reference page (or the Linux manpage) for more information.

2. Select the **Configure SSL** option.

3. Select the **Export certificate from OPSA server keystore** option.

4. The `$OPSA_HOME/bin/opsa-server-manager.sh` script prompts you for the alias name, listing the existing set of aliases from the OPSA keystore. Enter the alias name to be deleted from the list.

5. The `$OPSA_HOME/bin/opsa-server-manager.sh` script prompts you for the file path to which the certificate should be exported. Enter the path to export the certificate.

To change an OPSA keystore file, do the following:

1. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script, and log on with **super-admin** credentials. See the `opsa-server-manager.sh` reference page (or the Linux manpage) for more information.

2. Select the **Configure SSL** option.

3. Select the **Change OPSA keystore file** option.

4. The `$OPSA_HOME/bin/opsa-server-manager.sh` script prompts you with a set of prerequisites actions to take before proceeding. Enter yes after you complete these prerequisites.

5. Enter the absolute path of the keystore file.

To change an OPSA truststore file, do the following:

1. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script, and log on with **super-admin** credentials. See the `opsa-server-manager.sh` reference page (or the Linux manpage) for more information.

2. Select the **Configure SSL** option.

3. Select the **Change OPSA truststore file** option.

4. The `$OPSA_HOME/bin/opsa-server-manager.sh` script prompts you with a set of prerequisites actions to take before proceeding. Enter yes after you complete these prerequisites.

5. Enter the absolute path of the truststore file.

Configuring SSL for the Operations Analytics Collector Appliance

One-way SSL provides secure communication between the client and the Operations Analytics server. During an SSL session creation, the server sends a digital certificate (self-signed or CA signed) containing information about the server. This information, such as domain, organization, and location, helps the client verify the server’s identity. SSL is disabled by default.

It is recommended that customers enable SSL communication for those environments where security is a concern. When you configure a Collector Appliance for SSL communication, you must export the client certificate from the Collector Appliance, then import that certificate into the trust store on the Operations Analytics Server Appliance using the `$OPSA_HOME/bin/opsa-server-`

`manager.sh` script. See "Configuring SSL for the Operations Analytics Server Appliance" for more information about configuring SSL for the Operations Analytics Server Appliance.

Use the information in this section to set up SSL and other communication changes on the Operations Analytics collector appliance before registering the Operations Analyticscollector appliance with the Operations Analytics server appliance. See "Registering Each Collector Appliance" for more information.

Use the information in this section to manage SSL on the Operations Analytics Collector Appliance.

Configuring SSL with a Certificate Authority (CA) Signed Certificate for the Operations Analytics Collector Appliance

SSL provides secure communication between the client and the Operations Analytics Collector Appliance. During an SSL session creation, the server sends a digital certificate (self-signed or CA signed) containing information about the server. This information, such as domain, organization, and location, helps the client verify the server's identity. SSL is disabled by default.

Complete the following steps to enable SSL communication to the Operations Analytics Collector Appliance using a CA signed certificate:

1. Run the `$OPSA_HOME/bin/opsa-collector-manager.sh` script. See the *opsa-collector-manager.sh* reference page (or the Linux manpage), for more information.

2. Select the **Configure SSL** option.

3. Select the **Import CA certificate to OPSA server keystore** option to import a CA signed certificate to OPSA server keystore. The `opsa-collector-manager.sh` script prompts you for the certificate alias name and lists a set of used aliases.. Enter a unique alias name that has not been used.

   > **Note**: The administrator can get a CA signed certificate by generating a Certificate Signing Request file using the self-signed certificate stored in OPSA keystore. Submit this Certificate Signing Request to a certificate authority. To generate a Certificate Signing Request from a self-signed certificate, select the **Generate certificate signing request option** .The `opsa-collector-manager.sh` script prompts you for the alias of the self-signed certificate. Enter `opsa_server` from the list of aliases to generate Certificate Signing Request for a self-signed certificate.

4. Optional: Select the **Import trusted certificate to OPSA server truststore** option to import trusted certificates (if any). For example, you can add HP ArcSight Logger's server certificate to the OPSA truststore file.

   > **Note**: Although SSL does not need to be enabled for rawlog and structured log queries to work, this step is mandatory for rawlog and structured log queries to work properly. You must complete this certificate import on both the Operations Analytics server (for the

> rawlog query) and the Operations Analytics collector appliance (for the structured log query). Follow these steps:
>
> a. Log on to the Logger console, then click **System Admin**.
>
> b. Select the **SSL Server Certificate** option under **security** on the left side of the screen.
>
> c. Click the View Certificate button at the bottom of the screen.
>
> d. After the dialog box opens, copy the certificate text and save it to a file on both the Operations Analytics Collector Appliance and on the Operations Analytics Server Appliance.
>
> e. Complete this step on both the Operations Analytics Collector Appliance and on the Operations Analytics Server Appliance to import the certificate.

5. Select the **Enable/Disable SSL** option to enable SSL. The `opsa-collector-manager.sh` script prompts you for the certificate alias to be used for SSL communication. Enter one of the aliases from the listed aliases.

6. Select the **Go back to main menu** option; then select the **Restart OPSA Collector** option to restart the Operations Analytics Collector Appliance.

   > **Note**: Your configuration changes will not occur unless the Operations Analytics collector is restarted.

7. If you have already registered the Operations Analytics Collector Appliance with the Operations Analytics Server Appliance, you will need to re-register this Operations Analytics Collector Appliance for the new configuration changes to be used . Use the following command:

   ```
   $OPSA_HOME/bin/opsa-collection-config.sh –register -collectorhost
   <collectorhost> -port <port> -username <username> [-ssl] [-coluser
   <collector_username> -colpass <collector_password]
   ```

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

Configuring SSL with a Self-Signed Certificate for the Operations Analytics Collector Appliance

Complete the following steps to enable SSL communication to the Operations Analytics Collector Appliance using a self-signed certificate:

1. Run the `$OPSA_HOME/bin/opsa-collector-manager.sh` script. See the *opsa-collector-manager.sh* reference page (or the Linux manpage), for more information.

2. Select the **Configure SSL** option.

3. Select the **Generate self-signed certificate for OPSA server** option to generate a self-signed certificate and add the certificate to the Operations Analytics Collector Appliance keystore.

   Note: The `$OPSA_HOME/bin/opsa-collector-manager.sh` script stores the self-signed certificate in the `keystore` file with the `opsa_server` alias name.

   Note: Set the self-signed certificate attributes, such as `common name`, `country`, and `validity` by editing the `/opt/HP/opsa/conf/ssl/cert/opsa_self_signed_cert.template` file.

4. Optional: Select the **Import trusted certificate to OPSA truststore** option to import trusted certificates (if any). For example, you can add HP ArcSight Logger's server certificate to the OPSA truststore file.

   Note: Although SSL does not need to be enabled for rawlog and structured log queries to work, this step is mandatory for rawlog and structured log queries to work properly. You must complete this certificate import on both the Operations Analytics server (for the rawlog query) and the Operations Analytics collector appliance (for the structured log query). Follow these steps:

   a. Log on to the Logger console, then click **System Admin**.

   b. Select the **SSL Server Certificate** option under **security** on the left side of the screen.

   c. Click the View Certificate button at the bottom of the screen.

   d. After the dialog box opens, copy the certificate text and save it to a file on both the Operations Analytics Collector Appliance and on the Operations Analytics Server Appliance.

   e. Complete this step on both the Operations Analytics Collector Appliance and on the Operations Analytics Server Appliance to import the certificate.

5. Select the **Enable/Disable SSL** option to enable SSL. The `opsa-collector-manager.sh` script prompts you for the certificate alias to be used for SSL communication. Enter `opsa-server`.

   `opsa_server` is one of the aliases shown by the script.

6. Select the **Go back to main menu** option; then select the **Restart OPSA Collector** option to restart the Operations Analytics Collector Appliance..

   Note: Your configuration changes will not occur unless the Operations Analytics Collector Appliance is restarted.

7. If you have already registered the Operations Analytics Collector Appliance with the Operations Analytics Server Appliance, you will need to re-register this Operations Analytics

Collector Appliance for the new configuration changes to be used . Use the following command:

```
$OPSA_HOME/bin/opsa-collection-config.sh –register -collectorhost
<collectorhost> -port <port> -username <username> [-ssl] [-coluser
<collector_username> -colpass <collector_password]
```

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

Editing the SSL Configuration for the Operations Analytics Collector Appliance

To change the server certificate used for SSL communication, do the following:

1. Run the `$OPSA_HOME/bin/opsa-collector-manager.sh` script. See the *opsa-collector-manager.sh* reference page (or the Linux manpage), for more information.

2. Select the **Configure SSL** option.

3. Select the **Change key alias to be used for SSL communication** option.

4. The `$OPSA_HOME/bin/opsa-collector-manager.sh` script prompts you for the alias name, and lists the existing set of certificate aliases from the OPSA keystore. Enter the desired alias name from the list.

5. Select the **Go back to main menu** option, then select the **Restart OPSA Collector** option to restart the Operations Analytics Collector Appliance.

   > **Note**: Your configuration changes will not occur unless the Operations Analytics Collector Appliance is restarted.

6. If you have already registered the Operations Analytics Collector Appliance with the Operations Analytics Server Appliance, you will need to re-register this Operations Analytics Collector Appliance for the new configuration changes to be used . Use the following command:

   ```
   $OPSA_HOME/bin/opsa-collection-config.sh –register -collectorhost
   <collectorhost> -port <port> -username <username> [-ssl] [-coluser
   <collector_username> -colpass <collector_password]
   ```

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

Disabling the SSL Configuration for the Operations Analytics Collector Appliance

To disable the SSL communication, do the following:

1. Run the `$OPSA_HOME/bin/opsa-collector-manager.sh` script. See the *opsa-collector-manager.sh* reference page (or the Linux manpage), for more information.

2. Select the **Configure SSL** option.

3. Select the **Enable/Disable SSL** option.

4. The `$OPSA_HOME/bin/opsa-collector-manager.sh` script prompts you for a confirmation. Enter `yes` to disable the SSL communication.

5. Select the **Go back to main menu** option, then select the **Restart OPSA Collector** option to restart the Operations Analytics Collector Appliance.

6. If you have already registered the Operations Analytics Collector Appliance with the Operations Analytics Server Appliance, you will need to re-register this Operations Analytics Collector Appliance for the new configuration changes to be used . Use the following command:
   ```
   $OPSA_HOME/bin/opsa-collection-config.sh –register -collectorhost
   <collectorhost> -port <port> -username <username> [-ssl] [-coluser
   <collector_username> -colpass <collector_password]
   ```
   See the *opsa-collection-config.sh* reference page (or the Linux manpage) for more information.

Managing the OPSA Keystore and Truststore for the Operations Analytics Collector Appliance

To modify the OPSA keystore and truststore password, do the following:

1. Run the `$OPSA_HOME/bin/opsa-collector-manager.sh` script. See the *opsa-collector-manager.sh* reference page (or the Linux manpage), for more information.

2. Select the **Configure SSL** option.

3. Select the **Modify OPSA keystore/truststore password** option.

4. The `$OPSA_HOME/bin/opsa-collector-manager.sh` script prompts you for the new password for the keystore and truststore. Enter the new passwords.

5. Select the **Go back to main menu** option, then select the **Restart OPSA Collector** option to restart the Operations Analytics Collector Appliance.

6. If you have already registered the Operations Analytics Collector Appliance with the Operations Analytics Server Appliance, you will need to re-register this Operations Analytics Collector Appliance for the new configuration changes to be used. Use the following command:
   ```
   $OPSA_HOME/bin/opsa-collection-config.sh –register -collectorhost
   <collectorhost> -port <port> -username <username> [-ssl] [-coluser
   <collector_username> -colpass <collector_password]
   ```
   See the *opsa-collection-config.sh* reference page (or the Linux manpage) for more information.

To delete a certificate from the OPSA keystore and truststore, do the following:

1. Run the `$OPSA_HOME/bin/opsa-collector-manager.sh` script. See the *opsa-collector-manager.sh* reference page (or the Linux manpage), for more information.

2. Select the **Configure SSL** option.

3. Select the **Delete certificate from OPSA keystore** or **Delete certificate from OPSA truststore** option.

4. The `$OPSA_HOME/bin/opsa-collector-manager.sh` script prompts you for the alias name, listing the existing set of aliases from the OPSA keystore/truststore. Enter the alias name to be deleted from the list.

5. Select the **Go back to main menu** option, then select the **Restart OPSA Collector** option to restart the Operations Analytics Collector Appliance.

6. If you have already registered the Operations Analytics Collector Appliance with the Operations Analytics Server Appliance, you will need to re-register this Operations Analytics Collector Appliance for the new configuration changes to be used . Use the following command:
   ```
   $OPSA_HOME/bin/opsa-collection-config.sh –register -collectorhost
   <collectorhost> -port <port> -username <username> [-ssl] [-coluser
   <collector_username> -colpass <collector_password]
   ```
   See the *opsa-collection-config.sh* reference page (or the Linux manpage) for more information.

To export a certificate from the OPSA keystore, do the following:

1. Run the `$OPSA_HOME/bin/opsa-collector-manager.sh` script. See the *opsa-collector-manager.sh* reference page (or the Linux manpage), for more information.

2. Select the **Configure SSL** option.

3. Select the **Export certificate from OPSA server keystore** option.

4. The `$OPSA_HOME/bin/opsa-collector-manager.sh` script prompts you for the alias name, listing the existing set of aliases from the OPSA keystore. Enter the alias name to be deleted from the list.

5. The `$OPSA_HOME/bin/opsa-collector-manager.sh` script prompts you for the file path to which the certificate should be exported. Enter the path to export the certificate.

To change an OPSA keystore file, do the following:

1. Run the `$OPSA_HOME/bin/opsa-collector-manager.sh` script, and log on with **super-admin** credentials. See the *opsa-collector-manager.sh* reference page (or the Linux manpage), for more information.

2. Select the **Configure SSL** option.

3. Select the **Change OPSA keystore file** option.

4. The `$OPSA_HOME/bin/opsa-collector-manager.sh` script prompts you with a set of prerequisites actions to take before proceeding. Enter yes after you complete these prerequisites.

5. Enter the absolute path of the keystore file.

To change an OPSA truststore file, do the following:

1. Run the `$OPSA_HOME/bin/opsa-collector-manager.sh` script, and log on with **super-admin** credentials. See the *opsa-collector-manager.sh* reference page (or the Linux manpage), for more information.

2. Select the **Configure SSL** option.

3. Select the **Change OPSA truststore file** option.

4. The `$OPSA_HOME/bin/opsa-collector-manager.sh` script prompts you with a set of prerequisites actions to take before proceeding. Enter yes after you complete these prerequisites.

5. Enter the absolute path of the truststore file.

Configuring the HTTPS and HTTPS Port for the Operations Analytics Collector Appliance

The Operations AnalyticsCollector Appliance comes with a pre-configured HTTP and HTTPS port of 9443. If you run into any port conflicts with this port, you might need to change it.

To change the HTTPS port to which the Operations Analytics Collector Appliance listens, do the following:

1. Run the `$OPSA_HOME/bin/opsa-collector-manager.sh` script. See the *opsa-collector-manager.sh* reference page (or the Linux manpage), for more information.

2. Select the **Configure HTTP(S) port** option.

3. When prompted, change the port to a value greater than 1024.

4. Select the **Restart OPSA Collector** option.

5. After the HTTPS port is changed, you must register the Operations Analytics Collector Appliance on the Operations Analytics Server Appliance using the following command:
   ```
   $OPSA_HOME/bin/opsa-collection-config.sh –register -collectorhost
   <collectorhost> -port <port> -username <username> [-ssl] [-coluser
   <collector_username> -colpass <collector_password]
   ```
   See the *opsa-collection-config.sh* reference page (or the Linux manpage) for more information.

   After you complete this step, future communication to this Operations Analytics Collector Appliance uses the new HTTPS port.

Configuring the HTTP and HTTPS User Name and Password for the Operations Analytics Collector Appliance

The Operations Analytics Collector Appliance comes with a pre-configured HTTPS user name, **opsa**, having an identical password, **opsa**. It is recommended that customers change the user name and password for those environments where security is a concern.

1. Run the `$OPSA_HOME/bin/opsa-collector-manager.sh` script. See the *opsa-collector-manager.sh* reference page (or the Linux manpage), for more information.
2. Select the **Configure username/password** option.
3. When prompted, change the username and password values.

   > The `opsa-collector-manager.sh` script prompts you for the user name and password , then prompts you for the password again and validates that the passwords you entered are identical.

4. Select the **Restart OPSA Collector** option.
5. After the HTTP and HTTPS port is changed, you must register the Operations Analytics Collector Appliance on the Operations Analytics Server Appliance using the following command:
   ```
   $OPSA_HOME/bin/opsa-collection-config.sh –register -collectorhost
   <collectorhost> -port <port> -username <username> [-ssl] [-coluser
   <collector_username> -colpass <collector_password]
   ```
   See the opsa-collection-config.`sh` reference page (or the Linux manpage) for more information.

   After you complete this step, future access to this Operations Analytics Collector Appliance uses the new username and password values.

Configuring and Enabling Single Sign-on to Access Operations Analytics

Enabling Single Sign-on (LWSSO) in Operations Analytics permits users to launch the Operations Analytics console from an OMi event browser without needing to log on again. LWSSO is not enabled by default.

1. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script, and log on with **super-admin** credentials. See the *opsa-server-manager.sh* reference page (or the Linux manpage), for more information.

2. Select the **Configure LWSSO** option.

3. Select the **Configure LWSSO parameters** option.

4. When prompted with **Enter the Token Creation Key (initString) [xxxxxxx]**, enter the `initString` key. The value must match the `initString` configured in OMi.

   > **Note**: To view the `initString` configured in OMi, log on to BSM and navigate to **BSM** > **Admin** > **Platform** > **Users and Permissions** > **Authentication Management**.

5. When prompted with **Enter the expiration period in minutes [60]**, enter the duration, in minutes, you want an LWSSO session to last before expiring.

6. When prompted with **Enter OPSA server domain**, enter the fully-qualified domain name of the Operations Analytics virtual appliance.

7. When prompted with **Enter trusted domains separated by comma**, the trusted domain names separated by a comma. Use the following form: `mytrusteddomain1.com, mytrusteddomain2.com`

8. Select the option **Enable/Disable LWSSO** to enable LWSSO.

9. Select the **Go back to main menu** option; then select the **Restart OPSA server** option to restart the Operations Analytics Server Appliance.

   > **Note**: Your configuration changes will not occur unless the server is restarted.

After completing the steps in this section, and configuring the correct URL on OMi , users can launch the Operations Analytics console from an OMi event browser without providing access credentials.

> **Note**: If you already enabled LWSSO, and need to make LWSSO configuration changes, complete the above instructions, skipping step 8.

Disabling Single Sign-on to Access Operations Analytics

To disable LWSSO, do the following:

1. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script, and log on with **super-admin** credentials. See the *opsa-server-manager.sh* reference page (or the Linux manpage), for more information.

2. Select the **Configure LWSSO** option.

3. Select the option **Enable/Disable LWSSO** to disable LWSSO.

4. Select the **Go back to main menu** option; then select the **Restart OPSA server** option to restart the Operations Analytics Server Appliance.

   > **Note**: Your configuration changes will not occur unless the server is restarted.

Configure Two-Way SSL Authentication for Accessing HP ArcSight Logger

Complete the following steps to configure two-way SSL authentication with ArcSight Logger:

1. Create an SSL truststore on Operations Analytics server with ArcSight Logger's server certificate:

   a. Copy the self-signed or CA certificate from HP ArcSight Logger. You will find the self-signed certificate in the following location: `<Install_Dir>/current/local/apache/conf/ssl.crt/server.crt`

   b. Create a trust store on the Operations Analytics server with ArcSight Logger's self-signed certificate using the following command:
   ```
   keytool -import -alias logger -file <server_cert_path>/server.crt
   -storetype JKS -keystore /opt/HP/conf/opsa_truststore.jks
   ```

   > **Note**: The keytool command prompts you for a password for the trust store. Provide a strong password and retain a copy of the password, as you will need it later. The keytool command also prompts you to trust the certificate. Type yes to trust the certificate

   .

2. Create a self-signed certificate and a keystore using OpenSSL for the Operations Analytics server:

   a. Create a private key using the following command:
   ```
   openssl genrsa -out /opt/HP/opsa/conf/opsa.key 1024
   ```

   b. Generate a certificate request using the following command:
   ```
   openssl req -new -key /opt/HP/opsa/conf/opsa.key -out
   /opt/HP/opsa/conf/opsa.csr
   ```

   c. Create a self-signed certificate using the following command:
   ```
   openssl x509 -req -days 365 -in /opt/HP/opsa/conf/opsa.csr -
   signkey /opt/HP/opsa/conf/opsa.key -out
   /opt/HP/opsa/conf/opsa.crt
   ```

d. Export the self-signed certificate to PKCS#12 format using the following command:

```
openssl pkcs12 -export -out /opt/HP/opsa/conf/opsa.p12 -inkey
/opt/HP/opsa/conf/opsa.key -in /opt/HP/opsa/conf/opsa.crt
```

> Note: Retain a copy of the export password.

e. Use the following command to create a keystore and import the generated PKCS#12 format certificate:

```
keytool -importkeystore -srckeystore /opt/HP/opsa/conf/opsa.p12 -
destkeystore /opt/HP/opsa/conf/opsa_keystore.jks -srcstoretype
pkcs12 -deststoretype JKS -deststorepass <keystore_password> -
srcstorepass <export_password_entered_in_above_step>
```

3. Configure ArcSight Logger to enable client authentication:

   a. Copy HP Operations Analytics Software's self-signed certificate from the following location:
   `$OPSA_HOME/conf/opsa.crt`
   to the following location on the ArcSight Logger server:
   `<Install_Dir>/current/local/apache/conf/ssl.crt`

   b. Edit ArcSight Logger's web server configuration file:
   `<Install_Dir>/current/local/apache/conf/httpd.conf`

   c. Modify the following lines and save your work:

   ```
   SSLVerifyClient require SSLVerifyDepth 0 SSLCACertificateFile
   <Install_Dir>/current/local/apache/conf/ssl.crt/opsa.crt
   ```

   d. Run the following command to restart ArcSight Logger's web server: `<Install_Dir>/current/arcsight/service/apache restart`

4. Configure the HP Operations Analytics Software configuration file:

   a. Edit the following file: `$OPSA_HOME/conf/opsa_config.prp`

   b. Add the following line and save your changes. `logger.ssl.enabled=true`

5. Configure the JBoss Application server:

   a. Edit the JBoss application server configuration file:
   `$JBOSS_HOME/bin/standalone.conf`

   b. Add the following lines and save your work:

   ```
   JAVA_OPTS="$JAVA_OPTS -
   Djavax.net.ssl.trustStore=/opt/HP/conf/opsa_truststore.jks" JAVA_
   OPTS="$JAVA_OPTS -Djavax.net.ssl.trustStorePassword=<password of
   trust store>" JAVA_OPTS="$JAVA_OPTS -
   Djavax.net.ssl.keyStore==/opt/HP/conf/opsa_keystore.jks" JAVA_
   OPTS="$JAVA_OPTS -Djavax.net.ssl.keyStorePassword=<password of
   key store>"
   ```

6. Use the following commands to restart the JBoss server:

   a. Run the following command to stop JBoss:
   `$OPSA_HOME/jboss/bin/ jboss-cli.sh --connect controller=<ip_` address>:19999 command=:shutdown

   b. Run the following command to start JBoss:
   ```
   $OPSA_HOME/jboss/bin/standalone.sh
   ```

1. Create an SSL truststore on Operations Analytics server with ArcSight Logger's server certificate:

   a. Copy the self-signed or CA certificate from ArcSight Logger. You will find the self-signed certificate in the following location: `<Install_Dir>/current/local/apache/conf/ssl.crt/server.crt`

   b. Create a trust store on the Operations Analytics server with ArcSight Logger's self-signed certificate using the following command:
   ```
   keytool -import -alias logger -file <server_cert_path>/server.crt
   -storetype JKS -keystore /opt/HP/conf/opsa_truststore.jks
   ```

   > **Note**: The keytool command prompts you for a password for the trust store. Provide a strong password and retain a copy of the password, as you will need it later. The keytool command also prompts you to trust the certificate. Type yes to trust the certificate

   .

2. Create a self-signed certificate and a keystore using OpenSSL for the Operations Analytics server:

   a. Create a private key using the following command:
   ```
   openssl genrsa -out /opt/HP/opsa/conf/opsa.key 1024
   ```

   b. Generate a certificate request using the following command:
   ```
   openssl req -new -key /opt/HP/opsa/conf/opsa.key -out
   /opt/HP/opsa/conf/opsa.csr
   ```

   c. Create a self-signed certificate using the following command:
   ```
   openssl x509 -req -days 365 -in /opt/HP/opsa/conf/opsa.csr -
   signkey /opt/HP/opsa/conf/opsa.key -out
   /opt/HP/opsa/conf/opsa.crt
   ```

   d. Export the self-signed certificate to PKCS#12 format using the following command:
   ```
   openssl pkcs12 -export -out /opt/HP/opsa/conf/opsa.p12 -inkey
   /opt/HP/opsa/conf/opsa.key -in /opt/HP/opsa/conf/opsa.crt
   ```

   > Note: Retain a copy of the export password.

e. Use the following command to create a keystore and import the generated PKCS#12 format certificate:

```
keytool -importkeystore -srckeystore /opt/HP/opsa/conf/opsa.p12 -
destkeystore /opt/HP/opsa/conf/opsa_keystore.jks -srcstoretype
pkcs12 -deststoretype JKS -deststorepass <keystore_password> -
srcstorepass <export_password_entered_in_above_step>
```

3. Configure ArcSight Logger to enable client authentication:

   a. Copy HP Operations Analytics Software's self-signed certificate from the following location: `$OPSA_HOME/conf/opsa.crt`
   to the following location on the ArcSight Logger server:
   `<Install_Dir>/current/local/apache/conf/ssl.crt`

   b. Edit ArcSight Logger's web server configuration file:
   `<Install_Dir>/current/local/apache/conf/httpd.conf`

   c. Modify the following lines and save your work:

   ```
   SSLVerifyClient require SSLVerifyDepth 0 SSLCACertificateFile
   <Install_Dir>/current/local/apache/conf/ssl.crt/opsa.crt
   ```

   d. Run the following command to restart ArcSight Logger's web server: `<Install_ Dir>/current/arcsight/service/apache restart`

4. Configure the HP Operations Analytics Software configuration file:

   a. Edit the following file: `$OPSA_HOME/conf/opsa_config.prp`

   b. Add the following line and save your changes. `logger.ssl.enabled=true`

5. Configure the JBoss Application server:

   a. Edit the JBoss application server configuration file:
   `$JBOSS_HOME/bin/standalone.conf`

   b. Add the following lines and save your work:

   ```
   JAVA_OPTS="$JAVA_OPTS -
   Djavax.net.ssl.trustStore=/opt/HP/conf/opsa_truststore.jks" JAVA_
   OPTS="$JAVA_OPTS -Djavax.net.ssl.trustStorePassword=<password of
   trust store>" JAVA_OPTS="$JAVA_OPTS -
   Djavax.net.ssl.keyStore==/opt/HP/conf/opsa_keystore.jks" JAVA_
   OPTS="$JAVA_OPTS -Djavax.net.ssl.keyStorePassword=<password of
   key store>"
   ```

6. Use the following commands to restart the JBoss server:

   a. Run the following command to stop JBoss:

   ```
   $OPSA_HOME/jboss/bin/ jboss-cli.sh --connect controller=<ip_
   address>:19999 command=:shutdown
   ```

   b. Run the following command to start JBoss:

   ```
   $OPSA_HOME/jboss/bin/standalone.sh
   ```

1. Create an SSL truststore on Operations Analytics server with ArcSight Logger's server certificate:

   a. Copy the self-signed or CA certificate from ArcSight Logger. You will find the self-signed certificate in the following location: `<Install_Dir>/current/local/apache/conf/ssl.crt/server.crt`

   b. Create a trust store on the Operations Analytics server with ArcSight Logger's self-signed certificate using the following command:

   ```
   keytool -import -alias logger -file <server_cert_path>/server.crt
   -storetype JKS -keystore /opt/HP/conf/opsa_truststore.jks
   ```

   > **Note**: The keytool command prompts you for a password for the trust store. Provide a strong password and retain a copy of the password, as you will need it later. The keytool command also prompts you to trust the certificate. Type yes to trust the certificate

   .

2. Create a self-signed certificate and a keystore using OpenSSL for the Operations Analytics server:

   a. Create a private key using the following command:

   ```
   openssl genrsa -out /opt/HP/opsa/conf/opsa.key 1024
   ```

   b. Generate a certificate request using the following command:

   ```
   openssl req -new -key /opt/HP/opsa/conf/opsa.key -out
   /opt/HP/opsa/conf/opsa.csr
   ```

   c. Create a self-signed certificate using the following command:

   ```
   openssl x509 -req -days 365 -in /opt/HP/opsa/conf/opsa.csr -
   signkey /opt/HP/opsa/conf/opsa.key -out
   /opt/HP/opsa/conf/opsa.crt
   ```

   d. Export the self-signed certificate to PKCS#12 format using the following command:

   ```
   openssl pkcs12 -export -out /opt/HP/opsa/conf/opsa.p12 -inkey
   /opt/HP/opsa/conf/opsa.key -in /opt/HP/opsa/conf/opsa.crt
   ```

   > Note: Retain a copy of the export password.

   e. Use the following command to create a keystore and import the generated PKCS#12 format certificate:

   ```
   keytool -importkeystore -srckeystore /opt/HP/opsa/conf/opsa.p12 -
   destkeystore /opt/HP/opsa/conf/opsa_keystore.jks -srcstoretype
   pkcs12 -deststoretype JKS -deststorepass <keystore_password> -
   srcstorepass <export_password_entered_in_above_step>
   ```

3. Configure ArcSight Logger to enable client authentication:

a. Copy HP Operations Analytics Software’s self-signed certificate from the following location: `$OPSA_HOME/conf/opsa.crt` to the following location on the ArcSight Logger server:

   ```
   <Install_Dir>/current/local/apache/conf/ssl.crt
   ```

b. Edit ArcSight Logger's web server configuration file:

   ```
   <Install_Dir>/current/local/apache/conf/httpd.conf
   ```

c. Modify the following lines and save your work:

   ```
   SSLVerifyClient require SSLVerifyDepth 0 SSLCACertificateFile
   <Install_Dir>/current/local/apache/conf/ssl.crt/opsa.crt
   ```

d. Run the following command to restart ArcSight Logger's web server: `<Install_Dir>/current/arcsight/service/apache restart`

4. Configure the HP Operations Analytics Software configuration file:

   a. Edit the following file: `$OPSA_HOME/conf/opsa_config.prp`

   b. Add the following line and save your changes. `logger.ssl.enabled=true`

5. Configure the JBoss Application server:

   a. Edit the JBoss application server configuration file:

      ```
      $JBOSS_HOME/bin/standalone.conf
      ```

   b. Add the following lines and save your work:

      ```
      JAVA_OPTS="$JAVA_OPTS -
      Djavax.net.ssl.trustStore=/opt/HP/conf/opsa_truststore.jks" JAVA_
      OPTS="$JAVA_OPTS -Djavax.net.ssl.trustStorePassword=<password of
      trust store>" JAVA_OPTS="$JAVA_OPTS -
      Djavax.net.ssl.keyStore==/opt/HP/conf/opsa_keystore.jks" JAVA_
      OPTS="$JAVA_OPTS -Djavax.net.ssl.keyStorePassword=<password of
      key store>"
      ```

6. Use the following commands to restart the JBoss server:

   a. Run the following command to stop JBoss:

      ```
      $OPSA_HOME/jboss/bin/ jboss-cli.sh --connect controller=<ip_
      address>:19999 command=:shutdown
      ```

   b. Run the following command to start JBoss:

      ```
      $OPSA_HOME/jboss/bin/standalone.sh
      ```

Configuring User Authentication using Public Key Infrastructure (PKI) to Access Operations Analytics

PKI authentication enables users to log on to the Operations Analytics console with a client-side X.509 certificate.

As part of user authentication, you can configure the Operations Analytics Server Appliance to check the certificate to make sure it has not been revoked. You can configure the revocation check to do one of the following:

- Validate the certificate using a Certificate Revocation List (CRL) .
- Validate the certificate using the Online Certificate Status Protocol (OCSP) to run a direct query to the PKI.

PKI authentication is disabled by default. To enable PKI authentication, do the following:

1. Before enabling SSL to the Operations Analytics Server Appliance, complete this step to create a user in JBoss **Management Realm**. do the following:
   a. Run the `$OPSA_HOME/jboss/bin/add-user.sh` script.

   b. For the first question, answer **"a" - Management User (mgmt-users.properties)**, then follow the instructions.

   > **Note**: You will need to provide the JBoss management realm credentials when enabling SSL later in these instructions.

2. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script, and log on with **super-admin** credentials. See the opsa-server-manager`.sh` reference page (or the Linux manpage), for more information.

3. Select the **Configure PKI Authentication** option.

4. Use one of the following approaches:

   - **Self-signed Certificate**: Select the **Generate self-signed certificate for OPSA server** option to generate a self-signed certificate and add the certificate to the Operations Analytics Server Appliance keystore.

   - **CA Signed Certificate**: Select the **Import CA certificate to OPSA server keystore** option to import a CA signed certificate to the Operations Analytics Server Appliance keystore.

5. **Mandatory Step**: Select the **Import trusted certificate to OPSA server truststore** option to import the trusted root CA certificate that will be used for PKI authentication.

   > **Note**: The certificate should be in base 64, otherwise the import will not work.

6. Select the **Enable/Disable PKI authentication** option to enable PKI. You will need to enter the JBoss **Management Realm** user and password you created in the first step.The `opsa-server-manager.sh` script prompts you for the certificate alias to be used for SSL communication, enter one of the aliases from the list. For example, you might enter `opsa-server`.

7. When prompted with **Allow smart card logon only [yes/no**], enter `yes` if only a smart log on is permitted. Enter `no` if a smart log on is not mandatory.

8. When prompted to select the field to use for a user name, enter the option you want Operations Analytics to use.

9. When prompted for **Check for certificate revocation [yes/no**], enter `yes` for Operations Analytics to check if the certificate provided by the client is revoked or not. Enter `no` to disable the revocation check. If you enter `yes`, the `opsa-server-manager.sh` script prompts you to select between the following revocation test methods:
   - **Option 1**: Validate the certificate using a Certificate Revocation List (CRL) .

   - **Option 2**: Validate the certificate using the Online Certificate Status Protocol (OCSP) to run a direct query to the PKI .

   > **Note**: If you select option 2 the `opsa-server-manager.sh` script prompts you to configure the OCSP responder URL. You can accept the default behavior and have Operations Analytics use the value of the `authorityInfoAccess` field of the client certificate to obtain the responder URL,or you can directly configure the OCSP responder URL.

10. When prompted with **Do you want to configure proxy host [yes/no]**, enter `yes` if you want to configure the proxy host to check for certificate revocation status. Enter `no` if you do not want to configure the proxy host to check for certificate revocation status (a local OCSP responder is available).

    If you enter `yes`, the `opsa-server-manager.sh` script prompts you for the following information:
    - proxy http proxy host

    - http port number

    - https proxy host

    - https port number

11. After successfully completing the registration, the `opsa-server-manager.sh` scrip shows an `authentication enabled successfully` message.

12. Select the **Go back to main menu** option; then select the **Restart OPSA server** option to restart the Operations Analytics Server Appliance.

    > **Note**: Your configuration changes will not occur unless the server is restarted.

After completing the above steps, Operations Analytics users can access the Operations Analytics console using HTTP or HTTPS as follows:

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

1. If an Operations Analytics user enters an HTTP URL, Operations Analytics automatically redirects the URL to HTTPS, and shows a **Login with digital certificate** button.

2. After clicking the **Login with digital certificate** button, Operations Analytics presents its digital certificate, and the browser verifies it against its truststore.

3. After verifying the Operations Analytics certificate, Operations Analytics prompts the user to select the client certificate. On selecting the client certificate, Operations Analytics verifies the client certificate and performs authentication.

   Note: The client certificate must be installed and imported to the browser, otherwise the user is not prompted for the client certificate.

4. If the authentication is successful, the browser opens the Operations Analytics home page.

Disabling User Authentication using Public (PKI) to Access Operations Analytics

To disable PKI authentication, do the following:

1. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script, and log on with **super-admin** credentials. See the `opsa-server-manager.sh` reference page (or the Linux manpage), for more information.

2. Select the **Configure Client Authentication** option.

3. Select the **Enable/Disable client authentication** button.

4. The `$OPSA_HOME/bin/opsa-server-manager.sh` script prompts you for confirmation. Enter `yes` to disable PKI authentication.

5. The `$OPSA_HOME/bin/opsa-server-manager.sh` script disables PKI, then prompts, **Do you want to disable SSL as well [yes/no]**. Enter `yes` to disable SSL communication or `no` to keep the existing SSL configuration.

6. Select the **Go back to main menu** option; then select the **Restart OPSA server** option to restart the Operations Analytics Server Appliance.

   Note: Your configuration changes will not occur unless the server is restarted.

After completing the above steps, Operations Analytics presents its users with a user name and password page to access the Operations Analytics console.

Editing User Authentication using Public (PKI) to Access Operations Analytics

To modify PKI authentication, do the following:

1. Run the `$OPSA_HOME/bin/opsa-server-manager.sh` script, and log on with **super-admin** credentials. See the `opsa-server-manager.sh` reference page (or the Linux manpage), for more information.

2. Select the **Configure Client Authentication** option.

3. Select the **Edit client authentication settings** button.

4. The `$OPSA_HOME/bin/opsa-server-manager.sh` script prompts you for PKI configuration information, similar to the prompts shown in "Configuring User Authentication using Public Key Infrastructure (PKI) to Access Operations Analytics"

5. Select the **Go back to main menu** option; then select the **Restart OPSA server** option to restart the Operations Analytics Server Appliance.

   > **Note**: Your configuration changes will not occur unless the server is restarted.

Chapter 8: Maintaining Operations Analytics Collections

The information in this section helps you check the status of your collections and explains some common troubleshooting tools and techniques for collections.

Troubleshooting Operations Analytics Collections

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

Checking a Collector's Status

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

- Run the following command from an Operations Analytics Server Appliance to list the collections deployed to that Operations Analytics Collector Appliance:
  ```
  $OPSA_HOME/bin/opsa-collection-config.sh -list –collectorhost
  <collector hostname> -username <Tenant Admin User>
  ```
- Run the following commands from an Operations Analytics Collector Appliance to check the status of collector sources and processes:
  - `$OPSA_HOME/bin/opsa-collector status`
  - `$OPSA_HOME/bin/opsa-loader status`
- Run the following command from an Operations Analytics Server Appliance to check the status of the collector sources and processes configured on a Operations Analytics Collector Appliance:
  ```
  $OPSA_HOME/bin/opsa-collection-config.sh -status –collectorhost
  <collector hostname> -username <Tenant Admin User>
  ```

Troubleshooting Configurations from the Operations Analytics Server Appliance

To troubleshoot collector and collection configuration, do the following from the Operations Analytics Server Appliance:

- If you completed the instructions to set up Operations Analytics System Health in "Checking Operations Analytics System Health" and installed and configured the Operations Analytics Log File Connector for HP ArcSight Logger on the Operations Analytics Collector Appliances (to collect Operations Analytics log files), you can check the **OpsaSystemHealth** dashboard and look for `ERROR` and `WARN` severity log messages.

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

Troubleshooting the Absence of Collection Data

The information in this sections helps you troubleshoot collections that have been published to a Operations Analytics Collector Appliance, but are not collecting data. This troubleshooting takes place on the Operations Analytics Collector Appliance.

- Always run the following commands to check that the collector and data loader are functioning correctly.
  - `$OPSA_HOME/bin/opsa-collector status`
  - `$OPSA_HOME/bin/opsa-loader status`
- Look for any error messages in the `/opt/HP/opsa/log/opsa-collector.log` and `/opt/HP/opsa/log/loader.log` files.
- If you want to adjust the logging levels, edit the `/opt/HP/opsa/conf/opsa-collector-log.properties` file and set the following properties:
  - `log4j.logger.com.hp.opsa.collector = DEBUG`
  - `log4j.logger.com.hp.opsa.collector.common = DEBUG`
  - `log4j.logger.com.hp.opsa.collector.agent = DEBUG`
  - `log4j.logger.com.hp.opsa.collector.server = DEBUG`
- If your collection problem is with the following collections, look in the associated log files shown for the collection:
  - HP Operations Agent or HP Operations Smart Plug-in for Oracle Collections
    `/opt/HP/BSM/PMDB/log/collections.log`
    `/opt/HP/BSM/PMDB/log/hpacollector.log`
  - HP Operations Manager (HPOM or OMi) Collections
    `/opt/HP/BSM/PMDB/log/collections.log`
    `/opt/HP/BSM/PMDB/log/dbcollector.log`

- Any of associated HP BSM RTSM Collections
  `/opt/HP/BSM/PMDB/log/collections.log`
  `/opt/HP/BSM/PMDB/log/topologycollector.log`

- Custom SiteScope Collection: If your collection problem is with the Custom SiteScope Collection, do the following:
  - Check the `%SITESCOPE_HOME%/log/error.log` and `%SITESCOPE_HOME%/log/data_integration.log` files on the SiteScope server for any error messages about not being able to push SiteScope data to an Operations Analytics collector.
  - Check the Operations Analytics Collector Appliance data integration to make it is configured correctly on the SiteScope server. See "Configuring a Custom SiteScope Collection" for more information.
- Structured Log Collection: If your collection problem involves no structured log data being collected, check to make sure the configured query is correct. The easiest way to do this is to use the query in the ArcSight Logger console to see that the query works.
- For the following collections, look in the specific processed folder to check that the collector is collecting data for that collection:
  - HP Operations Agent Collection: `/opt/HP/opsa/data/pa_processed/<tenant>`
  - HP Operations Smart Plug-in for Oracle Collection: `/opt/HP/opsa/data/ora_pa_processed/<tenant>`
  - NNMi Custom Poller Collection: `/opt/HP/opsa/data/nnm_processed/<tenant>`

    > **Note**: The NNMi Custom Poller collector needs to have read/write access to the NNMi CSV files to move them to the processed directory. If the collector cannot move them, the NNMi Custom Poller CSV files will be reprocessed the next time the collector starts up. See "Configuring an NNMi Custom Poller Collection" for more information.

  - NNM ISPi Performance for Metrics Interface Health Collection: `/opt/HP/opsa/data/netinterface_processed/<tenant>`

    > **Note**: The NNM ISPi Performance for Metrics Interface Health collector needs to have read/write access to the NNM ISPi Performance for Metrics Interface Health CSV files to move them to the processed directory. If the collector cannot move them, the NNM ISPi Performance for Metrics Interface Health CSV files will be reprocessed the next time the collector starts up. See "Configuring an NNM ISPi Performance for Metrics Interface Health Collection" for more information.

  - NNM ISPi Performance for Metrics Component Health Collection: `/opt/HP/opsa/data/netcomponent_processed/<tenant>`

> **Note**: The NNM ISPi Performance for Metrics Component Health collector needs to have read/write access to the NNM ISPi Performance for Metrics Component Health CSV files to move them to the processed directory. If the collector cannot move them, the NNM ISPi Performance for Metrics Component Health CSV files will be reprocessed the next time the collector starts up. See "Configuring an NNM ISPi Performance for Metrics Component Health Collection" for more information.

- HP Operations Manager (HPOM) Collections: `/opt/HP/opsa/data/om_events_processed/<tenant>`
- HP Operations Manager (OMi) Collections: `/opt/HP/opsa/data/omi_events_processed/<tenant>`
- Custom SiteScope Collection:
  `/opt/HP/opsa/data/sis_processed/<tenant>`
  Look for collected Customer SiteScope Collection data in `/opt/HP/opsa/data/SIS_GDIAPI_DATA/<tenant>`.
- Custom CSV Collection: `<custom CSV source parent directory>_processed/<tenant>`

  > Note: The Custom CSV collector needs to have read/write access to the Custom CSV files to move them to the processed directory. If the collector cannot move them, the Custom CSV files will be reprocessed the next time the collector starts up. See "Configuring a Custom CSV Collection" for more information.

- To check if data is being loaded into the Operations Analytics database, a user can look at the files in the `/opt/HP/opsa/data/load/<tenant>` directory. Files with a `.working` extension are files to which the collector is actively writing. Working files should never be older than 10 minutes. So any files with a `.csv` extension are ready to be loaded into the Operations Analytics database. If the system is functioning correctly, there should not be any `*.csv` files older than 10 minutes as well.
  - If you do not find any files with a `.csv` extension in the `/opt/HP/opsa/data/load/<tenant>` directory, do the following:
    1) Check for any CSV files that were successfully loaded into the Operations Analytics database by looking in the `/opt/HP/opsa/data/archive/<tenant>` directory.
    2) If you do not see files for the collection in question, check to see if the data loader has rejected the load files by looking in the `/opt/HP/opsa/data/failed_to_load` directory.

Chapter 9: Maintaining Operations Analytics

The information in this section explains how to complete maintenance tasks to protect your investment in Operations Analytics.

Checking Operations Analytics System Health

You can configure Operations Analytics to display the metrics, topology, event, and log information available for the following Operations Analytics servers and applications:

- Operations Analytics Collector Appliances
- Operations Analytics Server
- Operations Analytics Database Servers
- HP ArcSight Logger

To configure Operations Analytics to monitor its own active components, do the following:

1. Make sure the following software is installed and configured:

   a. Vertica: See the installation and configuration instructions at "Task 2: Installing and Configuring the Vertica Software".

   b. HP ArcSight Logger: See the installation and configuration instructions at "Task 3: Installing and Configuring HP ArcSight Logger"

   c. Operations AnalyticsServer Appliance: See the installation and configuration instructions at "Task 4: Installing and Licensing the Operations Analytics Server Appliance using the VMware vSphere Client"

   d. Operations AnalyticsCollector Appliance: See the installation and configuration instructions at "Task 5: Installing and Configuring the Operations Analytics Collector Appliance using the VMware vSphere Client"

2. Edit the `yum.conf` file and add the proxy information for your network. Save your work.

3. Install the libstdc++ package on the Vertica database server, the Operations Analytics Collector Appliance, and the Operations Analytics Server Appliance.

4. To install the HP Operations Agent libraries, run the following command on the Vertica database server, the Operations Analytics Collector Appliance, and the Operations Analytics Server Appliance:

   ```
   yum install compat-libstdc++-33-3.2.3-69.el6.i686
   ```

5. Install the latest HP Operations Agent patches on the Vertica database server, the HP ArcSight Logger server, the Operations Analytics Collector Appliance, and the Operations Analytics Server Appliance.

6. Configure the syslogs from the Vertica database server, the Operations Analytics Collector Appliance, and the Operations Analytics Server Appliance to forward to the HP ArcSight Logger server by appending `“*.* @@<logger_hostname>:515″` to the `/etc/rsyslog.conf` file.)

7. Restart the `rsyslog` service.

8. Configure the Operations Analytics Log File Connector for HP ArcSight Logger. See the Operations Analytics Log File Connector for HP ArcSight Logger installation and configuration instructions at "Task 3: Installing and Configuring HP ArcSight Logger".

Deleting a Tenant

To delete a tenant from Operations Analytics, you must delete the tenant, then remove files from the Operations Analytics Collector Appliance being used by the tenant you delete.

1. Remove all of the collection registrations for a tenant before deleting the tenant. See "Removing a Collection Registration for a Tenant" for more information.

2. There are two methods to use to delete a tenant from Operations Analytics. To delete a tenant from Operations Analytics, **use only one of the following methods**:

   > **Note**: There are additional steps you must complete to remove files from your configured collectors after deleting a tenant.

   - **Method 1**: Run the `$OPSA_HOME/bin/opsa-tenant-manager.sh` command as a user assigned to the Super Admin User Group. Then follow the interactive commands to remove the tenant.

   - **Method 2**: Run the `$OPSA_HOME/bin/opsa-tenant-manager.sh -delete -loginUser <super admin user> -loginPassword <password> -tenant <tenant name>`

   See the *opsa-tenant-manager.sh* reference page (or the Linux manpage) for information about creating and managing tenants.

3. To remove files from your configured collectors, do the following:

   a. From each Operations Analytics Collector Appliance that contains collectors for the tenant being removed, run only one of the following commands to remove the tenant collection configuration:
      - If the Operations Analytics Collector Appliance is only collecting data for the tenant being removed:

        `rm -rf /opt/HP/opsa/conf/collection/config.files/<collector`

```
host>
```

- If the Operations Analytics Collector Appliance is collecting data for multiple tenants:

  ```
  rm –rf /opt/HP/opsa/conf/collection/config.files/<collector
  host>/<tenant>
  ```

b. *Only complete this step if a collector appliance currently collects data for tenants other than the one being deleted*. Run the following command from the Operations Analytics Server Appliance to publish this collection configuration to the Operations Analytics Collector Appliance.Use a Tenant Admin user for one of the other active tenants for which that this Operations Analytics Collector Appliance is collecting.

```
$OPSA_HOME/bin/opsa-collection-config.sh -publish -collectorhost
<fully-qualified domain name of the collector host> –username
<tenant admin user>
```

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

c. From the Operations Analytics Collector Appliance, run the following commands to remove specific files from the Operations Analytics Collector Appliance associated with the tenant being removed :

- `rm -rf /opt/HP/opsa/data/load/<tenant name>`
- `rm -rf /opt/HP/opsa/data/failed_to_load/<tenant name>`

Removing a Collection Registration for a Tenant

If you no longer want to analyze data for a collection, you must remove the collection registration and the stored data for that collection. Do the following:

1. Run the following command to list all of the collectors for the tenant:

   ```
   $OPSA_HOME/bin/opsa-collection-config.sh -list –collectorhosts -
   allversions -username <Tenant Admin User>
   ```

   See the `opsa-collection-config.sh` reference page (or the Linux manpage), for more information.

2. Unregister the collections you no longer want to analyze for a tenant using the following command:

   ```
   $OPSA_HOME/bin/opsa-collection-config.sh -unregister -source
   <collection source> -domain <collection domain> -group <collection
   group> -collectorhost <collector host> -username <Tenant Admin
   User>
   ```

> **Note**: The `unregister` option is the opposite of the `create` option.The `unregister` option removes a collection from being collected on an Operations Analytics Collector Appliance where the `create` option was used to create that collection.

3. Repeat the previous two steps until there are no collectors listed when running the command shown in step 1. If the command in step 1 lists no collectors, that means none of the original collectors for the tenant are collecting data for the collection you plan to remove.

4. After unregistering all of the collections you no longer want to analyze for a tenant (from all the tenant's collectors), remove the collection from the database using the following command:
   ```
   $OPSA_HOME/bin/opsa-collection-config.sh -purgecollection -source
   <collection source> -domain <collection domain> -group <collection
   group> -collectorhost <collector host> -username <Tenant Admin
   User>
   ```
   See the `opsa-collection-config.sh` reference page (or the Linux manpage), for more information.

Maintaining the Operations Analytics Database

To back up or restore data for the Operations Analytics Server and Collector Appliances, see the referenced sections in the following documents:

- The *Configuration Backup and Restore* section of the *HP ArcSight Logger 5.2 Administrator's Guide*
- The *Backing up and Restoring the Database* section of the *Vertica Enterprise Edition 6.1 Administrator's Guide*

Setting Collection Retention Periods

You can set the amount of time that Operations Analytics retains the data it is collecting. You can set the retention period for a collection or for all of the collections belonging to a tenant or a data source.

To set the amount of time to retain the data for a collection, use the following command:

```
$OPSA_HOME/bin/opsa-collection-config.sh -setretention <retention
period in months> –source <source name> -domain <domain name> -group
<group name> -username <Tenant Admin User>
```

See the `opsa-collection-config.sh` reference page (or the Linux manpage), for more information.

Operations Analytics Port Mapping

The well-know 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 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 your 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, Operations Analytics leverages existing 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-Know 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.
2506, 2507	Operations	Business Process	Operations	

Well-Know Port Mapping, continued

Port	Initiator	Sender	Receiver	Comments
	Analytics	Monitor(BPM)	Analytics Collector Appliance	
5443	Operations Analytics	Vertica	Operations Analytics Collector and Server Appliances.	The default Vertica port is 5443. 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.

Operations Analytics Security Hardening

The following information is a summary of the security hardening recommendations for 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 minumum, 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 OpsA 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`

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 entironment. 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.

Chapter 10: Maintaining Operations Analytics User Accounts

If you use a tenant model you will need to assign user groups. User Groups are predefined in Operations Analytics and determine which tasks each User Account that is assigned to the User Group can perform. See the following predefined User Groups table for more information.

- User Accounts must be unique across all Tenants.
- All User Groups can access the Operations Analytics console.
- You cannot add a new User Group to Operations Analytics.
- A User Account was assigned to the Super Admin User Group when you installed Operations Analytics.

Pre-defined User Groups

User Group	Description	Supported Tasks
Super Admin	User accounts assigned to this User Group can access the following information for each tenant defined: ▪ Collectors ▪ Collections ▪ Meta Data ▪ Tags ▪ User Accounts ▪ User Groups	Add, modify, and delete tenants.
Tenant Admin	User accounts assigned to this User Group can access the following information only for the tenant to which they are assigned: ▪ Collectors ▪ Collections ▪ Meta Data	Add, modify, and delete user accounts. Manage the collectors, collections, meta data, and tags for a specified tenant.

Pre-defined User Groups, continued

User Group	Description	Supported Tasks
	▪ Tags ▪ User Accounts ▪ User Groups	
User	User accounts assigned to this User Group can access the Operations Analytics console..	Access and perform tasks using the Operations Analytics Home Page and Guided Troubleshooting Dashboards.

From the command line, use the `/opt/HP/opsa/bin/opsa-user-manager.sh` script to manage users. See the *opsa-user-manager.sh* reference page (or the Linux manpage) for more information.

Listing Users

To list Tenant Admin users using the `opsa-user-manager.sh` script, run the following command:

```
$OPSA_HOME/bin/opsa-user-manager.sh -list -loginUser opsaadmin -
loginPassword <opsaadmin password>
```

To list users for a tenant using the `opsa-user-manager.sh` script, run the following command:

```
$OPSA_HOME/bin/opsa-user-manager.sh -list -loginUser <Tenant Admin
User> -loginPassword <Tenant Admin Password>
```

Adding a User Account

To add a user account using the `opsa-user-manager.sh` script, run the following command:

```
$OPSA_HOME/bin/opsa-user-manager.sh -add -loginUser <Super Admin or
Tenant Admin User Name> -loginPassword <password> -newUser <new
username> -newUserPassword <new user password>
```

Deleting a User Account

To delete a user account using the `opsa-user-manager.sh` script, run the following command:

```
$OPSA_HOME/bin/opsa-user-manager.sh -delete -loginUser <Tenant Admin
User> -loginPassword <Tenant Admin Password> -user <username>
```

Modifying a User Account

To modify the password for a user account using the `opsa-user-manager.sh` script, run the following command:

```
$OPSA_HOME/bin/opsa-user-manager.sh -modify -loginUser <User Name> -
loginPassword <password> -newUserPassword <new user password>
```

We appreciate your 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 and Configuration Guide (Operations Analytics 2.00)

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.

Java™
COMPATIBLE