Hewlett Packard
Enterprise

HPE Operations Analytics

Software Version: 2.32

HPE Operations Analytics for HPE OneView
Installation, Integration, and Upgrade Guide

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. HPE 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 HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Microsoft and Windows are trademarks of the Microsoft Group of companies.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hpe.com/group/softwaresupport/search-result?keyword=.

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

Support

Visit the HPE Software Support website at: **https://softwaresupport.hpe.com**

This website provides contact information and details about the products, services, and support that HPE Software offers.

HPE Software Support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE 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 HPE Passport user and sign in. Many also require a support contract. To register for an HPE Passport ID, go to **https://softwaresupport.hpe.com** and click **Register**.

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

HPE Software Integrations, Solutions and Best Practices

Access the Hewlett Packard Enterprise Software Support site (**https://softwaresupport.hpe.com/manuals**) to search for a wide variety of best practice documents and materials.

Contents

Chapter 1: Prerequisites

Read the information in this section before deploying the Operations Analytics All-in-One for HPE OneView Appliance.

Management Environment

This document provides information about setting up the Operations Analytics All-in-One for HPE OneView Appliance and enabling the integration between Operations Analytics and HPE OneView. It provides additional information about how to scale out the Operations Analytics All-in-One for HPE OneView Appliance to a distributed environment if the need arises.

The Operations Analytics All-in-One for HPE OneView Appliance can typically collect data from no more than 640 nodes. This number could be significantly less, depending on the amount of data each collection is receiving and the amount of data each data center node is generating.

> **Note:** The Operations Analytics All-in-One for HPE OneView Appliance does not support the configuration of other types of collections. Only Operations Analytics All-in-One for HPE OneView Appliance collections that are configured as explained in "About Data Collections for the HPE Operations Analytics - HPE OneView Integration" on page 26 are supported.

For larger environments, you must scale out your Operations Analytics All-in-One for HPE OneView Appliance to use a distributed environment. For example, for larger environments, you must configure collections on a separate Operations Analytics Collector Appliance. To expand this Operations Analytics All-in-One for HPE OneView Appliance to a distributed environment, complete the tasks shown in "Expanding to a Distributed Operations Analytics " on page 28.

System Requirements

The Operations Analytics All-in-One for HPE OneView Appliance is a virtual appliance you deploy using an .ova file. This .ova file needs to be deployed in the VMware virtual center before it can be used. To deploy the Operations Analytics All-in-One for HPE OneView Appliance, the servers must meet the following requirements:

- Minimum memory required for the Virtual Machine: 24 GB
- Minimum disk space required for the Virtual Appliance: 200 GB
- Minimum CPU requirements: 4 CPUs
- IP Address: The Operations Analytics All-in-One for HPE OneView Appliance installation needs either a static IP address or a permanently-leased DHCP IP address and the IP address must resolve to a valid fully-qualified-domain-name.

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

> **Note:** The system clocks for the HPE OneView server and the Operations Analytics All-in-One for HPE OneView Appliance must be synchronized.

Note: `$OPSA_HOME` is set to `/opt/HP/opsa` in the Operations Analytics All-in-One for HPE OneView Appliance.

HPE Operations Analytics All-in-One for HPE OneView Appliance Port Mapping

The well-known network ports described in the section need to be open in a secured environment for the Operations Analytics All-in-One for HPE OneView Appliance to be able to function and collect data from HPE OneView.

The communication ports shown in "Well-Known Port Mapping" below must be open on theOperations Analytics All-in-One for HPE OneView Appliance.

Well-Known Port Mapping

Port	Purpose
443	Communication with REST interface
514 (UDP)	Obtains syslog messages from HPE OneView
5671	Communication with the State-Change Message Bus (SCMB) and the Metric Streaming Message Bus (MSMB)

Chapter 2: Setting up the HPE Operations Analytics All-in-One for HPE OneView Appliance

Follow the instructions in this section to deploy, power on, and test the Operations Analytics All-in-One for HPE OneView Appliance.

Caution: Operations Analytics uses Logger 6.0 with the reporting feature deactivated (the Operations Analytics license does not include this Logger feature). Do not attempt to activate the reporting mechanism in Logger.

Note: Operations Analytics integrates with HPE OneView so you can view analytics and summary information using management data from HPE OneView (log and metric data).

Note: The Operations Analytics Server Appliance and the HPE OneView Server must each be able to resolve each other's fully-qualified domain names for the Operations Analytics - HPE OneView integration to function correctly.

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

1. Go to the Software Depot Site.
2. Search for **HPE Operations Analytics for HPE OneView**.
3. Download **HPE Operations Analytics 2.31 OneView Virtual Appliance** and extract the product files to a local directory.
4. Log on to the VMware ESX or VMware workstation.

   Note: You must deploy Operations Analytics into a VMware vSphere environment. Do not deploy Operations Analytics directly to an ESX Server host.

5. Select **File** -> **Deploy OVF Template**.
6. Enter the URL or the file path of the `HP_Opsa_OneView_OVF10.ova` file, based on where you extracted the product files; then click **Next**.
7. Specify a name and location for the deployed template.
8. Follow the instructions to select the host or cluster on which you want to deploy the Server Appliance; then click **Next**.
9. Select a resource pool.
10. Select the destination storage for the Server Appliance files; then click **Next**.

11. Select the format on which you want to store the virtual disks; then click **Next**. A display similar to the following should appear:

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

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

> **Note:** You can configure the Operations Analytics All-in-One for HPE OneView Appliance to work with static IP addresses or permanently-leased DHCP IP addresses as shown in "Network Properties" on the next page.

Network Properties

Address Type	Field	Value
DHCP	DHCP or Static IP	Select DHCP **Note**: The Operations Analytics installation needs either static IP addresses or permanently-leased DHCP IP addresses.
	Host Name (The VA Host Name)	Enter the fully-qualified domain name of the Operations Analytics All-in-One for HPE OneView Appliance.
	All Fields	Leave all other fields blank.
	DNS	The IP address of the DNS Server.
	Timezone	Select the desired timezone setting.
Static	DHCP or Static IP	Select Static
	Host Name (The VA Host Name)	Enter the fully-qualified domain name of the Operations Analytics All-in-One for HPE OneView Appliance.
	Static IP Address	The IP address of the server.
	Subnet Mask IP	The network mask for your network.
	Default Gateway	The fully-qualified domain name or IP address of the network's default gateway.
	DNS	The IP address of the DNS Server.
	Timezone	Select the desired timezone setting.

13. Make sure you entered the correct network settings and hostname (from the previous step); then click **Next**.

14. Click **Finish**.

15. Power on the virtual appliance.

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

Terminology Used in this Document

Operations Analytics All-in-One for HPE OneView Appliance: A self-contained system that combines the Operations Analytics Server Appliance, Collector Appliance, Vertica Database, and the HPE ArcSight Logger virtual appliance.

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.Collections can be separated by tenant and collection information cannot be shared among tenants.

Common Event Format (CEF): The standard data format of HPE ArcSight Logger.

Default Tenant: This Operations Analytics All-in-One for HPE OneView Appliance document uses the default Tenant, opsa_default and its corresponding default tenant username (opsatenantadmin) and password (opsatenantadmin). The Operations Analytics All-in-One for HPE OneView Appliance is not intended to fully demonstrate the tenant model as explained in the Tenant definition in this section.

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

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.

Configure the Database

Operations Analytics includes vertica-7.1.1-.x86_64.RHEL5.rpm for the Vertica installation and vertica-R-lang-7.1.1-3.x86_64.RHEL5.rpm and vertica-R-lang-7.1.1-5.x86_64.RHEL5.rpm for the R Language Pack from Vertica. Use these packages for optimum Vertica performance. You can find these packages in the `/opt/HP/opsa/installation/rpm` folder on the Operations Analytics All-in-One for HPE OneView Appliance.

The Vertica database server should already be configured for the Operations Analytics All-in-One for HPE OneView Appliance. It should be configured with a `MAXMEMORYSIZE` of 50% of the machine's RAM (using a 24GB RAM machine). If it is not, do the following:

1. Log on to the Vertica server as an opsa user.
2. Run the following command to become the root user: `su -`
3. Run the following command to become the Linux dbadmin user: `su - dbadmin`
4. Enter the following command to access the SQL console: `dbadmin$>VSQL`
5. Enter the following command from the SQL console: `ALTER RESOURCE POOL general MAXMEMORYSIZE '12G';`
6. Exit the VSQL console using the following sequence:
   a. `\q`
   b. `Enter`

7. Restart the Vertica database by running `/opt/vertica/bin/admintools` and restarting the opsadb database.

8. Run the `$OPSA_HOME/bin/opsa-server restart` command on the Operations Analytics All-in-One for HPE OneView Appliance for the changes to take effect.

> **Note:** After running an `opsa-server restart` command, information logged in the `/opt/HP/opsa/log/opsa-server.log` file is removed. To view the files that retain this information across restarts, see the log files located in the `/opt/HP/opsa/jboss/standalone/log` directory. Look for log file names that begin with `server.log`.

Configuring Logger to Forward CEF Messages to Operations Analytics

The feature being configured in this section is also known as the **TCP Forwarding** feature. After you complete the configuration instructions in this section, the performance of the Operations Analytics All-in-One for HPE OneView Appliance significantly improves. You will also observe more real-time log messages in the Operations Analytics All-in-One for HPE OneView Appliance.

To configure Logger version 6.0 to forward CEF messages to the Operations Analytics All-in-One for HPE OneView Appliance, do the following from the Operations Analytics All-in-One for HPE OneView Appliance:

1. Edit the following
   file: `/opt/HP/arcsight/current/arcsight/logger/config/logger/logger.defaults.properties`

2. Change the following text:

   from
   ```
   # forwarder disallow localhost or not
   forwarder.disallow.localhost=true
   ```
   to
   ```
   # forwarder disallow localhost or not
   forwarder.disallow.localhost = false
   ```

3. Save your work.

4. Run the following commands to restart Logger: `service arcsight_logger stop; sleep 30; service arcsight_logger start`

5. From Logger, navigate to **Configuration** > **Forwarders**.
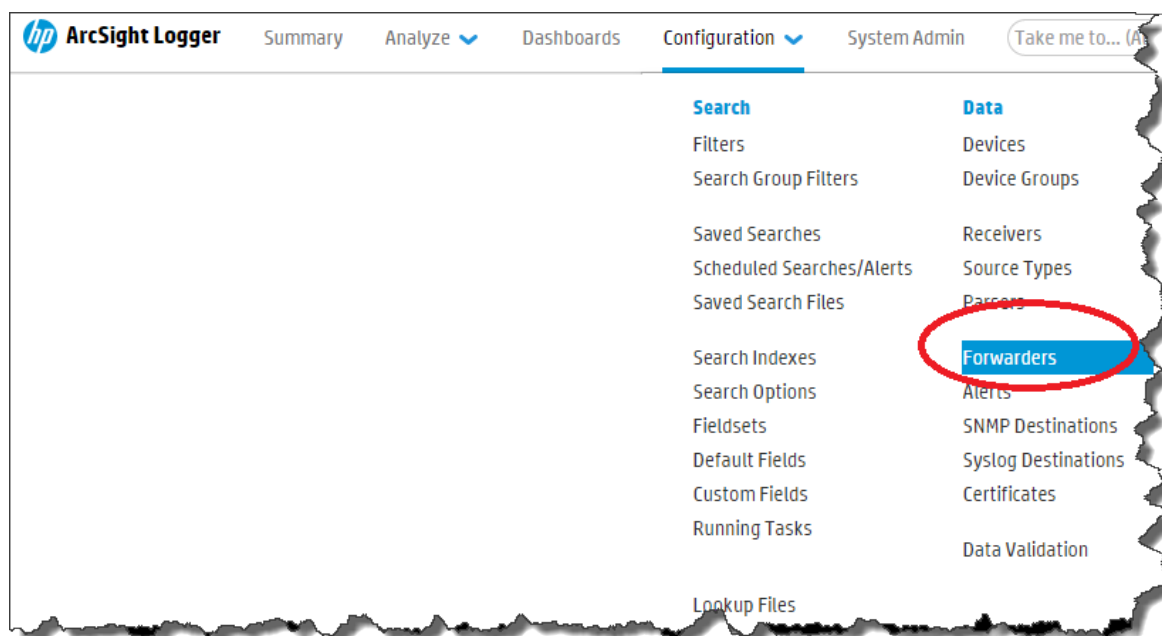
6. Select the **Forwarders** tab; set the values following the example highlighted below; then click **Next**:
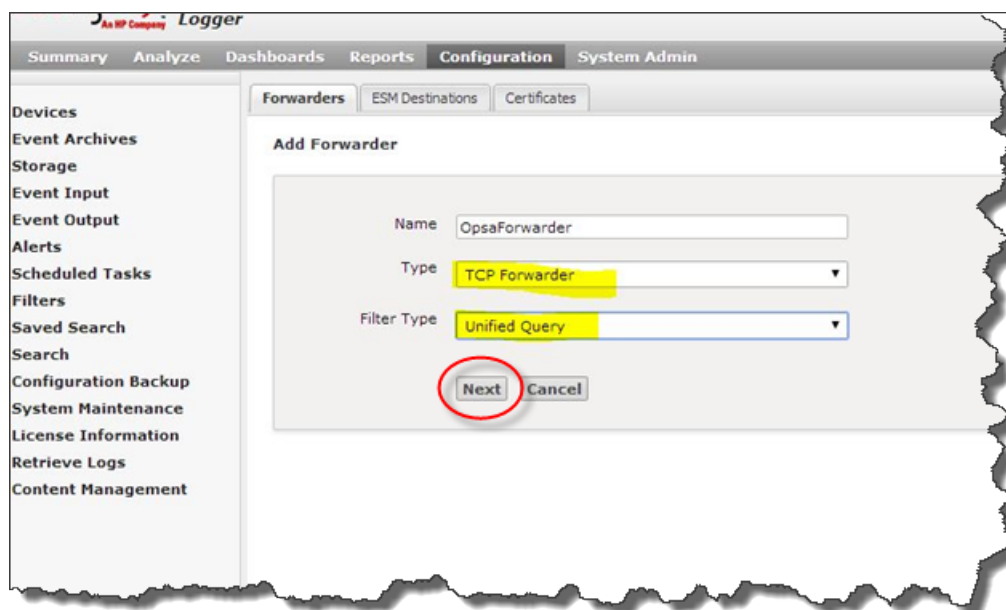
7. Enter the values following the example highlighted below; then click **Save**:

Note:

- The query highlighted above is for Log Analytics (all fields). Make sure the query you configure represents the collection you plan to configure.

- Change the highlighted IP address to the fully-qualified domain name of the Operations Analytics Collector Appliance for the collection you plan to configure. You must use the same value that is returned when you run the `opsa-log-integration-config.sh -list` command .

8. Enable the new configuration by clicking the highlighted area as follows:
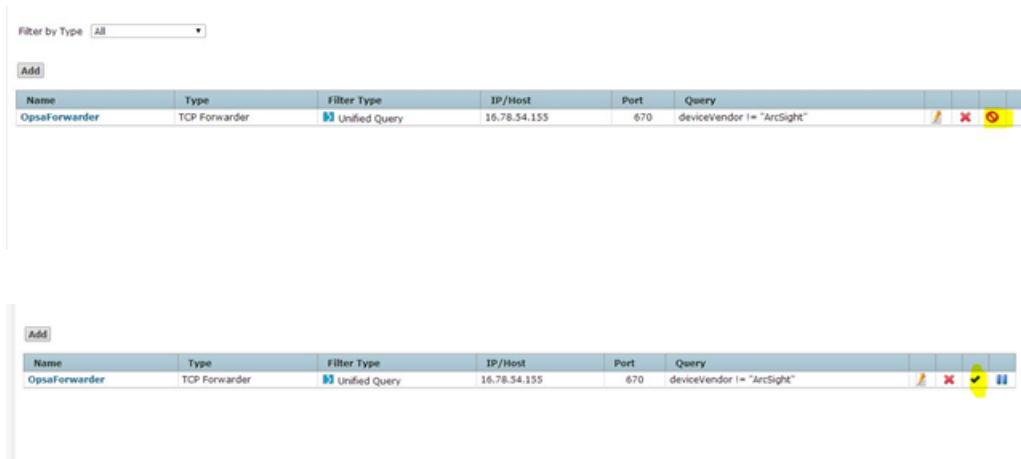
9. Open the Operations Analytics console.

10. Edit the Arcsight Logger Instance for which you want to make this change.

11. Select the check **TCP Forwarding** checkbox.

12. Click **OK** to commit your changes.

Now that you completed the above steps, Logger forwards CEF messages to the Operations Analytics All-in-One for HPE OneView Appliance.

# Configuring SSL for the HPE Operations Analytics All-in-One for HPE OneView Appliance

Note: Completing the steps shown in this section is **optional**. If you prefer not to enable SSL communication to the Operations Analytics All-in-One for HPE OneView Appliance, skip this section and continue with "Licensing the HPE Operations Analytics All-in-One for HPE OneView Appliance " on page 18.

Use the information in this section to manage SSL on the Operations Analytics All-in-One for HPE OneView Appliance.

One-way SSL provides secure communication between the web browser and the Operations Analytics All-in-One for HPE OneView 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 web browser verify the server's identity. SSL is disabled by default.

Configuring SSL with a Certificate Authority (CA) Signed Certificate for the HPE Operations Analytics All-in-One for HPE OneView Appliance

Complete the following steps to enable SSL communication to the Operations Analytics All-in-One for HPE OneView Appliance using a CA signed certificate:

1. Before enabling SSL to the Operations Analytics All-in-One for HPE OneView 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.

   > **Note:** The predefined super-admin login name is opsaadmin and the predefined super-admin password is opsaadmin.

   > **Note:** The predefined super-admin login name is opsaadmin and the predefined super-admin password is opsaadmin.

3. Select the **Configure SSL** option.

4. When using a CA signed public key of a server certificate obtained using a CSR generated from a self-signed certificate, select the **Import CA certificate to OPSA server keystore** option to import the certificate to the Appliance 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 the 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 HPE 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.

9. Run the `service opsa-collector restart` command to complete the configuration.

Configuring SSL with a Self-Signed Certificate for the HPE Operations Analytics All-in-One for HPE OneView Appliance

Complete the following steps to enable SSL communication to the Operations Analytics All-in-One for HPE OneView 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.

   > **Note:** The predefined super-admin login name is opsaadmin and the predefined super-admin password is opsaadmin.

   > **Note:** The predefined super-admin login name is opsaadmin and the predefined super-admin password is opsaadmin.

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 HPE 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`.

   Note: `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 theOperations 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.

10. Run the `service opsa-collector restart` command to complete the configuration.

Licensing the HPE Operations Analytics All-in-One for HPE OneView Appliance

The Operations Analytics All-in-One for HPE OneView Appliance comes with an Implicit node pack (Instant On) license that is valid for 60 days.To view the existing Appliance license, navigate to **Help** > **About**> **License** from the Operations Analytics console. See "Licensing HPE OneView" on page 20 for more information.

Review the following environment considerations:

Note: The following items are environment considerations, and are independent from licensing.

- Considering the HPE OneView customer, each HPE OneView application server manages 640 HPE servers + X number of other objects (interconnect, devices, power devices, and other objects) for an approximate total of 1024 objects.

- If an HPE OneView customer environment contains more than 1024 objects to be managed, they will need more than one HPE OneView application server.

- One Operations Analytics for HPE OneView deployment integrates with a single HPE OneView application server.

- An Operations Analytics for HPE OneView deployment could be one of the following, depending on the above environment considerations:

  - A single Operations Analytics for HPE OneView Appliance as explained in this manual.

  - A distributed Operations Analytics deployment, including Vertica, Logger, an Operations Analytics

Server Appliance, and an Operations Analytics Corrector Appliance. See the HPE Operations Analytics Installation Guide for more information.

Testing the HPE Operations Analytics All-in-One for HPE OneView Appliance

Complete the following steps to test the Operations Analytics All-in-One for HPE OneView Appliance.

> **Note:** You have not yet enabled the Operations Analytics - HPE OneView integration. This step only tests some basic Operations Analytics functionality.

1. Set up the Operations Analytics All-in-One for HPE OneView Appliance.
2. Take a snapshot of the Operations Analytics All-in-One for HPE OneView Appliance.
3. Using SSH, log on to the Operations Analytics All-in-One for HPE OneView Appliance.
4. When prompted, change the Operations Analytics All-in-One for HPE OneView Appliance password, and note the new password.

   > **Note:** To log on to the Operations Analytics All-in-One for HPE OneView Appliance for the first time, use the following authentication credentials:
   > User: `opsa`
   > Password: `opsa`
   >
   > The `opsa` user has the privileges to switch to the root user, if necessary. You need to provide the root password (initially set to `iso*help`) to switch to the root user.

5. Do the following to check the status of the Operations Analytics All-in-One for HPE OneView Appliance:
   a. Run the following command: `/opt/HP/opsa/bin/opsa-server status`
      Look for the following message: `opsa-server is running`
   b. Run the following command: `/opt/HP/opsa/bin/opsa-collector status`
      Look for the following message: `opsa-collector is running`

6. Do the following to log on to the Operations Analytics console and check the dashboard.
   a. Point your browser to **http://hostname:8080/opsa**
   b. Log on using `opsa` as a username and `opsa` as the password. You should see the **Welcome to Operations Analytics** page.
   c. Click the **Start Using Application** button. You should see the following dashboards:
      ○ **OpsA Health**: This dashboard shows system health information for Operations Analytics.

      > **Note**: You might need to wait 20 minutes or more for the HPE Operations Agent to publish its collected data.

      ○ **OA Environment Overview**: This dashboard shows the nodes having the top CPU, disk, memory, and network utilization. Although there is only one node in the database, you will see more data after you add more collection sources to Operations Analytics.
      ○ **OpsA Meta Info**: This dashboard shows the list of tables and tags configured by default.

Chapter 3: Enabling the HPE Operations Analytics- HPE OneView Integration

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

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

Supported HPE OneView Versions

To view a list of the HPE OneView versions supported by Operations Analytics, do the following:

1. Point your browser to Software Solutions Now.
2. Click the **Integrations** link.
3. Scroll to the Operations Analytics integrations; then select the Operations Analytics pull-down.
4. Select the integration with HPE OneView; then view the support matrix table to see the supported versions.

Note: Operations Analytics only supports an integration with HPE OneView if HPE OneView is installed on a Linux Operating System.

Licensing HPE OneView

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

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

  Note: The Operations Analytics All-in-One for HPE OneView Appliance does not support the configuration of other types of collections. Only Operations Analytics All-in-One for HPE OneView Appliance collections that are configured as explained in "About Data Collections for the HPE Operations Analytics - HPE OneView Integration" on page 26 are supported.

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

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

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

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

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

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

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

Configuring the HPE Operations Analytics - HPE OneView Integration

The information in this section explains how to configure the Operations Analytics - HPE OneView integration.

> **Note:** The Operations Analytics All-in-One for HPE OneView Appliance and the HPE OneView Server must each be able to resolve each other's fully-qualified domain names for the Operations Analytics - HPE OneView integration to function correctly.

> **Note: Important**: You must complete the licensing work in "Licensing HPE OneView" on the previous page before completing the instructions in this section.

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

To configure the Operations Analytics - HPE OneView integration, log on to Operations Analytics as a tenant administrator, then do the following:

> **Note:** You can enable the Operations Analytics - HPE OneView integration as the opsatenantadmin tenant administrator or as a tenant administrator for a tenant you created. You can only configure this integration using one tenant (this integration does not support multiple tenants).

- If this is the first time you have logged on as a tenant administrator, do the following:

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

b. Click the **Start Using Application** button and the HPE OneView settings dialog box opens.

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

> **Note:** You will be prompted for the fully-qualified domain name of the HPE OneView server (or its IP address), the user name to use for the HPE OneView server, and the password for the user name you provide.

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

> **Note:** If HPE OneView is configured with Active Directory, enter the User Principal Name in the **User name** field.
> Example: *<username>*@*<domain>*.com.

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

- If you have logged on as a tenant administrator before on this Operations Analytics server, do the following:

  a. Select ○ (**OneView Settings**) from the configuration menu. This opens the **OneView Settings** dialog box.

  b. Enter the HPE OneView setting information; then click **Integrate**.

  All of the integration steps automatically happen after entering the HPE OneView setting information.

  > **Note:** You will be prompted for the fully-qualified domain name of the HPE OneView server (or its IP address), the user name to use for the HPE OneView server, and the password for the user name you provide.

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

  > **Note:** If HPE OneView is configured with Active Directory, enter the User Principal Name in the **User name** field.
  > Example:*<username>*@*<domain>*.com.

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

> **Note:** It can take up to one hour for HPE OneView to forward a complete set of data to Operations Analytics.

If you encounter problems during setup, see "Troubleshooting the HPE Operations Analytics- HPE OneView Integration" below for more information.

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

Troubleshooting the HPE Operations Analytics- HPE OneView Integration

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

> **Note:** It is mandatory that the Operations Analytics All-in-One for HPE OneView Appliance have a valid fully-qualified domain name for this integration to function successfully.

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

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

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

1. Log on to the HPE OneView console.
2. Navigate to **Settings** > **users and groups**
3. **Do only one of the following** from the HPE OneView console:
   - Choose an existing infrastructure administrator for the integration like the **administrator** or **opsa** user shown below.
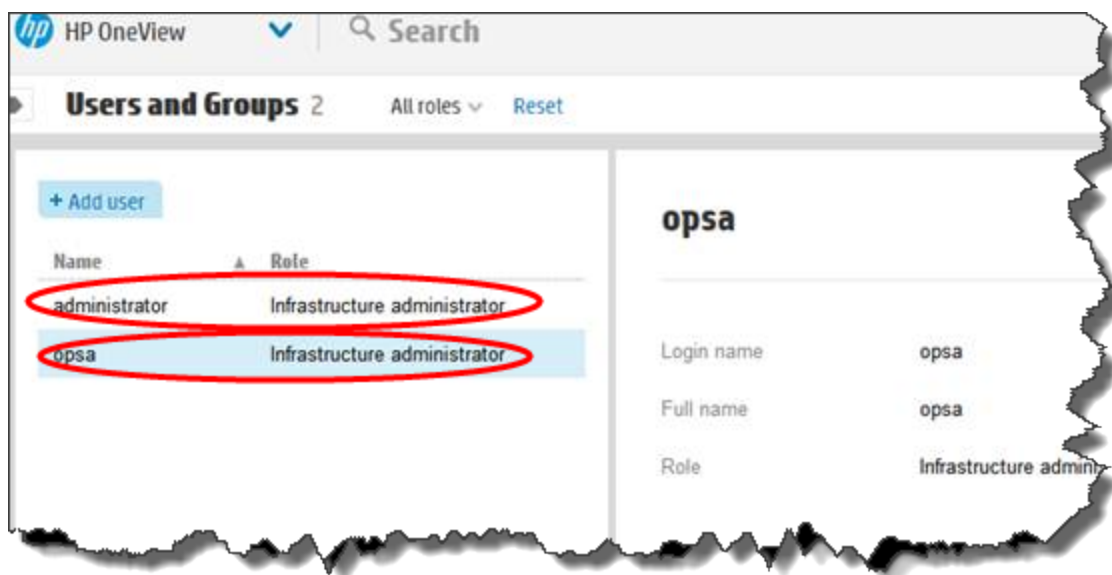
- Create an infrastructure administrator for the integration. Make sure to select the **Full** role when creating the infrastructure administrator.

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

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

1. Log on to the HPE OneView server.

2. Select **Servers** > **Server Hardware** from the HPE OneView console.

3. Locate the **Hardware** heading, scroll to the **iLO** row, then click the associated IP address to log on to the **Integrated Lights-Out** console.

4. Select **Administration** > **Management**.

5. Select the **Remote Syslog** tab.

6. Check that the IP address entry in the remote Syslog Server field matches the IP address of the Operations Analytics server.

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

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

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

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

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

1. Log on to the HPE Blade System Onboard Administrator (OA)

2. Select **Active Onboard Administrator**.

3. Click **System Log**.

4. Click the **Log Option** tab.

5. Check that the IP address entry in the remote Syslog Server field matches the IP address of the Operations Analytics server.

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

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

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

1. Log on to Operations Analytics as a tenant administrator user.

2. Select **Settings** > **OneView Settings**

3. Configure the Operations Analytics- HPE OneView integration and see if this action corrects the problem.

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

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

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

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

Question: When viewing the **OneView Interconnect 360** dashboard, you do not see any interconnects data. What should you do?

Answer: Do the following from the OneView console:

1. Verify that your LIG configuration matches your actual hardware.

2. If there is still no interconnect data, refresh the enclosures.

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

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

HPE OneView Data Collections

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

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

Note: The HPE OneView Syslog collection shown in "HPE OneView Data Collections" above includes an installed syslog daemon and uses port UDP 514.

Using the HPE Operations Analytics - HPE OneView Integration

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

HPE Operations Analytics - HPE OneView Integration Security Hardening

- **Authentication**: The Operations Analytics All-in-One for HPE OneView Appliance Inventory and Tree collections use the Rest API. This collection requires user names and passwords. The Operations Analytics All-in-One for HPE OneView Appliance Inventory Changes, Metrics and Alerts collections require the certificates that are stored in keystore and truststore files. These two stores require password authentication.

- **Key Management**: These keys are stored in the `/opt/HP/opsa/conf/ssl/opsa-truststore.jks` file.

- **Encryption**: Operations Analytics's Inventory Changes, Metrics and Alerts collections require the passwords for the keystore and truststore used by the HPE OneView server. These passwords are encrypted.

- **User Permissions**: To configure the Operations Analytics - HPE OneView integration, log on to Operations Analytics as a tenant administrator. See the *Operations Analytics Configuration Guide* for information about configuring the Operations Analytics users.

- **Certificates**: After you click the **Integrate** button, Operations Analytics sends the HPE OneView host, user name, and password to the HPE OneView server. The HPE OneView server returns the certificate data in forms that Operations Analytics places in the `/opt/HP/opsa/conf/ssl/opsa-truststore.jks` file on the Operations Analytics Server. After the Operations Analytics All-in-One for HPE OneView Appliance collections are published (this happens automatically during the integration setup), Operations Analytics moves this file to the Operations Analytics Collector host.

- **Data being Collected**: The Operations Analytics All-in-One for HPE OneView Appliance collections obtain data from HPE OneView, which includes logs, metrics, HPE OneView alerts, and topology data.

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

Chapter 4: Expanding to a Distributed Operations Analytics

After installing, configuring, and using the features of the Operations Analytics All-in-One for HPE OneView Appliance version 2.31, you might decide to expand it into a distributed version of Operations Analytics version 2.31.

Before starting through these steps, run the following command to list the existing collections:

```
/opt/HP/opsa/bin/opsa-collection-config.sh -list -collectorhosts -username
<opsaTenantAdminUser> -password <opsaTenantAdminPasswd>
```

You will need the details for these collections to register them on the new Operations Analytics Server Appliance as discussed towards the end of these steps.

Task 1: *Unregister* all of the Collections and the Collector

You must *unregister* all of the Operations Analytics All-in-One for HPE OneView Appliance collections as well as the predefined Operations Analytics collections from the Operations Analytics All-in-One for HPE OneView Appliance. You must *unregister* the registration for the Collector as well.

> **Note:** You will re-register all of the mentioned items during

To complete the mentioned *unregister* work, do the following:

1. Run the following command to *unregister* the Operations Analytics All-in-One for HPE OneView Appliance collections: `/opt/HP/opsa/support/publishOneViewCollections.sh UNREGISTER <collector fully-qualified domain name> <opsaTenantAdminUser> <opsaTenantAdminPasswd>`

   > **Note:** publishOneViewCollections.sh is an unsupported script used for troubleshooting and support purposes.

2. Run the following commands to *unregister* the other collections:

   ```
   /opt/HP/opsa/bin/opsa-collection-config.sh -unregister -collectorhost <collectorhost
   name or IP address> -username <opsaTenantAdminUser> -password
   <opsaTenantAdminPasswd> –source arcsight -domain log -group stream
   ```

   ```
   /opt/HP/opsa/bin/oopsa-collection-config.sh -unregister -collectorhost
   <collectorhost name or IP address> -username <opsaTenantAdminUser> -password
   <opsaTenantAdminPasswd> –source oa -domain sysperf -group global
   ```

3. Run the following command to *unregister* the Operations Analytics All-in-One for HPE OneView Appliance collector: `/opt/HP/opsa/bin/opsa-collection-config.sh -unregister -collectorhost <fully-qualified domain name of collector host> -username`

<opsaTenantAdminUser> -password *<opsaTenantAdminPasswd>*

4. Run the following command to *unregister* the Operations Analytics All-in-One for HPE OneView Appliance Logger:

```
/opt/HP/opsa/bin/opsa-log-integration-config.sh -loginUser <opsaTenantAdminUser> -
loginPassword <opsatenantAdminPasswd> -delete -host <fully-qualified domain name of
Loggerhost> -collectorHost <fully-qualified domain name of Collector host> -
loggerType arcsight -base64Decode true
```

Task 2: Expanding the HPE Operations Analytics All-in-One for HPE OneView Appliance

Carefully complete the following steps to expand your Operations Analytics All-in-One for HPE OneView Appliance into a distributed version that can use the integration with HPE OneView:

To check if you have the Operations Analytics All-in-One for HPE OneView Appliance configured for DHCP, and, if necessary, change the configuration to support a static IP address, do the following:

1. As root, edit the `/etc/sysconfig/network-scripts/ifcfg-eth0` file on the Operations Analytics Server Appliance.

2. Locate the line beginning with `BOOTPROTO`. If the value on that line is `none`, then the Operations Analytics All-in-One for HPE OneView Appliance is configured for static IP and you do not need to take any further action. Close the `/etc/sysconfig/network-scripts/ifcfg-eth0` file on the Operations Analytics Server Appliance and do not complete the remaining steps.

3. Locate the line beginning with `BOOTPROTO`. If the value on that line is something like `dhcp`, then the Operations Analytics All-in-One for HPE OneView Appliance is configured for DHCP, and you must complete the remaining steps in this section.

   Note: When using DHCP, Operations Analytics uses a standard `ifcfg-eth0` file configuration recommended by CentOS. If your network configuration is different from the standard described by CentOs, Operations Analytics might not be able to get an IP address from DHCP or access the VM using the hostname or fully-qualified domain name. See Configuring a DHCP Client in the Red Hat Enterprise Linux Deployment Guide for more information.

4. Locate the line beginning with `BOOTPROTO`. If the value on that line is something like `dhcp`, then the node is configured for DHCP and you must complete the remaining steps.

   Note: Run the `ifconfig -a` command if you want to know the server's current IP address and other network information.

5. From a command prompt on the Operations Analytics All-in-One for HPE OneView Appliance, shut down Operations Analytics (if it is running) by running, as the opsa user, the following commands:

   Note: In some environments, the DHCP node might only be accessible (routable) using the web and the vSphere console. In that case, use the vSphere console to sequentially run the commands shown below.

    a. `/opt/HP/opsa/bin/opsa-process-manager.sh stop`

    b. `/opt/HP/opsa/bin/opsa-server stop`

    c. `/opt/HP/opsa/bin/opsa-collector stop`

    d. `/opt/HP/opsa/bin/opsa-loader stop`

6. As the root user, edit the `/etc/sysconfig/network-scripts/ifcfg-eth0` file.

> **Note:** When using DHCP, Operations Analytics uses a standard `ifcfg-eth0` file configuration recommended by CentOS. If your network configuration is different from the standard described by CentOs, Operations Analytics might not be able to get an IP address from DHCP or access the VM using the hostname or fully-qualified domain name. See Configuring a DHCP Client in the Red Hat Enterprise Linux Deployment Guide for more information.

> **Note:** Make the changes for the steps in this task only after consulting your network administrator:

7. Make the remaining changes shown below only after consulting your network administrator:
   ```
   BOOTPROTO=none
   IPADDR=<your new IPv4 IP address>
   ```

8. Set the `NETMASK`, `GATEWAY`, and `BROADCAST` parameters appropriately. After you finish, it should look something like the following:
   ```
   DEVICE=eth0
   BOOTPROTO=none
   ONBOOT=yes
   TYPE=Ethernet
   IPV6INIT=no
   IPADDR=<your new IPv4 IP address>
   NETMASK=<your netmask>
   GATEWAY=<IP Address of the default gateway>
   BROADCAST=<broadcast IP Address>
   ```

> **Note**: When a system is using DHCP, the IP address, which is provided automatically, is not registered in DNS. However, static IP addresses are frequently registered in DNS. If that is the case, edit the `/etc/sysconfig/network` file and revise the `hostname` value.

9. After you save all of your changes, your remote connection to the Operations Analytics All-in-One for HPE OneView Appliance terminates because the old IP address no longer exists. Log on to the Operations Analytics All-in-One for HPE OneView Appliance using the vSphere client, bring up the console, then run the following commands:

    a. `/sbin/service network restart`

    b. `/etc/sysconfig/network-scripts/ifup eth0`

10. After the commands complete in the previous step, log on to the Operations Analytics All-in-One for HPE OneView Appliance remotely using the new IP address for the Operations Analytics All-in-One for HPE OneView Appliance.

Task 3: Testing and Configuring the Network

Complete the following to make sure the network is configured correctly for the Operations Analytics All-in-One for HPE OneView Appliance:

1. Run the `nslookup <Operations Analytics All-in-One for HPE OneView Appliance IP address>` command and the `hostname` command on the Operations Analytics All-in-One for HPE OneView Appliance.

2. Compare the two host names from the previous step. If they are not identical, do the following:

   a. Verify that the correct server names exist in the `resolv.conf` file.

   b. Verify that the correct host name resides in the following files:
   ```
   /etc/sysconfig/network
   /etc/hostname
   ```

3. If necessary, run the following command to force any changes you made to take effect:
   ```
   service network restart
   ```

4. Repeat the steps in this section until the network is configured correctly.

Task 4: Expanding Vertica

The information in this section explains how to install three new Vertica nodes on new VMs or servers. When combined with the Vertica application included with the Operations Analytics All-in-One for HPE OneView Appliance that you currently have installed, it totals four Vertica nodes in the Vertica Cluster. The Vertica license included on the Operations Analytics All-in-One for HPE OneView Appliance only supports three nodes. Before continuing with this expansion, you must obtain a Vertica license from Vertica and install it on the Operations Analytics All-in-One for HPE OneView Appliance.

> **Note:** One way to obtain a fourth Vertica license is to purchase an Operations Analytics production license. See *Obtaining Licenses* in the *Operations Analytics Installation Guide* for more information about obtaining and installing Operations Analytics licenses.

After obtaining a fourth Vertica license, carefully complete the following steps to expand Vertica on your Operations Analytics All-in-One for HPE OneView Appliance into a distributed version.

1. Rename `/opt/HP/opsa/conf/jmxNotHardened.tx` to `/opt/HP/opsa/conf/jmxNotHardened.txt`

   > **Note:** In this step you are changing the `.tx` extension to `.txt`.

2. Run the following command to restart the Operations Analytics server: `opsa-server restart`

   > **Note:** After running an `opsa-server restart` command, information logged in the `/opt/HP/opsa/log/opsa-server.log` file is removed. To view the files that retain this information across restarts, see the log files located in the `/opt/HP/opsa/jboss/standalone/log` directory. Look for log file names that begin with `server.log`.

3. Navigate to the following URL: **http://<IP Address of the Operations Analytics AIO VM>:8081/mbean?objectname=OPSA-Infrastructure%3Aservice%3DDeployment**

4. Provide the default user name (opsaadmin) and password (opsaadmin)

5. Run the `removeDeploymentForHost` method by entering the <*IP Address of the Operations Analytics AIO VM*> and then entering `yes` in the appropriate box.

6. Log on to the Vertica server as an opsa user.

7. Run the following command to become the root user: `su -`

8. Run the following command to become the Linux dbadmin user: `su - dbadmin`

> **Note:** Regardless of your use of DHCP or Static IP addresses, Vertica is using `local.host` for its address. This inhibits Vertica's ability to join a cluster. To remedy this, you must reconfigure Vertica on the Operations Analytics All-in-One for HPE OneView Appliance to use the Operations Analytics All-in-One for HPE OneView Appliance's new or existing static IP address.

9. Run the `/opt/vertica/bin/admintools` tool.

10. Complete the following steps to shut down the Vertica database:

    a. From the **Main Menu**, select **Advanced Tools**.

    b. Select option 2: **Stop Vertica on Host**.

    c. From the **Select Host(s)** window, select the **host** box; then click **OK**.

    d. When prompted about whether you are sure you want to stop Vertica, click **yes**.

    e. From the **Main Menu**, select **View Database Cluster State** to make sure that Vertica is shut down.

    > **Note:** If you are haing problems run /opt/HP/opsa/bin/opsa stop as root

11. Complete the following steps to convert Vertica from having a loopback address to having a static IP address:

    a. Contact Vertica or Operations Analytics support and download the latest `re_ip_cluster-2.1.py` script onto the Operations Analytics All-in-One for HPE OneView Appliance. Make sure the `re_ip_cluster-2.1.py` script has permissions to be run by the Linux dbadmin user.

    b. Log on as the root user.

    c. Shut down Vertica and Operations Analytics by running the following command: `/opt/HP/opsa/bin/opsa stop`

    d. As root, determine your IP address and broadcast address by running the following command: `/sbin/ifconfig`

    e. Log on as the Linux dbadmin user.

    f. Run the following command: `re_ip_cluster-2.1.py –c /opt/vertica/opsa_data/opsadb/v_opsadb_node0001_catalog -s`
    Running this command creates a `re_ip_batch.ini` file in the same directory from which you ran the command. Write down the location of this file.

    g. Edit the `re_ip_batch.ini` file

    h. Replace the loopback addresses and broadcast address with the IP address and broadcast address returned by the `/sbin/ifconfig` command you ran earlier.

    i. Save your work.

    j. Run the following command: `re_ip_cluster-2.1.py –c /opt/vertica/opsa_data/opsadb/v_opsadb_node0001_catalog –b <path to the re_ip_batch.ini file>`

    k. When prompted, press **Enter**.

12. Reserve IP addresses for three or four additional Vertica systems. Create new virtual appliances or set up hardware using these new IP addresses.

    > **Note:** Before adding any new Vertica nodes to the existing cluster on the Operations Analytics All-in-One for HPE OneView Appliance, it is recommended that you back up the Operations Analytics All-in-One for HPE OneView Appliance database. See the *Backing Up and Restoring* section of the *Vertica Administrator's Guide* for more information.

13. Run the following commands on the Operations Analytics All-in-One for HPE OneView Appliance for each Vertica server to test if ssh is functioning (without requiring passwords):

Run as a root user:

```
ssh -X root@<Vertica IP Address>
ssh -X dbadmin@<Vertica IP Address>
```

Run as a Linux dbadmin user:

```
ssh -X dbadmin@<Vertica IP Address>
```

If you find that passwords are required, run the following commands on each new Vertica server to set up ssh to not require passwords. Retest your changes using the `ssh` command shown in the previous paragraph after you finish:

```
ssh-copy-id -i root@<Vertica IP Address>
ssh-copy-id -i dbadmin@<Vertica IP Address>
```

Note: Using the commands shown in this step as a guide, confirm that ssh is functioning (without requiring passwords) from each Vertica server to the Operations Analytics All-in-One for HPE OneView Appliance and from each Vertica server to all other Vertica servers.

Note: If the `ssh-copy-id` script is not available on a server, look for a copy of it in the `/opt/HP/opsa/scripts` directory on the Operations Analytics All-in-One for HPE OneView Appliance; then do the following:

a. As the root user, copy the `ssh-copy-id` script to the `/tmp` directory.

b. As the root user, run the following command to change the script permissions: `chmod 555 ssh-copy-id`

Note: After completing this step, if you find that ssh does not function (without requiring passwords), here are a few possible causes:

- Edit the `/etc/sshd_config` file and make the following changes, if needed.
    i. Find `PermitRootLogin` and make sure it is set as follows: `PermitRootLogin Yes`
    ii. Find `DenyUsers` and make sure it does not have `dbadmin` in the list.
    iii. Save your changes.
    iv. Run the following command as the root user: `service sshd restart`

- The `/home` directory must be searchable with mod 755 permissions.

- The `/home/dbadmin` directory must be owned by the Vertica dbadmin user and have mod 700 permissions.

- If you see a `No identities found` message, you need to run the `ssh-keygen` command to create a public key for the `ssh-copy-id` command to overwrite.

14. Turn off the firewall on the Operations Analytics All-in-One for HPE OneView Appliance and all for the new ssh is functioning (without requiring passwords) Vertica servers by running the following command: `service iptables stop`

Note: Turn the firewalls on for the Operations Analytics All-in-One for HPE OneView Appliance and

all for the new Vertica servers after completing this task by running the following command:

```
service iptables start
```

15. From a command prompt on the Operations Analytics All-in-One for HPE OneView Appliance, run the following command (as root) :

```
/opt/vertica/sbin/update_vertica -A <IP Address of VM1>,<IP Address of
VM2>,<IP Address of VM3> -r <rpm_package>
```

Note: The `update_vertica` command assumes that Vertica is not installed on any of the destination systems. Before running this command, make sure that the destination systems do not already have Vertica installed.

Note: When you run the `update_vertica` command in this step, replace the < *IP Address of VM1>* with the IP address of the Operations Analytics All-in-One for HPE OneView Appliance. Replace the remaining VM IP addresses in the command with a comma separated list of all of the external Vertica servers you are adding.

16. Complete the following steps on each new virtual appliance to install the R Language Pack from Vertica:

Note: Run any commands shown in this list as the root user.

a. Go to My software updates (use your HPE Passport credentials) and download HPE Operations Analytics 2.31 Vertica Integration.zip.

b. Extract the contents of the `HPE Operations Analytics 2.31 Vertica Integration.zip` file to a temporary location.

c. Copy the files from the `MASS` and `vertica` folders located in the local directory to which you downloaded and extracted the `HPE Operations Analytics 2.31 Vertica Integration.zip` file to the `/home` directory:

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

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

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

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

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

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

g. Run the following command to install the `compat-libgfortran` package:

```
rpm -Uvh compat-libgfortran-41-4.1.2-39.el6.x86_64.rpm
```

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

```
rpm -Uvh vertica-R-lang-7.1.1-0.x86_64.RHEL5.rpm
rpm -Uvh vertica-R-lang-7.1.1-3.x86_64.RHEL5.rpm
```

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

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

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

        ii. If you see a message similar to the following, the installation was successful:

            `vertica-R-lang-<VERSION>`

    j. Complete the following steps to install the MASS package:

        i. Run the following command to set the correct permissions: `chmod 770 MASS_7.3-23.tar.gz`

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

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

17. From the Operations Analytics All-in-One for HPE OneView Appliance, do the following to add the new Vertica nodes to the database:

    a. Run `/opt/vertica/bin/admintools` as the Linux dbadmin user.

    b. Start the database.

    c. From the **Main Menu**, select **Advanced Tools**, select **Cluster Management**, then select **Add Host(s)**.

    d. Select the database (**opsadb**) to which you want to add one or more hosts.

    e. Select the hosts from the list that you want to add to the database; then click **OK** and **Yes**.

> **Note:** You will need to enter the database password (the database password for the Vertica dbadmin user is dbadmin. You must click **OK** several times to complete this step.

18. After completing the previous step, Vertica automatically starts the rebalancing process to populate the new hosts with data:

    a. When prompted, enter the path to a (large) temporary directory that the Database Designer can use to rebalance the data in the database; then select **OK**.

    b. Either press **enter** to accept the default K-Safety value, or enter a new higher value for the database; then select **OK**. See the *Vertica Administrator's Guide* for more information.

    c. Select the option that enables HPE Vertica to immediately start rebalancing the database.

    d. Review the summary of the rebalancing process; then select **Proceed**.

19. Designate the IP address of one of the newly added Vertica nodes as the representative node for the cluster.

20. Do the following to remove the Operations Analytics All-in-One for HPE OneView Appliance Vertica instance from the new Vertica cluster. Perform this action from the newly designated representative node.

    a. Run the `/opt/vertica/bin/admintools` command as the Linux dbadmin user.

    b. Select Advanced Tools

    c. Select Cluster Management

    d. Select Remove Host(s)

    e. Select the Operations Analytics database.

    f. Select the box for the Operations Analytics All-in-One for HPE OneView Appliance.

Vertica will go through another rebalancing process, then remove the HPE OneView Vertica.

Task 5: Installing a New Collector

Install and configure a new Operations Analytics Collector Appliance by following the instructions located in the Operations Analytics Installation Guide. Look for the section title *Installing and Configuring the Operations Analytics Collector Appliance*.

> **Note:** You will register this newly configured Operations Analytics Collector Appliance in a later task.

Task 6: Adding a New Logger

Carefully complete the following steps to add a new Logger to support a distributed Operations Analytics version.

1. Reserve an IP address for an additional Logger server. Create a new virtual appliance or set up hardware using this new IP address.

2. Install Logger using the instructions in the *Operations Analytics Installation Guide* (just as you would for a regular distributed system).

3. Install the SysLog Daemon by running the `<path>/ArcSightSmartConnectors/current/bin/runagentsetup.sh` script as the root user.

4. Run the following command to register Logger with the new Operations Analytics Server Appliance:

   `/opt/HP/opsa/bin/opsa-log-integration-config.sh -loginUser <tenant username> -loginPassword <tenant user password> -add -host <fully-qualified domain name of Logger> -collectorHost <fully-qualified domain name of Collector host> -username <loggeruser1> -loggerType arcsight -password <loggeruser1pwd> -port 443 -sslEnabled true -base64Decode true -allFields true -tcpMode passive`

5. Complete the following steps to configure the arcsight_log_stream collection:

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

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

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

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

   c. Enter `9` to begin configuring an HPE ArcSight Logger Collection.

   d. When prompted, choose the following option: `5: Log Analytics-All Fields (130)`

   e. Enter the HPE ArcSight Logger host name from which to collect the data.

   f. Enter `execute 9 active` and wait for the setup process to complete.

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

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

h. When prompted to confirm your setup, enter `y` to exit the script.

6. Install the HPE OneView SysLog Daemon parser by copying the following file from the Operations Analytics All-in-One for HPE OneView Appliance to the same location on the new Logger server : `/opt/HP/arcsight/ArcSightSmartConnectors/current/user/agent/flexagent/syslog/OneView Mapping.sdkrfilereader.properties`

7. Run the following command, as root, to start the SysLog Daemon: `Service Arc_SysLog start`

8. Go to the Logger console and disable the UDP Receiver. Make sure that the Smart Receiver is enabled.

Task 7: Adding a New Operations Analytics Server

Carefully complete the following steps to add a new Operations Analytics Appliance to support a distributed Operations Analytics version.

1. Reserve an IP address for a new Operations Analytics Server Appliance. Create a new virtual appliance or set up hardware using this new IP address.

2. Deploy the Operations Analytics Server Appliance using instructions in the *Operations Analytics Installation Guide*.

3. Complete this step to copy the zookeeper files from the Operations Analytics All-in-One for HPE OneView Appliance to the Operations Analytics Server Appliance. Do the following from the Operations Analytics All-in-One for HPE OneView Appliance:

   a. Change directories to `/opt/HP/opsa/zookeeper/data/`

   b. Run the following command: `tar -cvf /tmp/zoo.tar version-2`

   c. Copy the `zoo.tar` file to `/tmp/zoo.tar` file on the Operations Analytics Server Appliance.

   Do the following from the new Operations Analytics Server Appliance:

   a. Run the following command as the opsa user: `mkdir /opt/HP/opsa/zookeeper/data`

   b. Change directories to `/opt/HP/opsa/zookeeper/data`

   c. Run the following command: `tar -xvf /tmp/zoo.tar`

   d. Verify that the `version-2` directory now resides in the `/opt/HP/opsa/zookeeper/data` folder.

4. Run the opsa-server-postinstall.sh script using the `-scaleout` syntax shown below. When prompted, specify the IP address of one of the new Vertica systems.
   `/opt/HP/opsa/bin/opsa-server-postinstall.sh -scaleout`

   After the `opsa-server-postinstall` script finishes, run the following commands:

   a. `opsa-zookeeper restart`

   b. `opsa-server restart`

   > **Note:** After running an `opsa-server restart` command, information logged in the `/opt/HP/opsa/log/opsa-server.log` file is removed. To view the files that retain this information across restarts, see the log files located in the `/opt/HP/opsa/jboss/standalone/log` directory. Look for log file names that begin with `server.log`.

5. Run the opsa-collector-postinstall.sh script shown below. When prompted, specify the IP address of one of the new Vertica systems.

   `/opt/HP/opsa/bin/opsa-collector-postinstall.sh`

6. Run the following command to register the newly added Operations Analytics Collector Appliance with the new Operations Analytics Server Appliance:

   `/opt/HP/opsa/bin/opsa-collection-config.sh -register -collectorhost <fully-qualified domain name of Newly Added Operations Analytics -port 9443 Collector> -username opsatenantadmin`

7. Run the following command to register Logger with the new Operations Analytics Server Appliance:

   `/opt/HP/opsa/bin/opsa-log-integration-config.sh -loginUser <tenantadmin1> -loginPassword <tenantadmin1Pwd> -add -host <fully-qualified domain name of Logger> -collectorHost <fully-qualified domain name of Collector host> -username <loggeruser1> -loggerType arcsight -password <loggeruser1pwd> -port 443 -sslEnabled true -base64Decode true -allFields true -tcpMode passive`

8. Complete the following steps to register all of the original collections on the new Operations Analytics Server Appliance

   a. Run the following command: `/opt/hp/opsa/support/publishOneViewCollections.sh PUBLISH <ovHOst> <ovUser> <ovPw> <collectorIP> <loggerIP> <opsaTenantAdminUser> <opsaTenantAdminPasswd> 3600`

      > **Note:** publishOneViewCollections.sh is an unsupported script used for troubleshooting and support purposes.

      > **Note:** Review the following information before using the publishOneViewCollections.sh script:
      >
      > ○ `PUBLISH` is a keyword.
      >
      > ○ *ovHost*, *ovUser*, and *ovPw* are the HPE OneView credentials used when enabling the Operations Analytics - HPE OneView integration from the Operations Analytics welcome page.
      >
      > ○ The *collectorIP* is the hostname of the original Operations Analytics All-in-One for HPE OneView Appliance (Do not use the IP address).
      >
      > ○ The *loggerIP* is the hostname of the new Logger server,
      >
      > ○ The last argument is optional, and specifies the metrics collection frequency (in seconds).

Congratulations, you finished converting your Operations Analytics All-in-One for HPE OneView Appliance version 2.31 into a distributed version of Operations Analytics version 2.31.

Troubleshooting Actions for Expanding to a Distributed Operations Analytics

If you encounter errors when running (and rerunning) the `publishOneViewCollections.sh PUBLISH` command, run the following series of commands before running the `publishOneViewCollections.sh PUBLISH` command again:

> **Note:** publishOneViewCollections.sh is an unsupported script used for troubleshooting and support

purposes.

```
/opt/vertica/bin/vsql -c "drop view IF EXISTS opsa_default.oneview_inventory_server_view
cascade;" -d <dbname> -U <dbuser> -w <db passwd> -h <vertica hostname>

/opt/vertica/bin/vsql -c "drop view IF EXISTS opsa_default.oneview_inventory_enclosure_
view cascade;" -d <dbname> -U <dbuser> -w <db passwd> -h <vertica hostname>

/opt/vertica/bin/vsql -c "drop view IF EXISTS opsa_default.oneview_inventory_powerdevice_
view cascade;" -d <dbname> -U <dbuser> -w <db passwd> -h <vertica hostname>

/opt/vertica/bin/vsql -c "drop view IF EXISTS opsa_default.oneview_metrics_server_view
cascade;" -d <dbname> -U <dbuser> -w <db passwd> -h <vertica hostname>

/opt/vertica/bin/vsql -c "drop view IF EXISTS opsa_default.oneview_metrics_enclosure_view
cascade;" -d <dbname> -U <dbuser> -w <db passwd> -h <vertica hostname>

/opt/vertica/bin/vsql -c "drop view IF EXISTS opsa_default.oneview_metrics_powerdevice_
view cascade;" -d <dbname> -U <dbuser> -w <db passwd> -h <vertica hostname>

/opt/vertica/bin/vsql -c "drop view IF EXISTS opsa_default.oneview_alerts_server_view
cascade;" -d <dbname> -U <dbuser> -w <db passwd> -h <vertica hostname>

/opt/vertica/bin/vsql -c "drop view IF EXISTS opsa_default.oneview_alerts_enclosure_view
cascade;" -d <dbname> -U <dbuser> -w <db passwd> -h <vertica hostname>

/opt/vertica/bin/vsql -c "drop view IF EXISTS opsa_default.oneview_alerts_powerdevice_
view cascade;" -d <dbname> -U <dbuser> -w <db passwd> -h <vertica hostname>

/opt/vertica/bin/vsql -c "drop view IF EXISTS opsa_default.oneview_logs_server_view
cascade;" -d <dbname> -U <dbuser> -w <db passwd> -h <vertica hostname>

/opt/vertica/bin/vsql -c "drop view IF EXISTS opsa_default.oneview_logs_enclosure_view
cascade;" -d <dbname> -U <dbuser> -w <db passwd> -h <vertica hostname>
```

Chapter 5: Configuring Collections

After you have expanded the Operations Analytics All-in-One for HPE OneView Appliance to a distributed environment, use the information in the Operations Analytics Configuration Guide to configure all metrics, events, inventory, and topology collections.

Chapter 6: Managing Data Retention

After you purchase and apply an Operations Analytics production license, use the information in this section to manage the data retention for Operations Analytics, including both Logger and Vertica.

Managing Vertica Data

By default, the Operations Analytics- HPE OneView deployment uses the Vertica Community Edition license, which is a non-expiring 1TB license. To avoid any disruptions in service, it is a good practice to monitor the size of the Operations Analytics database.

To check or verify the size of the Operations Analytics database, do the following:

1. Log on to the Vertica server as an opsa user.

2. Run the following command to become the root user: `su -`

3. Run the following command to become the Linux dbadmin user: `su - dbadmin`

4. Run the following command: `/opt/vertica/bin/vsql -U dbadmin -c 'select get_compliance_status();'`

   > **Note:** Only use the `-U dbadmin` option if you log on as a root user.

5. Review the compliance status. The message you see resembles the following example, which shows a 70 percent utilization percentage (70 percent of the 1TB that is available is currently in use):

```
                              get_compliance_status
------------------------------------------------------------------------------
------------------------------------------------------------------------------
----------
Raw Data Size: 0.00TB +/- 0.00TB
License Size : 1.00TB
Utilization  : 70%
Audit Time      -12-31 17:00:00-07
Compliance Status : The database is in compliance with respect to raw data size.

No expiration date for a Perpetual license
(1 row)
```

If you have exceeded your licensed database size, do one or more of the following:

- **Shorten the data retention period:** See "Setting the Data Retention Period" on the next page for more information.

- **Set a Purge Policy for the Vertica database**: See *Purging Deleted Data* in the *Vertica Administrator's Guide*.

- **Manually purge data from the Vertica database**: See *Purging Deleted Data* in the *Vertica*

Administrator's Guide

- **Increase the Vertica license size**: See *Managing Licenses* in the *Vertica Administrator's Guide*

See *Monitoring Database Size for License Compliance* in the *Vertica Administrator's Guide* for more information.

Setting the Data Retention Period

By default, the Operations Analytics All-in-One for HPE OneView Appliance includes a two month data retention period. After purchasing and applying a production license, you can modify the data retention period as follows:

- To set the retention period for a specific source, domain, and group, use the following command:
  `/opt/HP/opsa/bin/opsa-collection-config.sh -setretention` *`<retention period in months>`* `-source` *`<source>`* `-domain` *`<domain>`* `-group` *`<group>`* `-username` *`<username>`* `[-force]`
- To set the retention period for a specific source, use the following command:
  `/opt/HP/opsa/bin/opsa-collection-config.sh -setretention` *`<retention period in months>`* `-source` *`<source>`* `-username` *`<username>`* `[-force]`
- To set the overall retention period, use the following command: `/opt/HP/opsa/bin/opsa-collection-config.sh -setretention` *`<retention period in months>`* `-username` *`<username>`* `[-force]`

After setting the retention period for specific collections belonging to a tenant, Operations Analytics removes any data record with a time stamp older than the listed retention period for those collections.

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

Managing Data in Logger

Logger supports several storage groups, each of which can have a different retention policy. Retention policy is specified in terms of number of days that events are stored, or overall maximum size (in GB). See *Retention Policy* in the *ArcSight Logger Administrator's Guide* for more information.

For software Loggers, the storage volume is set to the maximum capacity specified in the license or the available disk space, whichever is smaller. See *Storage Volume* in the *ArcSight Logger Administrator's Guide* for more information.

To manage adherence to the Logger license, do the following from the ArcSight Console:

1. Click **System Admin**.
2. Click **License & Update**.
3. Review the license information. If you have exceeded your licensed database size, do one or more of the following:

   - Increase the Logger licensed capacity. See *License and Update* in the *ArcSight Logger Administrator's Guide* for more information

   - Add a storage group to Logger. See *Adding Storage Groups* in the *ArcSight Logger Administrator's Guide* for more information

- Regularly manage your Logger storage volume. See *Storage Volume* in the *ArcSight Logger Administrator's Guide* for more information

Chapter 7: Upgrading an HPE Operations Analytics All-in-One for HPE OneView Appliance to a Newer Version

To upgrade a version 2.30 Operations Analytics All-in-One for HPE OneView Appliance to a version 2.31 Operations Analytics All-in-One for HPE OneView Appliance, do the following:

1. Follow the instructions shown in "Setting up the HPE Operations Analytics All-in-One for HPE OneView Appliance " on page 8 to create a new version 2.31 Operations Analytics All-in-One for HPE OneView Appliance.

   Note: Do not integrate the HPE OneView server until you are directed to in a later step. .

   Note: If you are using DHCP for the Operations Analytics All-in-One for HPE OneView Appliance IP address, the DHCP IP address that you use should not be changing during a reboot. If the DHCP IP address changes for the Operations Analytics All-in-One for HPE OneView Appliance, Operations Analytics will not function correctly.

2. Preparing for a potential rollback:

   It is recommended that you complete a snapshot of both the version 2.30 and 2.31 Operations Analytics All-in-One for HPE OneView Appliances as a precaution.

3. Do the following to stop the Operations Analytics processes on both the Operations Analytics 2.30 and 2.31 Operations Analytics All-in-One for HPE OneView Appliances:

   a. Log on as an opsa user.

   b. Run the following commands:

      i. `/etc/init.d/opsa-loader stop`

      ii. `/etc/init.d/opsa-process-manager stop`

      iii. `/etc/init.d/opsa-server stop`

      iv. `/etc/init.d/opsa-collector stop`

   Wait a minimum of ten minutes for all processes to stop and for any intermediate collection data to be written to the database.

4. Run the following command as the root user to stop the Syslog Daemon Smart Connector on the version 2.30 Operations Analytics All-in-One for HPE OneView Appliance: `/etc/init.d/arc_syslog stop`

5. Do the following on both the Operations Analytics 2.30 and 2.31 Operations Analytics All-in-One for HPE OneView Appliances to configure the absolute IP address rather than the loopback IP address:

   a. Log on as a opsa user.

   b. Run the following command to become the root user: `su -`

   c. Run the following command to become the Linux dbadmin user: `su - dbadmin`

   d. Run the `/opt/vertica/bin/adminTools` command.

   e. To shut down the Vertica database, do the following:

     i.   From the Main Menu, select **Advanced Menu**.

     ii.   Select **option 2: Stop Vertica on Host**.

     iii.   From the **Select Host(s)** window, select the **host** box; then click **OK**.

     iv.   When prompted about whether you are sure you want to stop Vertica, click **yes**.

     v.   From the **Main** Menu, select **View Database Cluster State** to make sure that Vertica is shut down.

  f. Log on as the root user.

  g. Run the following command: `/opt/HP/opsa/scripts/ScaleOut.sh SETVERTICAROOT`.

  h. Specify the absolute DNS IP address of the Operations Analytics All-in-One for HPE OneView Appliance.

> **Note:** By default the 127.0.0.1 loopback IP address is used by Vertica on the Operations Analytics All-in-One for HPE OneView Appliance. Do not use that address, because it will not work for exporting data.

    Wait for the script to finish.

  i. Log on as the Linux dbadmin user on both the Operations Analytics 2.2 and 2.3 Operations Analytics All-in-One for HPE OneView Appliances:

     i.   Log on as an opsa user.

     ii.   Run the following command to become the root user: `su -`

     iii.   Run the following command to become the Linux dbadmin user: `su - dbadmin`

  j. Do the following on both the Operations Analytics 2.30 and 2.31 Operations Analytics All-in-One for HPE OneView Appliances to start each database:

     i.   Run the `/opt/vertica/bin/adminTools` command.

     ii.   Start the database.

6. To export the data from the version 2.30 Operations Analytics All-in-One for HPE OneView Appliance to the version 2.31 Operations Analytics All-in-One for HPE OneView Appliance, do the following from the version 2.30 Operations Analytics All-in-One for HPE OneView Appliance:

  a. Create an executable script, `script.sh`, that contains the following commands:

```
#!/bin/sh
column_names=`vsql -c "select column_name from columns where table_schema='$5'
and table_name='$6'" -d opsadb -w $4 -t | awk -vORS=, '{ print $1}' | sed
's/\,,$//'`
connect_cmd_to_run="connect to vertica opsadb user dbadmin password '$3' on '$1',
$2;"
export_cmd_to_run="export to vertica opsadb.$5.$6 ($column_names) from $5.$6
($column_names);"
disconnect_cmd_to_run="disconnect opsadb;"
echo "Connecting to destination database opsadb on $1 at port $2 and running
export";
echo $export_cmd_to_run;
vsql -d opsadb -w $4 -c "$connect_cmd_to_run$export_cmd_to_run$disconnect_cmd_to_
run";
```

  b. Run the following script as the Linux dbadmin user on the version 2.30 Operations Analytics All-in-One for HPE OneView Appliance for each table value shown below. Substitute one table value each time you run the command. Use the table values in the order they appear below:

```
script.sh <destination version 2.31 database IP Address> <destination version
```

*2.30 database port> <destination version 2.31 database password> <source version
2.30 database password>* opsa_default *<table name>*

For example, to export the `arcsight_log_stream table` values using default passwords for the dbadmin database user on both the source and destination databases, and using 5433 as the default port, the command would look like this: `./script.sh` *<destination version 2.31 database IP Address>* `5433 dbadmin dbadmin opsa_default arcsight_log_stream`

List of opsa_default schema table values:
```
oneview_rabbitmq_alerts
oneview_rabbitmq_metrics
oneview_rest_inventory
oneview_rabbitmq_inventory_update
oneview_rest_topologytree
oneview_rest_interconnect_metrics
arcsight_oneview_oneviewsyslogs
la_metrics
la_user_classification
la_cluster_frequency
la_samples_queue
la_metric_management
la_user_searches
la_custom_searches
la_parameter_values
la_parameter_functions
arcsight_log_stream
la_cluster_ranking
la_cluster_distribution
la_multiplier
la_problem_cause_properties
la_problem_cause
la_technologies
la_unique_msg
la_cluster_parameter
la_clustered_msg
```

c. Run the following script as the Linux dbadmin user on the version 2.30 Operations Analytics All-in-One for HPE OneView Appliance for each a table value shown below. Substitute one table value each time you run the command. Use the table values in the order they appear below:

`script.sh` *<destination version 2.31 database IP Address> <destination version 2.31 database port> <destination version 2.31 database password> <source version 2.30 database password>* opsa_admin *<table name>*

For example, to export the `arcsight_log_stream table` values using default passwords for the Vertica dbadmin database user on both the source and destination databases, and using 5433 as the default port, the command would look like this: `./script.sh` *<destination version 2.31 database host name>* `5433 dbadmin dbadmin opsa_admin la_log_level`

List of opsa_admin schema table values:
```
la_log_level
la_ootb_searches
la_user_defined_problem_events
```

7. Do the following on both the version 2.30 and 2.31 Operations Analytics All-in-One for HPE OneView

Appliances to start the Operations Analytics processes:

a. Login as an opsa user.

b. Run the following command: `opsa-process-manager.sh start`

c. Wait five minutes for all of the Operations Analytics processes to start up.

8. To export and import custom dashboards, do the following:

a. From the version 2.30 Operations Analytics All-in-One for HPE OneView Appliance, log on as an opsa user.

b. For every custom dashboard that you developed, run the following command:
`opsa-dashboard-manager.sh -u <dashboard creation user> -e "<dashboard name>" -f <export_file_name_with_path>`

c. As an opsa user, remote copy the exported files to the version 2.30 Operations Analytics All-in-One for HPE OneView Appliance.

d. Log on to the version 2.31 Operations Analytics All-in-One for HPE OneView Appliance as an opsa user and run the following command for every exported file to import them into the version 2.31 Operations Analytics All-in-One for HPE OneView Appliance:

`opsa-dashboard-manager.sh -u <As user> -i -f <export_file_name_with_path>`

e. From the version 2.31 Operations Analytics All-in-One for HPE OneView Appliance server, run the following command as the opsa user to restart the Operations Analytics processes:

`opsa-server restart`

> **Note:** After running an `opsa-server restart` command, information logged in the `/opt/HP/opsa/log/opsa-server.log` file is removed. To view the files that retain this information across restarts, see the log files located in the `/opt/HP/opsa/jboss/standalone/log` directory. Look for log file names that begin with `server.log`.

9. The approach for this step is to connect the Logger instance from the version 2.30 Operations Analytics All-in-One for HPE OneView Appliance to the version 2.31 Operations Analytics All-in-One for HPE OneView Appliance in parallel with the Logger instance already running on the version 2.31 Operations Analytics All-in-One for HPE OneView Appliance.

Using this approach, when you search for raw logs using the Operations Analytics 2.31, the results will include raw logs from both of the following:

- The version 2.30 Operations Analytics All-in-One for HPE OneView Appliance Logger (all the logs collected during the time the you were running Operations Analytics 2.30)

- The version 2.31 Operations Analytics All-in-One for HPE OneView Appliance Logger (the logs collected after you provisioned Operations Analytics 2.31).

You can keep the version 2.30 Operations Analytics All-in-One for HPE OneView Appliance Logger instance connected until the time you no longer want to retain the logs collected from Operations Analytics 2.30. When you no longer need the logs you are collecting from Operations Analytics 2.30, disconnect the version 2.30 Operations Analytics All-in-One for HPE OneView Appliance Logger from the version 2.31 Operations Analytics All-in-One for HPE OneView Appliance.

To migrate Logger data from a version 2.30 Operations Analytics All-in-One for HPE OneView Appliance to a version 2.31 Operations Analytics All-in-One for HPE OneView Appliance, complete the following steps.

> **Note:** Replace the passwords as appropriate in the following commands.

a. To connect the Logger running on Operations Analytics 2.30 to the version 2.31 Operations Analytics All-in-One for HPE OneView Appliance, do the following:

   i. Log on to the version 2.31 Operations Analytics All-in-One for HPE OneView Appliance as the opsa user.

   ii. Run the following command:

   ```
   opsa-log-integration-config.sh -loginUser <tenantadmin1> -loginPassword
   <tenantadmin1Pwd> -add -host <fully-qualified domain name of loggerhost1> -
   collectorHost <fully-qualified domain name of Collector host> -username
   <loggeruser1> -loggerType arcsight -password <loggeruser1pwd> -port 443 -
   sslEnabled true -base64Decode true -allFields true -tcpMode passive
   ```

b. To disconnect the Logger running on Operations Analytics 2.30 from the version 2.30 Operations Analytics All-in-One for HPE OneView Appliance, do the following:

   i. Log on to the version 2.31 Operations Analytics All-in-One for HPE OneView Appliance as the opsa user.

   ii. Run the following command:

   ```
   opsa-log-integration-config.sh -loginUser <tenantadmin1> -loginPassword
   <tenantadmin1Pwd> -delete -host <fully-qualified domain name of Logger host>
   -collectorHost <fully-qualified domain name of Collector host> -loggerType
   arcsight -base64Decode true
   ```

c. To test that you successfully connected and disconnected the Logger running on Operations Analytics 2.30, run the following command on the version 2.31 Operations Analytics All-in-One for HPE OneView Appliance as the opsa user:

   ```
   opsa-log-integration-config.sh -list -loginUser opsatenantadmin -loginPassword
   opsatenantadmin
   ```

10. To migrate the HPE OneView configuration from a version 2.30 Operations Analytics All-in-One for HPE OneView Appliance to a version 2.31 Operations Analytics All-in-One for HPE OneView Appliance, do the following:

   a. Point your browser to the version 2.31 Operations Analytics All-in-One for HPE OneView Appliance by entering the following URL: **http://<Operations Analytics2.31 VM>:8080/opsa**; then log on as the opsatenantadmin user.

   b. Click the **Settings** button on the top right; then select **Oneview Settings**:

      i. In the resulting dialog, supply the `HPE OneView hostname`, `HPE OneView username`, `HPE OneView password`, and `polling frequency` as specified in the version 2.30 Operations Analytics All-in-One for HPE OneView Appliance.

      ii. Click **Integrate** and wait for a **Success** message to appear.

      iii. Close the dialog.

This completes the migration of the version 2.30 Operations Analytics All-in-One for HPE OneView Appliance to a version 2.31 Operations Analytics All-in-One for HPE OneView Appliance.

Rollback

If at any point if you want to revert back to the original version 2.30 Operations Analytics All-in-One for HPE OneView Appliance or version 2.31 Operations Analytics All-in-One for HPE OneView Appliance, revert back to the snapshot you took earlier in "Preparing for a potential rollback: " on page 44

Chapter 8: Upgrading an HPE Distributed Operations Analytics for HPE OneView to a Newer Version

To upgrade version 2.30 Operations Analytics All-in-One for HPE OneView Appliance distributed servers to version 2.31 Operations Analytics All-in-One for HPE OneView Appliance distributed servers, do the following:

1. Follow the steps specified in the *Operations Analytics 2.30 to 2.31 Upgrade Guide* (for Operations Analytics version 2.31) to upgrade the Operations Analytics All-in-One for HPE OneView Appliance distributed servers to version 2.31.

2. Do the following to integrate the new version 2.31 HPE OneView setup with the HPE OneView server:

   a. Point your browser to the Operations Analytics 2.31 by typing the following URL:
      http://<*opsa2.31 server vm*>:8080/opsa; then log on as the opsatenantadmin user.

   b. Click the **Settings** button on the top right; then select **Oneview Settings**:

      i. In the resulting dialog, supply the `HPE OneView hostname`, `HPE OneView username`, `HPE OneView password`, and `polling frequency` as specified in the version 2.30 Operations Analytics All-in-One for HPE OneView Appliance.

      ii. Click **Integrate** and wait for a **Success** message to appear.

      iii. Close the dialog.

This completes the upgrade of a version 2.30 Operations Analytics All-in-One for HPE OneView Appliance distributed server to a version 2.31 Operations Analytics All-in-One for HPE OneView Appliance distributed server.

Chapter 9: Maintenance Tasks

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

Backing up and Restoring Data

To back up data for the Operations Analytics All-in-One for HPE OneView Appliance, make it a practice to take regular snapshots. You can use a snapshot if you experience a need to recover your data.

Changing the HPE OneView Server

To change the HPE OneView server used by Operations Analytics, do the following:

1. Run the following command to *unregister* the Operations Analytics All-in-One for HPE OneView Appliance collections: `/opt/HP/opsa/support/publishOneViewCollections.sh UNREGISTER` `<collector fully-qualified domain name> <opsaTenantAdminUser>` `<opsaTenantAdminPasswd>`

   > **Note:** publishOneViewCollections.sh is an unsupported script used for troubleshooting and support purposes.

   This script can run for 30 minutes or more. You must wait until the script completes to continue.

2. Configure the Operations Analytics - HPE OneView integration using information about the new HPE OneView server by following the instructions at "Configuring the HPE Operations Analytics - HPE OneView Integration" on page 21.

Restarting Operations Analytics Processes

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

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

1. Do the following to verify that the Vertica database is running.

   a. Run the `opsa-db status` command as the root user.

      > **Note:** Supply the dbadmin user's password when prompted. Typically the password is dbadmin.

   b. If the Vertica database is up, you should see a message that states that the database is up.

If the database is not up, wait a few minutes, then rerun the `opsa-db status` command.

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

2. Do the following to start the Operations Analytics processes:

   a. Run the `opsa start` command.

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

   c. If the Operations Analytics console is not accessible, run the `service opsa-server restart` command to reboot the Operations Analytics All-in-One for HPE OneView Appliance.

   > **Note:** After running an `opsa-server restart` command, information logged in the `/opt/HP/opsa/log/opsa-server.log` file is removed. To view the files that retain this information across restarts, see the log files located in the `/opt/HP/opsa/jboss/standalone/log` directory. Look for log file names that begin with `server.log`.

Chapter 10: Operations Analytics Security Hardening

The information in this sections summarizes the security hardening recommendations for the Operations Analytics All-in-One for HPE OneView Appliance.

Miscellaneous Security Recommendations

Anti-virus Software

The Operations Analytics All-in-One for HPE OneView Appliance is compliant with your anti-virus software. Use your preferred anti-virus software.

It is recommended that you scan the following folders:

- The path to the folder containing scripts: `/opt/HP/opsa/scripts`
- The path to the folder containing alerts scripts: `/opt/HP/opsa/inventory/lib/user/alerts/`
- The path to the folder you use for uploading files. For example, you might upload files to the `/opt/HP/opsa/data` folder.

Disabling Unnecessary CentOS Services

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

- It is highly recommended that you disable the SSH weak ciphers. To do this, the configuration entries already reside in the `sshd_config` file and need to be uncommented as follows:

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

  a. As the root user, edit the `sshd_config` file.
  b. To uncomment the following two lines, change:
     ```
     # Ciphers aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc
     # MACs hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160
     ```
     to
     ```
     Ciphers aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc
      MACs hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160
     ```
  c. Save your work.
  d. As a root user, run the following command to commit your changes: `service sshd restart`

Arcsight Logger Security Recommendations

As a minimum requirement, run Arcsight Logger at the application level privilege.

> **Note:** When creating a user, assign the least amount of privileges needed for the user to perform that user's tasks

Avoid co-locating Logger with another software application.

Minimize the number of operating system level users. If passwords are used, you must implement hard-to-guess passwords. When creating hard-to-guess passwords, combine length with complexity to make the passwords difficult to guess or compromise using forceful methods. At a minimum, use long passwords when complexity cannot be used.

To mitigate the risk of exposing the authentication token cookie in case of a client side attack, do the following:

- Set the inactivity timeout to a short duration.

  > **Note:** The default value for Logger is 15 minutes.

- Explicitly log out of Logger.
- Do not click links in emails or browse the web in the same browser being used to view Logger.
- Log on to Logger as a user that has only the necessary privileges.

  > **Note:** Do not log on as a user having administrator privileges.

To reduce the attack surface, do the following:

- Configure the firewall to permit only the following ports for inbound Traffic
  - TCP port 9000

  - TCP port 22

    > **Note:** ssh is not required byLogger, however it is useful for troubleshooting purposes.

- Limit the outbound traffic to the following ports:
  - TCP port 22

    > **Note:** This port is used for backups, however a user can specify a different port (that should be configured to be open in the firewall).

  - TCP port 25

    > **Note:** Used for SMTP.

  - TCP port 9000

    > **Note:** Used for communicating with other Loggers(for peering).

  - UDP and TCP port 53

    > **Note:** Used for DNS.

- UDP port 123

  Note: Used for NTP.

- If possible, filter on source IP addresses.

Do the following for ongoing Logger maintenance:

- Install operating system and application security fixes diligently.
- Carefully monitor log files and audit logs.
- Consider performing file integrity checks

  Note: For example use software applications such as Tripwire to perform file integrity checks.

Send Documentation Feedback

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

Feedback on HPE Operations Analytics for HPE OneView Installation, Integration, and Upgrade Guide (Operations Analytics 2.32)

Just add your feedback to the email and click send.

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

We appreciate your feedback!