HP Operations Analytics

Software Version: 2.20

HP Operations Analytics for HP OneView Installation Guide

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

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

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

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

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

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

Support

Visit the HP Software Support web site at: **https://softwaresupport.hp.com**

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

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

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to **https://softwaresupport.hp.com** and click **Register**.

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

HP Software Solutions & Integrations and Best Practices

Visit HP Software Solutions Now at **https://h20230.www2.hp.com/sc/solutions/index.jsp** to explore how the products in the HP Software catalog work together, exchange information, and solve business needs.

Visit the Cross Portfolio Best Practices Library at **https://hpln.hp.com/group/best-practices-hpsw** to access a wide variety of best practice documents and materials.

Contents

Chapter 1: Prerequisites

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

Management Environment

This document provides information about setting up the Operations Analytics for HP OneView Appliance and enabling the integration between Operations Analytics and HP OneView. It provides additional information about how to expand the Operations Analytics for HP OneView Appliance to a distributed environment if the need arises.

The Operations Analytics for HP 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:** TheOperations Analytics for HP OneView Appliance does not support the configuration of other types of collections. Only Operations Analytics for HP OneView Appliance collections that are configured as explained in the HP Operations Analytics - HP OneView Integration Guide are supported.

For larger environments, you must scale out your Operations Analytics for HP OneView Appliance to a distributed environment. For example, for larger environments, you must configure collections on a separate Operations Analytics Collector Appliance. To expand this Operations Analytics for HP OneView Appliance to a distributed environment, complete the tasks shown in "Expanding to a Distributed Operations Analytics " on page 18.

System Requirements

The Operations Analytics for HP 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.This document refers to this appliance as the Operations Analytics for HP OneView Appliance for the remainder of this document. To deploy the Operations Analytics for HP 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 for HP 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 for the IP address.

Note: The system clocks and time zones for the HP OneView server and the Operations Analytics for HP OneView Appliance must be synchronized.

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

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

Known Issues and Workarounds

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

Chapter 2: Setting up the HP Operations Analytics for HP OneView Appliance

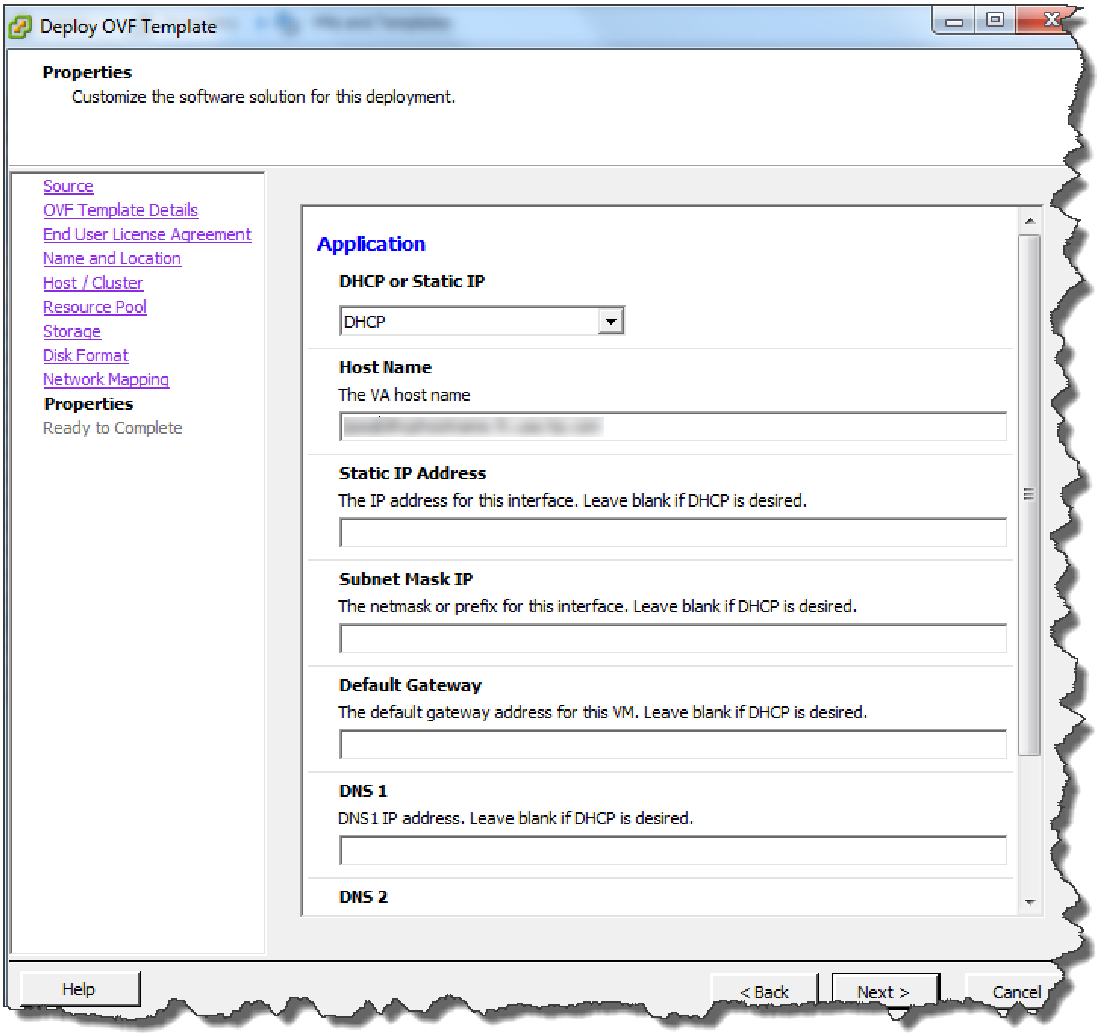
Follow the instructions in this section to deploy, power on, and test the Operations Analytics for HP OneView Appliance.

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

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

1. Log on to the VMware ESX or VMware workstation.
2. Select **File** -> **Deploy OVF Template**.
3. Enter the URL or the file path of the `HP_Opsa_AllinOne_OVF10.ova` file, based on where the OVA file is located; then click **Next**.
4. Specify a name and location for the deployed template.
5. Follow the instructions to select the host or cluster on which you want to deploy the Server Appliance; then click **Next**.
6. Select a resource pool.
7. Select the destination storage for the Server Appliance files; then click **Next**.

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



Properties

Customize the software solution for this deployment.

Application

DHCP or Static IP

DHCP

Host Name

The VA host name

[redacted]

Static IP Address

The IP address for this interface. Leave blank if DHCP is desired.

Subnet Mask IP

The netmask or prefix for this interface. Leave blank if DHCP is desired.

Default Gateway

The default gateway address for this VM. Leave blank if DHCP is desired.

DNS 1

DNS1 IP address. Leave blank if DHCP is desired.

DNS 2

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

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

> **Note:** You can configure the Operations Analytics for HP 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 for HP 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 for HP 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.

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

11. Click **Finish**.

12. 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 HP OneView Appliance or Operations Analytics for HP OneView Appliance: A self-contained system that combines the Operations Analytics Server Appliance, Collector Appliance, Vertica Database, and the HP 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 HP ArcSight Logger.

Default Tenant: This Operations Analytics for HP OneView Appliance document uses the default Tenant, opsa_default and its corresponding default tenant username (opsatenantadmin) and password (opsatenantadmin). The Operations Analytics for HP 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-6.1.3-12.x86_64.RHEL5.rpm for the Vertica installation and vertica-R-lang-6.1.3-12.x86_64.RHEL5.rpm for the R Language Pack from Vertica. Use these packages for optimum Vertica performance.

Configure the Vertica database server with a `MAXMEMORYSIZE` of 50% of the machine’s RAM as follows (using a 24GB RAM machine):

1. Log on to the Vertica server (using SSH) as a dbadmin user.

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

2. Enter the following command to access the SQL console: `dbadmin$>VSQL`
3. Enter the following command from the SQL console: `ALTER RESOURCE POOL general MAXMEMORYSIZE '12G';`
4. Exit the VSQL console using the following sequence:
   a. `\q`
   b. `Enter`
5. Restart the Vertica database by running `/opt/vertica/bin/admintools` and restarting the opsadb database.
6. Run the `$OPSA_HOME/bin/opsa-server restart` command on the Operations Analytics for HP OneView Appliance for the changes to take effect.

Configuring SSL for the Operations Analytics for HP OneView Appliance

> **Note:** Completing the steps shown in this section is not mandatory. If you prefer not to enable SSL communication to the Operations Analytics for HP OneView Appliance, skip this section and continue with "Licensing the Operations Analytics for HP OneView Appliance" on page 15.

Use the information in this section to manage SSL on the Operations Analytics for HP OneView Appliance.

One-way SSL provides secure communication between the web browser and the Operations Analytics for HP 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 Operations Analytics for HP OneView Appliance

Complete the following steps to enable SSL communication to the Operations Analytics for HP OneView Appliance using a CA signed certificate:

1. Before enabling SSL to the Operations Analytics for HP 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.

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 Operations Analtyics server keystore. The `opsa-server-manager.sh` script prompts you for the certificate alias name and lists a set of used aliases.. Enter a unique alias name that has not been used.

   > **Note:** The administrator can get a CA signed certificate by generating a Certificate Signing Request file using the self-signed certificate stored in OPSA keystore. Submit this Certificate Signing Request to a Certificate Authority. To generate a Certificate Signing Request from a self-signed certificate, select the **Generate certificate signing request option** .The `opsa-server-manager.sh` script prompts you for the alias of the self-signed certificate. Enter `opsa_server` from the list of aliases to generate Certificate Signing Request for a self-signed certificate.

5. Optional: Select the **Import trusted certificate to OPSA server truststore** option to import trusted certificates (if any). For example, you can add HP ArcSight Logger's server certificate to

the OPSA truststore file.

6. Select the **Enable/Disable SSL** option to enable SSL. You will need to enter the JBoss **Management Realm** user and password you created in the first step.The `opsa-server-manager.sh` script prompts you for the certificate alias to be used for SSL communication. Enter one of the aliases from the listed aliases.

7. Select the **Go back to main menu** option; then select the **Restart OPSA server** option to restart the Operations Analytics Server Appliance.

   > **Note:** Your configuration changes will not occur unless the server is restarted.

8. Operations Analytics users can access the Operations Analytics console using HTTP or HTTPS.

   > **Note:** If a user attempts to use HTTP when HTTPS is configured, the user will automatically be redirected using HTTPS.

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

Configuring SSL with a Self-Signed Certificate for the Operations Analytics for HP OneView Appliance

Complete the following steps to enable SSL communication to the Operations Analytics for HP OneView Appliance using a self-signed certificate:

1. Before enabling SSL to the Operations Analtyics 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.

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 Analtyics server keystore.

   > **Note:** The `opsa-server-manager.sh` script stores the self-signed certificate in the `keystore` file with the `opsa_server` alias name.

   > **Note:** Set the self-signed certificate attributes, such as `common name`, `country`, and `validity` by editing the `/opt/HP/opsa/conf/ssl/cert/opsa-self-signed-cert.template` file.

5. Optional: Select the **Import trusted certificate to OPSA server truststore** option to import trusted certificates (if any). For example, you can add HP ArcSight Logger's server certificate to the OPSA truststore file.

6. Select the **Enable/Disable SSL** option to enable SSL. You will need to enter the JBoss **Management Realm** user and password you created in the first step.The `opsa-server-manager.sh` script prompts you for the certificate alias to be used for SSL communication. Enter one of the aliases from the listed aliases.

7. Select the **Enable/Disable SSL** option to enable SSL. The `opsa-server-manager.sh` script prompts you for the certificate alias to be used for SSL communication. Enter `opsa_server`.

   > **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 Analtyics Server Appliance..

   > **Note:** Your configuration changes will not occur unless the server is restarted.

9. Operations Analtyics 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 Operations Analytics for HP OneView Appliance

The Operations Analytics for HP OneView Appliance comes with an Implicit node pack (Instant On) license that is valid for 60 days.To view the existing Operations Analytics license, navigate to **Help** > **About**> **License** from the Operations Analytics console. See *Licensing HP OneView* in the HP Operations Analytics - HP OneVew Integration Guide for more information.

Review the following environment considerations:

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

- Considering the HP OneViewcustomer, each HP OneViewapplication server manages 640 HP server + X number of other objects (interconnect, devices, power devices, and other objects) for an approximate total of 1024 objects.
- If an HP OneView customer environment contains more than 1024 objects to be managed, they will need more than one HP OneView application server.
- One Operations Analytics for HP OneView deployment integrates with a single HP OneView application server.
- An Operations Analytics for HP OneView deployment could be one of the following, depending on the above environment considerations:
  - A single Operations Analytics for HP 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 HP Operations Analytics Installation Guide for more information.

Testing the Operations Analytics for HP OneView Appliance

Complete the following steps to test the Operations Analytics for HP OneView Appliance.

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

1. Set up the Operations Analytics for HP OneView Appliance.

2. Take a snapshot of the Operations Analytics for HP OneView Appliance.

3. Using SSH, log on to the Operations Analytics for HP OneView Appliance.

4. When prompted, change the Operations Analytics for HP OneView Appliance password, and note the new password.

   > **Note:** When logging on to the Operations Analytics for HP OneView Appliance for the first time, use one of the following authentication credentials:
   > User: `opsa`
   > Password: `opsa`
   > User: `root`
   > Password: `iso*help`

5. Do the following to check the status of the Operations Analytics for HP 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 HP 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 HP Operations Analytics - HP OneView Integration

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

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

To integrate Operations Analytics with HP OneView, follow the instructions shown in the HP Operations Analytics - HP OneView Integration Guide.

Chapter 4: Expanding to a Distributed Operations Analytics

After installing, configuring, and using the features of the Operations Analytics for HP OneView Appliance, you might decide to expand it into a distributed version of Operations Analytics.

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 for HP OneView Appliance collections as well as the predefined Operations Analtyics collections from the Operations Analytics for HP OneView Appliance. You must *unregister* the registration for the Collector as well.

> **Note:** You will re-register all of the mentioned items during "Task 7: Adding a New Operations Analytics Server" on page 26

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

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

   > **Note:** If you receive an error message that reports a problem with removing the registration for this collection configuration, ignore the error and continue with the next step.

2. Run the following command to *unregister* the Operations Analytics for HP OneView Appliance Logger collection.

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

3. 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> -port 9443 -username <opsaTenantAdminUser> -
   password <opsaTenantAdminPasswd> –source oa -domain sysperf -group global
   ```

4. Run the following command to *unregister* the Operations Analytics for HP OneView Appliance collector: `/opt/HP/opsa/bin/opsa-collection-config.sh -unregister -collectorhost <fully-qualified domain name of collector host> -username <opsaTenantAdminUser> -password <opsaTenantAdminPasswd>`

5. Run the following command to *unregister* the Operations Analytics for HP OneView Appliance Logger:

   ```
   /opt/HP/opsa/bin/opsa-logger-config-manager.sh -loginUser <opsaTenantAdminUser>
   -loginPassword Dbadmin$123 -delete -host <fully-qualified domain name of
   Loggerhost>
   ```

Task 2: Expanding the Operations Analytics for HP OneView Appliance

Carefully complete the following steps to expand your Operations Analytics for HP OneView Appliance into a distributed version that can use the integration with HP OneView:

To check if you have the Operations Analytics for HP 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 for HP 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 for HP OneView Appliance is configured for DHCP, and you need to 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 https://www.centos.org/docs/5/html/Deployment_Guide-en-US/s1-dhcp-configuring-client.html 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 need to 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 for HP 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.

   When using DHCP, Operations Analytics uses a standard ifcfg-eth0 file configuration that is recommended by CentOS.if your network configuration is different from the standard that described by the CentOs you might not be able to get on IP from the DHCP or access the VM using host name\fully-qualified domain name. For more details please see: https://www.centos.org/docs/5/html/Deployment_Guide-en-US/s1-dhcp-configuring-client.html

   > **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 for HP OneView Appliance terminates because the old IP address no longer exists. Log on to the Operations Analytics for HP 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 for HP OneView Appliance remotely using the new IP address for the Operations Analytics for HP OneView Appliance.

Task 3: Testing and Configuring the Network

Complete the following to make sure the network is configured correctly for the Operations Analytics for HP OneView Appliance:

1. Run the `nslookup <Operations Analytics for HP OneView Appliance IP address>` command and the `hostname` command on the Operations Analytics for HP 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 for HP OneView Appliance that you currently have installed, it totals four Vertica nodes in the Vertica Cluster. The Vertica license included on the Operations Analytics for HP 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 for HP 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 for HP 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`

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 AnalyticsAIO VM*> and then entering `yes` in the appropriate box.

6. Log on to the Operations Analytics for HP OneView Appliance as dbadmin (the default password is 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 for HP OneView Appliance to use the Operations Analytics for HP OneView Appliance's new or existing static IP address.

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

8. 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.

9. As the root user, run the `/opt/HP/opsa/scripts/ScaleOut.sh SETVERTICAROOT` command to configure Vertica to use the Operations Analytics for HP OneView Appliance's static IP address. Wait for the script to finish before proceeding.

10. Edit the following file as the dbadmin user: `/opt/vertica/config/vspread.conf` and do the following:

    a. Locate the line containing `Spread_Segment`.

    b. Change the text that looks something like `127.255.255.255:4803` to be `<NN.NN.NNN>.255:4803` where `<NN.NN.NNN>` represents the high order bytes of the <*Operations Analytics for HP OneView Appliance IP address*>

    c. Save your work.

11. 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 for HP OneView Appliance, it is recommended that you back up the Operations Analytics for HP OneView Appliance database. See the *Backing Up and Restoring* section of the *Vertica Administrator's Guide* for more information.

12. You must place a Vertica installable image (`vertica-6.1.3-12.x86_64.RHEL5.rpm`) on each virtual appliance. Copy that image from the `$OPSA_HOME/installation/rpm` directory located on the Operations Analytics for HP OneView Appliance.

13. Run the following command as a root user to stop the `spread` process on the Operations Analytics for HP OneView Appliance: `/etc/init.d/spreadd stop`

14. Run the following commands on the Operations Analytics for HP 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 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 for HP OneView Appliance and from each Vertica server to all other Vertica servers.

> **Note:** If the `ssh-copy-id` command is not available on a server, look for a copy of it at `/opt/HP/opsa/scripts` on the Operations Analytics AIO VM.

15. Turn off the firewall on the Operations Analytics for HP 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 for HP OneView Appliance and all for the new Vertica servers after completing this task by running the following command:
    > `service iptables start`

16. From a command prompt on the Operations Analytics for HP 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 for HP 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.

17. Install the R Language Pack from Vertica on each new virtual appliance using the instructions shown in the *Use an Existing Vertica Installation and use the R Language Pack from Vertica* section of the *Operations Analytics Installation Guide*.

18. From the Operations Analytics for HP OneView Appliance, do the following to add the new Vertica nodes to the database:
    a. Run `/opt/vertica/bin/admintools` as the 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 dbadmin user is dbadmin. You must click **OK** several times to complete this step.

19. 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 HP Vertica to immediately start rebalancing the database.

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

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

21. Do the following to remove the Operations Analytics for HP 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 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 HP OneView AIO VM

    Vertica will go through another rebalancing process, then remove the HP 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 using the *Installing the Out of the Box SmartConnectors* instructions in the *Operations Analytics Installation Guide*. Run the installation on the SmartConnector and select the **SysLog Daemon**.

   > **Note:** You must point the SysLog Daemon to the SmartMessageReceiver.

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

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

6. 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 Server 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 for HP OneView Appliance to the Operations Analytics Server Appliance. Do the following from the Operations Analytics for HP 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`

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-logger-config-manager.sh -add -host fully-qualified
domain name of Logger -username admin -password <password> -loginUser <tenant
username> -loginPassword <tenant user password> -loggerType arcsight -port 443
-sslEnabled true
```

8. You must register all of the original collections on the new Operations Analytics Server Appliance using the following command: `/opt/hp/opsa/scripts/publishOneViewCollections.sh PUBLISH <ovHOst> <ovUser> <ovPw> <collectorIP> <loggerIP> <opsaTenantAdminUser> <opsaTenantAdminPasswd> 3600`

   > **Note:** Review the following information before using the publishOneViewCollections.sh script:
   >
   > - `PUBLISH` is a keyword.
   > - *ovHost*, *ovUser*, and *ovPw* are the HP OneView credentials used when enabling the Operations Analytics - HP OneView integration from the Operations Analytics welcome page.
   > - The *collectorIP* is the hostname of the original Operations Analytics for HP 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).
   >
   >   See the *publishOneViewCollections.sh* reference page (or the Linux manpage) for more information.

9. Do the following to publish the collection.

   a. Copy the `/opt/HP/opsa/conf/collection/server/config.templates/arcsight/1.0/OneView` directory from the Operations Analytics for HP OneView Appliance to the new Operations Analytics Server Appliance.

   > **Note:** This folder contains the structured log template to use in a later step.

   > **Note:** The `OneView` directory is not present on the new Operations Analytics Server Appliance, so that directory and the rest of the structure beneath it must be copied to the new Operations Analytics Server Appliance.

   b. Keep the owner, group, and permissions the same on the new Operations Analytics Server

Appliance.

c. Edit the `/opt/HP/opsa/content-packs/oneview/logger/structured_log_collection/OneviewSyslogNodeList.properties` file.

d. Look for a string the resembles the following:

   ```
   ## node properties for 'Arcsight'
   arcsightserver.hostdnsname=localhost
   ```

   Change the `localhost` to the fully-qualified domain name of the new Logger server.

   Save your work.

e. Run the following command from the Operations Analytics Server Appliance to create the collection:

   ```
   opsa-collection-config.sh -create -collectorhost <IP Address of collector> -
   nodelist /opt/HP/opsa/content-packs/oneview/logger/structured_log_
   collection/OneviewSyslogNodeList.properties -source arcsight -domain OneView
   -group OneViewSyslogs -username <opsaTenantAdminUser> -password
   <opsaTenantAdminPasswd>
   ```

   > **Note:** Be sure to specify the value of <*IP Address of collector*> as you did in previous steps.

f. Run the following command Operations Analytics Server Appliance to publish the collection:

   ```
   opsa-collection-config.sh -publish –collectorhost <collectorhost> -username
   <opsaTenantAdminUser> -password <opsaTenantAdminPasswd>
   ```

Congratulations, you finished converting your Operations Analytics for HP OneView Appliance into a distributed version of Operations Analytics.

Chapter 5: Configuring Collections

After you have expanded the Operations Analytics for HP 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 - HP 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:

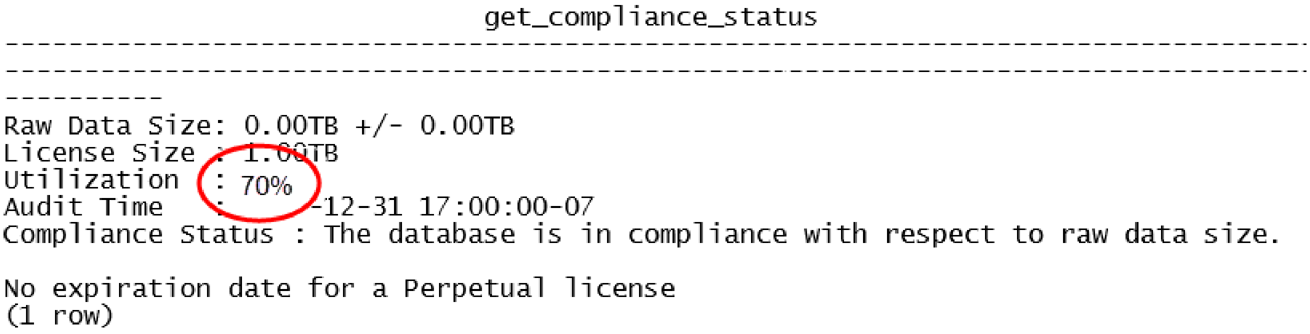
1. Log on to the Vertica server as a `root` or `dbadmin` user.

   > **Note:** The default dbadmin password is dbadmin.

2. 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.

3. 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 for HP 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 Analtyics 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: Maintenance Tasks

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

Restarting Operations Analytics Processes

There are times when the Operations Analytics for HP OneView Appliance might abruptly shut down, as in during a power outage, network issue, or other unintended shutdown. For the Operations Analtyics 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.

   > **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 shows a column and the value `1` in it.
   If the database is not up, an error message appears. If an error message appears, 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-process-manager.sh start` command.

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

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

Chapter 8: Operations Analytics Security Hardening

The information in this sections summarizes the security hardening recommendations for the Operations Analytics for HP OneView Appliance.

Miscellaneous Security Recommendations

Anti-virus Software

The Operations Analytics for HP 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.

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 HP Operations Analytics for HP OneView Installation Guide (Operations Analytics 2.20)

Just add your feedback to the email and click send.

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

We appreciate your feedback!