

HP Operations Agent

Software Version: 11.16

Linux, HP-UX, Solaris, AIX, and Windows® operating systems

User Guide: VMware Monitoring

Document Release Date: March 2017
Software Release Date: March 2017



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

© Copyright 2012-2017 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

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>

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

<https://hpp12.passport.hp.com/hppcf/createuser.do>

Or click the **the Register** link at the top of the HP Software Support page.

You will also receive updated or new editions if you subscribe to the appropriate product support service.

Contact your HP sales representative for details.

Support

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

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

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

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts

- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

<https://hpp12.passport.hp.com/hppcf/createuser.do>

To find more information about access levels, go to:

<https://softwaresupport.hp.com/web/softwaresupport/access-levels>

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is

<http://h20230.www2.hp.com/sc/solutions/index.jsp>

Contents

Chapter 1: Monitoring VMware vSphere Environments	6
Additional Benefits of Using the HP Operations Agent on the Virtual Appliance	6
Chapter 2: Monitoring vSphere Environments with the HP Operations Agent Virtual Appliance	7
Default Configuration of the HP Operations Agent Virtual Appliance	7
Deploying the Virtual Appliance with the HP Operations Agent	7
Deploying from the vSphere Console	8
Deploying from the Command Line	8
Verification	9
Ports Available with HP Operations Agent Virtual Appliance	10
Steps After Deployment	10
Enable Additional License	10
Configuring the HP Operations Agent with the HP Operations Agent Virtual Appliance Web Console	11
Configuring the HP Operations Agent from the Command Line	11
Configuring the HP Operations Agent on the Virtual Appliance to Use a Different Management Server	12
Delete the Data Manually	13
vCenter Events	13
Using the HP Operations Agent Virtual Appliance Web Console	14
Configure the HP Operations Agent on the Virtual Appliance	14
Configure Automatic Purging of Data	15
Modify the Collection Frequency of the HP Operations Agent	16
Configure Automatic Data Purging from the Command Line	16
Monitoring vCenters with the HP Operations Agent on the Virtual Appliance	17
Configuring Logging Levels for the status.viserver File	19
Configure Cluster Filtering	20
Adding the Cluster List in opsagt.viserver	20
Using the Command Line	21
Configure Collection Level	21
Adding the Collection Level in opsagt.viserver	21
Using the Command Line	22
Chapter 3: Downloading the Virtual Appliance with the Operations Agent	23

Version 11.16 24

Chapter 4: Deploying the Virtual Appliance with HP Operations agent Version 11.12 24

 Deploying the Virtual Appliance 11.12 from the vSphere Console 24

 Deploying the Virtual Appliance 11.12 from the Command Line 24

Chapter 5: Monitoring the vSphere Environment with vMA 25

 Installing the HP Operations Agent on a vMA 25

 Prerequisites 25

 Installation 25

 Configuring Data Collection on vMA Nodes 26

 viserver.properties 26

 Monitoring with the HP Operations Agent on vMA 27

Chapter 6: Troubleshooting 28

 The VI-Discovery Policy Fails to Discover vCenters 28

 The cpsv, padv, and mpadv Utilities Cannot Access the Complete Data Set 28

 Troubleshooting with Policies 28

Appendix A: Reference Page 30

 Support Tools 30

 easyoa 30

 oava_data_collector.sh 32

 oava_inst_report.sh 32

 oava_list_events.sh 32

 oava_dump_metrics.sh 32

Appendix B: RPMs Packaged with the HP Operations Agent Virtual Appliance 34

Appendix C: vCenter Events 41

Appendix D: Performance Metrics Collected from the HP Operations Agent Virtual Appliance 42

Send Documentation Feedback 43

Chapter 1: Monitoring VMware vSphere Environments

The HP Operations agent gives you the following options to monitor a VMware vSphere environment:

- **Monitoring with a virtual appliance**

The virtual appliance packaged with the *HP Operations Agent and Infrastructure SPIs 11.13* media contains a preinstalled and preconfigured HP Operations agent 11.16. The HP Operations agent on the virtual appliance can collect performance data directly from vCenter Servers. The HP Operations agent on the virtual appliance provides additional benefits like a robust data store and the capability to collect entity details and can monitor an environment with up to 2000 entities.

- **Monitoring with vSphere Management Assistant (vMA)**

The HP Operations agent installed on a vMA can monitor the environment by collecting the performance data from individual ESX/ESXi hosts. This type of monitoring requires you to manually install and configure the HP Operations agent on the vMA.

Additional Benefits of Using the HP Operations Agent on the Virtual Appliance

A major benefit of choosing the virtual appliance instead of monitoring through a vMA is the ease of installation and configuration. The HP Operations agent virtual appliance packaged with the HP Operations Agent and Infrastructure SPIs 11.13 media contains a preinstalled and preconfigured agent, and therefore, eliminates the need of installing the agent manually.

The HP Operations agent packaged with the virtual appliance includes the following additional features that are not available for use when you install the HP Operations agent on a vMA:

- **HP Operations agent data store**

The HP Operations agent on the virtual appliance uses a robust, embedded data store to store the collected performance data. Data is not stored in the form of log files on the virtual appliance.

- **Capability to store vCenter events**

The HP Operations agent on the virtual appliance enables you to store vCenter events into agent's embedded data store. You can use these events for advanced monitoring.

- Discovery and monitoring of VMware data center topology and relationship between different entities
- Easy and direct access to the performance data with the help of Perl script extensions

Chapter 2: Monitoring vSphere Environments with the HP Operations Agent Virtual Appliance

The HP Operations agent on the virtual appliance simplifies the monitoring of the VMware infrastructure by providing a mechanism for easy deployment of the agent. You can deploy a virtual appliance where the HP Operations agent is preinstalled. The preinstalled agent, once configured, is capable of collecting performance data from different vCenter Servers. The agent on the virtual appliance also enables you to find topology information and relationships between different entities in the VMware environment.

The HP Operations agent on the virtual appliance uses an embedded data store for storing performance data collected from different vCenters. In addition to collecting new metrics, the HP Operations agent on the virtual appliance collects and stores a set of vCenter events. Policies provided with the Virtualization Infrastructure SPI help you monitor those events.

Note: Ensure that time is always synchronized between the vCenter and the Operations Agent Virtual Appliance so that data collection happens correctly.

Default Configuration of the HP Operations Agent Virtual Appliance

The details are:

- CPU: 2 vCPUs
- Memory: 4 GB vRAM
- Disk: 64 GB (of which 48 GB is for the data file system)
- Swap: 8 GB

Deploying the Virtual Appliance with the HP Operations Agent

The vSphere virtual appliance that contains a preinstalled HP Operations agent is available with the *HP Operations Agent and Infrastructure SPIs 11.13* media in the form of the `HPOA_VM_OVF10.ova` file.

Note: Do not install or deploy any HP Software products or components (other than HPOM policies for VMware monitoring) on the virtual appliance. HP also recommends that you do not

install any third-party software products on the virtual appliance.

You can use one of the following methods to deploy the virtual appliance:

- [Using the vSphere console](#)
- [Using the command line](#)

If you want to upgrade from the previous version of Virtual Appliance to version 11.16, see [Upgrading the Virtual Appliance with HP Operations agent to Version 11.16](#).

Deploying from the vSphere Console

To deploy the virtual appliance with the HP Operations agent from the vSphere console:

1. Log on to the vSphere console.
2. Select the data center where you want to deploy the new virtual appliance.
3. Click **File > Deploy OVF Template**. The Deploy OVF Template window opens.
4. Follow the on-screen instructions.

While specifying configuration details, you can specify the FQDNs or IP addresses of the management server and certificate server for the HP Operations agent that is preinstalled on the virtual appliance. If you did not configure a separate certificate server, leave the Certificate Server field blank.

Deploying from the Command Line

To deploy the virtual appliance with the HP Operations agent from the command line with the OVF tool:

Note: Make sure to download the OVF tool from www.vmware.com.

1. Log on to a vCenter.
2. Run the following command if you want to use a static IP address:

```
ovftool -n=<name of the appliance> --network=<name of the network> -ds=<data store name> --  
powerOn -dm=thin --prop:dhcp_static=STATIC --prop:static_ip=<static_IP_address> --  
prop:subnet_ip=<Subnet_IP> --prop:gateway_ip=<gateway_IP> --prop:dns1=<DNS_IP>  
location_of_OVA_file> --prop:mgmt_server=<management_server> --prop:cert_  
server=<certificate_server> <location_of_the_VA>
```

Run the following command if you want to use a dynamic IP address:

```
ovftool -n=<name of the appliance> --network=<name of the network> -ds=<data store name> --  
powerOn -dm=thin --prop:dhcp_static=DHCP --prop:subnet_ip=<Subnet_IP> --  
prop:gateway_ip=<gateway_IP> --prop:dns1=<DNS_IP> location_of_OVA_file> --  
prop:mgmt_server=<management_server> --prop:cert_server=<certificate_server> <location_  
of_the_VA>
```

In this instance:

<name of the appliance> is the name that you want to assign to the new virtual appliance

<name of the network> is the name of the network where you want to deploy the virtual appliance

<static_IP_address> is the static IP address of the virtual appliance

<Subnet_IP> is the IP address of the subnet where you want to deploy the virtual appliance

<gateway_IP> is the IP address of the gateway server for the virtual appliance

<DNS_IP> is the IP address of the DNS server for the virtual appliance

<management_server> is the FQDN or IP address of the HPOM management server

<certificate_server> is the FQDN or IP address of the certificate server

Tip: You can skip the `--prop:cert_server=` option if you did not configure a separate certificate server.

<location_of_OVA_file> is the location where you stored the HP Operations agent OVA file

Verification

To verify that the agent is successfully installed on the virtual appliance:

1. Log on to the virtual appliance as root.

Tip: By default, the root password of the virtual appliance is `password`. You can modify this password if you like.

2. Run the following command:

/opt/OV/bin/opcagt

The agent is successfully installed if the command output shows all the agent processes are running.

```
midaemon    Measurement Interface daemon    (8873) Running
ttd         ARM registration daemon        (8982) Running
perfalarm   Alarm generator                 (9156) Running
oacore     Operations Agent Core AGENT,OA (9543) Running
opcacta     OVO Action Agent               AGENT,EA (9527) Running
opcmsga     OVO Message Agent              AGENT,EA(9490) Running
ovbbccb    OV CommunicationBroker CORE    (9453) Running
ovcd       OV Control CORE                 (9445) Running
ovconfd    OV Config and Deploy COREXT (9472) Running
```

Note: HP GlancePlus is not available with the HP Operations agent on the virtual appliance. The `cpsh` and `perfd` utilities are available on the virtual appliance.

Ports Available with HP Operations Agent Virtual Appliance

The ports available are 7, 22, 80, 383, 443, 902, 5480, 5488, and 5489. All the other incoming ports are blocked for security.

Additionally, postfix service is stopped.

Note: HTTPS port should be enabled on vCenter for communication between VA and vCenter. By default it is 443.

Steps After Deployment

After you deploy the virtual appliance, you must configure the HP Operations agent to start collecting data from different vCenter Servers. You can use the HP Operations Agent Virtual Appliance web console to perform this configuration task. Alternatively, you can log on to the virtual appliance as root and complete this task from the command line.

Tip: The default root password for the virtual appliance is `password`. You can change this password after the virtual appliance is successfully deployed.

Enable Additional License

The HP Operations OS Inst Adv SW LTU is permanently enabled on the virtual appliance. If you want to monitor the real-time data with the Diagnostic View of HP Performance Manager, you must purchase and enable the HP Ops OS Inst to Realtime Inst LTU on the virtual appliance.

To enable the HP Ops OS Inst to Realtime Inst LTU permanently:

1. Log on to the virtual appliance as root.
2. Run the following command:
`/opt/OV/bin/oalicense -set -type PERMANENT "HP Ops OS Inst to Realtime Inst LTU"`
3. After enabling the license, run the following commands:
`/opt/perf/bin/pctl stop`
`/opt/perf/bin/pctl start`
`/opt/OV/bin/opcagt -start`

Configuring the HP Operations Agent with the HP Operations Agent Virtual Appliance Web Console

The HP Operations Agent Virtual Appliance web console presents you an interface to configure the agent running on the virtual appliance to start collecting data from different vCenters. Along with adding vCenters of your choice for monitoring, you can perform the following tasks from this console:

- Restart the data collection cycle
- View the status of the agent running on the virtual appliance
- Shut down or restart the virtual appliance

To configure the agent with the HP Operations Agent Virtual Appliance web console:

1. Log on to the HP Operations Agent Virtual Appliance web console.

To go to the HP Operations Agent Virtual Appliance web console, open a web browser, and then type the following address in the address bar:

https://<IP_address>:5480

or

https://<FQDN>:5480

In this instance, <IP_address> and <FQDN> are the IP address and fully qualified domain name of the newly deployed virtual appliance.

Tip: When you launch this address, the web browser shows a security certificate exception. Ignore the exception and continue to proceed.

2. Log on with the root credentials of the virtual appliance.

Tip: By default, the root password of the virtual appliance is `password`.

3. Go to the Operations Agent tab.
4. In the vCenter Name box, type the name (fully qualified domain name) of the vCenter that you want to monitor.
5. In the User Name box, type the user name to access the data from the vCenter. Type the user name in the following format:
Domain\user name
6. In the Password box, type the password of the above user.
7. Click **Add/Update**. The vCenter name appears in the section above with the status information.

Configuring the HP Operations Agent from the Command Line

You can log on to the newly deployed virtual appliance as root and perform the configuration task from the command line.

To configure the agent from the command line:

1. Log on to virtual appliance as root.

Tip: By default, the root password of the virtual appliance is `password`. You can modify this password if you like.

2. From the command line, run the following command:

```
/opt/OV/bin/oaconfig -addtarget <vCenter_name> <user_name> <password>
```

In this instance:

`<vCenter_name>` is the fully qualified domain name of the vCenter.

`<user_name>` is the user name to access the vCenter. Specify the user name in the following format:

Domain\user name

Note: You must use `\\` instead of `\` while you add a target from the command line.

`<password>` is the password of the above user.

If you do not include the password in the command, a prompt to type the password appears at the command line.

Note: The password can be alphanumeric but must not include special characters.

3. To check that the HP Operations agent on the virtual appliance successfully started monitoring the vCenter, run the following command:

```
/opt/OV/bin/oaconfig -listtargets
```

The name of the vCenter appears in the list of monitored vCenters.

For more information about `oaconfig`, see ["Reference Page" on page 30](#).

Configuring the HP Operations Agent on the Virtual Appliance to Use a Different Management Server

At the time of deployment of the virtual appliance, the HP Operations agent is configured to use an HPOM management server. HPOM management server details are provided in the vSphere Console or with the `ovftool` command.

After deploying the virtual appliance, if you want to use a different HPOM management server, you must perform additional tasks that include running the `oainstall.sh` command on the virtual appliance.

To use a different HPOM management server:

1. In the HPOM console, add the virtual appliance as the managed node, but do not deploy an agent.
2. Log on to virtual appliance as root.

Tip: By default, the root password of the virtual appliance is `password`. You can modify this password if you like.

3. From the command line, run the following command:

```
/opt/OV/bin/OpC/install/oainstall.sh -a -configure -srv <management_server> -cert_srv <certificate_server>
```

In this instance:

`<management_server>` is the fully qualified domain name or IP address of the HPOM management server.

`<certificate_server>` is the fully qualified domain name or IP address of the certificate server.

4. After the HP Operations agent on the virtual appliance is configured to work with the HPOM management server, deploy the Virtualization Infrastructure SPI policies. For more information about those policies, see [Virtualization Infrastructure SPI Policies for the Virtual Appliance](#).

Note: Do not install or deploy any HP Software products or components (other than HPOM policies for VMware monitoring) on the virtual appliance. HP also recommends that you do not install any third-party software products on the virtual appliance.

Delete the Data Manually

The data purging feature enables you to delete the stored data to free up disk space. You can manually delete the data for a specific time range using the `oaconfig` tool, or you can configure the agent to automatically delete the selected data at a regular interval.

To delete the data manually:

1. Log on to the virtual appliance as root.
2. Run the following command:

```
/opt/OV/bin/oaconfig -purgelog <time>
```

You must specify the time in the following format:

```
YYYY-MM-DDThh:mm:ss
```

The command deletes the data collected before the specified time.

Alternatively, you can configure the HP Operations agent to automatically purge the data from the data store at a regular interval. For more information, see ["Configure Automatic Purging of Data" on page 15](#) or ["Configure Automatic Data Purging from the Command Line" on page 16](#).

vCenter Events

By default, the HP Operations agent collects and stores events from monitored vCenters, which you can use for advanced monitoring of the infrastructure. For a list of vCenter events that are collected by the HP Operations agent by default, see ["vCenter Events" on page 41](#).

You can extend the list of monitored vCenter events by modifying the entries in the `VIEventTypes.cfg` file, which is available in the `/var/opt/OV/conf/vispi/configuration` directory on the virtual appliance.

If you want to monitor all vCenter events, delete the contents of the `VIEventTypes.cfg` file, and then save the file in the same directory.

To disable the collection vCenter events:

1. Log on to the virtual appliance as root.
2. Run the following command:
`/opt/OV/bin/ovconfchg -ns opsagt.viserver -set CollectEvents false`

Using the HP Operations Agent Virtual Appliance Web Console

The HP Operations Agent Virtual Appliance web console provides a window to view the status of the HP Operations agent running on the virtual appliance. The console also enables you to perform different administrative tasks, such as:

- Configure the HP Operations agent to start monitoring vCenter Servers
- Configure automatic data purging
- Modify data collection intervals

Configure the HP Operations Agent on the Virtual Appliance

The Operations Agent tab of the HP Operations Agent Virtual Appliance web console enables you to configure the HP Operations agent running on the virtual appliance.

You already configured the HP Operations agent to collect data from the vCenter Server of your choice (see ["Configuring the HP Operations Agent with the HP Operations Agent Virtual Appliance Web Console" on page 11](#) or ["Configuring the HP Operations Agent from the Command Line" on page 11](#)).

By using the HP Operations Agent Virtual Appliance web console, you can now add an additional target vCenter Server for monitoring or stop monitoring a vCenter Server that is currently monitored by the agent. You can also restart the collection mechanism of the HP Operations agent.

To add a vCenter Server target:

1. In the HP Operations Agent Virtual Appliance web console, go to the Operations Agent tab.
2. Type the following details:

Field	Description
vCenter Name	Fully qualified domain name or IP address of the vCenter Server that you want to add.

Field	Description
User Name	User name to log on to the vCenter Server. Specify the user name in the following format: Domain\user name
Password	Password of the above user. Note: The password can be alphanumeric but must not include special characters.

3. Click **Add/Update**.

To delete a monitored vCenter target:

Click **Remove** against the vCenter Server name.

To restart the data collection process of the existing vCenter Servers, click **Restart Collection**.

Configure Automatic Purging of Data

The HP Operations Agent Virtual Appliance web console enables you to schedule purging of data from the HP Operations agent's data store at a regular interval. The automatic data purging feature helps you control the size of the HP Operations agent's data store. If you do not enable automatic data purging, the data continues to accumulate into the HP Operations agent's data store. This requires you to delete the data manually or increase the storage capacity of the virtual appliance.

To configure the automatic purging of data:

1. In the HP Operations Agent Virtual Appliance web console, go to the Operations Agent tab.
2. Click **Settings**.
3. Specify the following details:

Field	Description
Data Purging Interval (Days)	Specify the interval (in days) at which you want to delete the data from the agent's data store.
Data Retention Period (Days)	Specify the data retention period in days. The HP Operations agent deletes only the data that is older than the specified number of days from the data store. For example, if you specify 30, the HP Operations agent deletes all the data older than 30 days at the time of scheduled data purging.

4. Click **Apply Changes**.
5. Run the following command on the virtual appliance to start agent processes:

/opt/OV/bin/ovc -start oacore

If you do not want to configure automatic purging of data, make sure the *Data Purging Interval (Days)* field is not set to any values.

You can also configure this from the command line. For more information, see "[Configure Automatic Data Purging from the Command Line](#)" below.

Modify the Collection Frequency of the HP Operations Agent

The HP Operations Agent Virtual Appliance web console enables you to choose one of the following collection frequencies:

- Fast
- Moderate

By default, the HP Operations agent uses the fast frequency.

Each frequency uses a fixed set of collection intervals for monitored entities.

To modify the collection frequency of the HP Operations agent:

1. In the HP Operations Agent Virtual Appliance web console, go to the Operations Agent tab.
2. Click **Settings**.
3. Select Fast or Moderate depending on your requirement.
4. Click **Apply Changes**. The HP Operations agent automatically restarts the data collection process, and then the change takes effect.

Configure Automatic Data Purging from the Command Line

To configure automatic data purging from the command line:

1. Log on to the virtual appliance as root.
2. Run the following command:
`/opt/OV/bin/ovconfchg -ns opsagt -set AutoPurgeIntervalSecs <interval>`
You must specify the interval in seconds.
3. You must also specify the data retention period. Run the following command to specify the data retention period:
`/opt/OV/bin/ovconfchg -ns opsagt -set KeepDataForSecs <retention_period>`
You must specify the retention period in seconds.
4. Run the following command to start agent processes:
`/opt/OV/bin/ovc -start oacore`

Monitoring vCenters with the HP Operations Agent on the Virtual Appliance

The Virtualization Infrastructure SPI, packaged with the *HP Operations Agent and Infrastructure SPIs 11.13* media, contains a set of policies that help you monitor the vSphere environment with the help of the data collected by the HP Operations agent on the virtual appliance.

The Virtualization Infrastructure SPI 11.16 can be installed on the HPOM management server at the time of registering the deployment packages of the HP Operations agent 11.16. For more information about installing the Virtualization Infrastructure SPI, see the *HP Operations Agent and HP Operations Smart Plug-ins for Infrastructure Installation and Configuration Guide* (available on the product media or on the [HP Software Product Manual](#) web site).

These policies are available under the Infrastructure Management > en > Virtualization Infrastructure > Policies grouped by vendor > VMware vCenter - Quick Start and Infrastructure Management > en > Virtualization Infrastructure > Policies grouped by vendor > VMware vCenter - Advanced groups in the console tree of the HPOM console after you install the Virtualization Infrastructure SPI on the HPOM management server. Deploy these policies on the virtual appliance to start monitoring the vSphere environment.

Note: Measurement threshold policies with the source type set to Embedded Performance Component and the data source set to CODA cannot be deployed on the virtual appliance.

Virtualization Infrastructure SPI Policies for the Virtual Appliance

Policy Name	Type	Group	Description
VI-VMwareVCEventMonitor	Measurement Threshold	Infrastructure Management > en > Virtualization Infrastructure > Policies grouped by vendor > VMware vCenter - Quick Start	The HP Operations agent on the virtual appliance collects and stores vCenter events. This policy helps you monitor those events.
VI-VMwareVCEvent	ConfigFile	Infrastructure Management > en > Virtualization Infrastructure > Policies grouped by vendor >	Add or delete vCenter events for monitoring. For a complete list of vCenter events that are monitored by the agent by default, see " vCenter ".

Virtualization Infrastructure SPI Policies for the Virtual Appliance, continued

Policy Name	Type	Group	Description
		VMware vCenter - Quick Start	Events" on page 41.
VI-VMwareVCGuestStateMonitor	Measurement Threshold	Infrastructure Management > en > Virtualization Infrastructure > Policies grouped by vendor > VMware vCenter - Quick Start	Monitors the states of all logical systems in the VMware environment.
VI-VMwareVCDatastore SpaceUtilizationMonitor	Measurement Threshold	Infrastructure Management > en > Virtualization Infrastructure > Policies grouped by vendor > VMware vCenter - Advanced	Monitors the space utilization of each VMware datastore.
VI-VMwareVCGuestLatencyMonitor	Measurement Threshold	Infrastructure Management > en > Virtualization Infrastructure > Policies grouped by vendor > VMware vCenter - Advanced	Monitors the latency of guest systems (virtual machines). Latency of a virtual machine creates performance problems.
VI-VMwareVCCPUSaturationMonitor	Measurement Threshold	Infrastructure Management > en > Virtualization Infrastructure > Policies grouped by	Monitors the consumption of host CPUs by virtual machines. The alert message lists the virtual machines that continuously

Virtualization Infrastructure SPI Policies for the Virtual Appliance, continued

Policy Name	Type	Group	Description
		vendor > VMware vCenter - Advanced	use a significant amount of the CPU resource.
VI-VMwareVCCPUUtilMonitor	Measurement Threshold	Infrastructure Management > en > Virtualization Infrastructure > Policies grouped by vendor > VMware vCenter - Advanced	Monitors the CPU utilization of ESX/ESXi hosts.
VI-VMwareVCMemUtilMonitor	Measurement Threshold	Infrastructure Management > en > Virtualization Infrastructure > Policies grouped by vendor > VMware vCenter - Advanced	Monitors the memory utilization of ESX/ESXi hosts.

Configuring Logging Levels for the status.viserver File

The HP Operations agent on the virtual appliance uses the **Vllog4j.xml** file, located in **/var/opt/perf**, to log status information in the **status.viserver** file. The **log4j.dtd** file, available in **/var/opt/perf**, defines the template for the **Vllog4j.xml** file.

Note: There are elements in the XML file that are required for the logging to work correctly. Do not change or delete these elements. Only recommended change is the level of the com.hp.perfagent logger.

The XML file consist of the following major elements:

appender

logger

You can change only the following item within the [<logger name="com.hp.perfagent"> ... </logger>] element:

```
<level value = "info"/>
```

This entity determines the level of logging in the **status.viserver** file. You can set value to one of the following non-default settings:

fatal: Use this setting to log minimal information.

all: Use this setting to log all the information.

warn: Use this setting to log only warning messages.

error: Use this setting to log only error messages.

debug: Use this setting to log information for debugging.

Note: Use the debug setting only for troubleshooting purposes.

Configure Cluster Filtering

You can specify the clusters in a vCenter for the data collection process by any *one* of the following:

- Adding the cluster list in the opsagt.viserver namespace
- Using the command line

Adding the Cluster List in opsagt.viserver

Follow the steps:

1. Log on to the virtual appliance as root.
2. Run the command:

```
/opt/OV/bin/ovconfchg -edit
```

3. Open the opsagt.viserver file and add the list of the clusters to enable the data collection.

```
Cluster=<vCenter Name>:<Datacenter Name>:<Cluster Name>;
```

In this instance,

the *vCenterName* is the fully qualified name of the vCenter that is added to the VA for monitoring.

the *Datacenter Name*, is the fully qualified name of the datacenter.

the *Cluster Name* is the fully qualified name of the cluster that is added for monitoring.

Make sure that a colon is added in between vCenter Name, Datacenter Name, and Cluster Name. Specify a semi-colon in between the clusters. Semi-colon in the end is optional.

Note: The command is to start the data collection of the specified clusters for a vCenter target.

All other clusters of the specified vCenter will be excluded in the data collection process. In addition, there will be no change in the behavior for the other vCenter targets where the cluster filtering is not specified.

- Restart the data collection process of the vCenter servers from the HP Operations Agent Virtual Appliance web console. Go to the **Operations Agent** tab and click **Restart Collection**.

Using the Command Line

To configure cluster filtering from the command line:

- Log on to the virtual appliance as root.
- You must add the cluster list. Run the following command:

```
/opt/OV/bin/ovconfchg -ns opsagt.viserver -set Cluster=<vCenter Name>:<Datacenter Name>:<Cluster Name>;
```

In this instance,

the *vCenterName* is the fully qualified name of the vCenter that is added to the VA for monitoring.

the *Datacenter Name*, is the fully qualified name of the datacenter.

the *Cluster Name* is the fully qualified name of the cluster that is added for monitoring.

Make sure that a colon is added in between vCenter Name, Datacenter Name, and Cluster Name. Specify a semi-colon in between the clusters. Semi-colon at the end of the command is optional.

Note: The command is to start the data collection of the specified cluster for a vCenter target.

All other clusters of the specified vCenter will be excluded in the data collection process. In addition, there will be no change in the behavior for the other vCenter targets where the cluster filtering is not specified.

- Restart the data collection process of the vCenter servers from the HP Operations Agent Virtual Appliance web console. Go to the **Operations Agent** tab and click **Restart Collection**.

Configure Collection Level

The data collection is enabled for the entities available in the vCenter. You can configure the data collection by any *one* of the following:

- Adding the collection level values in the opsagt.viserver namespace
- Using the command line

Adding the Collection Level in opsagt.viserver

Follow the steps:

- Log on to the virtual appliance as root.
- Run the command:

/opt/OV/bin/ovconfchg -edit

3. Open the `opsagt.viserver` namespace and add the data collection value.

`Collection Level=<Value>`

In this instance,

the *Value* is defined to enable the data collection for the entities available in vCenter.

By default, the value is 4.

The value **4** depicts that the data collection is enabled for Datacenter, Clusters, Hosts, Virtual Machines, Datastore, Resource Pools and VirtualApps. In addition, relation of Virtual Machines and Datastore is also enabled.

The value **2** depicts that data collection is enabled for Datacenter, Clusters, and Hosts. The relation between Virtual Machine and Datastore is disabled.

4. Restart the data collection process of the vCenter servers from the HP Operations Agent Virtual Appliance web console. Go to the **Operations Agent** tab and click **Restart Collection**.

Using the Command Line

To configure cluster filtering from the command line:

1. Log on to the virtual appliance as root.
2. Run the following command to update the collection level value:

/opt/OV/bin/ovconfchg -ns opsagt.viserver -set CollectionLevel=<Value>

In this instance,

the *Value* is defined to enable the data collection for the entities available in vCenter.

By default, the value is 4.

The value **4** depicts that the data collection is enabled for Datacenter, Clusters, Hosts, Virtual Machines, Datastore, Resource Pools and VirtualApps. In addition, relation of Virtual Machines and Datastore is also enabled.

The value **2** depicts that data collection is enabled for Datacenter, Clusters, and Hosts. The relation between Virtual Machine and Datastore is disabled.

3. Restart the data collection process of the vCenter servers from the HP Operations Agent Virtual Appliance web console. Go to the **Operations Agent** tab and click **Restart Collection**.

Chapter 3: Downloading the Virtual Appliance with the Operations Agent Version 11.16

To download HP Operations agent VA ISO (OAVA_00002) file, follow these steps:

1. Go to the following web site:
<http://h20230.www2.hp.com/selfsolve/patches>.
2. Log on to the web site with your HP Passport credentials.
3. Search with the keyword HP Operations agent. The search result includes links to download the ISO files for the HP Operations agent 11.16.
4. Download the VA zip file on your system.

You can use the methods to upgrade the previous version of the virtual appliance to version 11.16. See [Upgrading the Virtual Appliance with HP Operations agent to Version 11.16](#).

Chapter 4: Deploying the Virtual Appliance with HP Operations agent Version 11.12

Make sure that you have already deployed Virtual Appliance with the HP Operations Agent Version 11.11. For more information, see [Deploying the Virtual Appliance with the HP Operations Agent Version 11.11](#).

You can use one of the following methods to deploy the virtual appliance 11.12:

- vSphere console
- Command line

Deploying the Virtual Appliance 11.12 from the vSphere Console

To deploy the virtual appliance with the HP Operations agent 11.12 from the vSphere console, follow the steps:

1. Download and extract the OAVA_00001.zip file. Place the content of the files in the `http://<ipaddress>/updates/`
2. Log on to the vSphere console. Example, `http://<ipaddress>:5480`.
3. Go to **Update -> Settings** and check the **Repository URL**. This is to make sure that the downloaded repository is available at the correct IP Address. For example, `http://<ipaddress>/updates/`
4. To check for the available updates, go to **Update -> Status** tab and click **Check Updates**. The available updates with this version will appear.
5. Click **Install Updates** to install all the new updates available with this 11.12 version.

Deploying the Virtual Appliance 11.12 from the Command Line

Follow the steps:

1. Log on to a vCenter.
2. Run the command to check for the available updates for this version: `vamcli update --check`
3. Run the command to install the available updates for this version: `vamcli update --install latest`

Chapter 5: Monitoring the vSphere Environment with vMA

As an alternative to monitoring the vSphere infrastructure with the virtual appliance, you can manually install the HP Operations agent on a vMA and monitor the environment with the help of the performance data collected by the agent running on the vMA.

This option requires you to manually install and configure the HP Operations agent on the vMA. Because the root user of a vMA is disabled by default, you cannot deploy the agent remotely from the HPOM console.

Installing the HP Operations Agent on a vMA

Prerequisites

- Make sure that the portmap service is started.
- Disable the floppy drive on the vMA.
- Increase the RAM size for the vMA to 1 GB.

Installation

To install the HP Operations agent on a vMA:

1. Enable the communication across firewalls on the vMA node.

The agent uses the port 383 to facilitate the communication with other systems across firewalls. You must configure the vMA node to accept communication traffic on the port 383. To achieve this, follow these steps:

- a. On the vMA node, run the following command:

```
sudo iptables -I RH-Firewall-1-INPUT 3 -p tcp -m tcp --dport 383 --tcp-flags SYN,RST,ACK SYN -j ACCEPT
```

The vMA is configured to accept communication traffic on the port 383.

- b. Run the following command:

```
sudo service iptables save
```

The command saves the configuration set in [step a](#).

- c. To verify the configuration settings, run the following command:

```
sudo vi /etc/sysconfig/iptables
```

The vi editor opens the `iptables` file from the `/etc/sysconfig` directory.

In the `iptables` file, verify that the following line is present:

```
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 383 --tcp-flags SYN,RST,ACK SYN  
-j ACCEPT
```

2. Extract the contents of the HP Operations agent 11.16 media into a local directory on the vMA.
3. Log on to the vMA (default user: `vi-admin`), and then type the following command:

sudo bash

The command line prompts you for the password of the root user.

4. Type the root password.
5. Go to the directory where you extracted the media contents, and then install the HP Operations agent by using the `oainstall.sh` command:

```
./oainstall.sh -i -a
```

Configuring Data Collection on vMA Nodes

The HP Operations agent uses the `viserver` daemon to log data on the vMA system. You can configure `viserver` settings in the following configuration files (available in `/var/opt/perf`):

- `viserver.properties`
- `VILog4j.xml`

`viserver.properties`

This file contains the following parameters:

- `port`
- `hosts`
- `instance`
- `jvmArgs`
- `log4jInterval`
- `connectionRetry`

You must restart `viserver` if you change the settings in the `viserver.properties` file. The new settings are effective only after you restart `viserver`.

port

The `port` parameter is the loopback port through which `viserver` and clients communicate. The `port` parameter is non-editable; the value of this parameter changes when you restart `viserver`.

hosts

The `hosts` parameter defines the number of hosts that `viserver` daemon can support. The default value is 20.

If you have more hosts in your environment, you can edit this parameter to specify your required setting. If the HP Operations agent is not able to collect data for the number of hosts that you specified, you must reduce `vifp` targets.

instance

The `instance` parameter defines the number of instances viserver can support. The default value is 200.

If you have more instances in your environment, you can edit this parameter to specify your required setting. If the HP Operations agent is not able to collect data for the number of instances that you specified, you must reduce `vifp` targets.

jvmargs

The `jvmArgs` parameter enables you to add jvm arguments and modify jvm as required in your environment.

The default configuration for `jvmArgs` is as follows:

```
jvmArgs=-Xms128m -Xmx2048m -classpath
/opt/perf/bin/java/activation.jar\:/opt/perf/bin/java/
axis-ant.jar\:/opt/perf/bin/java/axis.jar\:/opt/perf/bin/java/
commons-discovery-0.2.jar\:/opt/perf/bin/java/commons-logging-1.0.4.jar
\:/opt/perf/bin/java/jaxrpc.jar\:/opt/perf/bin/java/log4j-1.2.8.jar\:/
/opt/perf/bin/java/mailapi.jar\:/opt/perf/bin/java/saaj.jar\:/opt/perf/
bin/java/vim25.jar\:/opt/perf/bin/java/viserver.jar\:/opt/perf/bin/java/
wsdl4j-1.5.1.jar\:/opt/vmware/vma/lib64/vmatargetlib25.jar\:/
/opt/vmware/vma/lib64/vifplib25.jarcom.hp.perfagent.VI daemon
```

log4jInterval

The `log4jInterval` parameter specifies the interval at which viserver checks for changes in `VILog4j.xml` file. The default value is 60000 milliseconds (1 minute). You can modify this value as required.

connectionRetry

The `connectionRetry` parameter defines the number of trails viserver can support to reconnect vCenter. The default value is 6. You can modify this value as required. For example, set the `connectionRetry` parameter value to -1 if you want viserver to support infinite number of trails to reconnect vCenter.

```
connectionRetry=-1
```

Monitoring with the HP Operations Agent on vMA

The Virtualization Infrastructure SPI, packaged with the *HP Operations Agent and Infrastructure SPIs 11.13* media, contains a set of policies that help you monitor the vSphere environment with the help of the data collected by the HP Operations agent on a vMA. Those policies are available under the *VMware ESX - Quick Start* and *VMware ESX - Advanced* groups in the console tree of the HPOM console after you install the Virtualization Infrastructure SPI on the HPOM management server.

Chapter 6: Troubleshooting

While using the HP Operations agent on a virtual appliance or vMA, you may experience certain problems. This section helps you troubleshoot such problems and provides you with information to help you avoid problems from occurring.

The VI-Discovery Policy Fails to Discover vCenters

While using the HP Operations agent on a virtual appliance, the VI-Discovery policy fails to discover vCenters. As a result, you cannot view vCenters on the Service map in the HPOM console.

Solution:

This problem occurs when the HP Operations agent fails to resolve the FQDN of the vCenter to an IP address. To resolve this issue, make sure that the agent can resolve the FQDN of the vCenter to an IP address.

The cpsh, padv, and mpadv Utilities Cannot Access the Complete Data Set

The `cpsh`, `padv`, and `mpadv` utilities cannot access the data collected from the newly added vCenter Servers.

Solution:

After adding a new vCenter Server target (see [how to add a vCenter Server target](#)), the real-time metric access component of the HP Operations agent requires up to three minutes to retrieve the data from newly added vCenter Servers. If you run these utilities at least three minutes after adding the new target, you can access all the data.

Troubleshooting with Policies

The *HP Operations Agent and Infrastructure SPIs 11.13* includes a set of HPOM policies that help you monitor the status of the HP Operations agent running on the virtual appliance. The policies are installed on the HPOM management server as soon as you register the deployment package of the HP Operations agent 11.16. You can then deploy the policies to the virtual appliance.

The policies are available in the following location in the HPOM console:

```
HP Operations Agent > SelfMonitoring-Additional > VMware vCenter
```

Policies to Monitor the HP Operations Agent on the Virtual Appliance

Policy Name	Type	Group	Description
VMWareVC-SelfMonCPUUsage	Measurement Threshold	HP Operations Agent > SelfMonitoring-Additional > VMware vCenter	Monitors the CPU consumption of the HP Operations agent on the virtual appliance.
VMWareVC-SelfMonDiskUsage	Measurement Threshold	HP Operations Agent > SelfMonitoring-Additional > VMware vCenter	Monitors the disk consumption of the HP Operations agent on the virtual appliance.
VMWareVC-SelfMonMemoryUsage	Measurement Threshold	HP Operations Agent > SelfMonitoring-Additional > VMware vCenter	Monitors the memory consumption of the HP Operations agent on the virtual appliance.
VMWareVC-SelfMonDBCORRUPTIONMonitor	Logfile Entry	HP Operations Agent > SelfMonitoring-Additional > VMware vCenter	This policy checks that the HP Operations agent data store is healthy. If the policy detects data corruption in the HP Operations agent data store, alert messages are sent to the HPOM console.

Appendix A: Reference Page

Support Tools

The various support tools are listed below:

[easyoa](#)

[oava_data_collector.sh](#)

[oava_inst_report.sh](#)

[oava_list_events.sh](#)

[oava_dump_metrics.sh](#)

easyoa

The `easyoa` tool helps you to query the following:

- Metric values for all instances or a set of instances.
- List of the managed classes and metrics.
- Events for a specific set of instances or all instances of a managed class within a specified time range.

The `easyoa` tool works only when the status of the `oacore` process is **Running**. Run the command to check the status: **ovc -status**

Synopsis

For Metric Values

```
-dn <domainname> -c <classname> [-o metric(default)|event|model]
```

```
[-f <metric>=<value>,<metric>=<value>] [-m <metric>,<metric>...] [-si <interval>]
```

For Model

```
-dn <domainname> -c <classname> -o model [-m <Metric Name>,<Metric Name>...]
```

For Events

```
-dn <domainname> -c <classname> -o event [-if <key metric>=<value>,<key metric>=<value>...] [-last [hour]][[min]][[fivemin]]]
```

Options

Option	Description
dn (domain name)	Specifies the domain name of the managed class. This field is mandatory.

Option	Description
	Example: Virtualization or Infrastructure
c (class)	Specify the managed class name. A class name is unique with in the domain. This field is mandatory. An error appears if the specific class is not available.
f (filter option)	Provides the filter option for a specified class under the domain. You can filter the instances from the available option. You can specify one or more valid metrics of the class and their values based on which you can filter the instances. This field is optional. Syntax is -<Metric Name>=<Metric Filter Value>,[<Metric Name>=<Metric Filter Value>...] Note: The example is as follows: The managed class is < Node>. Metric is SystemRole. Possible values of SystemRole are HOST, GUEST, and PROXY. When the agent data store contains a large number of instances and you want to access only the HOST instance then use the filter option as: <code>-dn <i>Virtualization</i> -c <u>Node</u> -f SystemRole=HOST</code>
m (metric)	For a specific class under the domain, you can get the metrics for the specific instances. You can specify multiple metrics separated by comma. The field is optional. Syntax is <Metric Name>,[<Metric Name>...] Note: The example is as follows: <code>-dn <i>Virtualization</i> -c <u>Node</u> - m MemPhysUtil</code>
si (Summarization Interval)	Specify the interval (in minutes) for summarization. Default value is 5 minutes.

Examples

- **`./easyoa.pl -dn Infrastructure -c Node -m MemPhysUtil`**
The output provides all the instances of the defined domain name - Infrastructure, class Node and metric as MemPhysUtil.
- **`./easyoa.pl -dn Virtualization -c Datacenter -m LSName`**
The output provides all the instances of the metric LS Name.
- **`./easyoa.pl -dn Infrastructure -c Node -o model -m NumCPU`**
The output appears as:
Metric Name : NumCPU
Type : COUNTER

Description : The number of virtual CPUs configured for this logical system. Metric Equivalent on VMWare Systems, for Host, HostSystem->summary->hardware->numCpuThreads for Guest, VirtualMachine->config->hardware->numCPU for RP, NA

- **./easyoa.pl -dn Infrastructure -c Node -m MemPhysUtil -f SystemRole=GUEST**

The output appears with the filter option enabled.

For more information about the tool, follow the steps:

1. Go to the location: opt/OV/ support
2. Run the command: **./easyoa.pl -h**

oava_data_collector.sh

The oava_data_collector.sh tool collects OAVA data into the following directory:

/var/opt/OV/tmp/oava_data.tar.gz

For more information about the tool, follow the steps:

1. Go to the location: opt/OV/ support
2. Run the command: **./oava_data_collector.sh -h**

oava_inst_report.sh

The oava_inst_report.sh tool provides a report of all instances collected by OAVA.

For more information about the tool, follow the steps:

1. Go to the location: opt/OV/ support
2. Run the command: **./oava_inst_report.sh -h**

oava_list_events.sh

The oava_list_events.sh tool provides a report of all events collected by OAVA.

For more information about the tool, follow the steps:

1. Go to the location: opt/OV/ support
2. Run the command: **./oava_list_events.sh -h**

oava_dump_metrics.sh

The oava_dump_metrics.sh tool provides a report of all metric values of a specified class over a specified time range.

For more information about the tool, follow the steps:

1. Go to the location: `opt/OV/ support`
2. Run the command: `./oava_dump_metrics.sh -h`

Appendix B: RPMs Packaged with the HP Operations Agent Virtual Appliance

The list of RPMs is as follows:

- setup-2.8.14-20.el6.noarch
- basesystem-10.0-4.el6.noarch
- tzdata-2012j-1.el6.noarch
- glibc-common-2.12-1.107.el6.x86_64
- ncurses-libs-5.7-3.20090208.el6.x86_64
- libattr-2.4.44-7.el6.x86_64
- zlib-1.2.3-29.el6.x86_64
- audit-libs-2.2-2.el6.x86_64
- popt-1.13-7.el6.x86_64
- db4-4.7.25-17.el6.x86_64
- nspr-4.9.2-1.el6.x86_64
- bzip2-libs-1.0.5-7.el6_0.x86_64
- libselinux-2.0.94-5.3.el6.x86_64
- sed-4.2.1-10.el6.x86_64
- glib2-2.22.5-7.el6.x86_64
- gawk-3.1.7-10.el6.x86_64
- sqlite-3.6.20-1.el6.x86_64
- libxml2-2.7.6-8.el6_3.4.x86_64
- libstdc4.4.7-3.el6.x86_64
- dbus-libs-1.2.24-7.el6_3.x86_64
- grep-2.6.3-3.el6.x86_64
- findutils-4.4.2-6.el6.x86_64
- cyrus-sasl-lib-2.1.23-13.el6_3.1.x86_64
- libblkid-2.17.2-12.9.el6.x86_64
- keyutils-libs-1.4-4.el6.x86_64
- libgssglue-0.1-11.el6.x86_64
- libpgp-error-1.7-4.el6.x86_64
- vim-minimal-7.2.411-1.8.el6.x86_64
- checkpolicy-2.0.22-1.el6.x86_64
- sysvinit-tools-2.87-4.dsf.el6.x86_64
- perl-Pod-Escapes-1.04-129.el6.x86_64

- perl-Module-Pluggable-3.90-129.el6.x86_64
- perl-libs-5.10.1-129.el6.x86_64
- pth-2.0.7-9.3.el6.x86_64
- keyutils-1.4-4.el6.x86_64
- grubby-7.0.15-3.el6.x86_64
- upstart-0.6.5-12.el6.x86_64
- libusb-0.1.12-23.el6.x86_64
- nss-softokn-3.12.9-11.el6.x86_64
- xz-lzma-compat-4.999.9-0.3.beta.20091007git.el6.x86_64
- MAKEDEV-3.24-6.el6.x86_64
- net-tools-1.60-110.el6_2.x86_64
- tar-1.23-11.el6.x86_64
- pinentry-0.7.6-6.el6.x86_64
- e2fsprogs-libs-1.41.12-14.el6.x86_64
- which-2.19-6.el6.x86_64
- diffutils-2.8.1-28.el6.x86_64
- dash-0.5.5.1-4.el6.x86_64
- groff-1.18.1.4-21.el6.x86_64
- coreutils-libs-8.4-19.el6.x86_64
- cracklib-2.8.16-4.el6.x86_64
- coreutils-8.4-19.el6.x86_64
- module-init-tools-3.9-21.el6.x86_64
- redhat-logos-60.0.14-12.el6.centos.noarch
- libpciaccess-0.13.1-2.el6.x86_64
- rpcbind-0.2.0-11.el6.x86_64
- nss-3.14.0.0-12.el6.x86_64
- nss-tools-3.14.0.0-12.el6.x86_64
- libuser-0.56.13-5.el6.x86_64
- pciutils-libs-3.1.10-2.el6.x86_64
- mingetty-1.08-5.el6.x86_64
- ustr-1.0.4-9.1.el6.x86_64
- libffi-3.0.5-3.2.el6.x86_64
- newt-0.52.11-3.el6.x86_64
- ca-certificates-2010.63-3.el6_1.5.noarch
- python-libs-2.6.6-36.el6.x86_64
- libssh2-1.4.2-1.el6.x86_64
- curl-7.19.7-35.el6.x86_64
- rpm-4.8.0-32.el6.x86_64

- python-pycurl-7.19.0-8.el6.x86_64
- gnupg2-2.0.14-4.el6.x86_64
- pygpgme-0.1-18.20090824b2r68.el6.x86_64
- yum-metadata-parser-1.1.2-16.el6.x86_64
- yum-plugin-fastestmirror-1.1.30-14.el6.noarch
- bind-libs-9.8.2-0.17.rc1.el6.x86_64
- fipscheck-lib-1.2.0-7.el6.x86_64
- kbd-misc-1.15-11.el6.noarch
- policycoreutils-2.0.83-19.30.el6.x86_64
- iproute-2.6.32-23.el6.x86_64
- util-linux-ng-2.17.2-12.9.el6.x86_64
- udev-147-2.46.el6.x86_64
- plymouth-0.8.3-27.el6.centos.x86_64
- dracut-004-303.el6.noarch
- rsyslog-5.8.10-6.el6.x86_64
- cyrus-sasl-2.1.23-13.el6_3.1.x86_64
- crontab-anacron-1.4.4-7.el6.x86_64
- crontabs-1.10-33.el6.noarch
- nfs-utils-1.2.3-36.el6.x86_64
- selinux-policy-3.7.19-195.el6.noarch
- kernel-firmware-2.6.32-358.el6.noarch
- dhclient-4.1.1-34.P1.el6.centos.x86_64
- system-config-firewall-base-1.2.27-5.el6.noarch
- bfa-firmware-3.0.3.1-1.el6.noarch
- iwl100-firmware-39.31.5.1-1.el6.noarch
- b43-openfwfw-5.2-4.el6.noarch
- aic94xx-firmware-30-2.el6.noarch
- iwl1000-firmware-39.31.5.1-1.el6.noarch
- authconfig-6.1.12-13.el6.x86_64
- gettext-0.17-16.el6.x86_64
- grub-0.97-81.el6.x86_64
- wget-1.12-1.8.el6.x86_64
- passwd-0.77-4.el6_2.2.x86_64
- audit-2.2-2.el6.x86_64
- acl-2.2.49-6.el6.x86_64
- ql2400-firmware-5.08.00-1.el6.noarch
- ql2100-firmware-1.19.38-3.1.el6.noarch
- libertas-usb8388-firmware-5.110.22.p23-3.1.el6.noarch

- ql2500-firmware-5.08.00-1.el6.noarch
- zd1211-firmware-1.4-4.el6.noarch
- rt61pci-firmware-1.2-7.el6.noarch
- ql2200-firmware-2.02.08-3.1.el6.noarch
- ipw2100-firmware-1.3-11.el6.noarch
- ipw2200-firmware-3.1-4.el6.noarch
- vmware-studio-vami-tools-2.6.0.0-631426.x86_64
- vmware-studio-vami-servicebase-2.6.0.0-631426.x86_64
- vmware-studio-vami-service-system-2.6.0.0-0.x86_64
- vmware-studio-vami-service-oaconfig-1.0.0.0-0.x86_64
- vmware-studio-appliance-config-2.6.0.0-130820235403.noarch
- vmware-studio-vami-login-2.6.0.0-631426.x86_64
- libgcc-4.4.7-3.el6.x86_64
- filesystem-2.4.30-3.el6.x86_64
- ncurses-base-5.7-3.20090208.el6.x86_64
- nss-softokn-freebl-3.12.9-11.el6.x86_64
- glibc-2.12-1.107.el6.x86_64
- bash-4.1.2-14.el6.x86_64
- libcap-2.16-5.5.el6.x86_64
- info-4.13a-8.el6.x86_64
- libcom_err-1.41.12-14.el6.x86_64
- chkconfig-1.3.49.3-2.el6.x86_64
- libacl-2.2.49-6.el6.x86_64
- nss-util-3.14.0.0-2.el6.x86_64
- libsepol-2.0.41-4.el6.x86_64
- shadow-utils-4.1.4.2-13.el6.x86_64
- gamin-0.1.10-9.el6.x86_64
- readline-6.0-4.el6.x86_64
- xz-libs-4.999.9-0.3.beta.20091007git.el6.x86_64
- libidn-1.18-2.el6.x86_64
- file-libs-5.04-15.el6.x86_64
- tcp_wrappers-libs-7.6-57.el6.x86_64
- pcre-7.8-6.el6.x86_64
- lua-5.1.4-4.1.el6.x86_64
- bzip2-1.0.5-7.el6_0.x86_64
- libuuid-2.17.2-12.9.el6.x86_64
- expat-2.0.1-11.el6_2.x86_64
- krb5-libs-1.10.3-10.el6.x86_64

- elfutils-libelf-0.152-1.el6.x86_64
- libtirpc-0.2.1-5.el6.x86_64
- libselinux-utils-2.0.94-5.3.el6.x86_64
- cpio-2.10-11.el6_3.x86_64
- gdbm-1.8.0-36.el6.x86_64
- perl-version-0.77-129.el6.x86_64
- perl-Pod-Simple-3.13-129.el6.x86_64
- perl-5.10.1-129.el6.x86_64
- libgcrypt-1.4.5-9.el6_2.2.x86_64
- dbus-glib-0.86-5.el6.x86_64
- libnih-1.0.1-7.el6.x86_64
- gmp-4.3.1-7.el6_2.2.x86_64
- file-5.04-15.el6.x86_64
- xz-4.999.9-0.3.beta.20091007git.el6.x86_64
- libutempter-1.1.5-4.1.el6.x86_64
- procps-3.2.8-25.el6.x86_64
- psmisc-22.6-15.el6_0.1.x86_64
- db4-utils-4.7.25-17.el6.x86_64
- libss-1.41.12-14.el6.x86_64
- m4-1.4.13-5.el6.x86_64
- libgomp-4.4.7-3.el6.x86_64
- binutils-2.20.51.0.2-5.36.el6.x86_64
- ncurses-5.7-3.20090208.el6.x86_64
- less-436-10.el6.x86_64
- gzip-1.3.12-18.el6.x86_64
- cracklib-dicts-2.8.16-4.el6.x86_64
- pam-1.1.1-13.el6.x86_64
- hwdata-0.233-7.9.el6.noarch
- plymouth-scripts-0.8.3-27.el6.centos.x86_64
- cvs-1.11.23-15.el6.x86_64
- logrotate-3.7.8-16.el6.x86_64
- nss-sysinit-3.14.0.0-12.el6.x86_64
- openldap-2.4.23-31.el6.x86_64
- libcap-ng-0.6.4-3.el6_0.1.x86_64
- ethtool-3.5-1.el6.x86_64
- libevent-1.4.13-4.el6.x86_64
- libsemanage-2.0.43-4.2.el6.x86_64
- slang-2.2.1-1.el6.x86_64

- plymouth-core-libs-0.8.3-27.el6.centos.x86_64
- openssl-1.0.0-27.el6.x86_64
- python-2.6.6-36.el6.x86_64
- libcurl-7.19.7-35.el6.x86_64
- rpm-libs-4.8.0-32.el6.x86_64
- rpm-python-4.8.0-32.el6.x86_64
- python-urlgrabber-3.9.1-8.el6.noarch
- gpgme-1.1.8-3.el6.x86_64
- newt-python-0.52.11-3.el6.x86_64
- python-iniparse-0.3.1-2.1.el6.noarch
- yum-3.2.29-40.el6.centos.noarch
- mysql-libs-5.1.66-2.el6_3.x86_64
- fipscheck-1.2.0-7.el6.x86_64
- centos-release-6-4.el6.centos.10.x86_64
- iptables-1.4.7-9.el6.x86_64
- iputils-20071127-16.el6.x86_64
- initscripts-9.03.38-1.el6.centos.x86_64
- libdrm-2.4.39-1.el6.x86_64
- kbd-1.15-11.el6.x86_64
- dracut-kernel-004-303.el6.noarch
- openssh-5.3p1-84.1.el6.x86_64
- postfix-2.6.6-2.2.el6_1.x86_64
- cronie-1.4.4-7.el6.x86_64
- nfs-utils-lib-1.1.5-6.el6.x86_64
- iptables-ipv6-1.4.7-9.el6.x86_64
- dhcp-common-4.1.1-34.P1.el6.centos.x86_64
- kernel-2.6.32-358.el6.x86_64
- selinux-policy-targeted-3.7.19-195.el6.noarch
- openssh-server-5.3p1-84.1.el6.x86_64
- iwl5150-firmware-8.24.2.2-1.el6.noarch
- iwl6050-firmware-41.28.5.1-2.el6.noarch
- iwl6000g2a-firmware-17.168.5.3-1.el6.noarch
- iwl6000-firmware-9.221.4.1-1.el6.noarch
- bind-utils-9.8.2-0.17.rc1.el6.x86_64
- man-1.6f-32.el6.x86_64
- libxml2-python-2.7.6-8.el6_3.4.x86_64
- gdb-7.2-60.el6.x86_64
- efibootmgr-0.5.4-10.el6.x86_64

- sudo-1.8.6p3-7.el6.x86_64
- e2fsprogs-1.41.12-14.el6.x86_64
- attr-2.4.44-7.el6.x86_64
- iwl5000-firmware-8.83.5.1_1-1.el6_1.1.noarch
- ivtv-firmware-20080701-20.2.noarch
- xorg-x11-drv-ati-firmware-6.99.99-1.el6.noarch
- atmel-firmware-1.3-7.el6.noarch
- iwl4965-firmware-228.61.2.24-2.1.el6.noarch
- iwl3945-firmware-15.32.2.9-4.el6.noarch
- rt73usb-firmware-1.8-7.el6.noarch
- ql23xx-firmware-3.03.27-3.1.el6.noarch
- rootfiles-8.1-6.1.el6.noarch
- vmware-studio-init-2.6.0.0-130820235404.noarch
- vmware-studio-vami-cimom-2.6.0.0-631426.x86_64
- vmware-studio-vami-service-core-2.6.0.0-0.x86_64
- vmware-studio-vami-service-network-2.6.0.0-0.x86_64
- vmware-studio-vami-service-update-2.6.0.0-0.x86_64
- vmware-studio-vami-lighttpd-2.6.0.0-631426.x86_64

Appendix C: vCenter Events

The HP Operations agent on the virtual appliance collects the following vCenter events by default:

- VmSuspendedEvent
- VmResumingEvent
- VmPoweredOffEvent
- VmPoweredOnEvent
- DrsEnteredStandbyModeEvent
- DrsExitedStandbyModeEvent
- DrsDisabledEvent:DrsEnabledEvent
- VmRenamedEvent
- VmRemovedEvent
- DrsVmPoweredOnEvent
- DrsVmMigratedEvent
- NotEnoughResourcesToStartVmEvent
- VmBeingHotMigratedEvent
- VmFailedMigrateEvent
- VmMigratedEvent
- VmDiskFailedEvent
- VmFailoverFailed
- VmNoNetworkAccessEvent
- VmUuidChangedEvent
- VmUuidConflictEvent
- VmOrphanedEvent
- HostRemovedEvent
- HostShutdownEvent

Appendix D: Performance Metrics Collected from the HP Operations Agent Virtual Appliance

This topic will append the vSphere-specific metrics that are collected by the agent on VA.

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 User Guide: VMware Monitoring (Operations Agent 11.16)

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 docfeedback@hpe.com.

We appreciate your feedback!