Legal Notices

Warranty
The only warranties for Hewlett Packard Enterprise Development Company, LP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

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

Copyright Notice
© Copyright 2016 Hewlett Packard Enterprise Development LP

Trademark Notices
Adobe © is a trademark of Adobe Systems Incorporated.
Microsoft® and Windows® are U.S. registered trademarks of the Microsoft group of companies.
UNIX® is a registered trademark of The Open Group.

Documentation Updates
The title page of this document contains the following identifying information:
- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:
https://softwaresupport.hpe.com

This site requires that you register for an HPE Passport and sign in. To register for an HPE Passport ID, go to:
https://hpp12.passport.hpe.com/hppcf/createuser.do

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

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

Support
Visit the HPE Software Support Online web site at: https://softwaresupport.hpe.com

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

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

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

https://hpp12.passport.hpe.com/hppcf/createuser.do

To find more information about access levels, go to:

https://softwaresupport.hpe.com/web/softwaresupport/access-levels
# Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Chapter 1: Introduction</strong></td>
<td>................................................................. 5</td>
</tr>
<tr>
<td>HPE Operations Agent Health View Architecture</td>
<td>................................................................. 6</td>
</tr>
<tr>
<td>Health Monitoring Process and the Parameters Monitored</td>
<td>................................................................. 7</td>
</tr>
<tr>
<td>Health Parameters</td>
<td>................................................................. 8</td>
</tr>
<tr>
<td>Convention Used in this Document</td>
<td>................................................................. 11</td>
</tr>
<tr>
<td><strong>Chapter 2: Installing HPE Operations Agent Health View</strong></td>
<td>................................................................. 13</td>
</tr>
<tr>
<td>Install HPE Operations Agent Health View Package on the Server</td>
<td>................................................................. 13</td>
</tr>
<tr>
<td>Verifying HPE Operations Agent Health View Configuration on the Server</td>
<td>................................................................. 15</td>
</tr>
<tr>
<td>Install HPE Operations Agent 12.02 and Enable Health Monitoring on the Node</td>
<td>................................................................. 16</td>
</tr>
<tr>
<td>Verifying HPE Operations Agent Health Monitoring Configuration on the Node</td>
<td>................................................................. 18</td>
</tr>
<tr>
<td>Accessing HPE Operations Agent Health View</td>
<td>................................................................. 18</td>
</tr>
<tr>
<td>Supported Browsers</td>
<td>................................................................. 20</td>
</tr>
<tr>
<td>Removing HPE Operations Agent Health View from the Server</td>
<td>................................................................. 20</td>
</tr>
<tr>
<td><strong>Chapter 3: Configuring HPE Operations Agent Health View</strong></td>
<td>................................................................. 22</td>
</tr>
<tr>
<td>Configuring HPE Operations Agent Health View on the Server</td>
<td>................................................................. 22</td>
</tr>
<tr>
<td>Configuring HPE Operations Agent Health Monitoring on the Node</td>
<td>................................................................. 25</td>
</tr>
<tr>
<td>Configuring HPE Operations Agent Health Monitoring Capabilities Using ovconfchg</td>
<td>................................................................. 26</td>
</tr>
<tr>
<td>Configuring LDAP</td>
<td>................................................................. 27</td>
</tr>
<tr>
<td>Configuring the Web Server to Disable TLSv1.0</td>
<td>................................................................. 31</td>
</tr>
<tr>
<td>Configuring the Variable for Heartbeat Messages</td>
<td>................................................................. 32</td>
</tr>
<tr>
<td><strong>Chapter 4: Using the HPE Operations Agent Health View</strong></td>
<td>................................................................. 34</td>
</tr>
<tr>
<td>Using the HPE Operations Agent Health Dashboard View</td>
<td>................................................................. 34</td>
</tr>
<tr>
<td>Using the HPE Operations Agent Health Node View</td>
<td>................................................................. 37</td>
</tr>
<tr>
<td>Using the HPE Operations Agent Health Process View</td>
<td>................................................................. 39</td>
</tr>
<tr>
<td><strong>Chapter 5: Launching the HPE Operations Agent Health View from the HP Operations Manager</strong></td>
<td>................................................................. 42</td>
</tr>
<tr>
<td>Launching the HPE Operations Agent Health View from the HP Operations Manager for Linux</td>
<td>................................................................. 42</td>
</tr>
<tr>
<td>Launching the HPE Operations Agent Health View from the HP Operations Manager for Windows</td>
<td>................................................................. 44</td>
</tr>
<tr>
<td><strong>Chapter 6: Use Case</strong></td>
<td>................................................................. 47</td>
</tr>
<tr>
<td><strong>Chapter 7: Troubleshooting</strong></td>
<td>................................................................. 51</td>
</tr>
<tr>
<td><strong>Chapter 8: Performance and Sizing of the HPE Operations Agent Health View</strong></td>
<td>................................................................. 55</td>
</tr>
<tr>
<td>Test Environment</td>
<td>................................................................. 55</td>
</tr>
<tr>
<td>Recommendations</td>
<td>................................................................. 55</td>
</tr>
<tr>
<td>Conclusion</td>
<td>................................................................. 57</td>
</tr>
</tbody>
</table>

Send Documentation Feedback ................................................................. 58
Chapter 1: Introduction

HPE Operations Agent Health View is a health monitoring tool that provides a quick overview of the HPE Operations Agent health.

HPE Operations Agent Health View plays an important role in a complex environment that has many HPE Operations Agents deployed on multiple nodes. For example, on a specific managed node if any of the health or policy parameters have failed or if any of the processes have issues, then you will not receive alerts or messages from that managed node.

HPE Operations Agent Health View enables you to quickly identify issues in a complex environment with several managed nodes.

**Note:** You can set the HPOM Management Server as the Health View Server or you can install HPE Operations Agent Health View on a server other than the HPOM Management Server.

User Interface

HPE Operations Agent Health View offers the following features:
- Provides a consolidated dashboard that shows the health of all the HPE Operations Agents configured with HPE Operations Agent Health View.
- Allows you to drill-down into each managed node and view the list of HPE Operations Agent processes and resources that are used.
- Allows you to drill-down into each HPE Operations Agent process and identify issues related to health and policy parameters.

**HPE Operations Agent Health View Architecture**

HPE Operations Agent Health View is a health monitoring tool that provides a quick overview of the HPE Operations Agent health.

The HPE Operations Agent Health View architecture is as follows:

HPE Operations Agent Health View consists of the server and the agent components. The server component has the **HPCS Server process (hpcsrvd)** running, which acts as a registry that contains the details of the nodes available in the environment. On
every node, Heart Beat Polling (HBP) is enabled and the node pushes its information to the HPCS Server process (hpcsvd).

The agent component collects and provides the collected information to the Health View Server.

At every configured interval, **Action Agent** (opcacta) triggers the **AHSCollector** (Agent Health and System Data Collector is a BBC client process and it is not configurable) to collect the agent health information. Each sub agent maintains its state information based on the defined health and policy parameters. AHSCollector queries the sub agents for the health data through the HTTP interface. It analyzes the collected data for potential issues. Also, for every failed parameter, AHSCollector runs the configured diagnostic commands to find a potential cause for the failure. AHSCollector saves the processed state data in the **Agent Log Files**. **HP Compute Sensor process (hpsensor)** running on the node exposes this data to the Health View Server along with the system performance data.

**Note:** HP Compute Sensor (hpsensor) is a light-weight performance and log data collection process.

**Authentication**

HPE Operations Agent Health View server runs on a Tomcat server. The default Tomcat server port is 8444 and the URL to access the HPE Operations Agent Health View is:

```
https://<servername>:tomcatserverport/HV
```

If LDAP is configured, then user authentication is required to access HPE Operations Agent Health View. Authentication is provided using Microsoft Active Directory or OpenLDAP. The user name and password entered in the message browser is sent to the Tomcat server and then to the LDAP server for authentication. The user name and password is validated against LDAP server database. If authentication is successful, then the HPE Operations Agent Health Dashboard View appears. For more information about configuring LDAP, see **Configuring LDAP**.

If LDAP server is not configured, then user authentication is not required.

**Health Monitoring Process and the Parameters Monitored**

HPE Operations Agent Health View monitors the health of different agent processes based on the following:

- State change notifications at node view level is enabled by default for all the processes listed under **ovc** and **ovpa**:  
  - To view the processes listed under ovc, run the following command:
    ```
    ovc -status
    ```

HPE Operations Agent (12.02)  
Page 7 of 58
• To view the processes listed under ovpa, run the following command:
  ○ On Windows: perfstat -o
  ○ On Unix/Linux: ovpa -status perf

• Running processes list in the node view is driven by the HPE Operations Agent application configuration in the param file and it includes the agent, LCore, and perf processes.

• In the process view tab, resource utilization and performance data table is available for all the processes listed in the running process list in the node view table.

• In the process view tab, health parameters and policy parameters table is available for the agent processes which provide the agent health interface (run bbcutil -reg to see the list of processes which provide the agent health interface).

• Additionally, health parameters are implemented for some perf processes (perfd and perfalarm) through external collection method. These processes do not provide any health interface.

Health Parameters

Health Parameters are the parameters or the set of attributes defined for a process depending on what the process is expected to do.

The following table provides the health parameter details that affect the performance and utilization of different agent processes:

<table>
<thead>
<tr>
<th>Process</th>
<th>Health Parameter</th>
<th>Parameter Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>opcmsga</td>
<td>Buffer File Garbage</td>
<td>Message agent (opcmsga) uses msgagtdf as temporary storage for outgoing messages. It</td>
</tr>
<tr>
<td>(Message Agent)</td>
<td>Collector</td>
<td>is also used to buffer messages when the server is not reachable. Buffer file garbage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>collector removes unwanted messages from msgagtdf.</td>
</tr>
<tr>
<td></td>
<td>Message Forwarding to</td>
<td>This parameter ensures that the agent is able to forward alerts and events to the</td>
</tr>
<tr>
<td></td>
<td>Server</td>
<td>server. If this parameters fails, then the agent will be in the buffering mode.</td>
</tr>
<tr>
<td>opcacta</td>
<td>Read Action Request</td>
<td>This parameter indicates whether the action agent is able to successfully read an</td>
</tr>
<tr>
<td>(Action Agent)</td>
<td></td>
<td>action request from the action queue.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Failed Actions in Last One Hour</td>
<td>The action agent (opcacta) is responsible for starting automatic actions, operator-initiated actions, and scheduled actions. This parameter indicates any failed actions in the last one hour.</td>
<td></td>
</tr>
<tr>
<td>Scheduled Action Request Count in Last One Hour</td>
<td>This parameter indicates the total number of scheduled actions in the last one hour.</td>
<td></td>
</tr>
<tr>
<td>Auto Action Request Count in Last One Hour</td>
<td>This parameter indicates the total number of auto actions in the last one hour.</td>
<td></td>
</tr>
<tr>
<td>oacore (Data Collector)</td>
<td>Total Requests in Last One Hour</td>
<td></td>
</tr>
<tr>
<td></td>
<td>oacore provides a read and write interface for system performance and custom data. This parameter indicates the number of requests processed in the last one hour.</td>
<td></td>
</tr>
<tr>
<td>Last Model Update</td>
<td>oacore provides a read and write interface for system performance and custom data based on model defined. This parameter indicates when the last successful model update occurred.</td>
<td></td>
</tr>
<tr>
<td>Time to Log Data into DataStore</td>
<td>oacore provides a read and write interface for system performance and custom data. This parameter provides the time required to log data into datastore.</td>
<td></td>
</tr>
<tr>
<td>opclog (Logfile Encapsulator)</td>
<td>Log File Processing</td>
<td>This parameter indicates the state of the log file processing.</td>
</tr>
<tr>
<td></td>
<td>Windows Event Log Processing</td>
<td>This parameter indicates the state of the event log processing. It also indicates whether opclog is able to subscribe to the event channel (Parameter: Windows Event Channel Subscription).</td>
</tr>
<tr>
<td></td>
<td>Log File Conversion Commands</td>
<td>Checks whether opclog is able to execute log file pre-processing commands successfully.</td>
</tr>
<tr>
<td>opcmsgi (Message Interceptor)</td>
<td>Policy Initialization</td>
<td>This parameter indicates whether opcmsgi is able to load the msgi type of policies correctly and convert them into required</td>
</tr>
<tr>
<td><strong>opctrapi</strong> (Trap Interceptor)</td>
<td><strong>Read Message Interceptor Queue</strong></td>
<td>This parameter indicates whether the opcmsgi is able to read the message interceptor queue file.</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>opcmona</strong> (Monitoring Agent)</td>
<td><strong>Incoming Traps</strong></td>
<td>Checks whether the trap interceptor (opctrapi) is able to receive incoming traps successfully.</td>
</tr>
<tr>
<td></td>
<td><strong>Traps Received in Last One Hour</strong></td>
<td>SNMP Trap interceptor (opctrapi) is the message interface for feeding SNMP events. This parameter indicates the number of traps received in the last one hour.</td>
</tr>
<tr>
<td></td>
<td><strong>Policy Loading</strong></td>
<td>This parameter indicates whether the trap interceptor (opctrapi) is able to load the SNMP type of policies correctly and convert them into the required format.</td>
</tr>
<tr>
<td></td>
<td><strong>SNMP Session</strong></td>
<td>This parameter indicates whether trap interceptor (opctrapi) is able to open a SNMP session to receive traps.</td>
</tr>
<tr>
<td></td>
<td><strong>DataStore Connection</strong></td>
<td>This parameter indicates the monitoring agent (opcmona) connection to datastore.</td>
</tr>
<tr>
<td></td>
<td><strong>AdvMon Schedule Actions</strong></td>
<td>This parameter indicates whether the monitoring agent (opcmona) is able to schedule the action as mentioned in the schedule policy.</td>
</tr>
<tr>
<td></td>
<td><strong>DataStore Feed</strong></td>
<td>This parameter indicates whether the monitoring agent (opcmona) is able to feed the custom data to the datastore successfully.</td>
</tr>
<tr>
<td></td>
<td><strong>SNMP Session</strong></td>
<td>This parameter indicates whether the monitoring agent (opcmona) is able to open a session to connect to the SNMP daemon.</td>
</tr>
<tr>
<td></td>
<td><strong>SNMP GET</strong></td>
<td>This parameter indicates whether the monitoring agent (opcmona) is able to fetch SNMP MIB information.</td>
</tr>
</tbody>
</table>
### SNMP WALK
This parameter indicates whether the monitoring agent (opcmona) is able to fetch SNMP information from multiple MIBs.

### WMI Connection
This parameter indicates whether the monitoring agent (opcmona) is able to collect data from local or remote system.

### Perl Engine Creation
This parameter indicates whether the monitoring agent (opcmona) is able to load the embedded Perl engine for executing Perl scripts.

### Perl Script Execution
This parameter indicates whether the monitoring agent (opcmona) is able to run the embedded Perl scripts to monitor or schedule policies successfully.

### perfd License Check
This parameter checks the perfd license.

### Client Connection
This parameter indicates the cpsh connection to perfd.

### perfalarm License Check
This parameter checks the perfalarm license.

---

### Convention Used in this Document
The following conventions are used in this document.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
</table>
| `<OvBinDir>` | `<OvBinDir>` is used in this document to imply the following location:  
  - On Windows:  
    - Windows x64: %OvInstallDir%bin\win64\  
    - Windows x86: %OvInstallDir%bin\  
  - On Linux/HP-UX/Solaris: /opt/0V/bin/  
  - On AIX:/usr/lpp/0V/bin/ |

### Health View
System on which the HPE Operations Agent Health View server is
| Server | installed. |
Chapter 2: Installing HPE Operations Agent Health View

HPE Operations Agent Health View can be installed using the following steps:

1. **Install HPE Operations Agent Health View package on the server.**
   
   **Note:** HPE Operations Agent Health View is supported on Linux and Windows x64 platforms only.

2. **Install HPE Operations Agent 12.02 and enable health monitoring on the node.**

### Install HPE Operations Agent Health View Package on the Server

HPE Operations Agent Health View package can be installed by one of the following methods:

- **Install HPE Operations Agent Health View during the registration of the HPE Operations Agent 12.02 on the HPOM Management Server.**

  **Note:** Irrespective of the platform you want to register, Health View package can be installed during the registration of the HPE Operations Agent 12.02.

  **Or**

- **Install HPE Operations Agent Health View without registering HPE Operations Agent 12.02 on the HPOM Management Server.**

  **Or**

- **Install HPE Operations Agent Health View on a server other than the HPOM Management Server.**

### Prerequisites

- Local agent on the Health View Server must be upgraded to HPE Operations Agent 12.02.

- Trust must be established between the server and the nodes for successful communication. Ensure certificates from the same authority are installed on the Health View Server and the nodes. If the certificates are from different certificate authorities, then exchange the CA certificates and import them into the node and the trusted keystores. For more information, see "Establishing a Trust Relationship Between the
Two Management Servers" in the HP Operations Manager Installation Guide for Linux or "Configure trusted certificates for multiple management servers" in the HP Operations Manager Online Help for Windows.

- If you use only the Performance Collection Component of the HPE Operations Agent (HP Operations OS Inst Performance LTU):
  - Ensure that you disable the default HBP configuration to the HPOM Management Server. For more information, see Configuring Health View Capabilities.

- In the profile file, add the OPC_SELFMON_SERVER variable to update the Health View Server and set the OPC_SELFMON_ENABLE variable to TRUE.

  **Note:** If you set the OPC_SELFMON_ENABLE variable to TRUE after installation, you must start the action agent (opcacta) manually.

- If certificates are installed on the server and the nodes, ensure that the certificates are from the same authority. When certificates are installed, the communication between the server and the nodes is through HTTPS mode.

- If no certificates are installed either on the server or the nodes, then the communication between the server and the nodes is through HTTP mode.

  **Note:** Local agent on the Health View Server is considered as any other node in your environment.

### Install HPE Operations Agent Health View

<table>
<thead>
<tr>
<th>Task</th>
<th>Follow these steps</th>
</tr>
</thead>
</table>
| Install HPE Operations Agent Health View during the registration of the HPE Operations Agent 12.02 on the HPOM Management Server. | 1. Make sure that you have downloaded the .ISO file or obtained the physical DVD of the HPE Operations Agent 12.02.  
2. Log on to the server as an administrator.  
3. Extract the contents of the .ISO file into a local directory on the server or mount the .ISO file.  
4. Go to the media root and run the following command to register the agent deployment packages and install the health view package:  
  - On Windows: cscript oainstall.vbs -i -m -hv|healthview  
  - On Linux: ./oainstall.sh -i -m - |
### Install HPE Operations Agent Health View, continued

<table>
<thead>
<tr>
<th>Install HPE Operations Agent Health View without registering on the HPOM Management Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Make sure that you have downloaded the .ISO file or obtained the physical DVD of the HPE Operations Agent 12.02.</td>
</tr>
<tr>
<td>2. Log on to the server as an administrator.</td>
</tr>
<tr>
<td>3. Extract the contents of the .ISO file into a local directory on the server or mount the .ISO file.</td>
</tr>
<tr>
<td>4. Go to the media root and run the following command to install the health view package:</td>
</tr>
<tr>
<td>- <strong>On Windows:</strong> `cscript oainstall.vbs -i -hv</td>
</tr>
<tr>
<td>- <strong>On Linux:</strong> `./oainstall.sh -i -hv</td>
</tr>
<tr>
<td>5. Verify HPE Operations Agent Health View configuration on the server.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Or</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install HPE Operations Agent Health View on a Server other than the HPOM Management Server</td>
</tr>
</tbody>
</table>

1. **Verify HPE Operations Agent Health View configuration on the server.**

### Note:
For additional configuration settings, see [Custom Settings for HPE Operations Agent Health View on the Server](#).

---

**Verifying HPE Operations Agent Health View Configuration on the Server**

Run the following command to verify HPE Operations Agent Health View configuration on the server:

```
<OVBinDir>ovc -status
```

Check if the `hpcsrvd` process is running on the server to verify the configuration of HPE Operations Agent Health View on the server.
Install HPE Operations Agent 12.02 and Enable Health Monitoring on the Node

You can enable HPE Operations Agent health monitoring on the node either during the installation or after the installation of HPE Operations Agent 12.02.

- Enable health monitoring on the node during the installation of HPE Operations Agent 12.02 using one of the following methods:
  - Health monitoring is enabled on the node by default when you remotely deploy HPE Operations Agent 12.02 from a HPOM Management Server.
  - If you use HP Operations OS Inst Adv SW LTU and if you want to set the HPOM Management Server as the Health View Server, then health monitoring is enabled on the node by default when you upgrade the node to HPE Operations Agent 12.02.
  - Enable health monitoring during installation of the HPE Operations Agent 12.02 using the profile file (see HPE Operations Agent Installation Guide for more information about using the profile file):
    - If you use HP Operations OS Inst Adv SW LTU and if you want to set the HPOM Management Server as the Health View Server, then health monitoring is enabled on the node by default.
      Or
    - If you use HP Operations OS Inst Performance LTU or if you have installed HPE Operations Agent Health View on a server other than the HPOM Management Server, then add `set agent.health:OPC_SELFMON_ENABLE=TRUE` and also add `set agent.health:OPC_SELMON_SERVER=<health view server IP address>` in the profile file to enable health monitoring on the node.
  - If you use Glance Pak Software LTU, then add `set agent.health:OPC_SELFMON_ENABLE=TRUE` and also add `set agent.health:OPC_SELMON_SERVER=<health view server IP address>` in the profile file to enable health monitoring on the node.
- Enable health monitoring on the node after the installation of HPE Operations Agent 12.02 using one of the following methods:
  - If you use HP Operations OS Inst Adv SW LTU and if you want to set the HPOM Management Server as the Health View Server, then run the following command to enable health monitoring on the node:
On UNIX:
- On Linux/HP-UX/Solaris: /opt/perf/bin/selfmon_configure.pl -enable
- On AIX: /usr/lpp/perf/bin/selfmon_configure.pl -enable
- On Windows: %OvInstallDir%nonOV\perl\a\bin\perl.exe
  %OvInstallDir%bin\selfmon_configure.pl -enable

If you use HP Operations OS Inst Performance LTU or if you have installed HPE Operations Agent Health View on a server other than the HPOM Management Server, then run the following command to enable health monitoring on the node:

On UNIX:
- On Linux/HP-UX/Solaris: /opt/perf/bin/selfmon_configure.pl -enable -s <health view server IP address>
- On AIX: /usr/lpp/perf/bin/selfmon_configure.pl -enable -s <health view server IP address>
- On Windows: %OvInstallDir%nonOV\perl\a\bin\perl.exe
  %OvInstallDir%bin\selfmon_configure.pl -enable -s <health view server IP address>

If you use Glance Pak Software LTU, then run the following command to enable health monitoring on the node:

On UNIX/Linux: /opt/perf/bin/selfmon_configure.pl -enable -s <health view server IP address>

### Note:
- If you use HP Operations OS Inst Performance LTU, then you must start action agent (opcacta) manually after running the selfmon_configure.pl script to enable health monitoring. Run the following command to start opcacta:
  `<OvBinDir>ovc -start opcacta`

- If you have installed HPE Operations Agent Health View on a server other than the HPOM Management Server, then configure the nodes with the IP address of the system where HPE Operations Agent Health View is configured. For more information, see Configuring HPE Operations Agent Health Monitoring on the Node.

- HPE Operations Agent Health View is not available if you use only the Glance Software LTU.
Verifying HPE Operations Agent Health Monitoring Configuration on the Node

Run the following command to verify HPE Operations Agent health monitoring on the node:

```
<OvBinDir>ovc -status
```

Check if the `hpsensor` process is running on the node to verify the configuration of HPE Operations Agent health monitoring on the node.

**Note:** If you use **HP Operations OS Inst Adv SW LTU** or **HP Operations OS Inst Performance LTU**, then set the configuration variable `OPC_SELFMON_ENABLE` to **TRUE** for `hpsensor` to run.

Accessing HPE Operations Agent Health View

Follow the steps to access HPE Operations Agent Health View:

1. Enter the following address on a browser to open the **HPE Operations Agent Health View**:

   ```
   https://<server_name>:<tomcat_port>/HV
   ```

   In this instance:

   `<server_name>`: Name of the server where Tomcat is running and the Health View Server is configured. By default, the HPOM Management Server is configured as Health View Server.

   `<tomcat_port>`: Port number on which the Tomcat server is running. By default, port 8444 is configured.

   **Note:** Configure nodes with HPE Operations Agent health monitoring. For more information, see *Configuring HPE Operations Agent Health Monitoring on the Node*. After configuring nodes with HPE Operations Agent health monitoring, the configured node appears on the Health View Server only after 5 minutes.

2. If LDAP is configured, then user authentication is required to access HPE Operations Agent Health View. Log in using the LDAP user credentials. For more information about configuring LDAP see, *Configuring LDAP*. If LDAP server is not configured, then user authentication is not required.

   If LDAP server is configured, the HPE Operations Agent Health View Login page appears.
Enter the User name, Password and then click **Login**. The **HPE Operations Agent Health Dashboard View** appears.

3. Click any **Host Name** on the Health View Server to open the **HPE Operations Agent Node Health View** for the specific managed node. You can monitor the health and performance status of the node.

4. Click any **Process Name** on the node health view to open the **HPE Operations Agent Process Health View** of the specific HPE Operations Agent process. You can monitor the resource utilization, health, and policy parameter details of the process.

5. To log out of HPE Operations Agent Health View, click the user name drop-down and then click **LogOut**.

The following message is displayed:

You have successfully logged out of HPE Operations Agent Health View.

**Note:**
- Once logged-in, if a user session is inactive for 20 minutes, the session expires and the system logs out the user.
- On Windows, Health View Server will access the required files even if the file path contains special characters like ~ symbol. This will be restricted only if the Windows settings are updated to restrict special characters in the file path.
### Supported Browsers

Use the following web browsers to access the HPE Operations Agent Health View:

<table>
<thead>
<tr>
<th>Operating Systems</th>
<th>Supported Browsers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows</td>
<td>Internet Explorer 10 and 11</td>
</tr>
<tr>
<td></td>
<td>Google Chrome 43</td>
</tr>
<tr>
<td></td>
<td>Mozilla Firefox 38 (ESR)</td>
</tr>
<tr>
<td>Linux</td>
<td>Mozilla Firefox 38 (ESR)</td>
</tr>
<tr>
<td>Apple Mac OS X</td>
<td>Safari 7.1.6</td>
</tr>
</tbody>
</table>

### Removing HPE Operations Agent Health View from the Server

To remove the HPE Operations Agent Health View packages from the server, perform the following steps:

1. Log on to the server as an administrator.
2. Go to the following directory:
   - *On Windows:* `%ovinstalldir%\bin\OpC\agtinstall`
   - *On Linux:* `/opt/OV/bin/OpC/agtinstall`
3. Run the following command if you have set HPOM Management Server as the Health View Server:
   - *On Windows:* `cscript oainstall.vbs -r -m -healthview`
   - *On Linux:* `./oainstall.sh -r -m -healthview`
4. Run the following command if you have installed HPE Operations Agent Health View on a server other than the HPOM Management Server:
   - *On Windows:* `cscript oainstall.vbs -r -healthview`
   - *On Linux:* `./oainstall.sh -r -healthview`

**Note:** On Linux systems, removing the HPE Operations Agent Health View package
will not remove HPOvJREB and HPOvtomcat packages, these packages have to be removed manually.
Chapter 3: Configuring HPE Operations Agent Health View

You can update default configuration settings for HPE Operations Agent Health View on the Health View Server and HPE Operations Agent health monitoring on the node.

- Configuring HPE Operations Agent Health View on the Server
- Configuring HPE Operations Agent Health Monitoring on the Node

Configuring HPE Operations Agent Health View on the Server

After installing the HPE Operations Agent Health View on the server, you can use the `hpcsrv.conf` file to change the default configuration settings.

Follow the steps:

1. Log on to the server as an administrator.
2. Go to the following directory:
   - **On Windows**: `%OvDataDir%shared\server\hpcsrv\`
   - **On Linux**: `/var/opt/OV/shared/server/hpcsrv/`
3. Open the `hpcsrv.conf` file and edit the following values:

<table>
<thead>
<tr>
<th>Namespace</th>
<th>Parameter</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>hpcs.runtime</td>
<td>port</td>
<td>Update the default port number as <code>port=&lt;Value&gt;</code>. By default, port 8092 is configured. In this instance, <code>&lt;Value&gt;</code> is the port number that is used by the HPE Operations Agent Health View Server.</td>
</tr>
<tr>
<td>hpcs.runtime</td>
<td>num_threads</td>
<td>Update the default number of threads as <code>num_threads=&lt;Value&gt;</code>. By default, the number of threads is set to 30. In this instance, <code>&lt;Value&gt;</code> is the number of worker threads allocated to handle the</td>
</tr>
</tbody>
</table>
incoming requests from clients. Increase this value if the number of incoming requests are more.

**hpcs.runtime**

- **connection_backlog**
  - Update the default connection backlog as `connection_backlog=<Value>`. By default, the connection backlog is set to 16384 on Windows and 512 on Linux.
  - In this instance, `<Value>` is the length of the backlog socket queue for the web server. Set it to a higher value to obtain maximum scalability.

**hpcs.runtime**

- **regBBC**
  - Set `regBBC=true` for the hpcsrv component to get registered with BBC.

**hpcs.registry**

- **UpdateInterval**
  - Update the default update interval value as `UpdateInterval=<Value>`. The default value is 60 seconds.
  - In this instance, `<Value>` is the frequency at which HBP entries are consolidated. Set it to a higher value to obtain maximum scalability.

**hpcs.trace**

- **Debug_Level**
  - Update the debug level value as one of the following: `Debug_Level=<INFO/WARN/ERROR/DEBUG/ALL>`. Example: `Debug_Level=INFO` provides traces of INFO messages to `hpcsrvtrace.log`.

---

**Note:** If any of the parameters are configured manually, then you must restart **hpcsrvd**. Run the following command to restart **hpcsrvd**:

```
<OvBinDir>ovc -restart hpcsrvd
```

Additionally, you can use the XPL variable listed in the following table to configure the default behavior of the **hpcsrvd** process:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Namespace</th>
<th>Description</th>
<th>Restart Required</th>
<th>Default Value</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENFORCE_SERVER_SSL</td>
<td>hpcsrvd</td>
<td>This parameter controls the connections allowed at the HTTP server.</td>
<td>YES</td>
<td>ALL</td>
<td>String</td>
</tr>
<tr>
<td>Variable</td>
<td>Namespace</td>
<td>Description</td>
<td>Restart Required</td>
<td>Default Value</td>
<td>Type</td>
</tr>
<tr>
<td>----------</td>
<td>-----------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
<td>---------------</td>
<td>------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This parameter may be set to one of the following values:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NONE: Both SSL and non-SSL connections will be accepted by the HTTP server.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>REMOTE: All remote connections to the HTTP server must use SSL. Remote connections that do not use SSL will be automatically rejected. Local connections may use SSL or non-SSL.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ALL: All connections to the HTTP server must use SSL. Connections that do not use SSL will be rejected automatically.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>This parameter is ignored if set to any other value. The HTTP server will then use the authentication specified by the application that created the HTTP server. This parameter is not case sensitive.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Use caution when setting this parameter as it will disable security features if set to 'NONE' or 'REMOTE'.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Log Files**
HPCS log file `hpcsrvtrace.log` is available in the following directory:

- **On Windows**: `%OvDataDir%shared\server\hpcsrv\`
- **On Linux**: `/var/opt/OV/shared/server/hpcsrv/`

### Configuring HPE Operations Agent Health Monitoring on the Node

You can update default configuration settings for the HPE Operations Agent health monitoring using `selfmon_configure.pl` script after installing of the HPE Operations Agent 12.02. Follow the steps:

1. Log on to the node where you have installed HPE Operations Agent 12.02 as an administrator.
2. You can configure the following parameters using the `selfmon_configure.pl` script:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>`-e</td>
<td>--enable<code>or</code>-d</td>
</tr>
<tr>
<td>`-s</td>
<td>--server`</td>
</tr>
<tr>
<td>`-i</td>
<td>--interval`</td>
</tr>
</tbody>
</table>

**For Example:**

To update the HPE Operations Agent Health View Server, run the following command:

- **On UNIX:**
  - **On Linux/HP-UX/Solaris**: `/opt/perf/bin/selfmon_configure.pl -enable -s <health view server IP address>`
on AIX: /usr/lpp/perf/bin/selfmon_configure.pl -enable -s <health view server IP address>

On Windows:

%OvInstallDir\nonOV\perl\a\bin\perl.exe %OvInstallDir\bin\selfmon_configure.pl -enable -s <health view server IP address>

In this instance:
<server> is the IP address or the host name of the Health View Server.
%OvInstallDir\nonOV\perl\a\bin\perl.exe is the path to Perl on Windows.

Note: Set HP Operations OS Inst Adv SW LTU or HP Operations OS Inst Performance LTU to ensure that health monitoring is functional before running selfmon_configure.pl script.

Note: If any of the parameters are configured manually, then you must restart hpsensor.

Run the following command to restart hpsensor:
<OvBinDir>ovc -restart hpsensor

Log Files and hpcs.conf File

HPCS log files hpcstrace.log and hpcswatch.log and the hpcs.conf file are available in the following directory:

On Windows: %OvDataDir%hpcs\n
On UNIX/Linux: /var/opt/0V/hpcs/

Configuring HPE Operations Agent Health Monitoring Capabilities Using ovconfchg

You can also use ovconfchg to configure the following health monitoring capabilities:

To enable the HPE Operations Agent health monitoring, run the following command:
<OvBinDir>ovconfchg -ns agent.health -set OPC_SELFMON_ENABLE TRUE
The default value is FALSE.

To set the agent health monitoring interval, run the following command:
<OvBinDir>ovconfchg -ns agent.health -set OPC_SELFMON_INTERVAL <value>
The default value is 300 seconds and the minimum value recommended is 60 seconds.
- To disable the default HBP configuration, run the following command:
  
  ```
  <OvBinDir>ovconfchg -ns agent.health -set OPC_SELFMON_HBP FALSE
  
  The default value is TRUE.
  ```

- To update/modify the Health View Server, run the following command:
  
  ```
  <OvBinDir>ovconfchg -ns agent.health -set OPC_SELFMON_SERVER
  <health view server IP address>
  
  By default, the HPOM Management Server is configured as Health View Server.
  ```

## Configuring LDAP

User authentication in HPE Operations Agent Health View is provided using Microsoft Active Directory or OpenLDAP. You can configure LDAP from the Dashboard View of the HPE Operations Agent Health View.

To configure LDAP for HPE Operations Agent Health View, follow the steps:

1. From the Dashboard View, click (Settings). The **LDAP Configuration** page appears.

   ![LDAP Configuration Page](image)

2. Provide the following information to configure LDAP:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>The fully-qualified LDAP server domain name (server.domain.com) or</td>
</tr>
<tr>
<td>Port</td>
<td>SSL</td>
</tr>
<tr>
<td>Base DN</td>
<td>dc=my-domain,dc=com</td>
</tr>
<tr>
<td>User Group DN</td>
<td>cn=groupDC,ou=users</td>
</tr>
<tr>
<td>Admin Group DN</td>
<td>cn=adminGroup,ou=users</td>
</tr>
<tr>
<td>UserDN</td>
<td>cn=manager,dc=my-domain,dc=com</td>
</tr>
<tr>
<td>UserPassword</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IP</td>
<td>IP address.</td>
</tr>
<tr>
<td>Port</td>
<td>The port used to connect to the LDAP server. The default port number for LDAP and LDAPS (LDAP over SSL) server is 389 and 636 respectively.</td>
</tr>
<tr>
<td>SSL</td>
<td>If the LDAP server is configured to require LDAPS, select the SSL check box.</td>
</tr>
</tbody>
</table>
| Keystore Location | Location of the Keystore that stores the LDAP server certificate. This field is mandatory if the SSL check box is selected. To get the Keystore location, perform the following steps:  
   a. Obtain the Server Certificate  
      You must add the Microsoft Active Directory server SSL certificate to the list of accepted certificates used by the HPE Operations Agent Health View server. To add the certificate, export the certificate by running the following command on the Microsoft Active Directory server:  
      `certutil  -ca.cert <sample.crt>`  
      In this instance,  
      `sample.crt` is the name of the SSL certificate that you want to export to the HPE Operations Agent Health View server.  
   b. Import the Server Certificate  
      You must import the Microsoft Active Directory server certificate to the keystore for SSL enabled communication between the HPE Operations Agent Health View server and the Microsoft Active Directory. Follow the steps:  
      i. Run the following command to obtain the KeystoreFile value:  
         `<OvBinDir>ovconfget NONOV.TomcatB`  
         The KeystoreFile value will be as shown:  
         KeystoreFile=/var/opt/OV/certificates/tomcat/b/tomcat.keystore  
      ii. Run the following commands to import the server certificate:  
         - `/opt/OV/nonOV/jre/b/bin/keytool -importcert -keystore`  
         - `/opt/OV/nonOV/jre/b/lib/security/cacerts -file <LDAP_CA_certificate>` |
The keytool prompts you for a password. The default password is changeit. Select yes to confirm the key import when prompted with Trust this Certificate?[no]: yes

In this instance, `<keystore_file>` is the KeystoreFile value obtained during Step i.

`<LDAP_CA_certificate>` is the location and name of the CA certificate that you want to import. For example `/root/sample.crt`

iii. Restart the ovтомcat process, run the following commands:

```
ovc -stop ovтомcat
ovc -start ovтомcat
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Base DN</strong></td>
<td>The Base Distinguished Name represents the top most level of the LDAP directory from where the LDAP search begins. For example, <code>dc=mydomain,dc=com</code></td>
</tr>
<tr>
<td><strong>User Group DN</strong></td>
<td>The Distinguished Name of the Group or Organization Unit (OU) of users without administrator rights. The value is relative to the Base DN value. Multiple values should be separated with the `</td>
</tr>
<tr>
<td><strong>Admin Group DN</strong></td>
<td>The Distinguished Name of the Group or Organization Unit (OU) of users with administrator rights. The value is relative to the Base DN value. Multiple values should be separated with the `</td>
</tr>
<tr>
<td><strong>User ID (Full DN)</strong></td>
<td>The full Distinguished Name of the user with search permissions. For example, <code>cn=Manager,dc=mydomain,dc=com</code></td>
</tr>
<tr>
<td><strong>User Password</strong></td>
<td>Password of the User ID.</td>
</tr>
</tbody>
</table>

3. Click the **Save LDAP** option.
After saving the LDAP configuration, the user name is displayed on the top right corner.

![User name](image)

**Note:**
- All fields marked with asterisk (*) are mandatory. You can save the LDAP server information only after all the mandatory fields are filled.
- If required, **Admin Group** user can change the LDAP configuration any time.
- Click the **Skip LDAP** option, if you do not want to configure LDAP. If LDAP is configured for a user, then **Skip LDAP** option will be disabled.

**Removing the LDAP configuration**

Follow the steps to remove the LDAP configuration for HPE Operations Agent Health View:

1. Log on to HPE Operations Agent Health View as a root user.
2. Run the following command at the command prompt:
   ```
   /opt/OV/bin/ovconfchg -edit
   ```
   A text file opens.

   **For example:**
   ```
   [agent.health]
   BASEDN=dc=my-domain,dc=com
   HOST=iwfvm01230.hpswlabs.adapps.hp.com
   ISSSL=false
   OPC_SELFMON_ENABLE=True
   PORT=389
   SSL_KEY_STORE_PATH=
   USERDN=ou=qaou,dc=my-domain,dc=com
   ```

3. Delete all the contents in the [agent.health] namespace except OPC_
SELFMON_ENABLE=True.

4. Save and close the file.

Configuring the Web Server to Disable TLSv1.0

TLSv1.0 protocol is considered insecure as it cannot support strong cipher suites. The insecure protocol version prevents the protection mechanism for the data transmitted between the client and the web server. Therefore, it is recommended to configure the web server to use the most secure protocol such as, TLSv1.1 or TLSv1.2. The insecure protocol, TLSv1.0 must be disabled for secure communication.

Follow these steps to disable the TLSv1.0 protocol in OvTomcatB:

1. Log on to HPE Operations Agent Health View as a root user.
2. Run the following command at the command prompt:
   ```
   <OVBinDir>/bin/ovconfchg -edit
   ```
   A text file opens.
3. In the text file, edit the following values under the NONOV.TomcatB namespace:
   a. Modify the SslProtocol value by setting it to either TLSv1.1 or TLSv1.2:
      ```
      SslProtocol=TLSv1.1
      ```
      The default value for SslProtocol is TLSv1.
   b. Modify the sslEnabledProtocols value by removing TLSv1 and then setting it to the following:
      ```
      sslEnabledProtocols=TLSv1.1, TLSv1.2
      ```
      The default value for sslEnabledProtocols is TLSv1, TLSv1.1, TLSv1.2.

   **Note:** Once you install the HPE Operations Agent Health View server, the NONOV.TOMCATB namespace is created by default.

4. Create the following namespace in the text file:
   ```
   [sec.core.ssl]
   COMM_PROTOCOL=TLSv1.1 or TLSv1.2
   ```

   **Note:** The supported values for COMM_PROTOCOL are TLSv1, TLSv1.1 and TLSv1.2. If any values other than the supported values are set, then the communication between all the protocols are allowed.

   - If you set TLSv1, then TLSv1, TLSv1.1 and TLSv1.2 protocols are used for secure communication.
If you set TLSv1.1, then TLSv1.1 and TLSv1.2 protocols are used for secure communication.

If you set TLSv1.2, then only the TLSv1.2 protocol is used for secure communication.

5. Save and close the text file.

6. Run the following commands to restart HPE Operations Agent for the changes to take effect:
   a. `ovc -kill`
   b. `ovc -start`

A cipher suite is a named combination of authentication, encryption, message authentication code (MAC) and key exchange algorithms which is used to transfer the security settings for a network connection using the Transport Layer Security (TLS) or Secure Sockets Layer (SSL) network protocol.

### Configuring the Variable for Heartbeat Messages

The HPE Operations Agent sends heartbeat messages to the management server only if there is no regular message sent within the heartbeat interval. The OPC_HB_MSG_INTERVAL variable is disabled by default. Only if the OPC_HB_MSG_INTERVAL variable is enabled, the HPE Operations Agent can send alive messages to the management server in a configurable interval. The normal heartbeat messages are sent as log-only messages. If you stop the HPE Operations Agent, a critical heartbeat message is sent to the management server.

Run the following command to configure the OPC_HB_MSG_INTERVAL variable, available under the agent.health namespace:

```
<OvBinDir>ovconfchng -ns agent.health -set OPC_HB_MSG_INTERVAL <value>
```

In this instance, `<value>` is the configurable time interval in seconds.

**Note:** The following message key identifier is used for heartbeat messages:

`MsgKey = 8c72e1fa-b1f1-4def-8c7e-71ec8e643351:<coreId>`

The other message attributes used for heartbeat messages include MSGTXT, APPLICATION, OBJECT, SEVERITY, SERVICEID, MSGKEYRELATION and ICON.

The heartbeat messages with Normal severity must be sent as log only events.

The following configuration setting is used for the OPC_HB_MSG_INTERVAL variable:

```
[agent.health]
```
OPC_HB_MSG_INTERVAL= <time in seconds>

For example:

If you want the HPE Operations Agent to send heartbeat messages at a interval of 10 minutes, use the following configuration setting for the OPC_HB_MSG_INTERVAL variable:

[agent.health]
OPC_HB_MSG_INTERVAL= 600

The following image illustrates the heartbeat messages:
Chapter 4: Using the HPE Operations Agent Health View

HPE Operations Agent Health View provides the following three views:

- Dashboard View
- Node View
- Process View

Using the HPE Operations Agent Health Dashboard View

HPE Operations Agent Health View provides a consolidated view about the health of HPE Operations Agents. The Dashboard View helps you to monitor HPE Operations Agents in a centralized environment. The health of HPE Operations Agents distributed across various environments is represented as pie charts and bar graphs.

**Note:** You can monitor the health and performance of only those nodes that are configured with HPE Operations Agent Health View.

The HPE Operations Agent Dashboard View provides you the following:

- Health overview of the nodes configured with HPE Operations Agent Health View.
- Quickly view the health, operating system and version details of the nodes configured with the HPE Operations Agent Health View. You can also get the count of HPE Operations Agents that require attention.
- Drill-down into each managed node to view the health and performance status of the HPE Operations Agent.

**User Interface**
The UI elements listed in the image are described in the following table:

<table>
<thead>
<tr>
<th>Legend</th>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Overview</td>
<td>Provides an overview of the number of agents configured with the HPE Operations Agent Health View. You can also see the number of agents that require attention and the number of agents with <strong>Insufficient Data</strong>. Here, all the agent nodes that are in <strong>Error</strong> or <strong>Warning</strong> state are denoted as Agent(s) that require attention.</td>
</tr>
<tr>
<td>2</td>
<td>Agents Health</td>
<td>Provides an overview of the health of agents running on the nodes configured with the HPE Operations Agent Health View. The pie chart provides the following details:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Status</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Error</td>
</tr>
<tr>
<td>3</td>
<td>Agents By OS</td>
<td>Provides an overview of the agents running on different operating systems (AIX, HP-UX, Linux, Solaris or Windows) as a bar graph. This information is available only for nodes configured with HPE Operations Agent Health View.</td>
</tr>
<tr>
<td>4</td>
<td>Agents By Version</td>
<td>Provides an overview of the agents running with different versions of HPE Operations Agent. This information is available only for nodes configured with HPE Operations Agent Health View.</td>
</tr>
<tr>
<td>5</td>
<td>Agents State</td>
<td>Provides tabs to view the list of agents based on their current state. Error tab is selected by default. In your environment, if no agents are in aborted state, then the agents where one or more parameters have failed (Warning tab) will be listed. Click any tab to view the list of agents in respective state.</td>
</tr>
<tr>
<td>6</td>
<td>Results Table</td>
<td>Results table groups agents by state. View the list of agents for any selected state or all the agents in your environment that are configured with HPE Operations Agent Health View. Following is the list of entities and their description:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Entity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warning</td>
<td>One or more parameters have failed on these agent nodes.</td>
</tr>
<tr>
<td>Normal</td>
<td>All the agent processes are in running state and all the parameters are in good state on these agent nodes.</td>
</tr>
<tr>
<td>Insufficient Data</td>
<td>Data not received from these agent nodes.</td>
</tr>
</tbody>
</table>

**Note:** Each color represents a different state of the agents running on the nodes configured with the HPE Operations Agent Health View.

**Note:** HPE Operations Agent Health View is only available with HPE Operations Agent 12.02.
<table>
<thead>
<tr>
<th>Host Name</th>
<th>Node where HPE Operations Agent health monitoring is configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Specifies the state of the node (Error/Warning/Normal/Insufficient Data).</td>
</tr>
<tr>
<td>Health</td>
<td>Specifies the health of the node.</td>
</tr>
<tr>
<td>Version</td>
<td>Specifies the version of the HPE Operations Agent installed on the node.</td>
</tr>
<tr>
<td>OS</td>
<td>Specifies the operating system of the node.</td>
</tr>
<tr>
<td>System Type</td>
<td>Physical Machine, Virtual Machine, or Host.</td>
</tr>
<tr>
<td>Up Since</td>
<td>Last started time of the agent.</td>
</tr>
</tbody>
</table>

You can search for any agent node and also re-order the results table in ascending or descending order based on any of the above listed entities.

Click **Host Name** to drill-down and check the processes running under the selected node.

### Using the HPE Operations Agent Health Node View

The HPE Operations Agent Node View helps you to view the list of processes and resources that are currently being used. Node view provides drill-down view into each managed node providing the health and performance status of the HPE Operations Agent installed. You can view the system resource utilization of HPE Operations Agent processes such as CPUs, memory, and file systems against the overall resource utilization in the form of comparative graphs.

The **HPE Operations Agent Node View** helps you do the following:

- Monitor the resource utilization of the node.
- Monitor the health of the HPE Operations Agent processes.
- Drill-down to view the process health view.
- View the version and license information of the HPE Operations Agent.

**User Interface**
The UI elements listed in the image are described in the following table:

<table>
<thead>
<tr>
<th>Legend</th>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Agent Resource Utilization</td>
<td>View resource utilization of the HPE Operations Agent processes such as CPU and memory against the overall resource utilization in the form of comparative graphs. You can also view the version, primary manager, and the license information of the HPE Operations Agent installed. The utilization graphs gets updated every 10 seconds and 4 minutes of utilization data is available at any given instance.</td>
</tr>
<tr>
<td>2</td>
<td>Failed Processes</td>
<td>View the failed processes for the selected node and the time when the process has failed. Click to update the table. Following is the list of entities and their description:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Entity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the failed processes.</td>
</tr>
<tr>
<td>Process</td>
<td>State of the process (Running/Aborted/Stopped).</td>
</tr>
<tr>
<td>State</td>
<td>Last agent health collection time/last process abort time.</td>
</tr>
</tbody>
</table>
Click **Process Name** to drill-down and check the health or policy parameters that have failed for the selected process.

### Running Processes

View all the HPE Operations Agent processes running on the selected node and also view CPU utilization, memory utilization, and utilization state of each process. If any of the processes are in the **Warning** state, the CPU or memory utilization of that process may have violated the defined threshold. The CPU and memory utilization threshold is set to 10% for all processes. Click 🔄 to update the table. Following is the list of entities and their description:

<table>
<thead>
<tr>
<th>Entity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process ID</td>
<td>Process ID of the running process.</td>
</tr>
<tr>
<td>Process Name</td>
<td>Name of the process.</td>
</tr>
<tr>
<td>Total CPU Utilization %</td>
<td>CPU utilization of the process.</td>
</tr>
<tr>
<td>Total Memory Utilization %</td>
<td>Memory utilization of the process.</td>
</tr>
<tr>
<td>Utilization State</td>
<td>Utilization state of the process [ <img src="https://example.com/" alt="Valid" /> (Normal) or <img src="https://example.com/" alt="Warning" /> (Warning)].</td>
</tr>
</tbody>
</table>

You can search for any agent process and also re-order the table in ascending or descending order based on any of the entities listed earlier.

Click **Process Name** to drill-down and check the health and policy parameters for the selected process.

---

**Using the HPE Operations Agent Health Process View**

Process view enables you to view the health and policy parameter details of each HPE Operations Agent process. It provides drill-down view into each agent process and gives the resource utilization details.
The HPE Operations Agent Process View enables you do the following:

- View health and policy parameter details of the process.
- View events for the process for the last 1 hour, 1 day, or 3 days.
- View the resource utilization of the selected process.
- Monitor the deployed policies of the HPE Operations Agent process.
- View information about the failed health parameters.

User Interface

The UI elements listed in the image are described in the following table:

<table>
<thead>
<tr>
<th>Legend</th>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Health Parameters</td>
<td>View the process health parameters and their respective state for the selected process. Click any of the parameters to check the parameter details and if the parameter is in failed state, you can see possible corrective actions based on the diagnostic commands executed.</td>
</tr>
<tr>
<td>2</td>
<td>Process Resource Utilization</td>
<td>View resource utilization by the various metrics defined for the selected process. Following is the list of entities and their description:</td>
</tr>
<tr>
<td>Entity</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Metric Name</td>
<td>Name of the metric.</td>
<td></td>
</tr>
<tr>
<td>Value</td>
<td>Value of the metric.</td>
<td></td>
</tr>
<tr>
<td>Unit</td>
<td>Unit of the metric.</td>
<td></td>
</tr>
</tbody>
</table>

3 Process Details

View process start time. Click 🔄 to update the health and utilization details of the process. The process details are updated every 300 seconds by default.

4 Process Policy Parameter Details

View the process policy parameter details such as policy name, policy type, policy state, policy interval and the last run time. Following is the list of entities and their description:

<table>
<thead>
<tr>
<th>Entity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Name</td>
<td>Name of the policy.</td>
</tr>
<tr>
<td>Policy Type</td>
<td>Type of the policy or collection parameters.</td>
</tr>
<tr>
<td>Policy State</td>
<td>State of the policy (Active/Not Responding/Failed).</td>
</tr>
<tr>
<td>Policy Interval</td>
<td>Defines how often the policy should run.</td>
</tr>
<tr>
<td>Last Run Time</td>
<td>Last run time of the policy.</td>
</tr>
</tbody>
</table>

The policy details will be for the selected process under the selected node where HPE Operations Agent health monitoring is configured.

5 Events

View event details for the selected process. You can view events for 1 hour, 1 day, or 3 days by selecting the respective tab. By default, events logged during the last one hour are displayed. If no events were logged in the last one hour, then events logged during the last 1 day or 3 days are displayed.

You can view the time, severity and description of the events. Mouse over the 🔄 icon to get more information on the severity.
Chapter 5: Launching the HPE Operations Agent Health View from the HP Operations Manager

You can also access the health and performance status of the HPE Operations Agent from the HP Operations Manager GUI.

Launching the HPE Operations Agent Health View from the HP Operations Manager for Linux

Launching the HPE Operations Agent Health View from the HP Operations Manager for Windows

Launching the HPE Operations Agent Health View from the HP Operations Manager for Linux

You can get the health perspective of the HPE Operations Agent from the HP Operations Manager for Linux Java GUI.

**Note:** HPE Operations Agent Health View supports integration with HP Operations Manager for Linux version 9.21.130 or above.

To access the health and performance status of the HPE Operations Agent from the HP Operations Manager for Linux Java GUI, perform the following steps:

1. Log on to the HP Operations Manager for Linux server as an administrator.
2. Open the HP Operations Manager for Linux Java GUI.
3. Right-click the node on the left-panel.
4. Go to **Start --> HPE Operations-agent --> HPE Operations Agent HealthDashboard** (or HPE Operations Agent HealthNode View)
5. HPE Operations Agent Health View Server is launched.

6. Drill-down to view the health and performance status of the HPE Operations Agent.

**Note:** If the Health View Server port is manually configured to a non-default port, then update the **Tools** menu by changing the port to the configured server port.

Follow the steps:
Run the following command to open the applications.dat file:
/var/opt/OV/share/databases/OpC/mgd_node/tools/C/APPLICATIONS/applications.dat

For the application OperationsAgent HealthDashboard, update the following:
Change APPL_CALL "https://$OPC_MGMTSV:8092/#/dashboardview" to APPL_CALL "https://$OPC_MGMTSV:<configured server port>/#/dashboardview"

Update the Tools menu by using the following:
/opt/OV/bin/OpC/opccfgupld -replace
/var/opt/OV/share/databases/OpC/mgd_node/tools

Launching the HPE Operations Agent Health View from the HP Operations Manager for Windows

You can get the health perspective of the HPE Operations Agent from the HP Operations Manager for Windows. To access the health and performance status of the HPE Operations Agent, perform the following steps:

1. Log on to the HP Operations Manager for Windows server as an administrator.
2. Open the HP Operations Manager for Windows.
3. Click HPE Operations Agent under the Tools menu on the left-panel.
4. Click OperationsAgent HealthDashboard to view the HPE Operations Agent Health View Server.
5. HPE Operations Agent Health View Server will open in a browser window.

6. Click **Host Name** to drill-down into each managed node and view the health and performance status of the HPE Operations Agent.

7. To launch HPE Operations Agent Health of a specific node directly from the HP Operations Manager for Windows, go to **Tools --> HPE Operations Agent --> OperationsAgent Health NodeView**

---

**User Guide: Health View**

**HPE Operations Agent (12.02) Page 45 of 58**
8. Select the node from the pop-up window and click **Launch**.

9. HPE Operations Agent Health View will open in a browser window.

10. Click **Process Name** to drill-down and view the health and policy parameter details of each HPE Operations Agent process.

**Note:** If the Health View Server port is manually configured to a non-default port, then access the Health View Server from the **Tools** menu by changing the default port to the configured server port in the browser URL itself.
Chapter 6: Use Case

This use case demonstrates how HPE Operations Agent Health View enables you to quickly identify issues in a complex environment with several managed nodes.

**Use Case:** Alerts are not being generated as one or more parameters have failed on the agent node.

**Description**

Consider a scenario where you have multiple managed nodes; however, you do not see any alerts from a specific managed node for a long time. This may be because the agent node has some issues or all the applications are running fine on the managed node and there is no event for HPE Operations Agent to generate any alert message.

**Prerequisite**

HPE Operations Agent health monitoring must be enabled on the specific managed node and the node must be configured with a health view server.

**Standard flow**

1. Open the **HPE Operations Agent Health View Server**.
2. Click **Warning** to view the list of agent nodes where one or more parameters have failed.

3. The **Health** of the specific node shows **opcmona requires attention**. Click **Host Name** to open the node view of the specific managed node.
4. Check **Process with failure** on the specific node view. It lists the **opcmona** process with brief description about the issue.

5. Click **Process Name** to open the process view.
6. Check the **Health Parameter** details. The health parameter corresponding to the source (as per policy) from where the process is unable to collect data will show the status as failed. For example, the status of the health parameter **SNMP GET** is Failed.

7. Mouse over the **Health Parameter** to view the parameter description.
8. Click the Health Parameter to view if any diagnostic commands are executed and view suggestions to take corrective actions.

Conclusion

The opcmona process of the HPE Operations Agent is unable to fetch SNMP MIB information as the health parameter SNMP GET has failed. Hence, alerts are not being generated from the managed node.
Chapter 7: Troubleshooting

This section helps you troubleshoot the problems experienced during the configuration or accessing health view.

**Note:** For any issues you can use the XPL tracing for processes running on the agent node, enable debug mode for the hpsensor process (using hpcs.conf file on the agent node) and the hpcsrvd process (using hpcsrv.conf file on the server) and check for errors in the log files to troubleshoot.

To enable debug mode, edit the following value under the **hpcs.trace** namespace:

Modify the debug level value as following: **Debug_Level=DEBUG**.

**Problem:** Node does not appear on the HPE Operations Agent Health View Server.

**Solution:** To resolve this issue, check the following:

1. Log on to the node and check for errors in the **hpcstrace.log** file. The log file is available in the following location:
   - **On Windows:** `%OvDataDir%hpcs\hpcstrace.log`
   - **On UNIX/Linux:** `/var/opt/OV/hpcs/hpcstrace.log`

   Check and resolve all the errors related to the HBP push, certificate issues, or the http/https mode.

2. Check if the communication between the node and the health view server is successful.
   Follow the steps:
   a. Log on to the health view server as an administrator.
      Run the following command:
      ```bash
      bbcutil -ping <node_ip_address>
      ```
   b. Log on to the node as an administrator.
      Run the following command:
      ```bash
      bbcutil -ping <server_ip_address>
      ```

   **Note:** Trust must be established between the server and the nodes for successful communication. Ensure certificates from the same authority are installed on the Health View Server and the nodes. If they are from different certificate authorities, then exchange the CA certificates and import them into
the node and the trusted keystores. For more information, see "Establishing a Trust Relationship Between the Two Management Servers" in the HP Operations Manager Installation Guide for Linux or "Configure trusted certificates for multiple management servers" in the HP Operations Manager Online Help for Windows.

3. Restart hpsensor on the node. For more information, see Restart.

Note: After configuring the nodes with HPE Operations Agent health, the configured node appears on the Health View Server only after 5 minutes.

Problem: Running Processes drill down does not show any processes if an agent node is upgraded to HPE Operations Agent 12.02.

Solution: To resolve this issue from occurring, follow the steps:

1. Log on to the node as an administrator.
2. Open the parm file from the following location:
   - On Windows: %OvDataDir%parm.mwc
   - On Unix/Linux: /var/opt/perf/parm
3. Check the following text in the parm file:
   application = OperationsAgent
   file = ovcd, ovbbccb, ovconfd, ovbbcrcp, ovcdaututil, extract, utility
   file = opcgeni, ompolparm, opceca, opcecaas, agtrep, dsilog, perfalarm
   file = opcmona, opcmsga, opcmsgi, opcacta, opcle, opcwbemi, opctrapi
   file = oacore, midaemon, ttd, perfd, hpsensor, glance, xglance
   file = AHSCollector, opcconfigfile, xglance-bin
4. If the above text or part of the text is missing in the parm file, then add the above text in the parm file. If the parm file is updated manually, then restart hpsensor on the node. For more information, see Restart.

Problem: Data collection is not happening on the node.

Solution: Follow the steps to resolve this issue:

1. Run the following command to check the status of opcacta:
   <OvBinDir>ovc -status
2. If opcacta is not running, then run the following command to restart opcacta:
   <OvBinDir>ovc -restart opcacta
If opcacta is running, then enable xpl tracing for AHSCollector (Agent Health and System Data Collector).

**Problem:** Data not received from the node for the last 3 intervals (or HBP is missing or Insufficient Data).

**Solution:** This issue is because hpcsrvd process has not received HBP for more than 3 intervals. To resolve this issue, check the following:

- Check if ovbbccb is reachable

  1. Check if the communication between the node and the server is successful.
     - Ping the node from the server, run the following command:
       ```bash
       bbcutil -ping <node_ip_address>
       ```
     2. If the above step fails, check if the node is reachable using the following command:
       ```bash
       ping <node_ip_address>
       ```

- Check if hpsensor process is running

  a. Run the following command to check the status of hpsensor on the node:
     ```bash
     <OvBinDir>ovc -status
     ```
     If hpsensor is not running, then run the following command to restart hpsensor:
     ```bash
     <OvBinDir>ovc -restart hpsensor
     ```
  
  b. Check the hpcstrace.log file on the node to get more information. This log file is available in the following location:
     - On Windows: `%OvDataDir%hpcs\hpcstrace.log`
     - On UNIX/Linux: `/var/opt/OV/hpcs/hpcstrace.log`

- Check the certificate on the node

  Certificate on the node may have some issues or it may not be installed. Check the certificates on the node using the following commands:
  ```bash
  ovcert -list
  ovcert -check
  ```

**Problem:** Removed agent node appears on the Health View Server.

**Solution:** Whenever an agent node is removed, the agent node entry exists on the Health View Server for 24 hours.

**Problem:** Duplicate agent nodes appear on the Health View Server.

**Solution:** Whenever an agent node is cleaned up and re-installed, the agent node entry exists on the Health View Server for 24 hours. Entry with No Data can be ignored. Check the Core_ID of the agent nodes to differentiate the nodes when two different nodes with same the host name appear on the Health View Server. Mouse-over the node name in Dashboard View to check the Core_ID of the agent node.
**Problem:** Health View UI does not change locale on Internet Explorer.

**Solution:** To resolve this issue, follow the steps:

1. Close all the tabs of the browser.
2. Open the browser again.
3. Open the HPE Operations Agent Health View Server.

**Problem:** Health data is not available for a Windows node configured with agent health monitoring on a Health View Server other than the HPOM Management Server.

**Cause:** This may be seen if the licenses are set after the installation.

**Solution:** To resolve this issue, manually start `opcacta` on the Windows node. Run the following command to start `opcacta`:

```
<OvBinDir>/ovc -start opcacta
```

**Problem:** Updated agent health data is not available on the Health View Server as data collection is not occurring.

**Cause:** This may be because the action agent (`opcacta`) is in Stopped/Aborted state. When the process `opcacta` is in Stopped/Aborted state, the process state change information gets updated on the Health View Server only after 3 HBP intervals.

**Solution:** To resolve this issue, restart `opcacta` on the node. Run the following command to restart `opcacta`:

```
<OvBinDir>/ovc -restart opcacta
```

**Problem:** Getting multiple alert messages for the same events.

**Cause:** This may happen if you have the Selfmon Policies deployed on the node and then upgraded the node to the HPE Operations Agent 12.02.

**Solution:** To resolve this issue, de-assign the Selfmon Policies deployed on the node from the HPOM Management Server. For more information, see "Deleting Policies" in the HP Operations Manager Administrator’s Reference for Linux or "Remove policy from node" in the HP Operations Manager Online Help for Windows.
Chapter 8: Performance and Sizing of the HPE Operations Agent Health View

This section provides the test setup information and the recommendations for using the HPE Operations Agent Health View.

**Note:** The performance will vary based on the test environment and the test setup.

Test Environment

The tests are performed using the following test setup:

<table>
<thead>
<tr>
<th>Server</th>
<th>Operating System</th>
<th>Architecture</th>
<th>Hardware (Physical/VM)</th>
<th>System Configuration</th>
<th>CPU Clock Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP Operations Manager 9.20</td>
<td>Linux</td>
<td>x64</td>
<td>VM</td>
<td>6 CPU 6 GB RAM</td>
<td>2.67 GHz</td>
</tr>
<tr>
<td>Local Agent: HPE Operations Agent 12.02</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Recommendations

Based on the test results and the performance observations, the following recommendations are provided for using the HPE Operations Agent Health View.

<table>
<thead>
<tr>
<th>Numbe of Agent Nodes</th>
<th>System Configuration ulimit -n</th>
<th>Server Side Configuration /var/opt/0V/shared/server/hpcsrv/hpcsrv.conf</th>
<th>Open File Descriptors</th>
<th>UpdateInterval</th>
<th>connection_backlog</th>
<th>num_threads</th>
</tr>
</thead>
<tbody>
<tr>
<td>2500</td>
<td>3000</td>
<td>60</td>
<td>512</td>
<td>20</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


Use the following graphs to view and analyze the performance of the HPE Operations Agent Health View:

HPE Operations Agent Health View performance graph for `UpdateInterval = 300` seconds.
Conclusion

If the number of node instances are increased, it is recommended to increase the UpdateInterval time for optimal CPU utilization. The default value for UpdateInterval is 60 seconds.

If you increase the UpdateInterval time, then the time taken for the Health View Server to reflect the node state change also increases.

For example, keeping the UpdateInterval to 300 seconds is optimal for CPU utilization but the Health View Server will update any issues found on the agent node after 300 seconds or more.

To avoid this, there is an option to configure multiple Health View Servers in your environment with optimum number of node instances.
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: Health View (Operations Agent 12.02)

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!