The HP Operations Agent Self-Monitoring Feature

White Paper

In this Document

The information in this white paper applies to both HP Operations Manager for UNIX (HPOM for UNIX) and HP Operations Manager for Windows (HPOM for Windows). To avoid repetition and confusion where different platforms use different terms to refer to the same concepts, the descriptions in this document use one term for both platforms. For example, the generic term “policy” applies to both the HPOM for UNIX “template” and the HPOM for Windows “policy”. Similarly, the term “deploy” replaces the HPOM for UNIX-specific terms “assign” and “distribute”, the HPOM for Windows term “instrumentation” also refers to HPOM for UNIX “actions, commands, and monitors”, and the term “tool” is used to refer to HPOM for UNIX “applications”. However, references to specific elements that appear in the GUI retain the original terms, for example; this document does not use the term “policy” when referring to the HPOM for UNIX “Message Source Templates” window.

Introducing the HP Operations Agent Self-Monitoring Feature

HPOM does not currently provide any convenient way to establish whether a sudden and unexpected reduction in the number of messages in the message browser is an indication that the managed environment is running as (or better than) expected. Indeed, it is possible that the lack of messages is due to a problem with the HP Operations (HPO) agent. For example, if the HPO agent stops suddenly or one of its processes is hanging for some reason, the HPO agent is no longer able to report problems. If you want to make sure your IT environment is available all the time, not only is it important to be able to use HPOM to monitor what is happening on the managed nodes you have configured in your IT environment, it is also essential that you know when HPOM itself runs into problems which might affect its ability to monitor and report on the environment it is managing.

The HPO agent’s new self-monitoring feature extends the scope of the HPO-agent functionality to ensure that problems with the agent’s own core components do not compromise the agent’s ability to continue monitoring the nodes it is managing. Using the self-monitoring feature, you can easily establish if the HPO agent is working correctly by configuring the agent to poll its own core components and generate an alert if it finds any problems. Standard HPOM functionality links the alerts to automatic or operator-initiated actions, too. In this way, you can configure the HPO agent to try to fix itself automatically, while keeping a record of the problems it encounters in the form of a message in the message browser.

Note that the self-monitoring functionality described in this whitepaper is not a default feature of the HPO agent; you first need to install the self-monitoring functionality on the management server and then enable it by deploying the appropriate policies and instrumentation to the managed nodes. In addition, the self-monitoring functionality is designed to monitor all HPO-agent components on a managed node; it is not possible to configure the self-monitoring feature to monitor only a particular selection of agent components.

The self-monitoring functionality is currently available as a contrib. tool without official support; the contrib. tool is only available as a separate package, which the administrator installs on the HPO management server. For more information about where to find the tool, see Installing the HPO-Agent Self-Monitoring Feature.

Heartbeat Polling

You can use the agent’s self-monitoring feature in addition to the heartbeat-polling feature already provided with HPOM. The heartbeat-polling feature allows you not only to configure the HPO agent to broadcast its availability to the management server but also to ensure that, in the event of a communication breakdown, the management server can confirm that the HPO agent is no longer reachable and start the process of solving the problem. The self-monitoring functionality described in this document is distinct from the heartbeat-polling feature and extends the agent-management capability beyond determining availability and into areas such as the monitoring and management of the individual HPO agent processes and services, too. For more information about the heartbeat-polling feature, see the HPOM product documentation.

Understanding the HPO-Agent Self-Monitoring Feature

The information in this section helps you to understand the underlying concepts on which the HPO agent's self-monitoring feature is based. After you read this section, you should be able to decide whether you need to configure the agent to suit the demands of your particular environment and, if so, how. The information in this section covers the following high-level topics:

- Example Self-Monitoring Scenario
- Core Self-Monitoring Components
- HPOM Configuration Elements

Since HPOM is already able to detect stopped agent processes, the HPO agent's self-monitoring feature focuses primarily on determining whether HPO agent processes are hanging. However, since "hanging" is a very broad term in the context of processes and services, the HPO agent's self-monitoring feature limits itself to establishing that the HPO agent functionality is working as expected. If the HPO agent's self-monitoring feature discovers that the HPO agent (or any part of it) is not working normally, it sends a message indicating which process has a problem that requires attention.

Example Self-Monitoring Scenario

To understand where the HPO agent's self-monitoring functionality can add value to the way you manage your IT environment, imagine a scenario where an administrator uses the HPO agent to monitor a server which acts as the central point of contact for the collection and management of syslog messages from hundreds of servers in a large heterogeneous network. One day, for reasons outside the administrator's control, the HPO agent hangs and, as a consequence, cannot send any messages indicating that there is a problem. More often than not, the lack of messages indicates that everything is running normally. However, in the example described here, this is not the case.

In the scenario suggested, if the HPO agent stops, the management server notices as soon as it polls the agent for its status; status polling occurs regularly every few minutes. If, on the other hand, the HPO agent (or one of its core processes) hangs, the agent cannot send any messages to the management server to indicate that it is out of action. However, the management server assumes the agent is still alive and well since the status poll reports that the agent processes are still visible, because the corresponding PIDs on UNIX systems are available or, on Microsoft Windows systems, the expected services are still running.

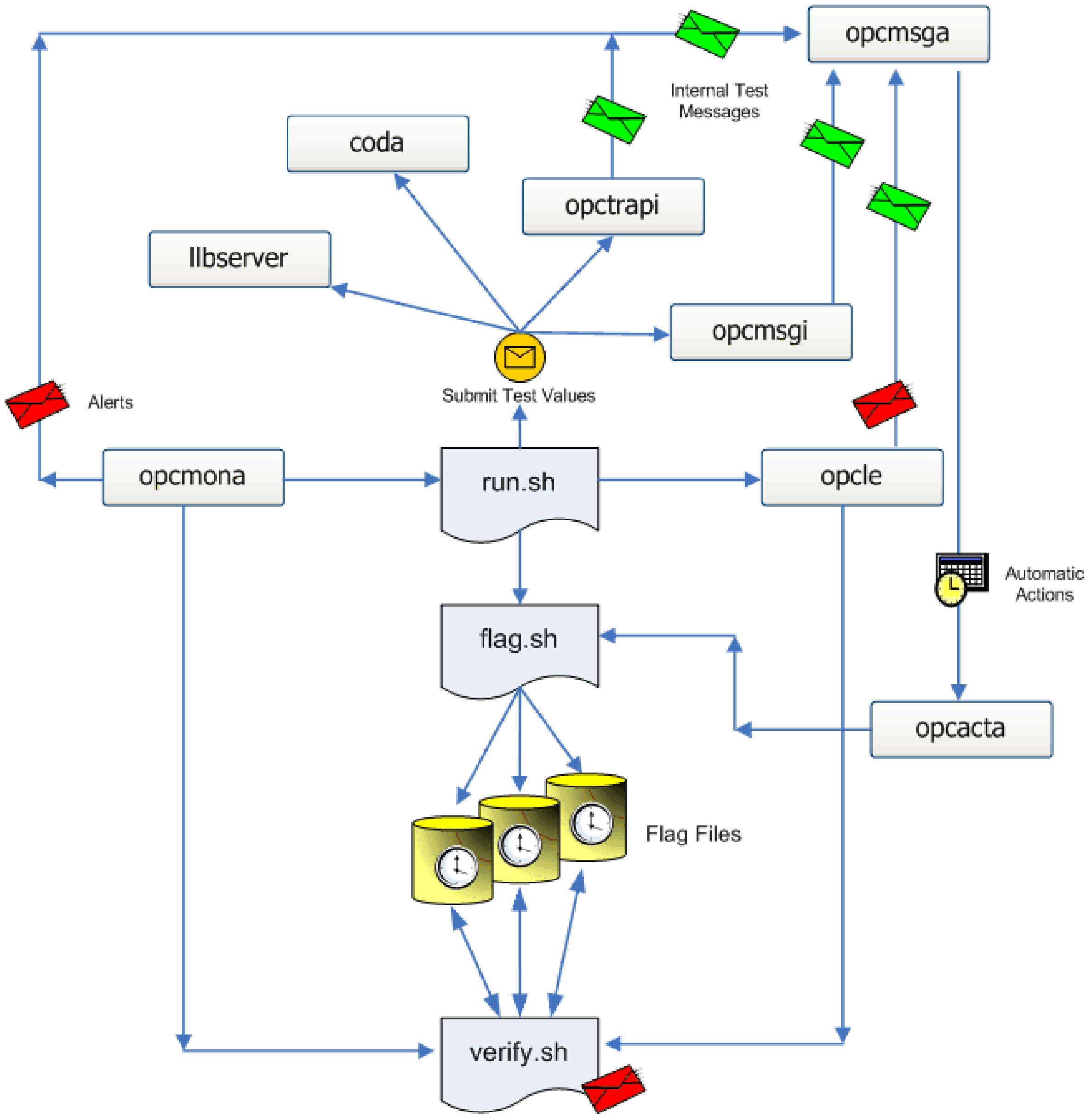
Without the self-monitoring feature, the situation can only be resolved by human intervention, which may or may not occur in a timely manner. With the help of the self-monitoring feature, HPOM not only knows about the problem as soon as it occurs, it also immediately notifies the appropriate people of the problem. In addition, HPOM can perform automatic actions to help resolve the problem and record the sequence of events in the message browser.

This scenario demonstrates how, in certain situations, there is clearly a benefit to gain from monitoring HPO's own agents in order to ensure that the HPOM operator knows at any point in time if the agent has a problem that is preventing it from performing its monitoring tasks as expected.

Core Self-Monitoring Components

The HPO-agent self-monitoring functionality uses a combination of policies and HPOM instrumentation that is linked to the policies to ensure that the HPO agent components are working reliably and efficiently. The functionality provided with the HPO agent's self-monitoring feature works with both DCE and HTTPS agents and integrates seamlessly with both HPOM for UNIX and HPOM for Windows. For more information about which versions of HPOM you can use the HPO agent's self-monitoring feature with, see the section Platforms and Software Versions on page 8.

Figure 1. Self-Monitoring Data Flow on UNIX for DCE Agents



The self-monitoring feature uses existing HPOM functionality to check whether the basic HPO agent features are working as expected. The HPO monitor agent, `opcmona`, and the log-file encapsulator, `opcle`, perform the basic monitoring of all other HPO subagents and, at the same time, monitor each other, too. In addition, the HPO agent's self-monitoring feature tests the following components in the HPO agent:

- **HPO Embedded Performance Agent (coda)**
  The HPO-agent self-monitoring functionality ensures that the embedded performance agent runs on schedule by verifying that last time the performance agent collected data was within the allowed time limit.
- **SNMP trap interceptor (opctrapi)**
  The HPO-agent self-monitoring functionality generates SNMP traps to test whether the SNMP trap interceptor is working. Note that the HPO agent's self-monitoring feature is only able to test the availability of the SNMP trap interceptor on HPOM Managed Nodes where the `snmptrap` command is present. The `snmptrap` command resides in the following location on the managed node:

  – UNIX operating systems: `/opt/OV/bin/snmptrap`
  – Microsoft Windows operating systems: `%OvAgentDir%\bin\snmptrap`
  On Windows managed nodes, the Windows SNMP-trap service must be installed and available. For more information about what happens to `opctrapi` if the SNMP-trap service is not available, see Understanding The HPO-Agent Self-Monitoring Feature in the Troubleshooting section.
- **Message interceptor (opcmsgi)**
  The HPO-agent self-monitoring functionality generates an opcmsg message to test whether the message interceptor is running.
- **Log-file Encapsulator (opcle)**
  The HPO-agent self-monitoring functionality writes entries to log files to check whether the log-file encapsulator opcle is monitoring log files.
- **Local Location Broker (llbserver)**
  The HPO-agent self-monitoring functionality checks that the local-location-broker server is listening for connections on the expected port. The HPO agent processes rely on the local-location broker for the allocation of ports. Note that the HPO agent's self-monitoring feature only checks the availability of the LLB on DCE managed nodes; on HTTPS managed nodes, the control component (`ovcd`) is responsible for monitoring the BBC communication broker, which manages the allocation of ports to HPO agent processes.
- **Monitor agent (opcmona)**
  The HPO-agent self-monitoring functionality checks the availability of the monitor agent, `opcmona`, using monitor policies, which ensure that the self-monitoring scripts run at the scheduled time.
- **Message agent (opcmsga)**
  The HPO-agent self-monitoring functionality relies on the availability of the message agent, `opcmsga`, to process all the messages generated by the various testing mechanisms as well as the automatic actions attached to the messages.
- **Action agent (opcacta)**
  The template started by the monitor agent (`opcmona`) runs a script that contains a scheduled action. If the scheduled action starts, it confirms the availability of the HPO action agent (`opcacta`).
- **Event-Correlation Agent (opceca)**
  The HPO-agent self-monitoring feature does not currently monitor the event-correlation agent.

The self-monitoring feature uses a system of flag files to record the results of the internal tests it performs and checks the time stamp associated with the flag files to ensure that the files are up to date. The time stamp of the flag files indicates the last time the HPO agent's self-monitoring feature checked the HPO agent processes and confirmed they were running and available. Up-to-date flag files are an indication that the HPO agent processes are working normally. For more information about configuring the HPO agent's self-monitoring feature, see Configuring the HPO-Agent Self-Monitoring Feature on page 10.

HPOM Configuration Elements

The HPO agent's self-monitoring functionality consists of a set of core components that you install on the management server. The component package includes policies which are designed to work in combination with a set of instrumentation scripts. The policies appear in the HPOM GUI in a top-level HPO-for-UNIX policy group called "OVO SelfMon" or, on HPO for Windows, a policy group called "HPOM Agent Self Monitoring". You deploy the policy group to the HPOM managed nodes whose agents you want to monitor with the self-monitoring functionality. Note that you cannot deploy individual policies; dependencies exist between the policies, which require you to install and deploy all the policies in the respective policy group. It is not possible to select and use only parts of the complete self-monitoring functionality.

The following table lists the policies provided with the HPO agent's self-monitoring feature, indicates what type of policies they are, and briefly describes what the policy does. For more information about where you can find the files before and after deployment, see Locating Instrumentation Components on page 15.

Policy Name	***Policy Type***	***Description***
OVOSelfMonTstActa	Scheduled action	Tests the scheduling capabilities of the HPO monitor and action agents `opcmona` and `opcacta` and updates the flag file `opcacta` if the test completes successfully
OVOSelfMonTstLe	Log file	Catches log-file test messages
OVOSelfMonTstMsgi	opcmsg	Catches `opcmsg` test messages
OVOSelfMonTstTrapi	SNMP trap	Catches test SNMP traps
OVOSelfMonTstMonaExt	Monitor (external)	Catches test monitor values
OVOSelfMonTstAll	Monitor (script)	Runs the script which generates all the test values captured by the interceptor processes
OVOSelfMonVerifyLe	Log file	Verifies the presence and last modification times of the monitor-related flag files (`opcmona`)
OVOSelfMonVerifyMon	Monitor (script)	Verifies the presence and last modification times of the non-monitor-related flag files (`opcle`, `optrapi`, `opcmsgi`, `opcacta`)

Installing the HPO-Agent Self-Monitoring Feature

This section explains how to install the HPO-agent's self-monitoring feature on the HPOM management server. The information in this section includes the following topics:

- Platforms and Software Versions
- To Install the Self-Monitoring Feature

The self-monitoring functionality is currently available as a contrib. tool without official support; the contrib. tool is only available as a separate package, which the administrator installs on the HPO management server. Note that there is one package for HP Operations Manager for UNIX 7.25 (and later) and one package for HP Operations Manager for Windows 7.5 (and later). The packages are available for download from the 'Contribution Tools for Operations Manager' section on the HP Software Downloads web site. Note that the packages contain a ReadMe file with information about the latest release.

Platforms and Software Versions

Dependencies on the $AGENT_USER variable mean that the HPO agent's self-monitoring feature is only available for use with HPOM for UNIX version 7.25 and later and HPOM for Windows from version 7.5. If you are using a supported version of HPO, you can install and run the HPO agent's self-monitoring feature on HPO managed nodes running either DCE or HTTPS agents for the following operating systems:

- HP-UX
- Solaris
- Microsoft Windows

For more information about which versions of the indicated operating systems the HPO agent's self-monitoring feature works with, see the product support matrix or the product-specific documentation for HPOM for UNIX and HPOM for Windows.

To Install the Self-Monitoring Feature

The procedure you use to install the self-monitoring feature is similar to the procedure to install and configure a Smart Plug-in for HPOM. After you have installed the software on the HPO management server, you assign the top-level HPO-agent self-monitoring policy group to the managed nodes whose agent you want to monitor (or node groups containing the managed nodes) and deploy the policies and instrumentation to the selected nodes. The way in which you install the HPO agent's self-monitoring feature depends on whether you are running an HPOM for UNIX or HPOM for Windows management server.

For HPOM for UNIX management servers:

To install the self-monitoring feature of the HPO agent on an HPOM for UNIX management server, you need to perform the following tasks:

1. Download the HPO-agent self-monitoring package for HPOM for UNIX (`OVOSelfMon_v2.tar.gz`) from the 'Contribution Tools for Operations Manager' section on the HP Software Downloads web site at the following location: http://h20229.www2.hp.com/downloads/other.html.
2. Copy the file `OVOSelfMon_v2.tar.gz` to a temporary location such as `/tmp` on the HPOM for UNIX management server.
3. Change to the temporary location, where you stored the `OVOSelfMon_v2.tar.gz` file:
   ```
   cd /tmp
   ```
4. Uncompress the HPO-agent self-monitoring package:
   ```
   gunzip OVOSelfMon_v2.tar.gz
   ```
5. Unpack the HPO-agent self-monitoring package:
   ```
   tar xvf OVOSelfMon_v2.tar
   ```
   Unpacking the file creates `OVOSelfMon/...,` a new sub-directory structure under `/tmp`
6. Change to the newly created directory containing the self-monitoring files:
   ```
   cd /tmp/OVOSelfMon
   ```

7. Check the ReadMe file for important information about the self-monitoring feature.
8. Stop the HPOM for UNIX administrator GUI
9. Stop the HPO server processes: **`opcsv -stop`**
10. Use the HPOM configuration-upload feature to upload the self-monitoring components to the HPOM database:

```
/opt/OV/bin/OpC/opccfgupld -replace /tmp/OVOSelfMon
```

11. Restart the HPO server processes: **`opcsv -start`**
12. Start the HPOM administrator's GUI by logging into HPOM as the administrator
13. In the HPOM node bank, select a node and assign the policy group "OVO SelfMon" to it. Alternatively assign the "OVO SelfMon" policy group to the node group that contains the managed nodes.
14. Deploy the assigned policies and instrumentation (monitor scripts) to the selected node using the standard HPOM deployment mechanism:

    `Actions > Agents > Install / Update OVO Software and Configuration`

    Remember to check both the "Templates" and "Monitors" options.
15. Verify the successful deployment of the self-monitoring functionality by checking that the directory `/var/opt/OV/tmp/selfmon` exists on the managed node; the `selfmon` directory stores important files, which the HPO-agent self-monitoring feature requires.

    Note that, due to scheduling differences, the `opcagt` and `selmon_verify.1` flag files appear first, followed by all the other flag files, after a further minute or two. For more information about which flag files you should find in the `selfmon` directory, see The Self-Monitoring Agent's Flag Files on page 12.

For HPOM for Windows management servers:

To install the HPO-agent self-monitoring feature on an HPOM for Windows management server, you need to perform the following tasks as either a local or a domain administrator:

1. Download the HPO-agent self-monitoring package for HPOM for Windows (`HPOMAgentSelfMonitoring.zip`) from the 'Contribution Tools for Operations Manager' section on the HP Software Downloads web site at the following location: http://h20229.www2.hp.com/downloads/other.html.
2. Copy the downloaded package to a temporary location on the HPOM for Windows management server.
3. Double-click the `HPOMAgentSelfMonitoring.zip;` setup copies the contents of the installation package to the location `%OvInstallDir%\contrib\OVOW` on the HPOM for Windows management server and starts the installation process.
4. Check the ReadMe file for important information about the self-monitoring feature.
5. Verify that the installation process successfully integrated the self-monitoring components into the HPOM for Windows GUI by checking that the new policy group 'HPOM Agent Self Monitoring' is visible in the HPOM for Windows console.
6. In the HPOM for Windows console, right-click the 'HPOM Agent Self Monitoring' policy group and use the Deploy policies on… option to deploy the policy group to the managed nodes, whose HPO agent you want to make use of the self-monitoring feature.
7. Verify the successful deployment of the self-monitoring functionality by checking that the `selfmon` directory exists on the managed node. The `selfmon` directory stores files, which the self-monitoring functionality requires. For example, on a managed node running Microsoft Windows, check that the following folder exists and contains files: `%OvAgentDir%\tmp\OpC\selfmon`.

    Note that, due to scheduling differences, the `opcagt` and `selmon_verify.1` flag files appear first, followed by all the other flag files, after a further minute or two. For more information about which flag files you should find in the `selfmon` directory, see The Self-Monitoring Agent's Flag Files on page 12.

Configuring the HPO-Agent Self-Monitoring Feature

The information in this section includes instructions for distributing or deploying the agent policies, and instrumentation (actions, commands, and monitors) and also demonstrates the ways in which you can modify default parameters such as polling intervals in order to fine-tune the self-monitoring feature to meet the demands of a particular environment. The information in this section covers the following topics:

- Default Configuration Settings
- Modifying Configuration Values

Default Configuration Settings

In its default configuration, the HPO agent's self-monitoring feature does not add any significant load to the system. This means that there should be no need to change default configuration values that are set during installation and deployment. However, if you feel that there is a need to adjust some of the values to suit the particular demands of your environment, use the information in the following list to help you learn what you can change:

- **Generation of test messages**
  You can modify the interval between the generation of test messages either for all the policies or for each, individual policy type, for example: opcmsg or SNMP trap. It is recommended to keep the interval identical for each policy type. By default, the interval between the generation of test messages is 1 (one) minute. The interval is defined in the policy OVOSelfMonTstActa.

- **Verification of the flag files**
  You can change how often the HPO agent's self-monitoring feature verifies whether the flag files exist and when they were last updated. By default, the verification interval is 3 minutes and is defined in the OVOSelfMonVerifyMon and OVOSelfMonVerifyLe policies.

- **Flag-files update interval**
  You can modify the maximum amount of time which can elapse before the flag files must be updated. This parameter is important since the HPO agent's self-monitoring feature uses the time stamp associated with the flag files to confirm that the HPO-agent components are behaving normally. If the time stamps indicate that a flag file has not been updated at the expected interval, the HPO agent's self-monitoring feature generates an alarm and sends a message to the HPO management server. By default, the HPO agent's self-monitoring feature checks the flag files' time stamp every 3 minutes; the interval is defined in the OVOSelfMonVerifyMon and OVOSelfMonVerifyLe policies.

- **Message-group assignment**
  You can change the name of the HPO message group that the HPO agent's self-monitoring feature associates with the messages it generates when it discovers problems with the HPO agent. By default, the HPO agent's self-monitoring feature assigns its messages to the "OpC" message group. If necessary, you can change this value in the message-defaults section of the appropriate policy.

- **Application name**
  You can modify the name of the application that you want to associate with the messages which the HPO agent's self-monitoring feature sends to the HPO management server. By default, the HPO agent's self-monitoring feature assigns its messages to the HPO application "SelfMon". If necessary, you can change this value in the message-defaults section of the appropriate policy.

- **Object name**
  By default, the “object” field of messages the HPO agent’s self-monitoring feature sends to the HPO management server indicates the name of the HPO agent process which discovered the problem to which the message relates, for example: “opcmsgi”. If necessary, you can change this value in the message-defaults section of the appropriate policy.

Modifying Configuration Values

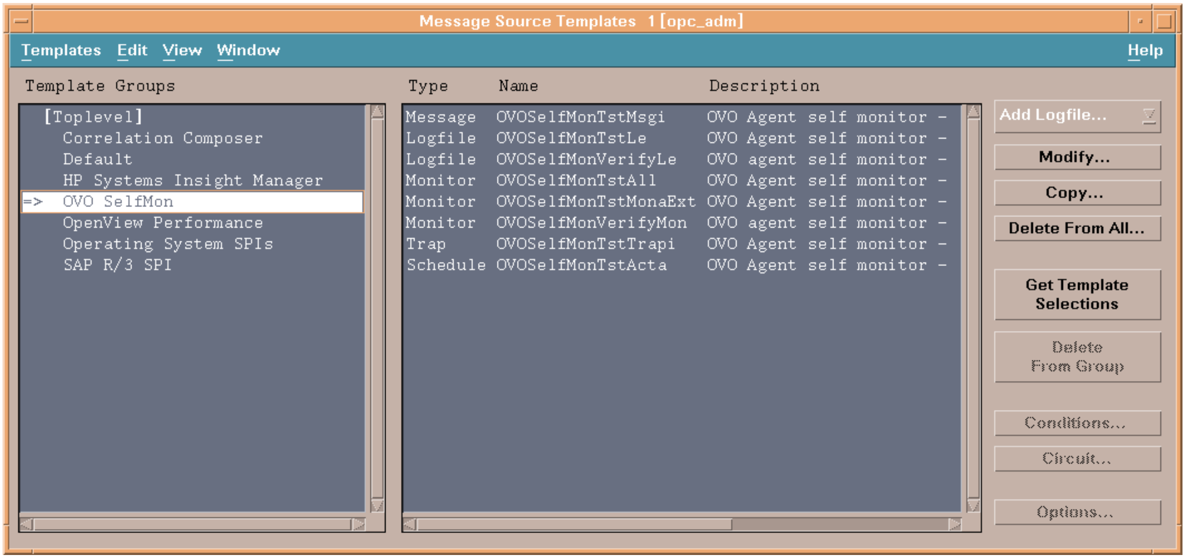
If you want to change any of the default configuration parameters defined in the self-monitoring policies, edit the appropriate policy. For more information about which policies define which parameters, see Default Configuration Settings on page 10. The way you configure the self-monitoring functionality of the HPO agent depends on whether you are using an HPOM for UNIX or an HPOM for Windows management server.

For HPO for UNIX management servers:

Figure 2. HPOM for UNIX Template Groups shows the policies installed with the HPO agent’s self-monitoring feature on an HPOM for UNIX management server. To configure a policy:

1. In the HPOM Administrator’s GUI, open the message-source-templates window.
2. Expand the OVO SelfMon template group.
3. Select the template whose configuration you want to modify.
4. Click the Modify button.
5. Make the changes you require. For example, you can set the polling interval in the Monitoring Options section of the Modify Template window.
6. Click OK to save the changes you made.
7. Re-distribute the templates to the managed nodes.
8. Restart the HPO agent processes

Figure 2. HPOM for UNIX Template Groups



Template Groups

- [Toplevel]
  - Correlation Composer
  - Default
  - HP Systems Insight Manager
  - => OVO SelfMon
  - OpenView Performance
  - Operating System SPIs
  - SAP R/3 SPI

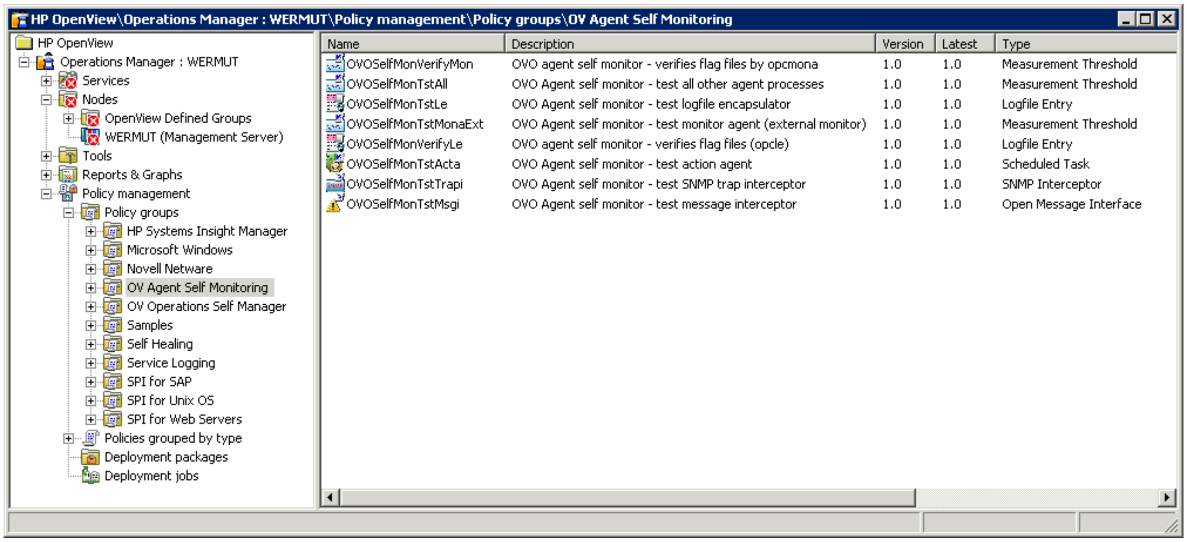
Type	Name	Description
Message	OVOSelfMonTstMsgi	OVO Agent self monitor -
Logfile	OVOSelfMonTstLe	OVO Agent self monitor -
Logfile	OVOSelfMonVerifyLe	OVO agent self monitor -
Monitor	OVOSelfMonTstAll	OVO Agent self monitor -
Monitor	OVOSelfMonTstMonaExt	OVO Agent self monitor -
Monitor	OVOSelfMonVerifyMon	OVO agent self monitor -
Trap	OVOSelfMonTstTrapi	OVO Agent self monitor -
Schedule	OVOSelfMonTstActa	OVO Agent self monitor -

For HPOM for Windows management servers:

Figure 3. HPOM for Windows Policy Groups shows the policies installed with the HPO agent's self-monitoring feature on an HPOM for Windows management server. To configure a policy:

1. In the HPOM for Windows console, expand Policy Management and Policy Groups
2. Select the HPOM Agent Self Monitoring policy group
3. Double-click the policy, which you want to edit
4. Make the desired changes and click Save and Close

Figure 3. HPOM for Windows Policy Groups



Name	Description	Version	Latest	Type
OVOSelfMonVerifyMon	OVO agent self monitor - verifies flag files by opcmona	1.0	1.0	Measurement Threshold
OVOSelfMonTstAll	OVO Agent self monitor - test all other agent processes	1.0	1.0	Measurement Threshold
OVOSelfMonTstLe	OVO Agent self monitor - test logfile encapsulator	1.0	1.0	Logfile Entry
OVOSelfMonTstMonaExt	OVO Agent self monitor - test monitor agent (external monitor)	1.0	1.0	Measurement Threshold
OVOSelfMonVerifyLe	OVO agent self monitor - verifies flag files (opcle)	1.0	1.0	Logfile Entry
OVOSelfMonTstActa	OVO Agent self monitor - test action agent	1.0	1.0	Scheduled Task
OVOSelfMonTstTrapi	OVO Agent self monitor - test SNMP trap interceptor	1.0	1.0	SNMP Interceptor
OVOSelfMonTstMsgi	OVO Agent self monitor - test message interceptor	1.0	1.0	Open Message Interface

Using the HPO-Agent Self-Monitoring Feature

This section explains how to use the HPO agent's self-monitoring feature to check that the HPO agent is working as expected. The information in this section is valid for HPO management servers running on either UNIX or Microsoft Windows operating systems and includes details about the following topics:

- The Self-Monitoring Agent's Flag Files
- HPO Messages

The Self-Monitoring Agent's Flag Files

During its first run, the HPO agent's self-monitoring feature creates a flag file for each monitored component of the HPO agent. Whenever the HPO agent's self-monitoring feature successfully completes its scheduled monitor run, an automatic action updates the time stamp of the flag file for each of the monitored components that passes the internal test. If the HPO agent's self-monitoring feature finds that one of the HPO agent components is not responding, it does not update the corresponding flag file and sends a message to the message browser reporting the failure. You can use the flag files and their individual time stamps either to confirm that the HPO agent is running correctly or, in the event that a problem occurs, show you the time at which the individual components of the HPO agent were last known to be running normally. The following example shows a list of flag files on a managed node running a UNIX operating system.

```
[root@tcbbn085]# ll /var/opt/OV/tmp/selfmon
-rw-rw-r--   1 root    sys      2 Jun  7 11:52 coda
-rw-rw-r--   1 root    sys      2 Jun  7 11:53 opcacta
-rw-rw-r--   1 root    sys      2 Jun  7 11:52 opcle
-rw-rw-r--   1 root    sys      2 Jun  7 11:52 opcmona_opcmon
-rw-rw-r--   1 root    sys      2 Jun  7 11:52 opcmona_schedule
-rw-rw-r--   1 root    sys      2 Jun  7 11:52 opcmsgi
-rw-rw-r--   1 root    sys      2 Jun  7 11:52 opctrapi
-rw-rw-r--   1 root    sys      2 Jun  7 11:52 selfmon_verify.0
-rw-rw-r--   1 root    sys      2 Jun  7 11:52 selfmon_verify.1
```

HPO Messages

This section describes the messages that the HPO agent's self-monitoring feature sends to the HPO management server and explains how to use the information in the messages to monitor the HPO agent. For more information about what to do when you receive messages indicating that the HPO agent's self-monitoring feature itself is not working as expected, see Troubleshooting the HPO-Agent Self-Monitoring Feature on page 14.

The HPO messages generated by the HPO agent's self-monitoring feature have a severity level of "major" and belong to the OpC message group. The object associated with the message is the name of the HPO agent process that did not respond to a query or failed to meet a scheduled reporting time. The text of the message sent to the message browser also reflects the HPO agent process which is not running normally. For example, if the HPO message interceptor, `opcmsgi`, does not pass the scheduled internal test, its flag file remains unchanged and the following message appears in the message browser:

```
OVO Agent self monitor: Flag file 'opcmsgi' not modified during last 355
secs (allowed max 180) - possibly OVO Message Interceptor (opsmsgi)
stuck.
```

Each message provides instruction text which explains the problem that the self-monitoring tests encountered and, where necessary, indicates if any actions are available (or required) to solve the problem. Most of the messages which the self-monitoring feature generates when it discovers that the HPO agent is not working as expected include an operator-initiated action; you can use the operator-initiated action to try to fix the problem that the HPO agent's self-monitoring feature has discovered. For example, if the HPO agent's self-monitoring feature discovers that one of the HPO agent processes is not responding, it sends a message with an operator-initiated action that allows you to restart the HPO agent processes immediately.

The HPO message-correlation feature ensures that a message with normal severity automatically clears the original warning or major message (such as the one illustrated in the example above) and then acknowledges itself. This means that, if the self-monitoring feature discovers a problem with the HPO agent, you only see the first critical message in the active message browser; duplicate messages and any normal messages that are sent after the problem has been solved all go straight to the history message browser. If you need to read the acknowledged messages, you can find them all in the history-messages browser.

Note that informational messages reporting that the HPO agent is working normally appear only once because the log-file policy OVOSelfMonVerifyLe uses the suppress-duplicates feature and the monitor policy OVOSelfMonVerifyMon uses the message-generation option "Without Reset" (in HPOM for UNIX) or "Reset value is the same as threshold limit" (in HPOM for Windows). If you need to change the configuration of the suppress-duplicates option for the self-monitoring feature, make sure that the suppression interval is always longer than the polling interval defined for the log file encapsulator by a factor of 1.5. You can set the suppression time interval in the message-correlation window.

Troubleshooting the HPO-Agent Self-Monitoring Feature

The information in this section explains how to troubleshoot problems with the HPO agent's self-monitoring feature and includes details concerning how to set up tests, which you can use to ensure that the self-monitoring feature is working as expected. The section contains information about the following topics:

- Understanding The HPO-Agent Self-Monitoring Feature
- Locating Instrumentation Components
- HPO Self-Monitoring-Agent Flag Files
- Internal Test Messages
- Stopping and Starting HPO Agent Processes

Understanding The HPO-Agent Self-Monitoring Feature

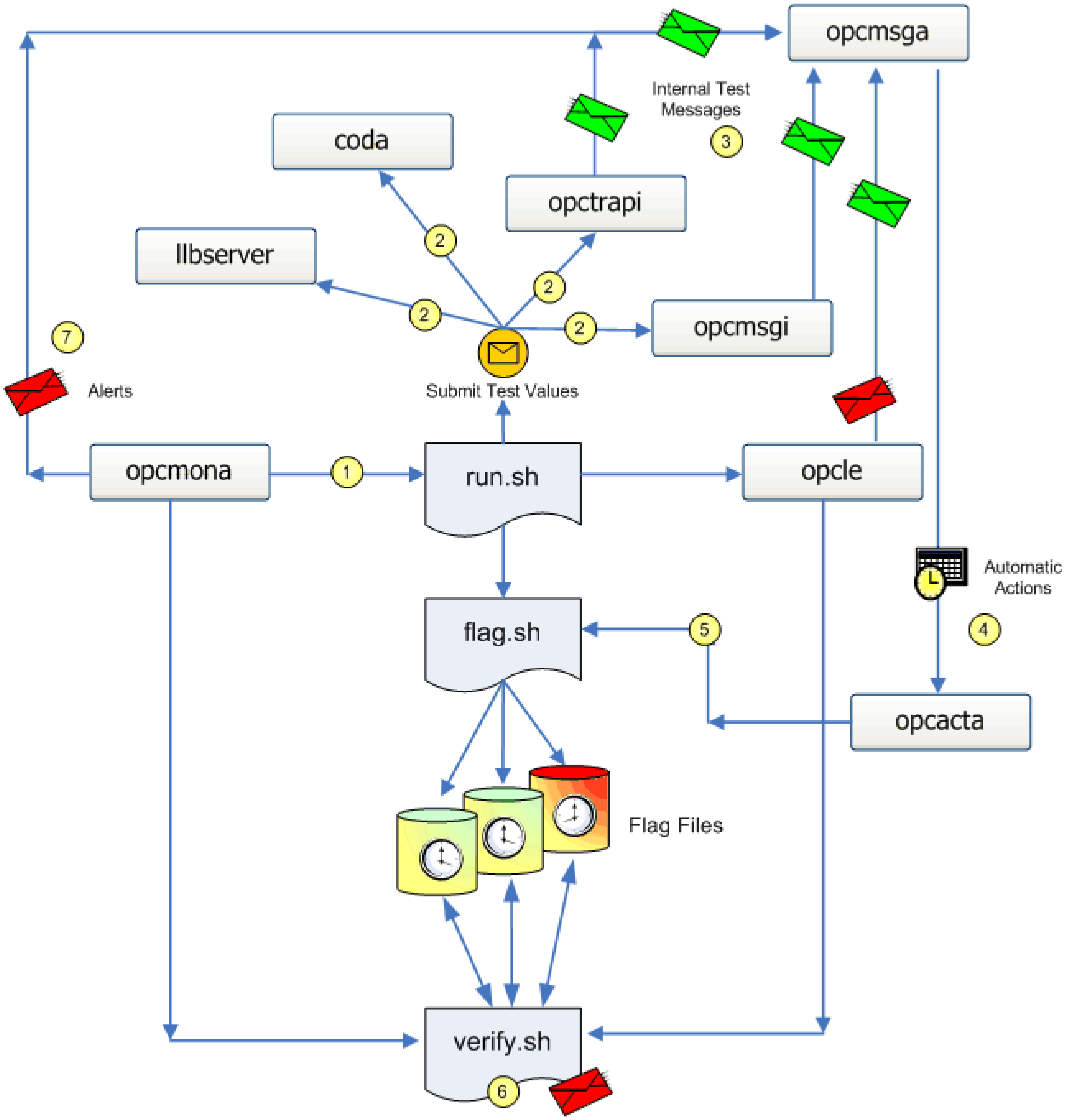
To better understand why the HPO agent's self-monitoring feature is not working as expected or is producing unexpected results, it helps to understand what the HPO agent's self-monitoring feature is supposed to do, when, and in what order. Figure 4. Sequence of Self-Monitoring Events illustrates the inner workings of the HPO agent's self-monitoring feature, the interaction and dependencies between the main self-monitoring components, and the relationship between the self-monitoring feature and the core elements of the HPO agent itself.

The following list explains the sequence of events that take place when the HPO agent's self-monitoring feature starts and gives you an idea of what tasks the agent performs and in what order. The numbers in the following list correspond to the numbers in Figure 4. Sequence of Self-Monitoring Events:

1. At a scheduled interval, by default every 3 minutes, the HPO monitor agent `opcmona` starts a self-monitoring script.
2. The HPO agent intercepts and assesses test values submitted by the self-monitoring script and generates internal HPO messages that contain automatic actions.
3. The HPO message agent processes and initiates the automatic actions
4. The action agent starts the automatic actions, which create or update the flag files for each of the individual HPO-agent processes that the HPO agent's self-monitoring feature is managing.
5. The monitor agent (`opcmona`) and the Log file encapsulator (`opcle`) frequently verify the presence and last modification times of the flag files.
6. If the HPO agent's self-monitoring feature discovers that the flag files have an unexpected time stamp, it generates an alarm and sends a message to the message browser.
7. If the expected time is violated an alarm message will be triggered.

Note that on Windows managed nodes the Windows SNMP-trap service must be installed and available to the SNMP-trap interceptor `opctrapi`. If the SNMP-trap service is not installed or is installed but set to "disabled", the SNMP-trap interceptor `opctrapi` cannot start or, if already started, shuts down. To avoid problems with the `opctrapi` on startup, make sure that, on Windows managed nodes, the SNMP-trap service is installed and either running or set to start automatically, when required.

Figure 4. Sequence of Self-Monitoring Events



Locating Instrumentation Components

All instrumentation files belonging to the HPO agent's self-monitoring feature have the prefix "ovo_selfmon_", for example: `ovo_selfmon_verify`. After successful upload of the self-monitoring components to the HPO database, the instrumentation files reside in the default location for monitor instrumentation on the HPO management server, which is the collection point for deployment of instrumentation scripts and files to the managed nodes. The location of the instrumentation files after deployment to the managed nodes depends on the type of managed node (DCE or HTTPS) and the operating system installed on the managed node.

If you encounter problems when deploying the self-monitoring feature, check that the instrumentation files are present in the agent directory structure on the managed node and, if not, that they are in the distribution directory on the management server. You can find the self-monitoring feature's instrumentation in the following locations on the management server before deployment and on the managed nodes after deployment:

HPO Management Server (before deployment)

- HPOM for UNIX:
  `/var/opt/OV/share/databases/OpC/mgd_node/customer/<platform>/<arch>/<os>/monitor`
  Where the following variable definitions apply:
  - <platform> = platform, for example: hp, ms, or sun
  - <arch> = architecture, for example: pa-risc, intel, x86, or sparc
  - <os> = operating system, for example: hp-ux11, hpux1100, nt, winnt, or solaris
- HPOM for Windows 7.x:
  `%OvShareDir%\instrumentation\<OSFamily>\<OSVersion>\OvAgtSelfMon\...`
- HPOM for Windows 8.x:
  `%OvShareDir%\instrumentation\ Categories\OvAgtSelfMon\<OSFamily>\<OSType>[[\<AgentBinaryFormat>]\<OSVersion>]`

  Where the following variable definitions apply:
  - <OSFamily> = operating-system family, for example: UNIX, OpenVMS, etc.
  - <OSType> = operating-system type, for example: HP-UX, Solaris, Windows…
  - <AgentBinaryFormat> = format of the agent binary, for example: IA32, IA64, PA-RISC, etc.
  - <OSVersion> = operating system version, for example: (HP-UX) 11.11, (Solaris) 10, (AIX) 5.2

HPO Managed Nodes (after deployment)

- Unix operating systems:
  - DCE: `/var/opt/OV/bin/OpC/[actions | commands | monitor]`
  - HTTPS: `$OVO_DATADIR/bin/instrumentation`
- Microsoft Windows operating systems:
  - DCE: `%OvAgentDir%\bin\Instrumentation\`
  - HTTPS: `%OvDataDir%\bin\Instrumentation\`

HPO Self-Monitoring-Agent Flag Files

The HPO agent's self-monitoring feature uses a system of flag files to monitor the availability of the HPO agent processes. The HPO agent's self-monitoring feature creates a flag file for each of the HPO agent processes it monitors and updates the time stamp of the flag file each time the monitor completes its run successfully. In this way, it can determine if the individual agent processes are available and responding and, if not, when an individual process last responded to the monitor test.

The flag files reside in the $OVO_DATADIR/`selfmon` directory, which you can find in the following location on the managed node:

- UNIX operating systems: `/var/opt/OV/tmp/selfmon/`
- Microsoft Windows operating systems: `%OvDataDir%\tmp\OpC\selfmon`

The names of the flag files reflect the agent process that the HPO agent's self-monitoring feature is checking. For example, the name of the flag file which the HPO agent's self-monitoring feature creates for the HPO action agent is opcacta; the name of the flag file for the HP Software Embedded Performance Component (CODA) is "coda".

In the following example, the list of the contents of the selfmon directory shows that the internal tests run by the HPO-agent self-monitoring feature did not update the time stamp for the opcmsgi flag file. The failure to update the file could mean that the HPO message interceptor has a problem that requires further investigation. In this case, the old time stamp for opcmsgi indicates the last time the message interceptor was known to be running normally.

```
[root@tcbbn085]# ll /var/opt/OV/tmp/selfmon
total 144
-rw-rw-r--   1 root    sys       2 Jun  7 11:58 coda
-rw-rw-r--   1 root    sys       2 Jun  7 11:58 opcacta
-rw-rw-r--   1 root    sys       2 Jun  7 11:58 opcle
-rw-rw-r--   1 root    sys       2 Jun  7 11:58 opcmona_opcmon
-rw-rw-r--   1 root    sys       2 Jun  7 11:58 opcmona_schedule
-rw-rw-r--   1 root    sys       2 Jun  7 11:52 opcmsgi
-rw-rw-r--   1 root    sys       2 Jun  7 11:58 opctrapi
-rw-rw-r--   1 root    sys       2 Jun  7 11:58 selfmon_verify.0
-rw-rw-r--   1 root    sys       2 Jun  7 11:58 selfmon_verify.1
```

Note that when you start the HPO agent processes, it can take a while for the self-monitoring policies to run their tests and, where appropriate, update the corresponding flag files. Since each policy runs according to a particular schedule, some flag files are updated before others. You should wait for five minutes or so before checking to see if all the flag files display the current time stamp.

Internal Test Messages

As long as the HPO agent is running as expected, the internal messages that the self-monitoring feature uses to test the availability of the HPO agent should not reach the message browser. In normal circumstances, the internal messages trigger an automatic action that updates the flag files for the individual components being tested. If an internal message from the HPO agent's self-monitoring feature reaches the messages browser, it is a sign that an automatic action failed and that there is a problem with the HPO agent that needs further investigation. For example, there is a general problem concerning the execution of actions or the instrumentation for the self-monitoring functionality has not been deployed. In any case, the message that appears in the message browser takes the following form:

```
OVO Agent self monitor: Automatic test action failed. See annotation for
details.
```

The message has the severity level "normal", is assigned to the OpC message group, and is generated by the SelfMon tool.

There are two other events which could result in the internal test messages from the HPO agent's self-monitoring feature appearing in the message browser. SNMP Traps and opcmsg messages could match a rule in a custom policy that uses one, catch-all condition to forward all input values. The only way to prevent the message appearing in the message browser is to set up a suppress condition in the policy.

Stopping and Starting HPO Agent Processes

This section explains how to test the functionality of the HPO agent's self-monitoring feature by stopping and restarting agent processes on the managed node and checking whether the HPO agent sends messages, as expected, to the management server. The way you stop and start agent processes depends on whether the managed node you are testing is running a UNIX or a Windows operating system.

For UNIX operating systems:

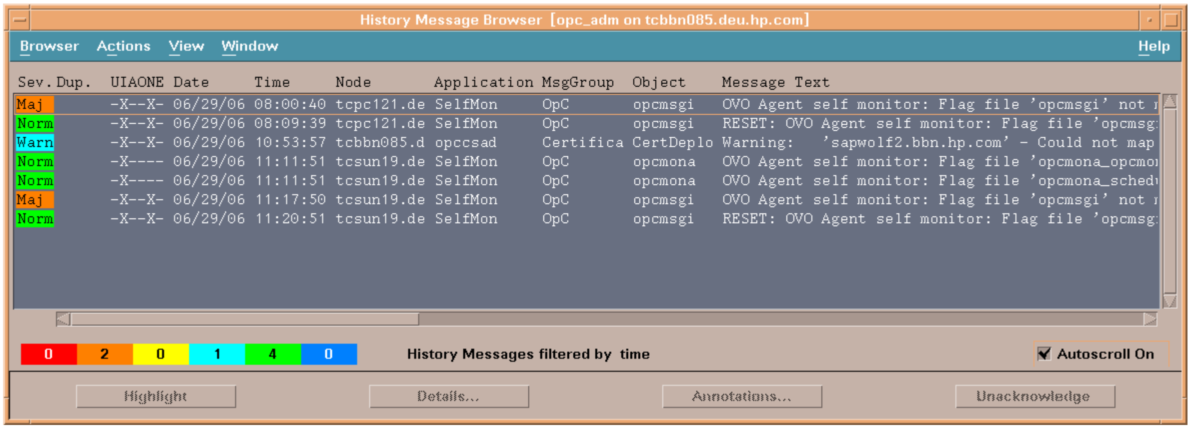
To stop and restart individual HPO-agent processes on a managed node running a Unix operating system, perform the following steps:

1. Determine the ID of the HPO agent processes you want to pause, for testing purposes, for example:
   ps –eaf | grep opcmsgi
   ```
   root  1683  6541  0  June 8  ?  0:07  /opt/OV/lbin/eaagt/opcmsgi
   ```
2. Pause the process on the managed node with the kill command and the –STOP option:
   kill –STOP 1683
   Note that the –STOP option ensures that the opcmsgi process retains its original PID, which could lead to some confusion. For example, while the opcmsgi command is "stopped", the `opcagt –status` command reports the opcmsgi process as running. However, the HPO agent's self-monitoring feature notes, correctly, that the process is not available and does not update the corresponding flag file.
3. After at least three minutes, check the `selfmon` directory which the HPO agent's self-monitoring feature uses to store its flag files, to verify that the self-monitoring feature does not update the flag file for the stopped process (opcmsgi) during the next monitor run. In the example shown in HPO Self-Monitoring-Agent Flag Files, `opcmsgi` still has the timestamp for the last successful monitor run when the process was running and available.
4. Check the HPO message browser for messages relating to the unavailability of the message interceptor, `opmsgi`, for example:

   ```
   OVO Agent self monitor: Flag file 'opcmsgi' not modified during last
   355 secs (allowed max 180) - possibly OVO Message Interceptor (opsmsgi)
   stuck.
   ```
5. The message that the HPO agent's self-monitoring feature generates contains an automatic action which attempts to restart the agent process.
6. Resume the paused opcmsg process using the kill command with the –CONT option, as follows:
   kill –CONT 1683
7. As soon as the HPO agent's self-monitoring feature finds that the `opsmsgi` process is available again, it resets the `opsmsgi` flag file and sends an informational message with severity "normal" to the message browser.

   ```
   RESET: OVO Agent self monitor: Flag file 'opcmsgi' not modified during
   last 57 secs (allowed max 180) - possibly OVO Message interceptor
   (opcmsgi) stuck.
   ```

Figure 5. HPOM for UNIX – Selfmon's Automatically Acknowledged Messages



Sev.	Dup.	UIAONE	Date	Time	Node	Application	MsgGroup	Object	Message Text
Maj		-X--X-	06/29/06	08:00:40	tcpc121.de	SelfMon	OpC	opcmsgi	OVO Agent self monitor: Flag file 'opcmsgi' not
Norm		-X--X-	06/29/06	08:09:39	tcpc121.de	SelfMon	OpC	opcmsgi	RESET: OVO Agent self monitor: Flag file 'opcmsg
Warn		-X--X-	06/29/06	10:53:57	tcbbn085.d	opccsad	Certifica	CertDeplo	Warning: 'sapwolf2.bbn.hp.com' - Could not map
Norm		-X----	06/29/06	11:11:51	tcsun19.de	SelfMon	OpC	opcmona	OVO Agent self monitor: Flag file 'opcmona_opcmo
Norm		-X----	06/29/06	11:11:51	tcsun19.de	SelfMon	OpC	opcmona	OVO Agent self monitor: Flag file 'opcmona_sched
Maj		-X--X-	06/29/06	11:17:50	tcsun19.de	SelfMon	OpC	opcmsgi	OVO Agent self monitor: Flag file 'opcmsgi' not
Norm		-X--X-	06/29/06	11:20:51	tcsun19.de	SelfMon	OpC	opcmsgi	RESET: OVO Agent self monitor: Flag file 'opcmsg

History Messages filtered by time

Note that the "reset" message acknowledges the original "warning" message to which it refers and sends the "warning" message to the history-message browser. In addition, the reset message is itself automatically acknowledged, which means it does not appear in the active message browser. If you want to read either the original "warning" message or the subsequent "reset" message, look in the history-message browser as indicated in Figure 5. HPOM for UNIX – Selfmon's Automatically Acknowledged Messages.

After starting or restarting the HPO agent processes, it takes a while for the self-monitoring policies to run their tests and, where appropriate, update the corresponding flag files. Since each policy runs according to a particular schedule, some flag files are updated before others. You should wait for five minutes or so before checking to see if all the flag files display the current time stamp.

For Microsoft Windows operating systems:

To stop and restart individual HPO-agent processes on a managed node running a Microsoft-Windows operating system, perform the following steps:

1. Use a process explorer to locate and isolate the HPO agent process you want to pause, for example: `opcmsgi.exe`. Note that under Microsoft Windows, the HPO agent processes run as child processes of the HPO control agent, `opcctla.exe`.
2. Pause the process temporarily by right-clicking the `opcmsgi.exe` element in the process tree and clicking Suspend.
3. Wait for at least three minutes for the next HPO-agent self-monitoring run to start.
4. Check that the HPO-agent self-monitoring feature sends a message with the severity "warning" to the HPO for Windows console indicating that there might be a problem with the HPO-agent message interceptor, `opcmsgi.exe`, because the corresponding flag file was not updated at the expected time. For example:

   ```
   OVO Agent self monitor: Flag file 'opcmsgi' not modified during last 236
   secs (allowed max 180) - possibly OVO Message interceptor (opcmsgi)
   stuck.
   ```
5. Open the warning message from the HPO-agent self-monitoring feature and click the Commands tab.
6. In the Operator-Initiated Action section of the Commands tab, check the status box. If the box indicates that the process is Not Started, click the Start button to restart the HPO agent. Note that

you might have to click the Refresh button to ensure that the Message-Properties dialog displays the current status of the HPO agent processes.

7. Check that the HPO-agent self-monitoring feature sends a reset message to the HPO for Windows console confirming that the opsmsgi process is available again and that it has reset the opsmsgi flag file. The message is for your information only, has the severity “normal”, and contains the following (or very similar) text:

```
RESET: OVO Agent self monitor: Flag file 'opcmsgi' not modified during
last 57 secs (allowed max 180) - possibly OVO Message interceptor
(opcmsgi) stuck.
```

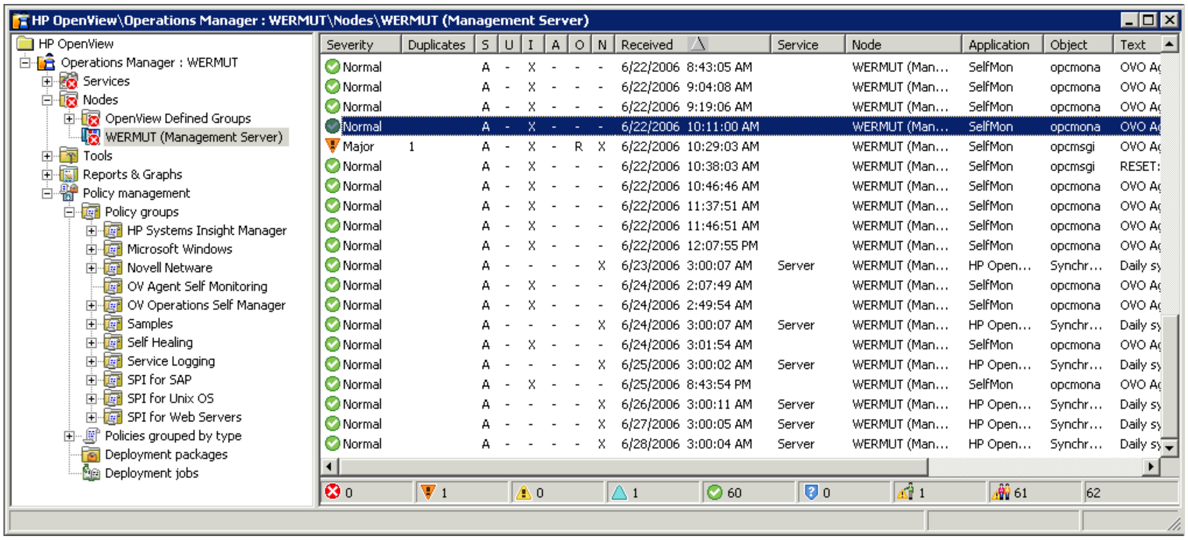
   Note that HPO for Windows message-correlation feature automatically acknowledges the reset message and places it in the acknowledged-messages browser. You do not see the message in the active-messages browser.

8. Check that the next message that the HPO-agent self-monitoring feature sends has the severity “normal” and confirms that the HPO monitor agent opcmona is working normally. For example:

```
OVO Agent self monitor: Flag file 'opcmona_schedule' OK - OVO Monitor
agent (opcmona) seems to be OK.
```

   This message also appears directly in the acknowledged-messages browser, as you can see in Figure 6. HPOM for Windows – Selfmon’s Automatically Acknowledged Messages.

Figure 6. HPOM for Windows – Selfmon’s Automatically Acknowledged Messages



Severity	Duplicates	S	U	I	A	O	N	Received	Service	Node	Application	Object	Text
Normal		A	-	X	-	-	-	6/22/2006 8:43:05 AM		WERMUT (Man...	SelfMon	opcmona	OVO A
Normal		A	-	X	-	-	-	6/22/2006 9:04:08 AM		WERMUT (Man...	SelfMon	opcmona	OVO A
Normal		A	-	X	-	-	-	6/22/2006 9:19:06 AM		WERMUT (Man...	SelfMon	opcmona	OVO A
Normal		A	-	X	-	-	-	6/22/2006 10:11:00 AM		WERMUT (Man...	SelfMon	opcmona	OVO A
Major	1	A	-	X	-	R	X	6/22/2006 10:29:03 AM		WERMUT (Man...	SelfMon	opcmsgi	OVO A
Normal		A	-	X	-	-	-	6/22/2006 10:38:03 AM		WERMUT (Man...	SelfMon	opcmsgi	RESET:
Normal		A	-	X	-	-	-	6/22/2006 10:46:46 AM		WERMUT (Man...	SelfMon	opcmona	OVO A
Normal		A	-	X	-	-	-	6/22/2006 11:37:51 AM		WERMUT (Man...	SelfMon	opcmona	OVO A
Normal		A	-	X	-	-	-	6/22/2006 11:46:51 AM		WERMUT (Man...	SelfMon	opcmona	OVO A
Normal		A	-	X	-	-	-	6/22/2006 12:07:55 PM		WERMUT (Man...	SelfMon	opcmona	OVO A
Normal		A	-	-	-	-	X	6/23/2006 3:00:07 AM	Server	WERMUT (Man...	HP Open...	Synchr...	Daily sy
Normal		A	-	X	-	-	-	6/24/2006 2:07:49 AM		WERMUT (Man...	SelfMon	opcmona	OVO A
Normal		A	-	X	-	-	-	6/24/2006 2:49:54 AM		WERMUT (Man...	SelfMon	opcmona	OVO A
Normal		A	-	-	-	-	X	6/24/2006 3:00:07 AM	Server	WERMUT (Man...	HP Open...	Synchr...	Daily sy
Normal		A	-	X	-	-	-	6/24/2006 3:01:54 AM		WERMUT (Man...	SelfMon	opcmona	OVO A
Normal		A	-	-	-	-	X	6/25/2006 3:00:02 AM	Server	WERMUT (Man...	HP Open...	Synchr...	Daily sy
Normal		A	-	X	-	-	-	6/25/2006 8:43:54 PM		WERMUT (Man...	SelfMon	opcmona	OVO A
Normal		A	-	-	-	-	X	6/26/2006 3:00:11 AM	Server	WERMUT (Man...	HP Open...	Synchr...	Daily sy
Normal		A	-	-	-	-	X	6/27/2006 3:00:05 AM	Server	WERMUT (Man...	HP Open...	Synchr...	Daily sy
Normal		A	-	-	-	-	X	6/28/2006 3:00:04 AM	Server	WERMUT (Man...	HP Open...	Synchr...	Daily sy

After starting or restarting the HPO-agent processes, it takes a while for the various self-monitoring policies to run their tests and, where appropriate, update the corresponding flag files. Since each policy runs according to a particular schedule, some flag files are updated before others. You should wait for five minutes or so before checking to see if all the flag files display the current time stamp.

Uninstalling the HPO-Agent Self-Monitoring Feature

This section briefly describes how to remove the HPO agent’s self-monitoring feature along with any associated files from the managed nodes and the management server. The information applies to node managed by either HPOM for UNIX or HPOM for Windows management servers. In both cases, you first remove the HPO configuration components from the managed nodes where the HPO agent's self-monitoring feature is running; then you remove the HPO agent's self-monitoring feature software from the management server. For more information about both these topics, see the following sections:

- Removing the HPO-Agent Self-Monitoring Feature from the Managed Node
- Removing the HPOM-Agent Self-Monitoring Feature from the Management Server

Removing the HPO-Agent Self-Monitoring Feature from the Managed Node

The information in the section describes how to remove the HPO self-monitoring agent components from the managed nodes. The instructions differ according to whether HPOM for UNIX or HPOM for Windows is managing the node:

For nodes managed by HPOM for UNIX:

1. *Optional*: Pause the HPO agent on the managed node where you want to remove the self-monitoring functionality:
   `opcagt -stop`
2. In the HPOM for UNIX administrator's GUI, remove the self-monitoring templates from the list of templates assigned to the managed node:
   `Actions > Agents > Assign Templates`…
3. Re-deploy the modified template-assignment list (which no longer includes the self-monitoring templates) to the managed node:
   `Actions > Agents > Install / Update OVO Software and Configuration`
4. Check the current template assignment to the managed node by generating a configuration report for the managed node:
   `Actions > Utilities > Reports > Node Configuration`
5. On the managed node, remove the directory containing the self-monitoring flag files:
   – UNIX operating systems: `/var/opt/OV/tmp/selfmon/`
   – Microsoft Windows operating systems: `%OvDataDir%\tmp\OpC\selfmon`
6. *Optional*: Restart the HPO agent:
   `opcagt -start`

For nodes managed by HPOM for Windows:

1. Remove the self-monitoring feature's policies from the managed node, as follows:
   – In the HPOM for Windows console, expand Policy Management > Policy Groups
   – Locate and right-click the HPOM Agent Self Monitoring policy group
   – Select the option: All Tasks > Uninstall from…
   – In the Uninstall policies on… dialog, check the managed nodes from which you want to remove the HPO agent's self-monitoring policies and click OK.
2. Check that the folder `%OvDataDir%\tmp\OpC\selfmon` containing the self-monitoring feature's flag files has been removed. If it has not, then remove it now.

Removing the HPOM-Agent Self-Monitoring Feature from the Management Server

The information in the section describes how to remove the HPO agent's self-monitoring feature software from the HPO management server. The instructions differ according to whether the HPO management server is running on UNIX or Microsoft Windows operating systems, as follows:

For HPOM for UNIX management servers:

1. Remove the self-monitoring policies from the HPOM GUI:
   - In the Message Source Templates window, select the OVO SelfMon template group
   - Click Delete From All...
2. If you deployed the self-monitoring policies to manage the HPO agent on the HPO management server, remove the flag-file directory created during the installation of the self-monitoring feature, namely: `/var/opt/OV/tmp/selfmon/`
3. Remove the instrumentation for the self-monitoring functionality. HPO self-monitoring instrumentation has the prefix "ovo_selfmon" and resides in the following directory:
   - `/var/opt/OV/share/databases/OpC/mgd_node/customer/<platform>/monitor/`
4. Verify that the self-monitoring components are no longer present in the HPO GUI and that the self-monitoring instrumentation is no longer present in the instrumentation directories.

For HPOM for Windows management servers:

1. Remove the self-monitoring components from the HPOM for Windows console:
   - In the HPOM for Windows console, expand Policy Management > Policy Groups
   - Locate and right-click the HPOM Agent Self Monitoring policy group
   - Select the option: All Tasks > Uninstall from…
   - In the Uninstall policies on… dialog, check the managed nodes from which you want to remove the HPO agent's self-monitoring policies and click OK.
2. Check whether `%OvAgentDir%\tmp\OpC\selfmon`, the folder containing the self-monitoring feature's flag files, exists. If the selfmon folder does exist, you can remove it now.
3. Start the HPOM Agent Self Monitoring `setup.exe` tool, select the "Remove" option, and confirm that you want to remove the selected applications.
4. After the removal process completes, check whether the folders containing the self-monitoring feature's instrumentation exist; if they do, you can safely remove them now, for example:

   HPOM 7.5:
   ```
   %OvDataDir%\shared\Instrumentation\HPUX\B.11.11\OvAgtSelfMon
   %OvDataDir%\shared\Instrumentation\Windows XP\5.1\OvAgtSelfMon
   ```

   HPOM 8.X:
   ```
   %OvShareDir%\instrumentation\Categories\OvAgtSelfMon\
   <OSFamily>\<OSType>\[<AgentBinaryFormat>]\<OSVersion>]
   ```

For more information

www.hp.com/go/managementsoftware

Call to action

www.hp.com/go/managementsoftware

08/2007