HP Operations Agent

Software Version: 11.16
Windows ®, HP-UX, Linux, Solaris, and AIX operating systems

Concepts Guide

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

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

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.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

Acknowledgements

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright ©1995-2002 Jean-loup Gailly and Mark Adler.

Documentation Updates

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

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

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

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

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

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

Support

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

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

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

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

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

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

To find more information about access levels, go to:

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

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

Chapter 1: Introduction

The HP Operations agent helps you monitor a system by collecting metrics that indicate the health, performance, and availability of essential elements of the system. While HP Operations Manager (**HPOM**) presents you with the framework to monitor and manage multiple systems through a single, interactive console, the HP Operations agent deployed on individual nodes helps you gather vital information to facilitate the monitoring process.

When you use the HP Operations agent in conjunction with HPOM and Smart Plug-ins (**SPIs**), you can add the capability to monitor business applications running on monitored systems. When used in isolation (in an environment where HPOM is not deployed), you can use the log file-based data store of the HP Operations agent to read system performance data.

Based on your requirement, you can install the HP Operations agent in one of the following uses:

- **Centralized monitoring with HPOM:** In this scenario, HPOM and the HP Operations agent together build up a distributed monitoring environment that helps you manage heterogeneous systems and applications.
- **Performance monitoring of an isolated system:** When installed without the presence of HPOM, the HP Operations agent enables you to monitor the health and performance of the system using the performance data stored into its log file-based storage system.

HP Operations Agent in an HPOM-Managed Environment

The management concept of HPOM is based on communication between a management server and managed nodes. Processes running on the central management server communicate with the HP Operations agent processes running on managed nodes across the network. The HP Operations agent collects data and processes events on the managed nodes, and then forwards the relevant information to the HPOM console in the form of messages. HPOM responds to the messages with actions to prevent or correct problems on the managed nodes.

This HP Operations agent sets up a secure communication channel between the management server and the managed nodes, and thereby helps you implement a secure monitoring process in your organization.

Policies, deployed from the HPOM management server to the monitored node, provide the agent with necessary details on the monitoring plan. Based on the rules specified in available policies, the HP Operations agent generates messages that are forwarded to the HPOM console.

With its embedded **data collector**, the HP Operations agent collects a rich set of system performance metrics from the monitored system to help you analyze the system health. With the help of SPIs, which introduce additional collectors to the system, you can collect important metrics of the applications running on the system. The combination of system performance and application metrics enables you to perform a well-rounded study of the health and performance of hardware and software assets on which your critical business services run.

HP Operations Agent on an Isolated System

In an environment where HPOM is not installed, you can use the HP Operations agent to collect and monitor performance data of individual systems. The embedded data collector of the HP Operations agent enables you to collect and log performance metrics of systems in your environment. You can use different utilities available with the HP Operations agent to read and analyze the performance data stored into log files, or use data analysis tools like HP Performance Manager to identify performance bottlenecks of the monitored system.

Features and Benefits

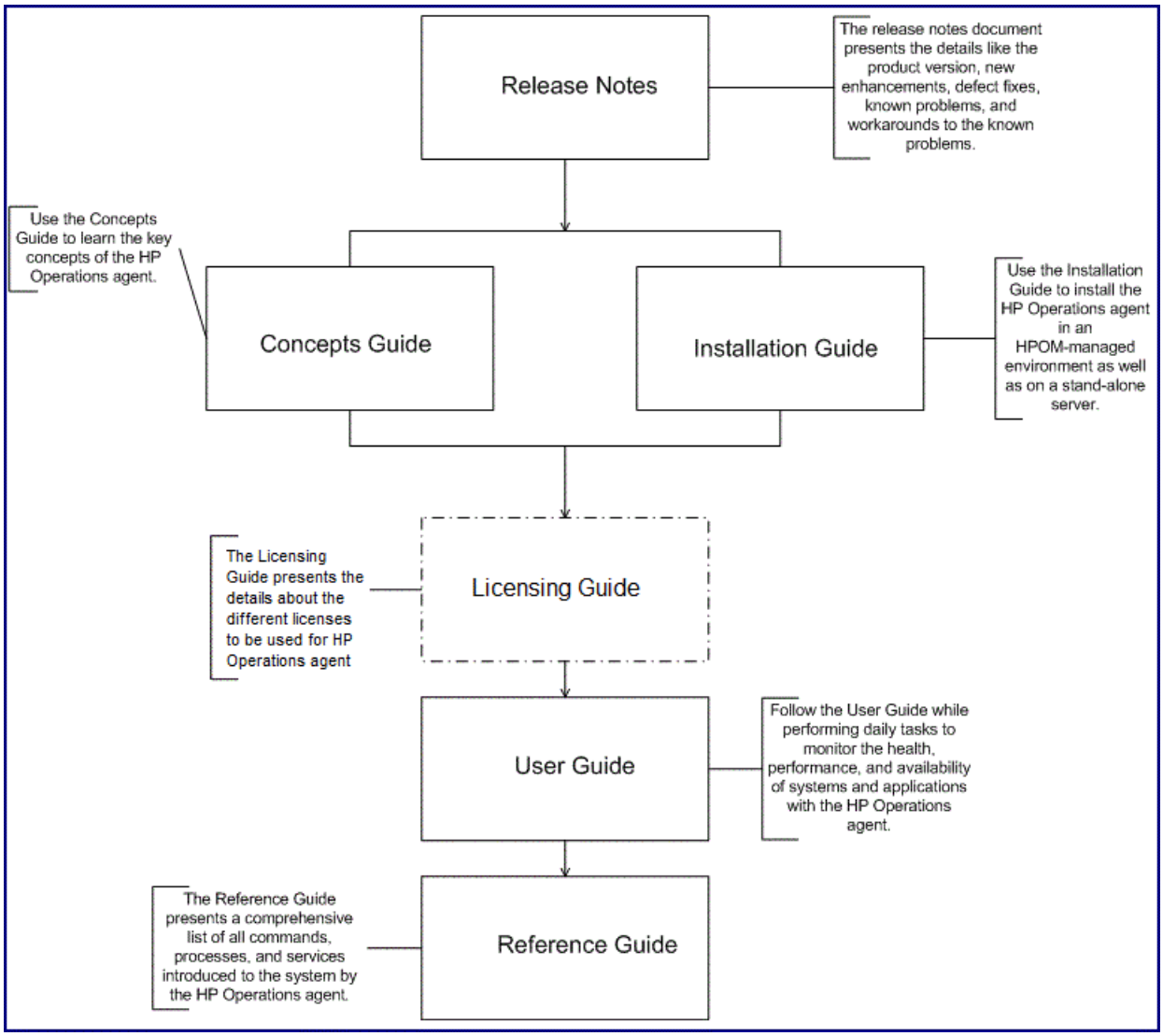
The following list explains the major features of the HP Operations agent available with the version 11.16:

- **Collecting system performance details:** The HP Operations agent collects a rich set of metrics that indicate the health and performance of the system. The collected data is stored in log files. You can configure the frequency of the collection cycle and types of information the agent collects.
- **Collecting real-time performance data:** The HP Operations agent helps you collect and monitor system performance metrics of the monitored system on a real-time basis.
- **Generating alerts based on rules:** Based on rules and specifications, the HP Operations agent can compare obtained data with preset conditions and generate events and perform certain actions.
- **Monitoring remote nodes:** You can configure the HP Operations agent to monitor remote systems (where the HP Operations agent is not installed) by intercepting SNMP traps and WMI instances or classes that originate from the systems.

Documentation Map

The documentation map presents a list of all the major documents for the HP Operations agent. You can use the map to identify the necessary document when you need assistance.

Figure 1: Documentation Map for the HP Operations Agent


Release Notes
The release notes document presents the details like the product version, new enhancements, defect fixes, known problems, and workarounds to the known problems.
Use the Concepts Guide to learn the key concepts of the HP Operations agent.
Concepts Guide
Installation Guide
Use the Installation Guide to install the HP Operations agent in an HPOM-managed environment as well as on a stand-alone server.
The Licensing Guide presents the details about the different licenses to be used for HP Operations agent
Licensing Guide
User Guide
Follow the User Guide while performing daily tasks to monitor the health, performance, and availability of systems and applications with the HP Operations agent.
The Reference Guide presents a comprehensive list of all commands, processes, and services introduced to the system by the HP Operations agent.
Reference Guide

Chapter 2: HP Operations Agent with HPOM

HPOM, along with the HP Operations agent, helps you monitor and manage systems and applications deployed in your network environment from a central console. In an HPOM-based management environment, you can start monitoring the systems of your interest after installing the HP Operations agent on them. With the help of policies deployed from the HPOM console on the agent node, you can enable different monitoring capabilities of the agent.

Primary responsibilities of the agent in a distributed environment are:

- **Monitoring data**
  The HP Operations agent can compare the value of a specific metric with a preset value and take necessary actions based on its configuration. Policies, deployed from the HPOM console to the node, play a major role in facilitating the monitoring capability of the HP Operations agent.
- **Collecting and storing data**
  You can program the embedded data collector of the HP Operations agent to collect and log the data of your interest on the monitored system. You can add additional collection capabilities by installing SPIs and log the data collected by SPIs into agent's data store.

Policies

To work with the agent, you must deploy collections of configuration details and specifications called policies on the managed nodes from the HPOM console. Depending on the types of policies deployed, different components of the HP Operations agent are enabled. A policy can provide the following details to the agent:

- **Monitoring source details**
  - Objects to monitor
  - Polling interval for monitoring an object
  - Threshold value for the monitored object
  - Rules and conditions for analysis of data against the set threshold
- **Event details**
  You can configure the HP Operations agent using policies to generate events with messages, instructions, and severity flags when a monitored object violates the threshold rule. The events are forwarded to the HPOM console in the form of messages. You can set the agent to perform certain action against these events.
- **Data collection details**
  If you want to monitor the data collected by an external program, you can program the HP Operations agent to log the data into its embedded data store.

Workflow of the HP Operations Agent

The HP Operations agent functions in the following sequence to enable HPOM to monitor events generated on different nodes available on the network:

1. **Data collection**
   After installation and configuration, the HP Operations agent starts collecting and logging system performance data. The collected system parameters are stored into agent's data store in the form of metrics. You can configure the HP Operations agent to modify the default collection schedule and the range of metrics it stores.
2. **Monitoring**
   Based on the specification in the deployed policies, the HP Operations agent compares values of metrics (either logged into its data store or gathered by external programs) with preset values.
3. **Alerting**
   In the event of threshold violation, the HP Operations agent can forward messages with severity flags to the HPOM console to notify you about the performance bottlenecks on the monitored system.
4. **Actions**
   The HP Operations agent can perform specific actions on the monitored system.

HTTPS Mode of Communication

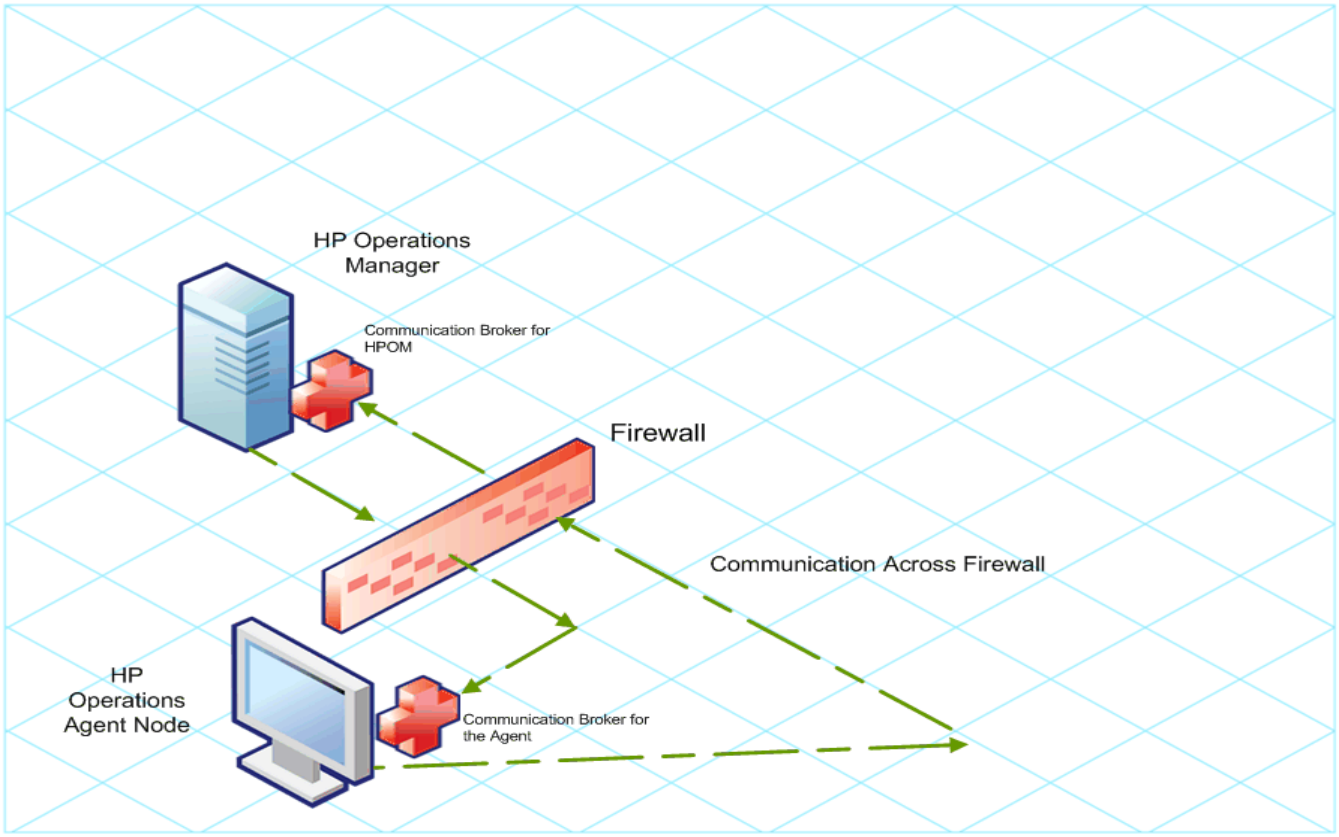
The HP Operations agent nodes, by using the HTTPS mode of communication, can easily communicate with each other, as well as with other industry-standard products.

Benefits of the HTTPS Communication

- **Communication Over Firewalls**
  With the help of the HTTPS protocol, the HP Operations agent nodes can communicate with other systems available across firewalls. You can deploy the HP Operations agent in a secure environment built with HTTP proxies and firewalls.

  Figure 2 illustrates how to cross a firewall using HTTPS-communication.

  Figure 2: Crossing a Firewall with HTTPS Communication

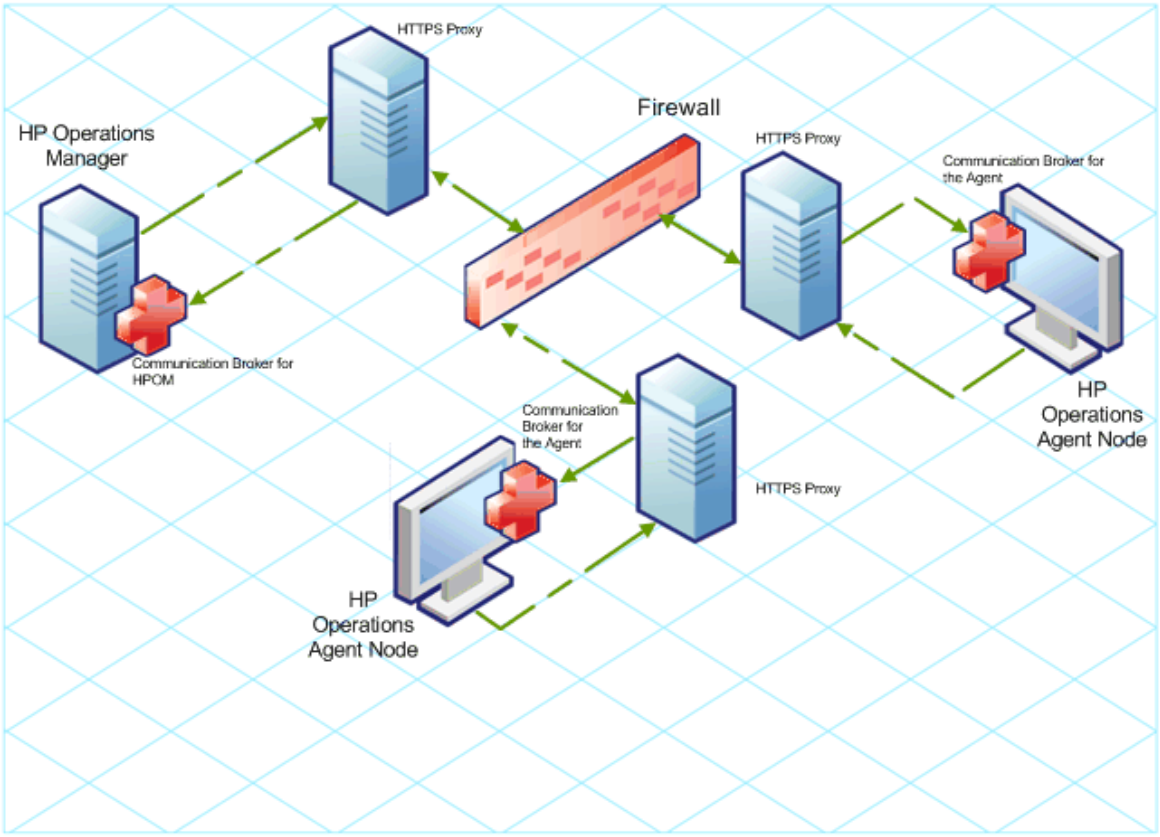


- **Advanced Security**
  The HP Operations agent product uses the Secure Socket Layer (SSL) to restrict and control user access. With the help of SSL, the HP Operations agent product compresses and encrypts all the data involved in its communication with other systems.

  In addition, all remote messages arrive through the Communication Broker component, providing a single port entry to the HP Operations agent node.

  From an HP Operations agent node, if you want to send messages, files, or objects, you can configure one or more standard HTTP proxies to cross a firewall or reach a remote system.

  Figure 3: Crossing a Firewall using External HTTPS Proxies



- **Open Standards**
  HP Operations agent's HTTPS communication is built on the industry standard HTTP 1.1 protocol and SSL sockets. HP Operations agent's adherence to open standards, such as HTTP, SSL, and SOAP, enables you to maximize the use of your current HTTP infrastructure.
- **Scalability**
  HP Operations agent's HTTPS communication is designed to perform well, independent of the size of the environment and the amount of data sent and received. HP Operations agent's HTTPS communication can be configured to suit the requirement of your organization.

Communication Broker

The Communication Broker component provides a single-port solution for an HP Operations agent node. In a typical deployment scenario, multiple servers can be registered with the HP Operations agent node for data communication. The HP Operations agent product directs the requests for all registered servers on the node through the Communication Broker. The Communication Broker transparently forwards the request to the registered server in the same way as an HTTP proxy forwards an HTTP request. The default port for the Communication Broker is 383. You can configure the HP Operations agent product to use a different port for the Communication Broker.

For higher security on UNIX systems, the Communication Broker starts up with `chroot`. `chroot` restricts the part of the file system visible to the Communication Broker process by making the specified path act as the root directory, therefore reducing exposure to unauthorized access.

The Communication Broker runs as a daemon on a UNIX system and as a service on a Windows system.

The Communication Broker uses a minimum of one port for accepting incoming data to a node. The port is associated with a unique node identifier (`OVCoreID`) to identify the node. You can configure the Communication Broker to use multiple ports for high availability nodes.

Firewall Scenarios

Firewalls can protect systems in a network from external attacks. They usually separate the Internet from a private Intranet. You can implement multiple levels of firewalls to restrict access to the more trusted environments from those of lower sensitivity.

A firewall separates a networked environment into two basic zones: the **trusted zone** and the **Demilitarized zone** (**DMZ**) (for example, the Internet). A firewall configuration ensures that data transmission from DMZ to the trusted zone is restricted or controlled. Based on the configuration, the firewall can allow a **two-way communication** or an **outbound-only communication**.

If you configure the firewall in your environment to allow a two-way communication, the network allows the HTTPS communication across the firewall in both directions with certain restrictions. You can configure the firewall settings in this environment to use the following configuration options:

- *Proxies*: If your network allows only certain proxy systems to connect through the firewall, you can redirect HP Operations agent communication through these proxies.
- *Local ports*: If your network allows outbound connections from only certain local ports, you can configure HP Operations agent to use specific local ports.
- *Communication broker ports*: If your network allows inbound connections to only certain destination ports, but not to port 383, you can configure alternate communication broker ports.

When the firewall in your environment allows outbound-only communication, you can configure a **Reverse Channel Proxy** (**RCP**) with the HP Operations agent product. The RCP configured with the HP Operations agent node works like an HTTP proxy and enables you to transfer data from DMZ to the trusted (secure) zone. Instead of directly communicating to HP Software systems, RCPs establish a communication channel to the Communication Broker. The Communication Broker verifies and authenticates the information originating from DMZ, and then transfers the validated information to the HP Operations agent node present in the trusted (secure) zone.

HTTPS-Based Security Components

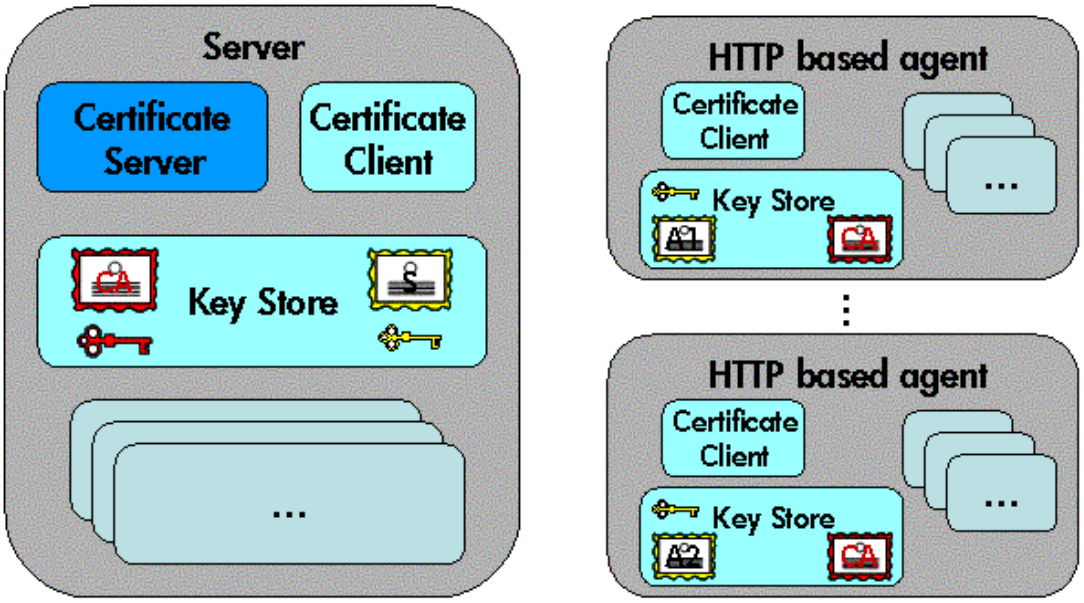
To communicate with other HP Operations agent nodes or the HPOM server, an HP Operations agent node must have a valid, industry standard, X509 certificate. The nodes communicate with one another after exchanging certificates signed by 1024-bit keys. The exchange of certificates helps a node identify another node or server in the managed environment.

The major components responsible for creating and managing certificates are:

- Certificate Server (resides on the HPOM server)
- HP Operations agent Key Store
- HP Operations agent Certificate Client

Figure 4 illustrates these components:

Figure 4: Components of Authenticated Communication



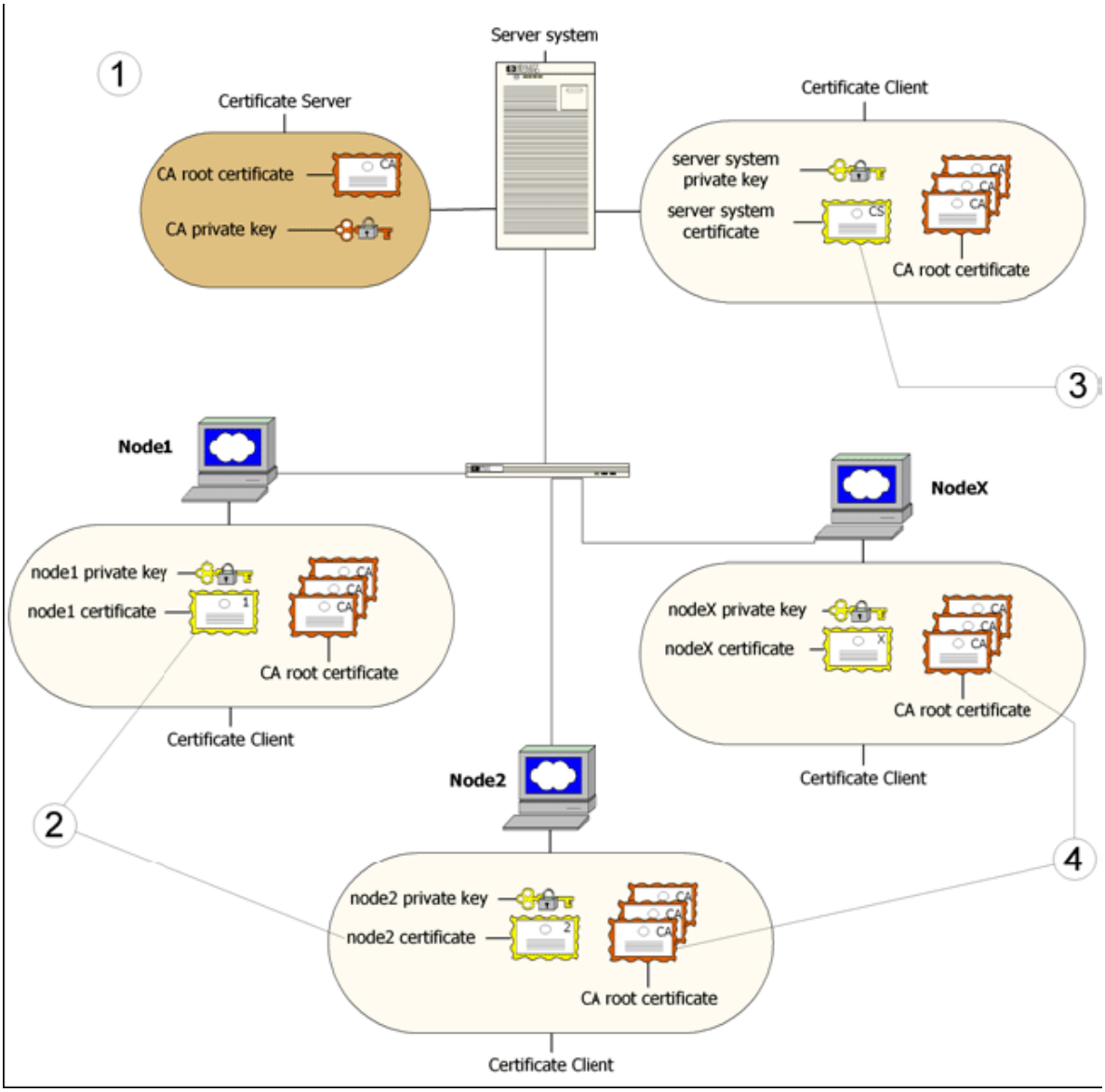
Each system hosting an HP Operations agent is allocated a unique identifier value for the parameter `OvCoreId`, which is created during installation of the HP Operations agent on that system.

Note: The `OvCoreId` parameter does not change for an agent node even after changing the hostname or IP address of the system.

For each agent node, `OvCoreId` is used as a unique identifier and contained in the corresponding node certificate. `OvCoreId` is allocated its value during installation.

Figure 5 illustrates an environment for authenticated communication in an HP Operations agent deployment.

Figure 5: Environment for Authenticated Communication



1. A server system hosts the Certificate Server, which contains the required certification authority (CA) functionality.
2. Every system has a certificate that was signed by the Certificate Server with the certification authority private key.
3. The server system also needs a certificate to manage its identity.
4. Every system has a list of trusted root certificates, which must contain at least one certificate. The trusted root (CA) certificates are used to verify the identity of the communication partners; a communication partner is trusted if the presented certificate can be validated using the list of trusted certificates.

   A list of trusted root certificates is required when the certificate client is being managed by more than one HPOM server.

Certificates

The HP Operations agent uses the following two types of certificates:

- Root certificates
- Node certificates

A root certificate is a self-signed certificate, which contains the identity of the certification authority of the certificate server. The private key belonging to the root certificate is stored on the certificate server system and protected from unauthorized access. The certification authority uses its root certificate to digitally sign all certificates.

Every agent node in the managed environment receives a node certificate issued by the certificate server. While issuing the certificate, the certificate client running on the agent node stores a corresponding private key in the file system.

Note: A node certificate contains a unique node identifier—`OvCoreId`. The following is an example of `OvCoreId`:
`d498f286-aa97-4a31-b5c3-806e384fcf6e`

Each node can be securely authenticated through its node certificate. The node certificate can be verified by all other nodes in the environment using the root certificate(s) to verify the signature. Node certificates are used to establish SSL-based connections between two HTTPS nodes that use client and server authentication, and can be configured to encrypt all communication.

The `ovcert` tool provided by the certificate client lists the contents of the Key Store or shows information about an installed certificate.

HP Operations Agent Certificate Server

The certificate server is responsible for the following:

- Creating and installing self-signed root certificates.
- Importing self-signed root certificates from the file system.
- Storing the private keys of root certificates.
- Granting or denying certification requests.
- Creating a new certificate and a corresponding private key or creating an installation key for manual certificate installation.
- Offering a service for clients to automatically retrieve trusted root certificates.

Certification Authority

Note: Every HPOM server is automatically configured as a Certificate Authority. The default certificate server for every agent node is the HPOM server associated with the node.

The certification authority is a part of the certificate server and is the center of trust in certificate management. Certificates signed by this certification authority will be regarded as valid certificates and

therefore be trustworthy. The certification authority must be hosted in a highly secure location. By default, it is installed on the system hosting HPOM.

Since the certification authority is the root of trust, it operates with a self-signed root certificate. This root certificate and the corresponding private key are created and stored on the file system with the level of protection to allow the certification authority to operate. After initialization, the certificate authority signs granted certificate requests using its root certificate.

Certificate Client

The certificate client runs on every agent system.

The certificate client operates as follows:

- The certificate client checks whether the node has a valid certificate.
- If the node has no certificate, the certificate client generates a new public and private key pair and creates a certificate request based on the unique identity (`OvCoreId` value) of the node. The certificate client sends the certificate request to the certificate server with additional node properties, and then the certificate client waits for a response.
- The additional node properties, for example DNS name and IP address of the node helps the certificate server identify the origin of the request.
- When the certificate server issues a new certificate, the certificate client installs the certificate on the node. The certificate client can ensure that all HTTPS-based communication uses this certificate.
- If the request is not successfully processed, a descriptive error is logged and the associated status is set.

In addition, the certificate client performs the following tasks:

- The certificate client contacts a certificate server to update the server's trusted root certificates.
- It supports the import of a node certificate and the corresponding private key from the file system.
- It supports the import of trusted root certificates.
- It provides status information. Status includes `OK`, `valid certificate`, `no certificate`, `certificate requested`, and `certificate request denied`.

Root Certificate Update and Deployment

It may be necessary to update the trusted root certificates of one or more nodes, for example, in environments hosting several certificate servers.

It is possible to supply all currently trusted root certificates to certificate clients in a secure way. It is usually sufficient to supply the root certificate of the certification authority. However, it may be necessary to deploy one or more additional root certificates to selected certificate clients, for example when there is more than one certification authority in the environment.

The certificate client enables you to request the certificate server to update the trusted root certificates through the command line tool `ovcert`.

Chapter 3: HP Operations Agent on a Standalone Server

The HP Operations agent captures performance, resource, and transaction data from a system of your interest. Using minimal system resources, the software continuously collects and summarizes performance data across your system and stores the collected data into the log file-based data store. If you want to use the HP Operations agent without HPOM, you can use the **extract** program provided with the HP Operations agent to extract the collected data. You can integrate the HP Operations agent with data analysis tools like HP Performance Manager or HP Reporter to analyze the data with the help of graphs and reports.

Introduction to System Performance Monitoring

The embedded data collector of the HP Operations agent collects hundreds of parameters from the monitored node that indicate the health of the system. The system parameters, or **metrics**, are then logged into HP Operations agent's data store.

Because the HP Operations agent can monitor systems with a wide range of operating systems, health indicating parameters of different operating systems can be dissimilar in appearance. To simplify the monitoring process, the HP Operations agent abstracts similar metrics collected from different operating systems by ordering and logging them with a common name.

Metrics

A metric is a measurement that defines a specific operational or performance characteristic of a system (or application). Operating systems (and applications) offer parameters that give an indication of the operational and performance characteristic of a system. The collection mechanism of the HP Operations agent collects these measurements and stores them into the log file-based data store for future use. Metric values can be numbers, boolean values, strings, and so on.

Metric Classes

To understand the characteristic of a particular system behavior or element, monitoring one metric is not sufficient. A set of related metrics gives you a complete, well-rounded picture of the performance of a system element. Such sets are represented in the agent's data store as **metric classes**.

A system runs with a combination of elements and components. Each component can exhibit a unique performance characteristic, and the aggregation of these characteristics represents the true status of the system. These system components, or **resources**, are the actual sources of data for the HP Operations agent's collector. For every resource, the HP Operations agent uses a unique metric class.

With every collection cycle, the HP Operations agent collects metric data from all the resources on the monitored system (you can configure the software to collect data only from select resources).

A system can have multiple resources of the same type. For example, server-grade systems are often equipped with multiple CPUs. The HP Operations agent collects the metric data from all the instances of a resource, and then logs the data into the data store under the metric class designated for the resource.

The HP Operations agent uses the following metric classes:

- **Process:** Includes the metrics related to all the processes running on the monitored system. Metrics of this class are prefixed with `PROC_`.
- **Application:** The HP Operations agent provides you with a mechanism to define applications that are actually collections of multiple processes that run on the monitored system. After you define them in the HP Operations agent configuration, the application class includes the metrics related to all the predefined applications running on the monitored system. Metrics of this class are prefixed with `APP_`.
- **Transaction:** Includes the metrics related to all the system transactions performed on the monitored system. Metrics of this class are prefixed with `TTBIN_` or `TT_`.
- **Disk:** Includes the metrics related to the disk of the monitored system. Metrics of this class are prefixed with `BYDSK_`.
- **Network interface:** Includes the metrics related to all the network interfaces available on the monitored system. Metrics of this class are prefixed with `BYNETIF_`.
- **CPU:** Includes the metrics related to all the CPUs available on the monitored system. Metrics of this class are prefixed with `BYCPU_`.
- **Core CPU:** Includes the metrics that indicate the per core values of a CPU on a hyper-threading enabled system. Metrics of this class are prefixed with `BYCORE_`.
- **File system:** Includes the metrics related to all the file systems available on the monitored system. Metrics of this class are prefixed with `FS_`.
- **Logical system:** You can install the HP Operations agent on a virtual system. This class of metrics includes all the metrics that indicate the performance of the logical elements (elements of the guest systems) of the host system. Metrics of this class are prefixed with `BYLS_`.
- **Logical volume:** Includes the metrics related to the logical volumes of the monitored system. Metrics of this class are prefixed with `LV_`.
- **Global:** The HP Operations agent collect data from all instances of a resource. For a multi-instance resource, the HP Operations agent aggregates the metric values of all the instances, and then logs the aggregated (average) value under the Global class. Metrics of this class are prefixed with `GBL_`.

HP Operations Agent in a Virtualization Environment

You can use the HP Operations Agent to monitor the health and performance of a virtual system, as well as the physical system that hosts the virtual system. The HP Operations agent supports the following virtualization technologies:

- **Complete virtualization**
  - HP Integrity Virtual Machines (Integrity VM)
  - Hyper-V
- **Paravirtualization**
  - VMware
  - AIX Logical Partitions (LPAR)
- **OS-level virtualization**
  - Solaris Zones
  - AIX Workload Partitions (WPAR)

HP Operations Agent in the Integrity VM Environment

The Integrity VM environment includes the following major components:

- VM Hosts
- Virtual machines (guests)

When you install the HP Operations agent on the VM Host, you can collect the following data:

- System-wide performance, application, transaction, and resource usage data
- Performance and resource usage data for individual virtual machines
- Performance and resource data for individual guest operating systems (logged with the BYLS metric class)

When you install the HP Operations agent on a virtual machine hosted on a VM Host, you can collect all the information that you can collect when the agent is installed on a physical system.

HP Operations Agent with Hyper-V

The Windows Hyper-V technology introduces the concept of the root and child partitions. You can create and manage different child partitions from the root partition. The child partitions host the virtual systems.

You can install the HP Operations agent on both the root and child partitions.

From the child partitions, the HP Operations agent can collect the following data:

- Utilization of resources by the monitored guest
- Type and role of the monitored guest (only for Windows guests)

From the root partition, the HP Operations agent can collect and present the details of different logical (guest) systems available on the Hyper-V system. The BYLS metric class lists all the guest-specific information collected from the root partition.

HP Operations Agent with ESX VMware

You can install the HP Operations agent on virtual systems hosted on the ESX server. On a virtual system (guest machines), the HP Operations agent enables you to collect the performance data of the system. With the HP Operations agent installed on vSphere Management Assistant (vMA) node, you can enable logging of the BYLS metric class. The metrics logged against the BYLS metric class indicate the resource utilization of virtual systems that are hosted on the ESX server.

Note: The HP Operations agent cannot be installed on the ESX service console.

While logging the physical resource utilization data for virtual systems against the BYLS metric class, the HP Operations agent logs the resource utilization data of the ESX Server under the same BYLS metric class.

HP Operations Agent with Solaris Zones

A virtualization environment on a Solaris (10 or higher) server is made up of the following components:

- **Global zone:** The default zone of the system, which also acts as the system-wide administration console.
- **Non-global zones:** Non-global zones are logical entities created on the Solaris system. A logical system is equivalent of a guest system.

You can install the HP Operations agent on both the global and non-global zones.

On the global zone, the HP Operations agent can log resource utilization data by individual zones against the BYLS metric class.

The HP Operations agent deems a non-global zone as a single, physical system and logs the data indicating health and performance of the zone.

HP Operations Agent in an Extended Virtualized Environment

The HP Operations agent supports the following virtualization technologies:

- HP Operations agent in a Kernel-based Virtual Machine
- HP Operations agent in Xen environment

In a KVM or Xen environment, you can install the HP Operations agent on the host systems. KVM is complete virtualization solution. You can create a host and guest machines in a virtual environment. Xen supports both full virtualization and para-virtualization technologies.

Performance collection component of the HP Operations agent uses libvirt for BYLS metric collection. On a node where KVM or Xen packages are available, the HP Operations agent uses the libvirt library in the host machines and collects the BYLS metrics of the guest machines. The BYLS metrics shows the resource utilization of the guest system.

Note: The libvirt warning and error messages are generated from the libvirt library. Memory metrics on KVM using libvirt version 0.8.0 show missing value or <*Not applicable*>.

Limitations:

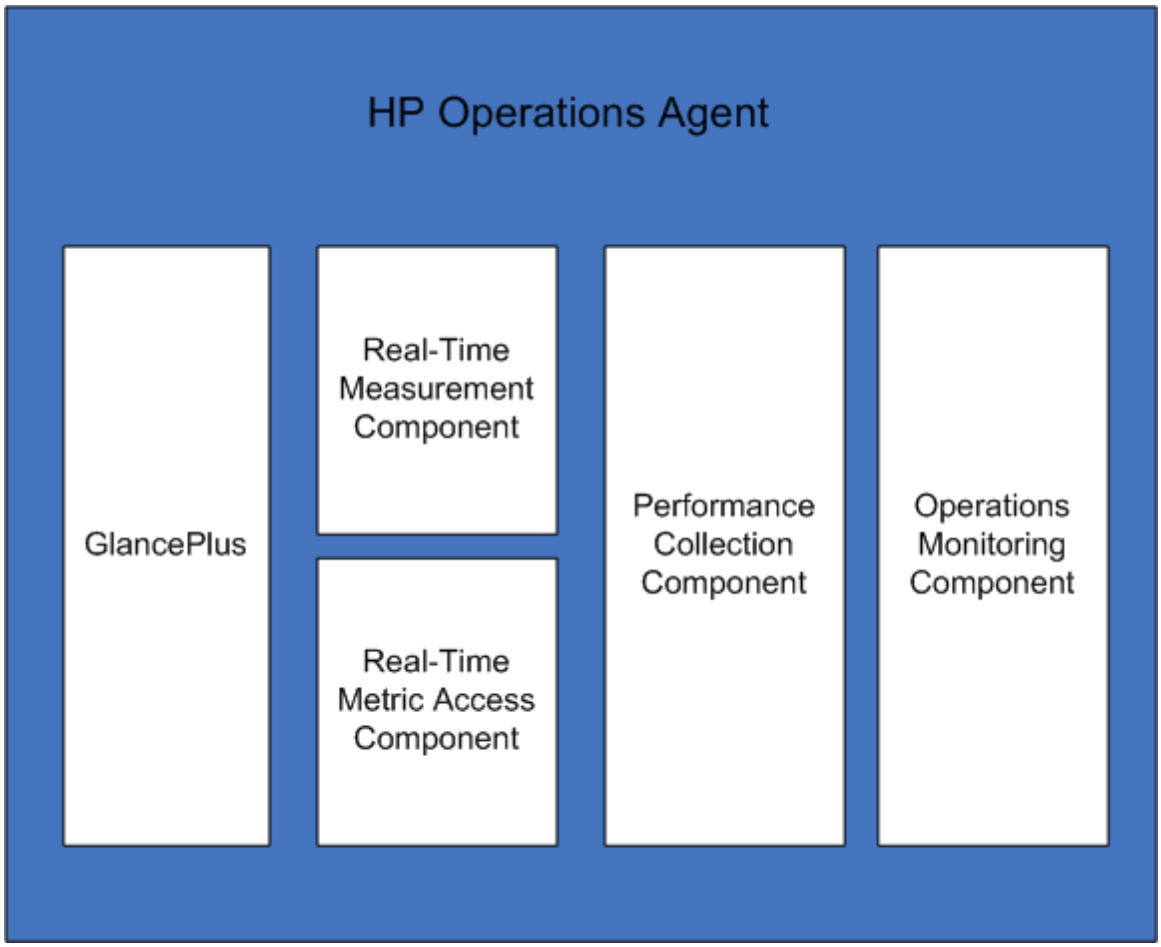
1. When the virtual machine is not in an active state, the BYLS_MEM_PHYS metric value is shown as <*Not applicable*>.
2. The BYLS_MEM_USED metric signifies the memory used by the guest system at the current interval, but the metric value displays the total memory of the virtual machine.
3. Warnings and error messages appear when you start XGlance and other utilities.Some of the messages are:
   - *Cannot find the CPU, memtune info for the guest XML config file*
   - *:libvir: error : no connection driver available for xen:///*

Chapter 4: Components of the HP Operations Agent

The HP Operations agent includes the following major operational components:

- Operations Monitoring Component
- Performance Collection Component
- Real-Time Measurement Component
- Real-Time Metric Access Component
- GlancePlus

Figure 6: Components of the HP Operations Agent



Introduction to the Operations Monitoring Component

You can use this component only if you use the HP Operations OS Inst Adv SW LTU and HP Ops OS Inst to Realtime Inst LTU.

The Operations Monitoring Component builds up the monitoring and messaging functionality of the HP Operations agent. With the Operations Monitoring Component, you can perform the following tasks:

- Monitor the data collected by data collectors against predefined thresholds
- Generate alert messages when the monitored metrics violate preset thresholds
- Forward the messages to the HPOM console

The Operations Monitoring Component of the HP Operations agent enables you to create a distributed monitoring environment that can be managed and controlled from the centralized HPOM console.

The Operations Monitoring Component consists of the following components:

Message Agent

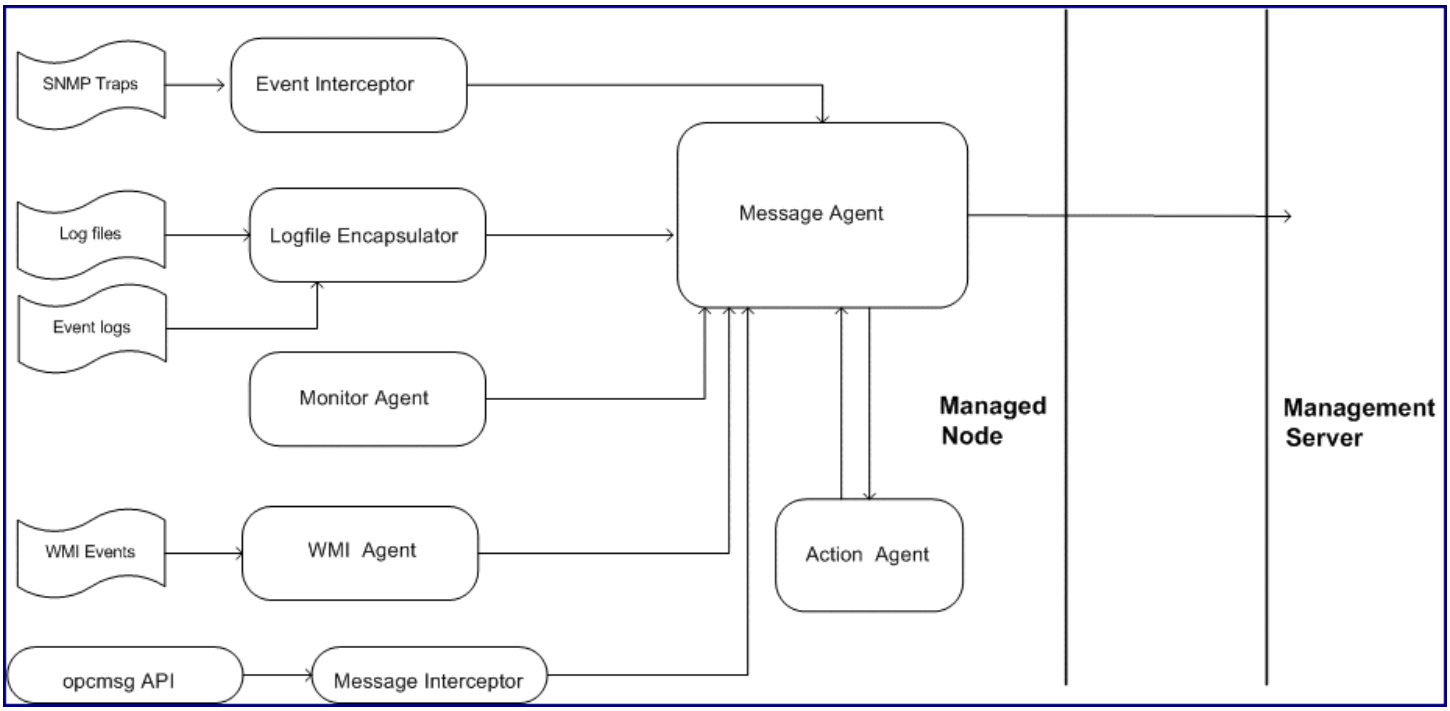
The **message agent** receives messages from different message sources such as the monitor agent, logfile encapsulator, and event interceptor to send appropriate alerts and notifications to the HPOM message browser. Messages, combined with additional attributes like the severity level, tell you the true nature of problems and incidents that occur on different managed nodes. Messages that arrive at the message agent can be associated with tasks. The message agent forwards the task details to the action agent when necessary. After completion of a task, the action agent can send annotation messages to the message agent.

The `opcmsg` utility can forward messages to the message agent through the message interceptor.

If the HP Operations agent fails to contact the HPOM management server, the message agent can buffer the messages on the local node until the connection is restored.

The message agent sends the messages to the primary server, which is your HP Operations Manager. In a scenario, where the primary server is down and the messages cannot be sent to the primary server, you can configure the message agent to send the messages to a backup server. You can configure one or more servers as the backup server. When the primary server is up and running again, the messages that were sent to the backup server(s) while the primary server was down are not synced. For more information, see the *HP Operations Agent User Guide*.

Figure 7: Workflow of the Message Agent



Message Stream Interface

The **message stream interface** component, available with the message agent, provides the capability to extend the message forwarding process of the HP Operations agent. You can configure the HP Operations agent to forward the messages to an external application with the help of the message stream interface component.

Message Interceptor

The **message interceptor** component performs additional processing tasks on the messages that arrive from the `opcmsg` utility and different APIs. Based on the configuration details set in the message interceptor policies available on the managed node, the message interceptor can take the following actions:

- Filter messages
- Discard the message
- Forward the message to the HPOM console

Monitor Agent

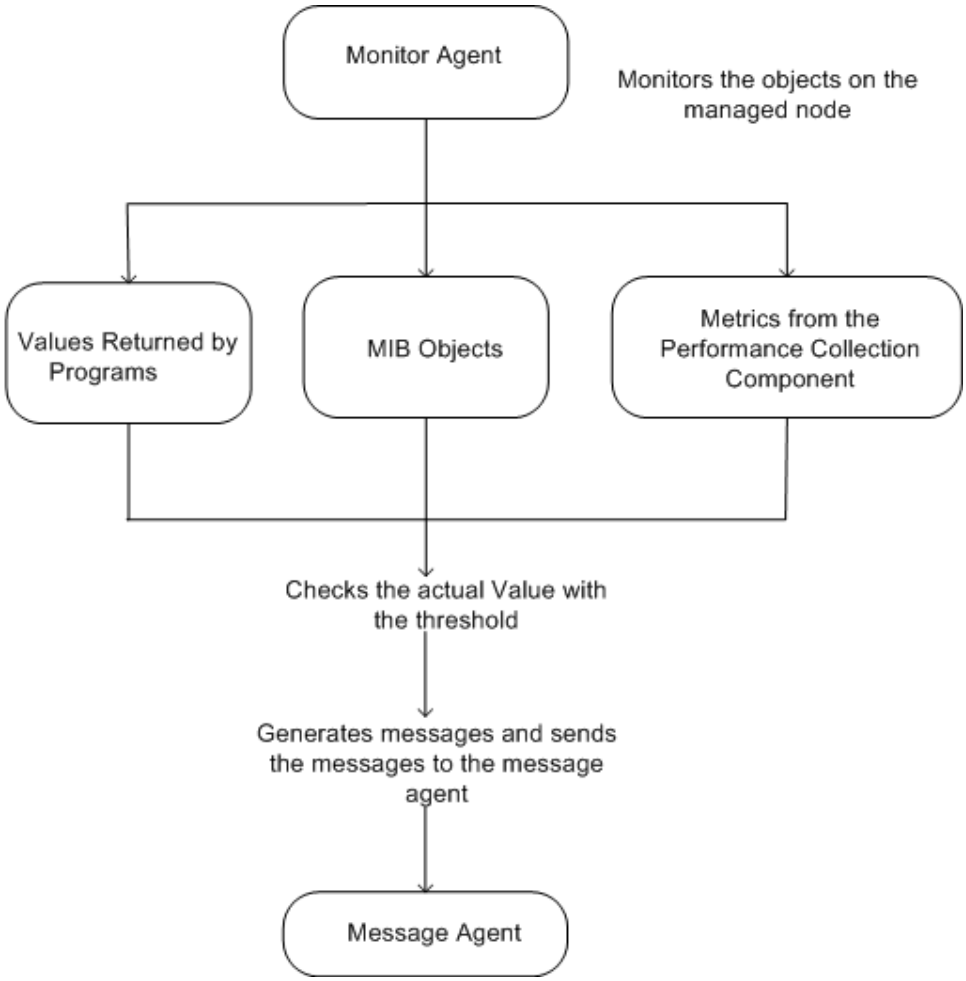
At regular intervals, the monitor agent evaluates the data obtained from different sources (**monitored objects**) against predefined thresholds and sends appropriate messages to the message agent in the event of threshold violation. Based on its configuration, the monitor agent monitors the following objects:

- System parameters (for example, CPU load, disk utilization, kernel parameters)
- MIB objects
- WMI events
- Application-specific parameters

The monitor agent uses the following mechanisms to monitor different objects:

- Monitoring with programs
  The monitor agent can run programs or scripts available on the node. You can create scripts to read the value of a monitored object on the node and send the value to the monitor agent by using the `opcmon` API. The monitor agent then compares the obtained value with the set threshold and sends messages to the message agent in the event of threshold violation. In addition, the agent checks the exit values of the script and sends a message to the message agent when the script does not run successfully.
- Monitoring MIB objects
  The monitor agent can monitor the available MIB objects on remote nodes. MIB objects are primarily SNMP traps originating from different devices or management stations. The agent compares the values returned by the monitored MIB object against a set threshold and sends messages to the message agent in the event of threshold violation.
- Monitoring WMI events
  The monitor agent can collect WMI events from the WMI database of a remote node and generate alert messages in the event of threshold violation.

Figure 8: Workflow of the Monitor Agent



In an HPOM environment, the monitor agent obtains threshold information from HPOM policies available on the managed node. The monitor agent compares the value collected from a monitored

object with the predefined threshold. If a violation of the threshold occurs, the monitor agent sends an alert message to the message agent. The HPOM policies provide the monitor agent with the display text and severity level (Critical, Major, Minor, Warning, or Normal) of the alert message.

In the event of an unexpected interruption or abrupt failure, the monitor agent can preserve the most recent value of the monitored object—a value that was collected during the last collection interval before the monitor agent stopped functioning. The interruption can occur in the form of an accidental restart of the agent, agent failure, or deactivation of a measurement threshold policy on the node. As a result, after resuming its operation, the monitor agent analyzes the current state of the monitored object with the preserved value before it starts the comparison with the threshold value. Based on the analysis, the monitor agent then instructs the message agent to send appropriate messages to the HPOM console.

Action Agent

The **action agent** enables you to start and stop different tasks on a managed node. The action agent receives instructions from the management server or the message agent, and then starts an action on the local node.

The action agent can perform the following types of actions:

- Running scripts and programs
- Starting an application
- Stopping an application

Logfile Encapsulator

The **logfile encapsulator** component can analyze different log files, which are generated by the operating system or an application running on the node. Based on the information available with the Logfile Entry policies available on the node, the logfile encapsulator scans the available log files for specific messages or patterns. When the message string or pattern is matched, the logfile encapsulator sends the message to the message agent, which sends appropriate notifications to the HPOM message browser.

If the message string or pattern of an event with a future timestamp is matched, the message agent sends notifications to the message browser for the same event every time the logfile encapsulator is restarted.

Event Interceptor

The **event interceptor** intercepts the SNMP traps generated on a node or from an application. The event interceptor uses the following workflow while operating on the node:

- Intercepts events generated from the local node or a remote system.
- Integrates or suppresses the events based on the conditions set by policies available on the node.
- Triggers the message agent to send the SNMP trap to the HPOM message browser

You can configure the event interceptor to forward the collected SNMP traps to multiple remote SNMP trap listeners.

When appropriate, the event interceptor generates messages and sends the messages to the message agent. The generated messages may then be passed through the correlation policies, along with messages generated by other sources, such as log files.

WMI Interceptor

The **WMI interceptor** enables you to communicate with remote nodes (or the local node) using the Windows Management Instrumentation (WMI). With the Windows Management Interface type of policies, you can instruct the HP Operations agent to monitor WMI classes and instances available locally or on a remote system. Based on the conditions set in the policy, the WMI interceptor can generate appropriate messages or initiate actions.

Event Correlation Agent

The **event correlation agent** works in conjunction with the message stream interceptor to process the generated messages based on the specifications in the available event correlation service (ECS) policies. Based on the processing, the event correlation agent can suppress a message, modify a message before sending to the HPOM message browser, or can generate a new message. The event correlation agent uses the following workflow while processing messages on the node:

1. Messages arrive at the message agent from the monitor agent, logfile encapsulator, and trap interceptor.
2. The message agent forwards the messages to the message stream interface, which in turn, forwards them to the event correlation agent.
3. The event correlation agent processes the messages based on the specifications in the ECS policy, and then takes one of the following actions:
   - Suppresses messages
   - Forwards necessary messages to the HPOM message browser
   - Generates a new message

Opsec

Opsec is the new event correlation agent that works in conjunction with the message stream interceptor to process the generated messages forwarded by the message agent. Opsec has an embedded script engine; it offers correlation capability revealing the message attributes and operations via the script based interface. Multiple correlation policies can be defined using scripts. Based on the correlation policy types, Opsec can perform a number of actions like modify a message, suppress a message, generate a new message before sending to the HPOM message browser.

Opsec uses the following workflow while processing messages on the node:

1. Messages arrive at the message agent.
2. The message agent forwards the messages to the message stream interface, which in turn, forwards them to Opsec.
3. Opsec processes the messages and then takes a number of actions based on the correlation policy types. The supported correlation types are as follows:
   - Message Storm
   - Transient
   - Enhance
   - Rate

- Multisource
- Suppress

For more information on the working of Opsec correlation types, see HP Operations agent 11.30 User Guide.

Discovery Agent

The **discovery agent** helps the HP Operations agent gather the details of the services running on the managed node and store the collected details into the local data store. With every discovery cycle, the discovery agent synchronizes the information present into the local data store with the repository on the management server. The discovery agent component is enabled by deploying the service discovery policies on the node, which include the specifications to discover and monitor different application- and system-specific services.

Performance Collection Component

You can use this component only if you use the HP Operations OS Inst Adv SW LTU, Glance Pak Software LTU, HP Operations OS Inst Perf SW LTU, and HP Ops OS Inst to Realtime Inst LTU.

At the core of the HP Operations agent is the Performance Collection Component, which helps you collect performance metrics from the node and store the collected information into the log file-based data store.

The data collector component—scope—helps you collect system performance metrics at regular intervals. You can configure the types of data collected by scope, as well as the collection interval. The *performance alarm* feature of the Performance Collection Component enables you to generate events based on predefined conditions.

Scope

The **scope** component is a data collection utility used by the Performance Collection Component of the HP Operations agent. The scope collector gathers and summarizes a large set of system performance metrics, which present a wide view of the health and performance of the system. Scope stores the collected information into different log files, which are available on the system for analysis and use with tools like HP Performance Manager and HP Reporter.

The scope component captures the following types of information:

- System-wide resource utilization information
- Process data
- Performance data for different devices
- Transaction data
- Logical systems data

The scope collector runs as a daemon on UNIX and Linux nodes and as a service on Windows nodes.

Collection Parameters File

The Collection Parameters file or the `parm` file contains instructions for the scope component to collect specific types of data and defines the data collection interval. This is an ASCII file that you can use to customize the default data collection mechanism. You can modify the `parm` file according to your performance data collection requirement.

After startup, the scope component searches for the `parm` file. If the `parm` file does not exist on the system, scope starts functioning with the default configuration.

The `parm` file specifies the following details for use with the scope component:

- The maximum amount of disk space for the scope log files
- The data types of the items to be logged
- The data collection interval
- Attributes of processes and metrics to be logged
- User-defined applications that should be monitored
- Instructions for daily log file maintenance activities

If you use the HP Operations agent with the HPOM management server, you can modify and deploy the `parm` file centrally from the management server to all managed nodes.

Performance Alarms

The Performance Collection Component of the HP Operations agent can perform actions based on the system performance data collected by the scope collector from the local system. These actions can be alerts sent to the HPOM console, actions performed on the local system, or messages sent to stdout. In addition, the Performance Collection Component can send SNMP traps for every alarm to SNMP trap listeners. The following major components build up the alarm generation mechanism of the Performance Collection Component:

- "Alarm Definitions File" below
- "Alarm Generator" on the next page

Alarm Definitions File

The alarm definition file (`alarmdef`) provides the Performance Collection Component with the default specification for the alarm generation process. You can modify the `alarmdef` file to configure the following parameters:

- Alarm conditions
- Alert messages
- Severity of the alert message
- Operating system commands against specific events

Based on the configuration information available in the `alarmdef` file, the Performance Collection Component generates alarms that notify you about the state of the monitored system.

Alarm Generator

The alarm generator component of the Performance Collection Component processes the `alarmdef` file and the available system performance data on the local system, and then generates alarms if necessary. The alarm generator consists of the following components:

- Alarm generator server (`perfalarm`)
- Alarm generator database (`agdb`)

The alarm generator server scans the information in the `alarmdef` file and sends alerts to the destinations based on the configuration information in the `alarmdef` file. The `agdb` database includes the list of target systems for the `perfalarm` component to forward SNMP traps against specific events. You can modify the default behavior of the `perfalarm` component and access the available data in the `agdb` database with the help of the `agsysdb` utility.

Data Store

The log file-based data store of the Performance Collection Component enables you to store the collected data in log files. You can configure the data retention period based on your requirement. The *archive* feature enables you to archive old data, which can later be extracted for analysis.

The HP Operations agent organizes the stored data in different log files. Based on the metric class, the HP Operations agent stores data in different log files assigned for different metric classes.

- **logglob:** Stores the data for the `GLOBAL` metric class.
- **logappl:** Stores the data for the `APP` metric class.
- **logproc:** Stores the data for the `PROC` metric class.
- **logdev:** Stores all the device-related data (includes the data collected for the `BYDISK`, `FS`, `BYCPU`, and `BYNETIF` metric classes).
- **logtran:** Stores the data for the `TT` metric class.
- **logls:** Stores the data for the `BYLS` metric class.

In addition, if you use SPIs to collect data from business applications, the HP Operations agent creates new log files with the help of Data Source Integrator (DSI) feature. SPIs add new log files and metric classes to the existing set.

Migration to the New Log File-Based Data Store

The HP Operations agent traditionally used the light-weight database, the **embedded performance component** (**EPC**)—also known as **coda**, to store the data collected from the system. This version of the HP Operations agent stores the system performance data into different log files. Despite the change in the data storing mechanism, data collection and threshold comparison process through policies and data analysis process with HP Performance Manager and HP Reporter continue without interruptions even after upgrading to the HP Operations agent 11.16 from an old version of the HP Operations agent.

Although the HP Operations agent 11.16 does not use EPC as the data store, any references to EPC as the data source in policies are directed to the new log file-based data store. Therefore, old policies, which were deployed on the node before the agent HP Operations agent 11.16 was installed on the node, continue to work with the agent 11.16 without failure.

Similarly, you can continue with the existing settings in HP Reporter and HP Performance Manager after upgrading the nodes to the HP Operations agent 11.16.

EPC as the Data Store

Although the data collection capabilities of the EPC are not available with this version of the agent, you can continue to use the data store of the EPC to store the data collected by custom collectors (collectors introduced by SPIs). A SPI may log the collected data into the log file-based data store by default. On the agent HP Operations agent 11.16 node, you can configure a SPI to log data into the data store of your choice (EPC or log file-based data store).

For information on the default data logging behavior of the SPI and instructions to modify the default data logging behavior, see the SPI documentation.

GlancePlus

You can use this component only if you use the Glance Pak Software LTU and Glance Software LTU. This component is available only on UNIX nodes.

HP GlancePlus is a powerful online real-time system performance monitoring and diagnostic tool. The GlancePlus tool provides metrics for system resources, processes, and applications data. It also enables you to identify and troubleshoot system performance problems as they occur on the local or a remote system.

GlancePlus provides an option to drill down to the root of a problem and enables you to visualize the problems that occurred on the system. For example, if the CPU utilization is found to be above the threshold value for a long period of time, you can look at a list of all the applications running, and then identify the process with the highest CPU utilization from the process list. Furthermore, you can see the threads associated with the particular process and drill down to the actual thread that consumes the most amount of the CPU resource.

Real-Time Metric Access

You can use this component only if you use the HP Ops OS Inst to Realtime Inst LTU, Glance Pak Software LTU, or Glance Software LTU.

The Real-Time Metric Access (RTMA) component provides you with real-time access to system performance metrics, locally or remotely. The central module of the RTMA component— the performance daemon (**perfd**)—starts by default when you start the HP Operations agent and facilitates accessing system performance metrics on a real-time basis. From a central HP Operations agent node, you can monitor the real-time performance metrics of other nodes where the RTMA component is available.

Real-Time Measurement Component

You can use this component only if you use the HP Ops OS Inst to Realtime Inst LTU.

The Real-Time Measurement (RTM) component helps you access real-time performance metrics over a secure communication channel. In the absence of this component, you can use the RTMA component only using TCP/IP. When you enable the RTM component, you can use the secure HTTPS mode of communication while communicating with different nodes using the RTMA component.

Chapter 5: Integration with Other HP Software Products

You can integrate HP Operations agent with other HP Software products to view and analyze the data collected by the HP Operations agent or the data stored into HP Operations agent's data store.

HPOM

The Operations Monitoring Component of the HP Operations agent provides you with the ability to integrate an agent node with the HPOM management server to create a distributed monitoring environment. If you install the HP Operations agent remotely from the HPOM console, the agent node is automatically configured to be integrated with HPOM. If you manually install the HP Operations agent, the installer script provides you with the options to configure the node to work with an HPOM management server. For more information, see *HP Operations Agent Installation Guide*.

HP Reporter

HP Reporter can create detailed reports in multiple formats from the data collected by the HP Operations agent. HP Reporter uses the *discovery* technique to identify systems where the HP Operations agent is installed, and then starts gathering the data from the agent's data store to construct reports. For information on the operation and the discovery feature of HP Reporter, see the *HP Reporter Concepts Guide*.

HP Performance Manager

You can use HP Performance Manager to view and analyze the data available with the data store of the HP Operations agent in the form of graphs and charts. HP Performance Manager can gather the historical data available with the persistent data store of the HP Operations agent and build graphs and trend analysis reports to simplify the task of data analysis.

HP Performance Manager with the Real-Time Measurement Component

If you purchase the additional license for the **Real-Time Measurement** (**RTM**) component of the HP Operations agent and if you use the **Diagnostic View** feature of HP Performance Manager 9.00, you can monitor real-time metric data (along with the historical data) gathered from different nodes. The **perfd** process on the node captures a rich set of system performance metrics on a real-time basis. The

RTM component enables you to establish a secure communication channel to the HP Performance Manager server. With the help of the communication channel set up by RTM, HP Performance Manager collects the real-time metric data collected by perfd on the node. With this data, HP Performance Manager creates graphs, charts, and reports that help you analyze performance bottlenecks in your environment and provides you the capability to drill down to the real-time system data for every monitored system. The Diagnostic View tab of the HP Performance Manager console presents a rich graphical interface to design and build graphs with real-time metrics collected from multiple nodes.

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 Concepts Guide (Operations Agent 11.16)

Just add your feedback to the email and click send.

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

We appreciate your feedback!