Hewlett Packard
Enterprise

HPE Agentless Management and the transition from OS-based agents

Technical white paper

Contents

Introduction 3
Server monitoring with OS-based agents 3
HPE Agentless Management 3
Agentless Management in ProLiant servers 4
HPE Agentless Management Architecture 5
Agentless Management Service 6
Implementing Agentless Management 8
iLO Configuration for Agentless Management 8
HPE RESTful API and Interface Tool 13
Agentless Management user environments 14
Management with HPE OneView 14
Management with HPE SIM 15
Management with HPE Insight Remote Support 16
Using Agentless Management with other management applications 16
HPE ProLiant Agentless Management extensions for Nagios 17
When to use OS-based management agents 17
Monitoring performance 17
Monitoring storage networks 17
Other reasons to install OS-based agents 17
Firmware and driver maintenance with HPE Intelligent Provisioning 18
Required firmware for Agentless Management 18
Hardware compatibility 18
Summary 18
Resources 20

Introduction

This document is useful as an initial guide to better understand the advantages of Hewlett Packard Enterprise (HPE) Agentless Management over traditional OS-based agents. The document includes sections on how Agentless Management works with HPE Systems Insight Manager (HPE SIM), HPE OneView, and other management applications that traditionally work with OS-based instrumentation.

Server monitoring with OS-based agents

Before the introduction of HPE Agentless Management, management consoles traditionally relied on OS-based Simple Network Management Protocol (SNMP) agents and Web-Based Enterprise Management (WBEM) Windows management instrumentation[1] (WMI) providers to manage and monitor host systems. Figure 1 provides a visual overview of the traditional OS-based management model.

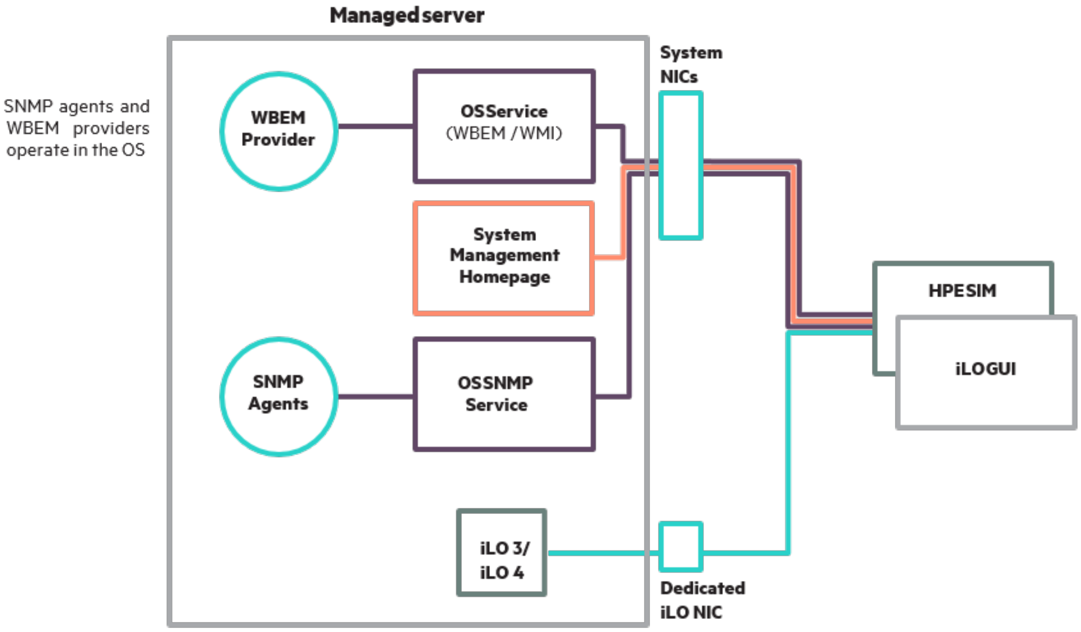


Figure 1. Traditional OS-based management model

In this traditional model, agent management software runs on the OS. This OS-based agent software plugs into the appropriate service to provide SNMP, WMI, or WBEM capabilities in the OS. The software collects server-specific, OS-specific, and industry-standard data. The agent bundles the data and makes it available to applications running on the managed server itself or remote applications.

HPE Agentless Management

HPE Agentless Management is an evolving architecture in which the hardware management capabilities run on the iLO hardware, independent of the host OS and processor. With HPE Agentless Management, health monitoring and alerting begin working the moment you supply power to the server. Agentless Management allows HPE ProLiant servers to collect and deliver hardware and other server management information to management consoles such as HPE OneView, HPE SIM, and HPE Insight Control without requiring the installation of traditional agents or

[1] WMI is the Microsoft implementation of Web-based Enterprise Management (WBEM), a set of industry-standard technologies for accessing system information in a distributed management environment.

providers on the host OS. With the Agentless Management solution, the SNMP management software operates within the iLO firmware instead of the host OS. This frees memory and processor resources on the server for use by the OS and server applications. Another advantage with Agentless Management is that in addition to monitoring all key internal subsystems (such as thermal, power, and memory), iLO sends SNMP management notifications directly to management consoles (such as HPE SIM), even with no host OS installed. Agentless Management not only simplifies agent management regardless of the host OS, but also provides an iLO-dedicated management network[2], isolated from the regular data network.

Agentless Management in ProLiant servers

The Agentless Management model was first introduced in HPE ProLiant Generation 8 (Gen8) servers featuring the iLO 4 management processor. HPE Agentless Management includes the traditional remote management and control capabilities delivered with the iLO 4 management processor, and the optional HPE Agentless Management Service (AMS). You will read more about AMS in the self-named section later in this paper.

Agentless Management, part of the iLO 4 firmware, can monitor the health of server and server components and supply this information directly to HPE OneView or to HPE SIM, including SNMP traps and Redfish notifications (see the Redfish section of this document for more information). You can use Agentless Management with HPE OneView or HPE SIM, as well as other data center infrastructure management (DCIM) application (such as Nagios), without installing the SNMP agents. HPE iLO 4 and Agentless Management are components of the HPE ProActive Insight architecture and integrated lifecycle automation built into HPE ProLiant Gen8 and Generation 9 (Gen9) servers. The benefits of this architecture and lifecycle automation include:

- Moving the SNMP Master from the Operating System to the iLO. This provides a secure management firewall between server management operations/data and customer operations/data. The customer application is no longer subject to potential security risks that sometimes appear in OS-based management stacks.
- The iLO processor is able to provide direct query and alerting through SNMP for CPUs, hard drives connected to HPE Smart Array, HPE SmartStorage Battery, SmartStorage Cache, fans, power, memory, and temperature. If you have installed the optional AMS, the iLO processor will report status and can alert for direct attached storage devices, legacy network, and Fibre Channel (FC) HBA adapters.
- Agentless Management on ProLiant Gen8 servers includes SNMPv3 and Internet Protocol version 4 (IPV4), and on ProLiant Gen9 servers includes SNMPv3 and IPv6 protocol compatibility with the iLO SNMP stack. SNMPv3 compatibility provides security missing in SNMP v1.
- An intelligent asynchronous device (iLO 4) on the physical server providing a single network target to monitor and manage the device
- A consistent GUI for configuration, regardless of the host OS
- Monitoring and management capabilities even when the OS is not up and running (monitoring of bare-metal servers)
- The ability to monitor the health of the server out-off-band, which is essential is cloud environments where tenants usually don’t want to include agents in their application stack.
- The capability to segregate the management network from the data network using the dedicated iLO Network port for out-of-band communication, for increased security and stability
- The option for the management network and the data network to be physically the same by using the “shared” system networking port capability on all HPE ProLiant servers, giving you a choice for configuration
- A reduced qualification matrix for system setup allows the elimination of agents.

To learn more about HPE OneView for Microsoft System Center, go to hpe.com/products/ovsc. User documentation for HPE OneView for Microsoft System Center can be found at hp.com/go/ovsc/docs.

You can find information on HPE OneView for VMware vCenter^{TM} at hpe.com/info/ovvcenter.

[2] Agentless Management is also included on the iLO Shared Network Port

HPE Agentless Management Architecture

The iLO Management processor includes the core instrumentation logic to monitor hardware and the embedded Agentless Management with its SNMP stack (Figure 2).

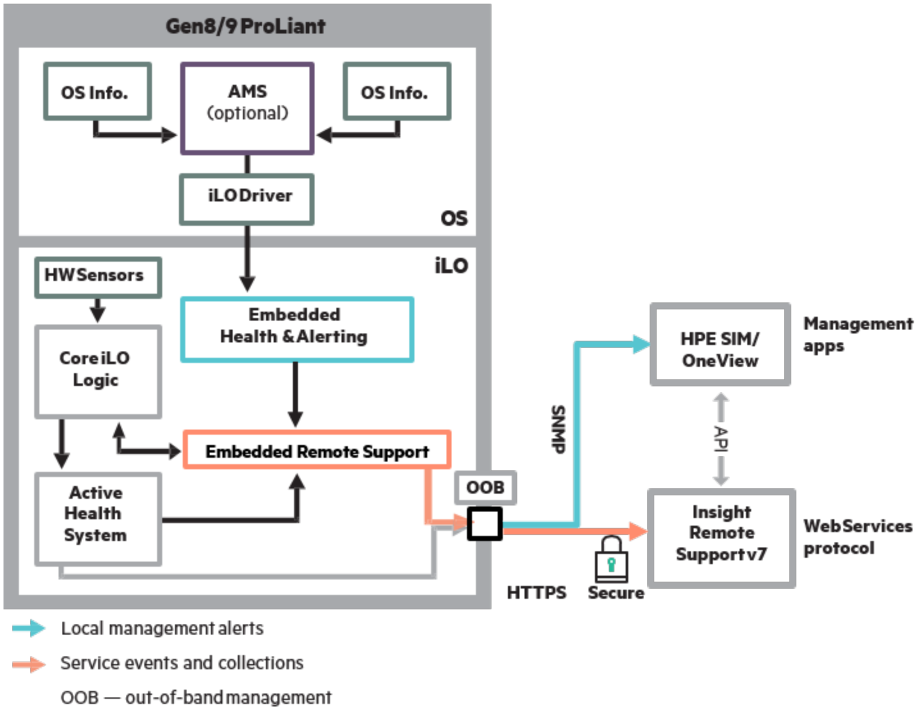


Figure 2. ProLiant Gen8/Gen9 Agentless management architecture

Agentless Management depends upon these underlying capabilities of iLO 4:

- Core embedded health firmware – The firmware monitors core platform hardware such as temperature sensors, power supplies, fans, memory, CPUs, and Smart Array storage. The iLO firmware has incorporated discovery and "health monitoring" of critical platform components since ProLiant G5 servers. The improved iLO 4 management processor provides a platform for new capabilities such as autonomous Agentless Management. iLO 4 adds new capabilities such as providing details about Smart Array subsystems and reporting firmware revisions.

- Embedded SNMP stack that resides in iLO 4 rather than in the host OS - This eliminates the need for the host CPU to use its processing cycles on SNMP management. It also increases security and stability because SNMP is embedded within iLO 4 rather than having SNMP loaded onto the host CPU.

- Out-of-band, dedicated iLO 4 NIC - This iLO 4 NIC sends SNMP traps directly to management applications such as HPE SIM, without affecting system performance. You can configure iLO 4 to use a shared network port on the server if you want to reduce the number of cables coming from your server. Some ProLiant servers have only shared port capability. HPE Agentless Management is included on these servers as well.

- RESTful API – Agentless Management communicates with the HPE RESTful API and the HPE Software Defined Compute Architecture to make Agentless Management status and data available, The Restful API provides a common interface for server configuration, provisioning, and monitoring. You can read more in the HPE RESTful API and Interface Tool section of this document.

- Redfish API – This is a new industry standard specification using a REST-based 'web' framework to define a modern remote API and data model for datacenter hardware management. The Redfish API also improves server monitoring capabilities.

- The inclusion of Agentless Management Service – AMS is optional, but it is part of the default configuration. AMS is important if you want to know OS-specific details such as the IP address of host-based NICs (version 4 or 6), or the OS name. AMS can also provide hardware data about devices such as SAS/SATA controllers and drives, and FC controllers, which do not have the ability to communicate with the iLO and cannot be monitored by the iLO directly. AMS also reports on Non-Volatile Memory Express (NVMe). AMS also enables iLO 4 to log events into the host operating systems' native event log (Windows NT Event Log, local Syslog). You will find detailed AMS information in the following Agentless Management Service section. AMS is not an agent and does not communicate through the network. Instead, it uses the iLO Management Controller (CHIF) driver to communicate with the iLO through the PCIe bus.

Note
HPE SIM has a dependency on AMS for Inventory collection and mandates that you install AMS for this capability.

Agentless Management also enables a "broadcast" SNMP (iLO-configurable) "Cold Start" TRAP for iLO and server resets. This feature allows Central Management Services (CMS) to quickly discover new devices or changes in existing devices. This technique is standard and will work for HPE OneView, HPE SIM, HPE Insight Control, and other SNMP-based CMS applications.

For HPE Gen 8 and Gen 9 servers, the iLO works very closely with the HPE power supplies and the HPE Intelligent PDU to monitor not only server power redundancy but also data center redundancy. HPE provides an advanced industry solution that allows large data center operations and administration (for power and cooling) to be separated from server management. This is a growing trend in cloud infrastructure and computing.

Agentless Management Service

The AMS is optional, and is not an agent. The AMS is a small "helper application" for Agentless Management that is loaded into the OS and routes the OS management information and alerting to the iLO processor, enabling this information to be processed by the iLO and routed over the management network. HPE SIM mandates that AMS is installed for management of ProLiant Gen8 and later servers in Agentless Management mode to provide additional information discovery. The AMS also provides additional information to HPE Active Health. AMS provides a wider range of server information (OS type and version, installed applications, IP addresses for example) allowing users to complement hardware management with OS information and alerting.

The AMS delivers more information about the server and the OS than Agentless Management alone. The AMS provides OS-specific detail that includes:

- The OS Host Name (if desired for TRAPs over the iLO sysName)
- Operating system and version
- Information about NIC teams and NIC bridges on Windows and Linux systems
- Information about installed applications
- Running processes and network IP addresses. Since the operating system owns the DHCP client, only the operating system knows the IP address.
- Drivers and firmware versions of installed NIC, Fibre Channel over Ethernet (FCoE), and SAS/SATA HBA devices
- Information about direct-attach disk drives (chipset-attached, not using an HPE Smart Array Controller or Smart HBA)

The AMS leverages the mature iLO technology for transferring data between host (or OS) memory and the iLO processor. This technology is based on industry standard PCI Express (PCIe) memory bus mastering used by other PCIe controllers such as network and storage adapters. This technology spans generations of iLO management processors and is very reliable. There is no need to enable any management protocol on the operating system if only Agentless Management via SNMP is desired.

It is important to know that AMS is a service that does not require configuration or network communications. So you don't need to open network ports for AMS to work.

One of the functional differences of Agentless Management on ProLiant Gen9 servers is that there is less dependence on AMS. Agentless data now visible through the iLO GUI includes:

- Health status and serial number for external storage attached to HPE Smart Array controllers
- Health status, model, serial number, and firmware version for storage attached to HPE Smart Array controllers

- Status of Smart Storage batteries providing model, serial number, and capacity
- Smart Cache health status information is displayed on the iLO 4 interface storage page as "logical drive"

Table 1 provides a more detailed comparison between the available capabilities provided by HPE Insight Management agents (traditional OS-based agents), iLO 4 (Agentless Management is part of iLO 4), and iLO 4 with AMS.

Table 1. Comparison of OS-based agents and Agentless Management

FEATURE	HPE INSIGHT MANAGEMENT AGENTS	ILO 4	ILO 4 +AMS
SERVER HEALTH	• Fans • Temps • Power supplies • Memory • CPU	• Fans • Temps • Power supplies • Memory • CPU • ProLiant Gen9 only: Smart Storage battery monitoring	• Fans • Temps • Power supplies • Memory • CPU • ProLiant Gen9 only: Smart Storage battery monitoring
STORAGE	• SmartArray ALL DASD • SAS/SATA HBA/RAID • Fibre channel / iSCSI • SMART drive monitoring (connected to Smart Array and SAS HBA) • Tape • External storage	• SmartArray • SMART Drive Monitoring (connected to Smart Array) • Internal and external drives connected to Smart Array • SmartArray attached external storage • ProLiant Gen9 HPE Branded HBA storage • Smart Storage Battery • Smart Cache • Device Inventory • Firmware Inventory	• SmartArray • SAS/SATA HBA2 • SMART Drive Monitoring (connected to Smart Array and SAS HBA) • Internal and external drives connected to Smart Array • Fibre Channel / HBA status
NIC	• MAC and IP addresses for standup and embedded NICs • Teaming information • Link up/link down traps • VLAN information	• MAC addresses for embedded NICs • Physical link connectivity for NICs that have NC-SI over MCTP	• MAC and IP address for standup and embedded NICs • NIC Link up/link down traps • FC link up/down and other FC traps • NIC bridging • NIC teaming information[1]
OTHER	• OS information (host SNMP MIB) • iLO data • Performance data • User-configurable thresholds • Logging events to OS logs • Clustering data	• iLO data • Firmware inventory • Device inventory	• iLO data • OS information (host SNMP MIB) • Logging events to OS logs[2]
Pre-Failure warranty alerts	• Memory • Drives (physical and logical)	• Memory • Drives (physical and logical)	• Memory • Drives (physical and logical)[3]

[1] Only compatible with Linux® and Windows - not with VMWare.

[2] iLO 4 1.10 and later includes Smart Array logging. Note that some IML events are logged during OS run-time.

[3] iLO and Agentless Management monitor drives associated with SmartArray/HBAs, while Agentless Management with AMS also monitors SAS/SATA drives.

Note

- ProLiant Gen8 and Gen9, Agentless Management also incorporates SNMPv3 and IPv6.
- With iLO 4 v2.40 and later, AMS-based OS logging is enabled for MS Windows, Linux (var/message/log), Solaris, and VMware vSphere® (logs are written to /var/log/syslog).

Implementing Agentless Management

With iLO 3 and earlier, SNMP management used the HPE Insight Management Agents running on the server operating system. With iLO 4, you can use either Agentless Management or the OS-based Insight Management Agents. The default iLO configuration uses Agentless Management. There are no additional requirements for implementing Agentless Management instead of OS-based agents.

The examples in this section are not intended to provide guidance for specific implementations, but rather an indication of the ease with which Agentless Management can be implemented and utilized.

iLO Configuration for Agentless Management

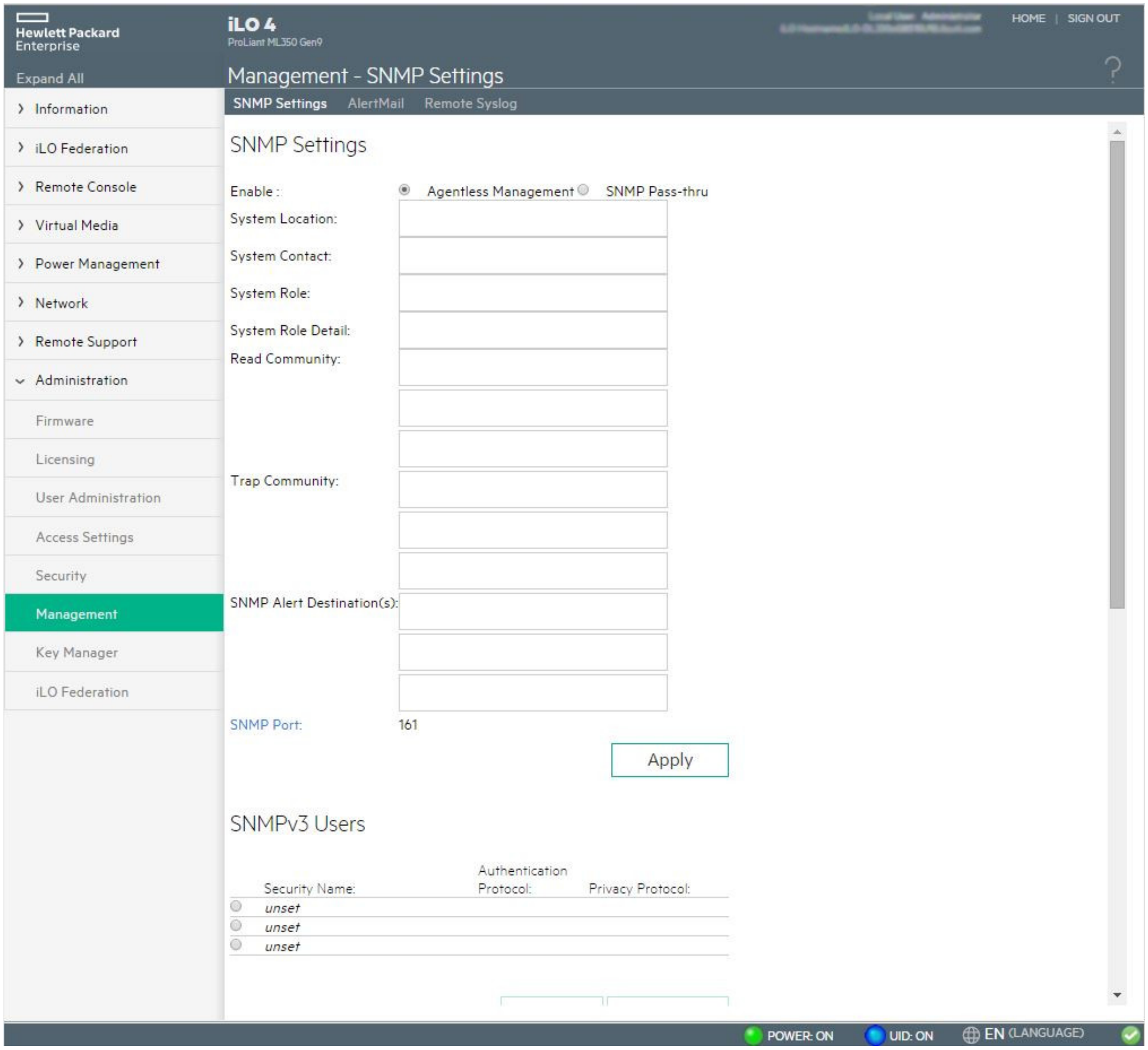
The default iLO configuration uses Agentless Management without any agent software running on the OS. While the optional AMS does run on the OS, it does so without an upper level interface for SNMP or WBEM. This is preferable to full agents because it is just a service that gathers information that iLO cannot and sends it to the iLO processor.

iLO 4 Agentless Management uses out-of-band communication for increased security and stability. With Agentless Management, health monitoring and alerting is built into the system and begins working the moment a power cord is connected to the server. This feature runs on the iLO hardware, independent of the operating system and processor. You can install the optional AMS to collect additional data.

Configuring SNMP settings

The **Management – SNMP Settings** page allows you to configure the iLO settings for SNMP, SNMP alerts, and Insight Manager integration. You must have the **Configure iLO Settings** privilege to change these settings.

Navigate to the **Administration→Management** page and click the SNMP Settings tab, as shown below in Figure 3.



SNMP Settings

Enable : ● Agentless Management ○ SNMP Pass-thru

System Location:

System Contact:

System Role:

System Role Detail:

Read Community:

Trap Community:

SNMP Alert Destination(s):

SNMP Port: 161

SNMPv3 Users

	Security Name:	Authentication Protocol:	Privacy Protocol:
○	*unset*		
○	*unset*		
○	*unset*		

Figure 3.

Note

While Agentless Management can be used with SNMP alerts, it is not compatible with SNMP SET. This means an environment requiring SNMP SET is one reason to look for an agent based solution. See the "Other reasons to install OS-based agents" section to understand how to deal with server management with this requirement.

Select the SNMP setting Agentless Management (default). Use SNMP agents running on the iLO to manage the server. The iLO processor fulfills SNMP requests sent by the client to the iLO over the network. This setting does not affect alerts.

Enter the following information:

- System Location (Agentless Management only)—A string of up to 49 characters that specifies the physical location of the server.
- System Contact (Agentless Management only)—A string of up to 49 characters that specifies the system administrator or server owner. The string can include a name, email address, or phone number.
- System Role (Agentless Management only)—A string of up to 64 characters that describes the server role or function.
- System Role Detail (Agentless Management only)—A string of up to 512 characters that describes specific tasks that the server might perform.
- Read Community (Agentless Management only) – This is the configured SNMP read-only community string. The read community includes the following formats:
  - A community string (for example, public).
  - A community string followed by an IP address or FQDN (for example, public 192.168.0.1). Use this option to specify that SNMP access will be allowed from the specified IP address or FQDN. For iLO 4 1.10 or later, you can enter an IPv4 address or FQDN.
- Trap Community – The configured SNMP trap community string.
- SNMP Alert Destination(s)—The IP addresses or FQDNs of up to three remote management systems that will receive SNMP alerts from the iLO. Typically, you enter the HPE SIM server console IP address in the one of the SNMP Alert Destination(s) boxes.

Note
You can configure a maximum of three read or trap community strings in iLO 4. And, you can configure a maximum of three trap destinations in iLO4.

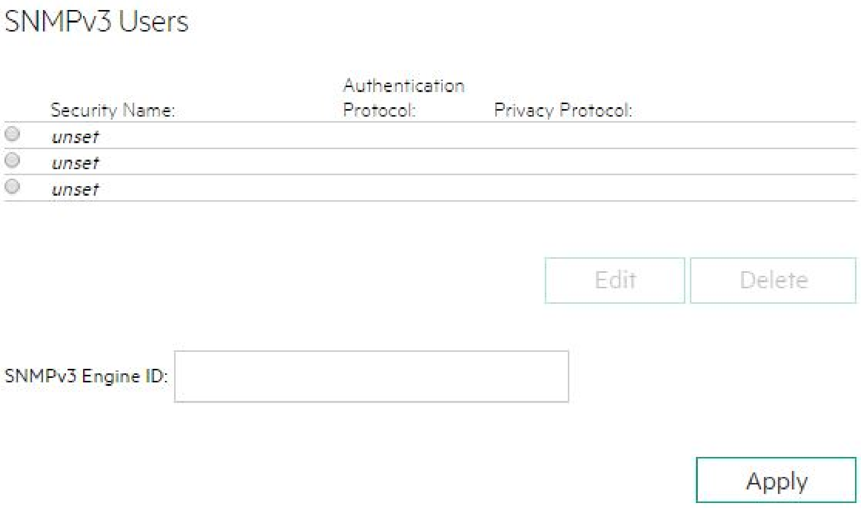
SNMP Port – This port is used for SNMP communications. This value is read-only, but can be modified on the Administration→Access Settings page.

- Click the SNMP Port link to navigate to the Administration→Access Settings page.
- Click Apply to save the configuration.

Configuring SNMPv3 users

iLO 4 1.20 or later is compatible with SNMPv3 authentication when you use Agentless Management. By default, SNMPv3 includes the User-based Security Model. With this model, security parameters are configured at both the agent level and the manager level. Messages exchanged between the agent and the manager are subject to a data integrity check and data origin authentication.

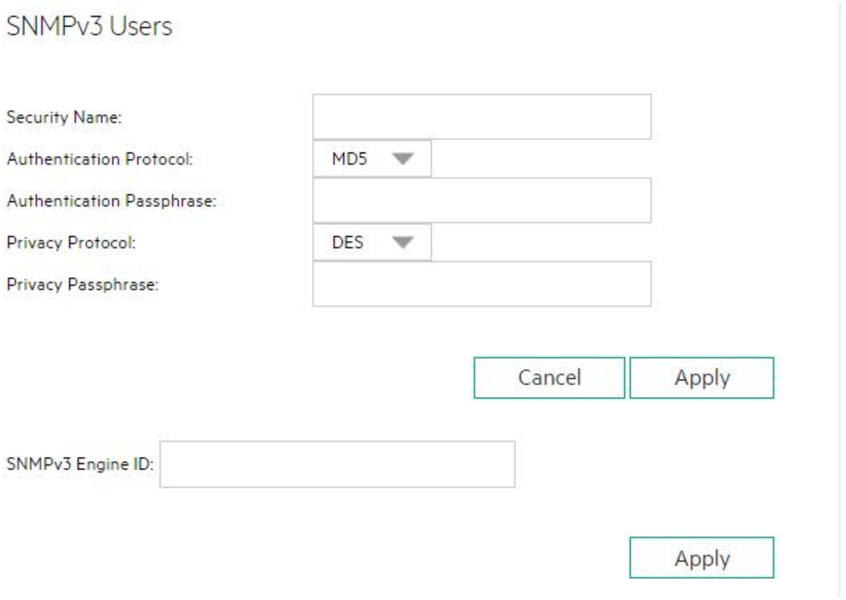
The iLO processor accommodates three user profiles in which you can set the SNMPv3 USM parameters. To edit SNMPv3 user profiles, click the **SNMP Settings** tab and scroll to the **SNMPv3 Users** section (Figure 4).



	Security Name:	Authentication Protocol:	Privacy Protocol:
○	*unset*		
○	*unset*		
○	*unset*		

Figure 4.

Select a user profile in the **SNMPv3 Users** section (Figure 5), and then click Edit.



Security Name:	
Authentication Protocol:	MD5
Authentication Passphrase:	
Privacy Protocol:	DES
Privacy Passphrase:	

Figure 5.

Enter the following information:

- **Security Name** – The user profile name. Enter an alphanumeric string between 1 and 32 characters.
- **Authentication Protocol** – Sets the message digest algorithm to use for encoding the authorization passphrase. The message digest is calculated over an appropriate portion of an SNMP message, and is included as part of the message sent to the recipient. Select MD5 or SHA.

- Authentication Passphrase – Sets the passphrase to use for sign operations. Enter a value between 8 and 49 characters.
- Privacy Protocol – Sets the encryption algorithm to use for encoding the privacy passphrase. A portion of an SNMP message is encrypted before transmission. Select AES or DES.
- Privacy Passphrase – Sets the passphrase used for encrypt operations. Enter a value between 8 and 49 characters.

Then click Apply to save the user profile.

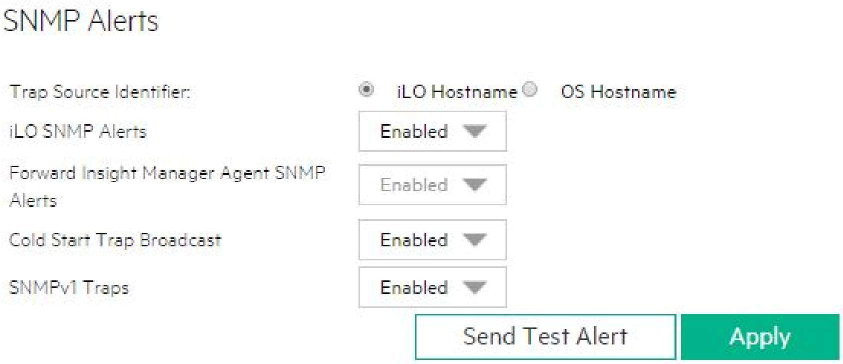
Configuring the SNMPv3 Engine ID

Click the SNMP Settings tab and scroll to the SNMPv3 Users section.

Enter a value in the SNMPv3 Engine ID box. The SNMPv3 Engine ID sets the unique identifier of an SNMP engine belonging to an SNMP agent entity. It must be a hexadecimal string of between 6 and 32 characters, and must be an even number of characters, excluding the preceding 0x (for example, 0x01020304abcdef). Click Apply.

Configuring SNMP alerts

You can configure the trap source identifier, iLO SNMP alerts, forwarding of Insight Management Agent SNMP alerts, Cold Start Trap broadcast, and SNMP traps. To configure an SNMP alert, click the SNMP Settings tab and scroll to the SNMP Alerts section, as shown in Figure 6.



SNMP Alerts

Trap Source Identifier: ● iLO Hostname ○ OS Hostname

iLO SNMP Alerts: Enabled

Forward Insight Manager Agent SNMP Alerts: Enabled

Cold Start Trap Broadcast: Enabled

SNMPv1 Traps: Enabled

Figure 6.

Configure the Trap Source Identifier by selecting iLO Hostname or OS Hostname. This setting determines the host name that is used in the SNMP-defined sysName variable when iLO generates SNMP traps. The default setting is iLO Hostname.

Note

You can configure a maximum of three read or trap community strings in iLO 4. And, you can configure a maximum of three trap destinations in iLO4.

Enable or disable the following alert types:

- iLO SNMP Alerts – Alert conditions that iLO detects independently of the host operating system can be sent to specified SNMP alert destinations, such as HPE SIM.
- Forward Insight Management Agent SNMP Alerts – Alert conditions detected by the host management agents can be forwarded to SNMP alert destinations through iLO. These alerts are generated by the Insight Management Agents, which are available for each compatible operating system. Insight Management Agents must be installed on the host server to receive these alerts.

- Cold Start Trap Broadcast—Cold Start Trap is broadcast to a subnet broadcast address if there are no trap destinations configured in the SNMP Alert Destination(s) boxes. The subnet broadcast address for an IPv4 host is obtained by performing a bitwise logical OR operation between the bit complement of the subnet mask and the host IP address. For example, the host 192.168.1.1, which has the subnet mask 255.255.252.0, has the broadcast address 192.168.1.1 | 0.0.3.255 = 192.168.3.255.
- SNMPv1 Traps – When enabled, SNMPv1 traps are sent to the remote management systems configured in the SNMP Alert Destination(s) boxes.

Optional - Click Send Test Alert to generate a test alert and send it to the TCP/IP addresses in the SNMP Alert Destination(s) boxes. Test alerts include an Insight Management SNMP trap, and are used to verify the network connectivity of iLO in HPE SIM. Only users with the Configure iLO Settings privilege can send test alerts. After the alert is generated, a confirmation dialog box opens. Check the HPE SIM console for receipt of the alert. Click Apply to save the configuration.

HPE RESTful API and Interface Tool

HPE Software-Defined Compute (SDC) architecture is a component of HPE Software-Defined Infrastructure (SDI) used to build agile and scalable data centers. SDI abstracts all the detail and complexity of everyday tasks away from physical and virtual infrastructure assets (network, server, storage, and facilities) to a single, unified, software control layer (Figure 7). SDI uses HPE Representational State Transfer RESTful APIs make this control layer capability possible.

You can read more about HPE SDI at: hpe.com/services/sdi

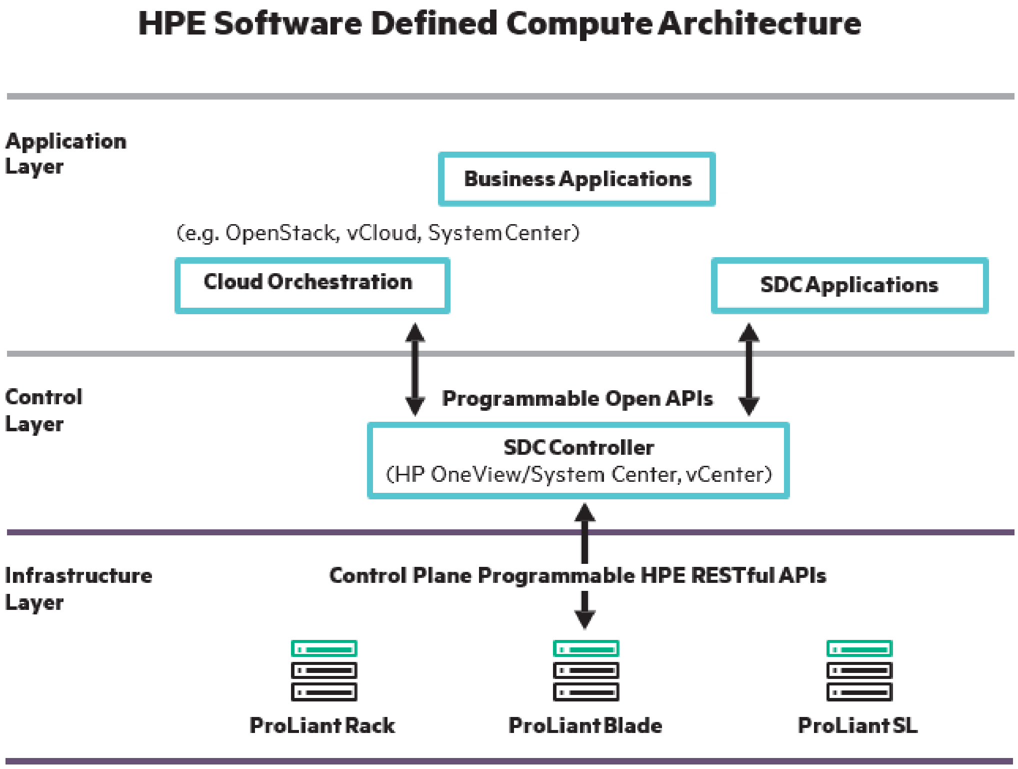


Figure 7. Defined compute architecture with unified software control layer

HPE Agentless Management information supplied to the HPE RESTful APIs allow you to easily, quickly, and securely discover and monitor configuration of your entire HPE ProLiant Gen9 server portfolio. And at the same time, RESTful APIs provide a common language and interface for integrating into cloud-based environments like OpenStack.

RESTful APIs are based on industry best practices and use an HTTP-style hypermedia foundation with web security standards. HPE RESTful APIs enable your IT staff to customize configuration and provisioning of the entire ProLiant Gen9 server portfolio. They provide a common language and interface for integration into cloud-based environments like OpenStack. A RESTful API allows enterprise data centers to script provisioning, automation of firmware/drivers, and server settings.

In the HTTP-style RESTful API language, nouns are resources (Web Services, Web Pages, pictures, video) and verbs are actions: (GET, PUT, POST, PATCH, DELETE). RESTful interfaces use nouns and verbs together to represent and transfer state between client and provider. HPE RESTful APIs work through HPE iLO and currently include HPE iLO 4, Agentless Management, and UEFI.

In addition to the existing HPE Lights-Out Online Configuration (HPONCFG) utility, you can now use HPE RESTful Interface Tool to configure HPE iLO 4 v2.00 (and newer), and UEFI BIOS on Gen 9 servers.

HPE RESTful Interface Tool

The HPE Restful interface Tool gives you a single command tool to configure the BIOS and the iLO processor. You also have remote and local management capabilities.

HPE RESTful API Interface tool has 3 modes of operation:

- Interactive mode – provide autocomplete capabilities for a friendly interaction while getting familiar with the tool
- Scriptable mode – script all the commands by letting users get and set properties of server objects or input files
- File-based mode –allows users of HPEREST to save and load settings from a file

You can read more about HPE RESTful APIs at: hpe.com/info/restfulapi and hpe.com/info/resttool

Redfish API

Redfish is a new specification using a REST-based ‘web’ framework to define a modern remote API and data model for datacenter hardware management. HPE is a major contributor in this Distributed Management Task Force (DMTF) initiative, and HPE is first to implement Redfish conformance in HPE ProLiant Gen9 servers already embedded with HPE RESTful APIs, and will function across heterogeneous environments.. DMTF has completed efforts to create and publish an open industry standard specification and schema that meets the expectations of end users for simple, modern and secure management of scalable platform hardware. The Redfish specification targets the needs of scale-out environments and multi-node systems as well as traditional servers. The specification defines a lightweight data model that is scalable, discoverable and extensible. It’s suitable for applications spanning single systems through HyperScale datacenters. Redfish is designed to be simple and human readable, using a REST-based web framework. It enables developers to take advantage of common scripting languages and development tools. You can learn more about Redfish at: hp.com/h20195/V2/GetDocument.aspx?docname=4AA6-1727ENW&cc=us&lc=en

Agentless Management user environments

This section documents common user environments for Agentless Management. These scenarios are meant to provide a high-level view of some of the ways that Agentless Management can work in your environment. HPE OneView and HPE SIM don’t affect the default Agentless Management ILO settings.

Management with HPE OneView

HPE OneView sets an entry on the SNMP Alert destination fields, so that the HPE OneView appliance receives the SNMP traps sent by iLO. HPE OneView also sets the “read community string” for limited health polling. There is additional data available only with AMS. This includes information associated with adapters, software based raids, OS name/IP, and specific traps.

When you configure a management application to use to use Agentless Management, all monitoring and management of ProLiant Gen8 and newer servers (and their options) is agentless and out-of-band for increased security and reliability. No OS software is required, no open SNMP ports on the host OS are required, and zero downtime updates can be performed for these embedded agents.

HPE OneView utilizes a combination of SNMP traps and polling to continuously monitor the datacenter. HPE ProLiant Gen8 and Gen9 servers with iLO 4 technology, and utilize the AMS for status reporting. AMS includes basic SNMP functions. HPE OneView aggregates status from multiple resource elements into a single overall status for easy identification and action. Duplicate events are filtered through the use of trap storm processing and the use of a monitored resource cache. This eliminates the requirement for administrators to determine whether there is alert duplication or a need for remediation. SNMP utilizes User Datagram Protocol (UDP), a connectionless TCP protocol requiring no special network configuration considerations.

HPE ProLiant Gen8 and Gen9 servers include agentless monitoring through iLO. HPE OneView uses SNMP in a ‘read-only’ mode (gets and traps, but not sets) to the iLO only – not to the host OS. HPE ProLiant G6 and G7 servers require host OS SNMP agents.

HPE OneView Standard and HPE OneView Advanced both provide proactive alert notifications via SNMP trap forwarding, email, and automated alert forwarding. You can view all alerts, filter your alerts, and search your alerts using HPE Smart Search. Alerts can be assigned to specific users and annotated with notes from administrators. Notifications or traps can be automatically forwarded to enterprise monitoring consoles or to centralized SNMP trap collectors.

Integration with HPE OneView for VMware vCenter (OV4VC) and HPE OneView for Microsoft System Center (OV4SC) can be used to monitor the health of servers that do not have an OS yet loaded, as well as ProLiant Gen8 and Gen9 servers running any operating system that has a compatible Agentless Monitoring Service.

OV4VC is software for VMware's vCenter management console which enables the vSphere administrator to quickly obtain context-aware information about HPE servers and HPE storage in their VMware vSphere environment directly from within vCenter. This allows the vSphere administrator to manage physical servers and storage, data stores, and virtual machines. By providing the ability to clearly view and directly manage relationships between virtual machines and HPE Infrastructure, the VMware administrator's productivity increases - as does the ability to ensure quality of service.

OV4SC provides a comprehensive integration of HPE Storage, HPE ProLiant Servers, HPE Blade System and HPE Virtual Connect with Microsoft System Center. It enables administrators to manage and monitor their HPE infrastructure running in Microsoft environment with a single pane-of-glass view for health monitoring, events/alerts, detailed inventory and HPE fabric visualization. Administrators can gain greater control of their technology environments reducing the risk of downtime and enabling a faster response.

You can find information on OV4VC at hpe.com/portal/swdepot/displayProductInfo.do?productNumber=HPVPR, and information on OV4SC at hpe.com/portal/swdepot/displayProductInfo.do?productNumber=System_Center

Management with HPE SIM

To manage a ProLiant Gen9 server using Agentless Management and HPE SIM, your management server must use HPE SIM 7.x or later. You also need to configure SNMP parameters so that HPE SIM can exchange information with the server. The iLO processor should be on the same networks as the management server and HPE recommends that you implement consistent network naming configurations through a shared Domain Name System (DNS). HPE SIM 7.x management features enable you to:

- Identify iLO processors
- Create an association between iLO and its server
- Create links between iLO and its server
- View iLO and server information and status

HPE SIM can discover, identify, and interact with iLO. With the OS running, you can use the HPE SIM Management Console from a standard web browser to establish a connection to iLO, as well as receive alerts and collect information from iLO. Integration with HPE SIM provides:

- SNMP trap delivery to HPE SIM - You can also configure HPE SIM to forward events as SNMP traps to another management application, or to a pager or email address.
- Identification for management processors - All iLO devices on the network are classified in HPE SIM as management processors.
- Grouping of iLO management processors - All iLO devices can be grouped logically and associated within collections. Collections are groups of systems and events that can be used for viewing information, or as a way to specify the targets for a particular action.
- HPE Management Agents or Agentless Management - iLO, combined with Agentless Management or the HPE Management Agents, provides remote access to system management information through the iLO network interface.
- SNMP management - HPE SIM can access Insight Management Agent information through iLO.

For more detailed information on Agentless Management and HPE SIM, see the “HPE Systems Insight Manager and Agentless Management overview” technology brief link in the “Resources” section at the end of this document.

Management with HPE Insight Remote Support

HPE iLO 4, HPE Intelligent Provisioning, and HPE Onboard Administrator include the embedded remote support feature, which allows you to register HPE ProLiant servers and HPE BladeSystem c-Class enclosures for HPE remote support. HPE Insight Remote Support v7.x can be configured for HPE Agentless Management in HPE ProLiant Gen8 and Gen9 servers either through the HPE iLO management engine or through HPE Intelligent Provisioning. You can choose from HPE Insight Online Direct Connect and HPE Insight Remote Support Central Connect configuration options.

HPE Insight Online Direct Connect

You can register a server or enclosure to communicate directly with HPE Insight Online without the need to set up an HPE Insight Remote Support centralized hosting device in your local environment. HPE Insight Online then becomes your primary interface for remote support information. HPE Insight Online is an HPE Support Center feature that enables you to view your remotely monitored devices anywhere, anytime. It provides a personalized dashboard for simplified tracking of IT operations and support information, including a mobile dashboard for monitoring when you are on the go.

HPE Insight Remote Support Central Connect

You can register a server or enclosure to communicate with HPE through an HPE Insight Remote Support centralized hosting device in your local environment. All configuration and service event information is routed through the hosting device. This information can be viewed using the local HPE Insight Remote Support Console, or the web-based view in HPE Insight Online (if enabled in Insight Remote Support).

For more information on how to get connected with HPE Insight Online Direct Connect and HPE Insight Remote Support Central Connect, go to hp.com/services/getconnected.

Using HPE Remote Support with HPE Proactive Care Service

HPE Proactive Care service customers must register ProLiant Gen8 and Gen9 servers for HPE Insight Remote Support Central Connect or HPE Insight Online Direct Connect in order to receive the HPE Proactive Care features, Proactive Scan and Firmware/Software Version Report and recommendations. The HPE Insight Remote Support Central Connect option requires the installation of AMS or the SNMP/WBEM agents for Gen8 or Gen9 servers. AMS is installed automatically if you use the Intelligent Provisioning Recommended installation method for Windows installation. For more information about the HPE Proactive Care service, see the following website: hp.com/services/proactivecarecentral.

For more detailed instructions on these options, see “HP Insight Remote Support and Insight Online Setup Guide for HP ProLiant Servers and HP BladeSystem c-Class Enclosures” (Central Connect/Direct Connect) at hp.com/us/en/enterprise/servers/solutions/info-library/index.aspx?cat=HP_Insight_Remote_Support#.VvV_LE3rtmM

Using Agentless Management with other management applications

You can use Agentless Management even if HPE Insight Management Agents and/or WBEM providers are installed. The AMS can run concurrently with HPE OS-based management software, but HPE recommends running only one: either AMS, or HPE OS-based management software. Running both concurrently consumes more memory and processor cycles. In addition, using both Agentless Management and the SNMP agents may result in different alerts or duplicate alerts in HPE SIM.

If HPE SIM identifies that Agentless Management is in use, HPE SIM first gathers data from the iLO. If the iLO, agents and providers are monitoring a particular component, HPE SIM may receive duplicate data, a subset of data, or a superset of data for that component.

To eliminate duplicate monitoring, you can perform either of the following procedures:

- Stop or uninstall the AMS. Stopping the AMS stops the service until you reboot the server. Rebooting re-enables the service. It’s important to know that following this procedure will result in loss of Active Health functionality and is not recommended.
- Uninstall the agents or providers by using the install or remove software tool available in your OS.
- For VMware, VMware vCenter depends upon the WBEM providers as does the SPP/HPE SUM, so you cannot uninstall or remove them. For VMware, AMS and the WBEM providers should both be left running. If you don’t want to use the WBEM providers for management and won’t be using the SPP and HPE SUM, you can install the “limited” providers. These providers that will continue to supply vCenter requirements.

Important

HPE SIM can be configured to use Agentless or the OS agents in order to avoid duplication. The duplication only occurs for traps. This occurs when the HPE SIM is monitoring a device in agentless mode, and there are Insight Management Agents also present in the managed device. In this configuration, the iLO as well as IM Agents may send the same traps/notification and HPE SIM processes all the traps. This may cause duplicate events in HPE SIM. This is also true for other applications such as HPE OneView, - and OneView plug-ins for vCenter and SystemCenter. When the iLO 4 default configuration for Agentless Management is active, the iLO Management Engine alerts HPE SIM and HPE OneView. This is the preferred configuration and eliminates any potential for duplicate information from the managed server.

HPE ProLiant Agentless Management extensions for Nagios

The Nagios plug-in for Agentless Management talks directly to the iLO4 management processor. The plug-in interacts with the Agentless Management infrastructure to provide out-of-band monitoring of ProLiant Gen8 and Gen9 servers. Nagios is an open source application that can be used to monitor computer systems, networks, and IT infrastructure.

The Nagios plug-in automates server health management, providing high-level health status for managed servers. Administrators can easily identify the failed server within the data center. Plug-in features include:

- Discovery and monitoring of HPE ProLiant servers within data center automatically. There are two discovery approaches: active discovery and passive discovery
- High-level server status
- Display of server status in real-time if the status changes.
- Categorization of the preferred servers into the same host group.

You can read more about the Nagios plug-in, view a video demo, and download the plug-in at Nagios Exchange.

When to use OS-based management agents

In some cases Agentless Management is not the best choice. This section expands on the information in Table 1 using examples of cases when OS-based agents continue to be a better monitoring and reporting solution.

Monitoring performance

If you want to detect, analyze, and explain hardware performance bottlenecks on HPE ProLiant servers, Insight Control performance management (ICperf) is an effective software solution to accomplish those objectives. ICperf provides the tools you need to receive proactive notification of developing bottleneck conditions, and debug existing performance issues. You can monitor performance on one or more servers and log the information to a database for later analysis or reporting, and set up proactive notification using the HPE SIM notification mechanism.

HPE SIM installs ICperf on the same server as the HPE SIM console and requires data from specific set of OS-based agents, in this case, Insight Management Performance agents. These agents record OS hardware and software performance counters and play them back for ICperf. OS-based tools, other than the agents, can provide this information.

Monitoring storage networks

Agentless Management with AMS currently features the ability to monitor Smart Array controllers attached to internal drives and SAS/SATA HBAs. There continue to be situations in which you need to use traditional OS-based agents to monitor elements of the storage network:

- ProLiant direct-attached storage in an expansion cabinet (JBOD) - While Agentless Management can monitor ProLiant direct-attached storage in a JBOD, AMS cannot monitor the external enclosures (temps, power supplies).
- Fibre Channel/FCoE HBA networks - You can use AMS to monitor these HBAs, but not information about the storage network itself.

Other reasons to install OS-based agents

There are other reasons to install OS-based agents. If you are managing a ProLiant Gen8 server using HPE SIM 7.X or HPE Insight Control 7, these reasons include:

- Unique features – Use OS-based agents when you need the unique features supplied by the Insight agents or providers, such as the ability to set disk utilization thresholds that generate an event when crossed. For example, in any configuration that requires SNMP SET, you cannot use Agentless Management to do an SNMP SET, unless iLO is compatible with SNMP SET for MIBs it owns and it is only the AMS on the host that does not. For security reasons, users don’t ordinarily allow SNMP SET.

- Consistency - You can continue to utilize existing practices for management established with earlier ProLiant generations and migrate, or not migrate, to Agentless Management at your convenience.
- Third-party management applications - Unless specifically enabled to understand iLO and Agentless Management, most management applications will treat the iLO as a separate device from the host in which it resides, and will present host information separately from the information gathered from iLO. In this case, continuing to utilize the management agents or providers will give you an integrated view of health and other metrics.
- Health threshold - Use OS-based agents when you want to use a system health threshold for disk utilization.
- HPE Insight Control ProLiant Essentials Performance Management Pack (IC PMP) does not accommodate Agentless Management and requires legacy management with OS agents.

Firmware and driver maintenance with HPE Intelligent Provisioning

If you decide to let the iLO 4 default configuration install Agentless Management, you do not have to worry about updates. HPE Intelligent Provisioning builds on proven technology and stores all required firmware and drivers on a NAND flash chip residing on the ProLiant Gen8 and Gen9 server motherboard. HPE Intelligent Provisioning replaces SmartStart and provides an improved user interface and all of the specific tools, drivers, and agents that you need (to setup, deploy, and maintain) for your specific ProLiant Gen8 or Gen9 server. With HPE Intelligent Provisioning, there is no media. Just press F10 to get started.

HPE Intelligent Provisioning uses a built-in version of HPE SUM to ensure that iLO 4 has the latest agents, software, drivers, and firmware from hpe.com, or a local repository on your own network. You can find the full suite of ProLiant server and blade server drivers, agents, firmware, and systems software in the SPP at: hpe.com/info/spp/download

VMware is the exception here. You cannot deploy VMware vSphere OS with the SPP alone. The SPP contains only the drivers included with the HPE custom image, not WBEM providers or other software. You need to install using a full HPE Custom Image.

Required firmware for Agentless Management

HPE Agentless Management is integrated into and runs on the iLO 4 management processor. Agentless Management relies on required iLO minimum firmware updates. You can find those minimum firmware requirements on the “Resources” tab of the iLO home page at hpe.com/info/ilo

You can also go to the Hewlett Packard Enterprise Support Center for the latest drivers and software at hpe.com/portal/site/hpsc.

Hardware compatibility

Agentless Management provides backward compatibility to ProLiant Gen8 servers. HPE ProLiant Gen8 and Gen9 servers both run Agentless Management and AMS, and as new Agentless Management features are added to HPE ProLiant Gen9 hardware, many of those features extend to include HPE ProLiant Gen8 servers. Some Agentless Management functionality in ProLiant Gen9 servers is hardware dependent, as a result some functions are not compatible with ProLiant Gen8 platforms.

All ProLiant Gen9 300-level servers are fully compliant with Agentless management and AMS. Some ProLiant Gen9 100-level servers may have limitations. See Table 1 in this document for guidelines on Agentless Management features included on ProLiant Gen8 and 9 servers.

Summary

HPE Agentless Management installs by default without additional requirements. HPE Agentless Management runs on the HPE iLO management processor, independent of the OS and the main CPU. Agentless Management offers robust basic server monitoring without the complexity of OS-based agents. The base hardware monitoring and alerting capabilities are built into the system. These capabilities start working the moment a power cord and an Ethernet cable are connected to the server. HPE Agentless Management offers important advantages over traditional OS-based agents. You have access to SNMP reporting on all core server hardware conditions without relying on OS-based agents, even in pre-OS conditions. This means you get reporting regardless of OS and without incurring server processor overhead.

AMS is not an agent, but rather a small helper service. Use AMS to deliver more information about the server and the OS than you get with Agentless Management alone. AMS lets you use only the OS-based agents you need in a lightweight service. This means faster reporting with less overhead.

All HPE Agentless Management and AMS features are ProLiant Gen 9 compliant, and most are ProLiant Gen 8 compliant with the exception of some hardware-based dependencies. Agentless Management and AMS protect your hardware infrastructure investment by continuing to extend server functionality.

Resources

All HPE iLO 4-related guides and manuals
hpe.com/info/ilo/docs

HPE technology white papers
hpe.com/docs/servertechnology

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA6-6053ENW, June 2016