HP Device Monitor for Microsoft System Center User Guide

Abstract

This guide provides information on using the HP Device Monitor to monitor hardware components in an HP Insight Control for Microsoft System Center environment. This information is for system administrators who use the HP Device Monitor and other HP tools to manage hardware components.

HP Part Number: 664823-001
Published: August 2011
Edition: 1

Warranty

The information contained herein is subject to change without notice. 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.

Acknowledgements

Contents

1 Overview

This guide is intended for system administrators who use the HP Device Monitor and other HP applications and tools to manage hardware components in a Microsoft System Center environment.

You should be familiar with the configuration and operation of Microsoft Windows and Microsoft Systems Center Operations Manager 2007. Because of the potential risk of data loss, only individuals who are experienced with using this software should implement the procedures described in this guide.

Complete information on supported hardware and software is included in the HP Insight Control for Microsoft System Center support matrix. For links to the support matrix and other product documentation, see "Related information" (page 28) .

Introduction

The HP Device Monitor complements and extends the System Center Operations Manager (SCOM) by adding monitoring of enclosures and other HP hardware. The HP Device Monitor is used with other HP management packs, such as the HP BladeSystem Management Pack and the HP ProLiant Linux and VMware Management Pack.

NOTE: The HP Device Monitor replaces the previous HP BladeSystem Enclosure Monitor Manager and HP BladeSystem Enclosure Monitor Service. If you have existing HP BladeSystem enclosures that are being monitored by the HP BladeSystem Enclosure Monitor Service, you can migrate your existing configuration information to use the new HP Device Monitor. For information on how to migrate your configuration, see the *HP Insight for Microsoft System Center Installation and Configuration Guide*.

Product operation

The HP Device Monitor comprises two components:

- HP Device Monitor Console—provides the user interface for connecting to the HP Device Monitor Service to configure devices for management inside of the System Center Operations Manager environment.
- HP Device Monitor Service—monitors HP hardware and reports status and events for managed devices to SCOM. The Device Monitor Service works in conjunction with HP Common Services.

The HP Device Monitor performs the following functions:

- Initiates a connection to the monitored device
- Receives SNMP traps from the device
- Collects server subsystem state
- Collects enclosure component state
- Collects hardware inventory

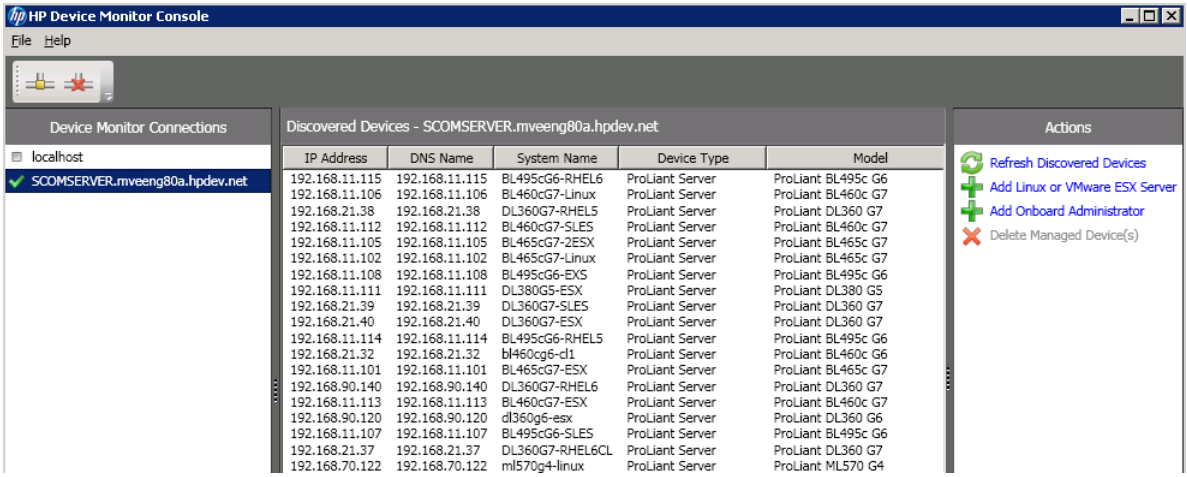
The HP Device Monitor Service uses the information entered through the Device Monitor Console to connect to and monitor HP hardware. If the connection succeeds, the HP Device Monitor Service continues to monitor the device for inventory, health state, and events.

2 Using the HP Device Monitor Console

The Device Monitor Console (DMC) provides the capability to connect to one or more HP Device Monitor Services (DMS) to configure devices for management inside of the System Center Operations Manager. The DMC enables you to configure the required credentials and configuration information for each managed device.

The DMC window includes the following panes:

- **Device Monitor Connections**—Displays the current DMS connections. The pane also displays the status of each monitor connection. See Table 1 (page 6).
- **Discovered Devices**—Displays the devices associated with the currently selected DMS. The list can be sorted on any of the device fields by clicking on the list column heading.
- **Actions**—Displays the various actions that can be performed from the DMC.
- **Status line**—Located at the bottom of the DMC, this field displays the status of the selected Device Monitor Connection.



TIP: You can get more information about a DMC field or control by moving the cursor over it. A tool tip will appear providing information.

Table 1 Device Monitor Connection status

Icon	Status	Description
	Connected to DMS	The selected Device Monitor Connection is connected to the DMS.
	Disconnected from DMS	The selected Device Monitor Connection is disconnected from the DMS.
	HP Device Monitor Service connection error	A problem has caused the connection to be lost. When the problem has been solved, the connection can be reestablished.
	HP Device Monitor Service internal error	The DMC has detected an internal DMS error but the connection has not been lost. If the error corrects itself, the connection transitions back to Connected status.

Opening the Device Monitor Console

IMPORTANT:

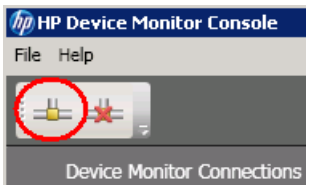
- By default, you must have Administrator rights to run the DMC. For access from a non-administrator account, see "Setting up non-administrator account to use the DMC" (page 12).
- The DMC can be run on systems other than the system on which the DMS is installed.
- The HP ProLiant Server Management Pack must be imported into SCOM to open the DMC from the SCOM console. You must also install at least one instance of the DMS and wait for SCOM to discover the service.

You can open the DMC from the SCOM console in the following ways:

- From the Windows **Start** menu on the systems where the DMC is installed, click Device Monitor Console.
- On the menu bar, select **Actions→HP Device Monitor Service Tasks→HP Device Monitor Console**.
- Select **HP Management Servers** under **HP Systems** in the Monitoring view pane. In the Actions pane under HP Device Monitor Service Tasks, click **HP Device Monitor Console**.
- Selecting an Enclosure State view or a Server State view. In the actions pane under HP Device Monitor Service Tasks, click HP Device Monitor Console.

Adding a DMS connection

1. Open the DMC.
2. In the Device Monitor Connections pane, click the **Add Connection** icon.



3. Enter the Host Name or IP Address of the Windows server where the DMS instance is running.
4. Click **Connect**.

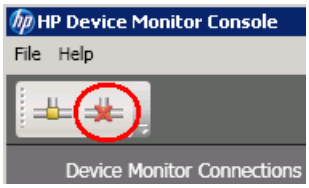
   A status indicator is displayed while the DMC attempts to connect to the DMS. When the connection is established, the devices currently managed by the DMS are displayed in the **Discovered Devices** pane.

Removing a DMS connection

Removing a connection disconnects it from the DMS and deletes the connection from the Device Monitor Connections pane. To reestablish the connection, it must be added again.

1. Open the DMC.
2. Select the monitor connection to remove.

3. In the **Device Monitor Connections** pane, click the remove connection icon.



The connection is removed.

TIP: You can also remove a connection by right-clicking on it and selecting the **Remove** menu option.

Disconnecting from the DMS

You can disconnect an existing connection from the DMS. This leaves the entry in the Device Monitor Connections pane, but changes its status to Disconnected. You can then reconnect without having to add it again.

1. Open the DMC.
2. Right-click the monitor connection you want to disconnect and select the **Disconnect** menu option.

   The status of the connection changes to Disconnected.

To reconnect to the DMS, right-click the monitor connection and select the **Connect** menu option.

Refreshing monitor data

The DMC automatically refreshes the Discovered Devices list using data from the DMS. The data is updated when a connection is first established and after adding a new device. You can manually refresh monitor data using the following procedure.

1. Open the DMC.
2. Select the monitor connection for which you want to refresh the connection data.
3. In the **Actions** pane, click **Refresh Discovered Devices**.

   The refresh icon is displayed during the refresh.

TIP: You can also refresh device information by pressing the **F5** key.

Adding devices to the DMS

There are two actions available to add devices to the DMS:

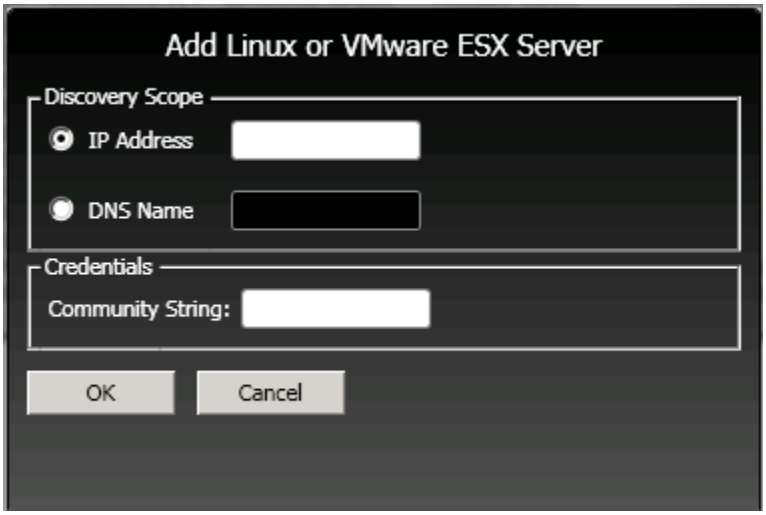
- **Add Linux or VMware ESX Server**—adds an HP ProLiant Server running either Linux or VMware ESX
- **Add Onboard Administrator**—adds the Onboard Administrator for an HP BladeSystem enclosure.

Adding a Linux or VMware ESX server

1. Open the DMC.
2. Select the monitor connection to which you are adding the device.

   The current devices on the connection are displayed in the Discovered Devices pane.
3. In the **Actions** pane, click **Add Linux or VMware ESX Server**.

   The Add Linux or VMware ESX Server dialog is displayed.



4. Enter the device IP Address or DNS Name.

IMPORTANT:

If a Linux or VMware ESX server is added that has the same host name as an existing server device, the server will be added but the existing Linux or VMware ESX server will no longer be displayed in the SCOM console. To avoid this situation, do not assign the same host name to multiple devices.

5. Enter the Community String.

   The community string must have read access to the SNMP agent of the target system.

6. Click **OK**.

   If the information is valid, the device is added to the **Discovered Devices** pane.

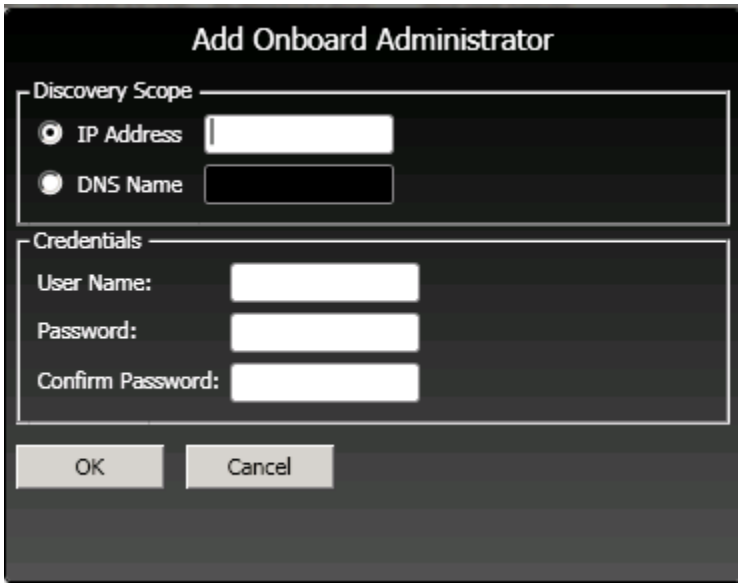
Adding an Onboard Administrator

1. Open the DMC.
2. Select the monitor connection to which you are adding the device.

   The current devices on the connection are displayed in the **Discovered Devices** pane.

3. In the **Actions** pane, click **Add Onboard Administrator**.

   The Add Onboard Administrator dialog is displayed.



4. Enter the device **IP Address** or **DNS Name**.
5. Enter the **User Name** and **Password** credentials for accessing the Onboard Administrator.
6. Click **OK**.

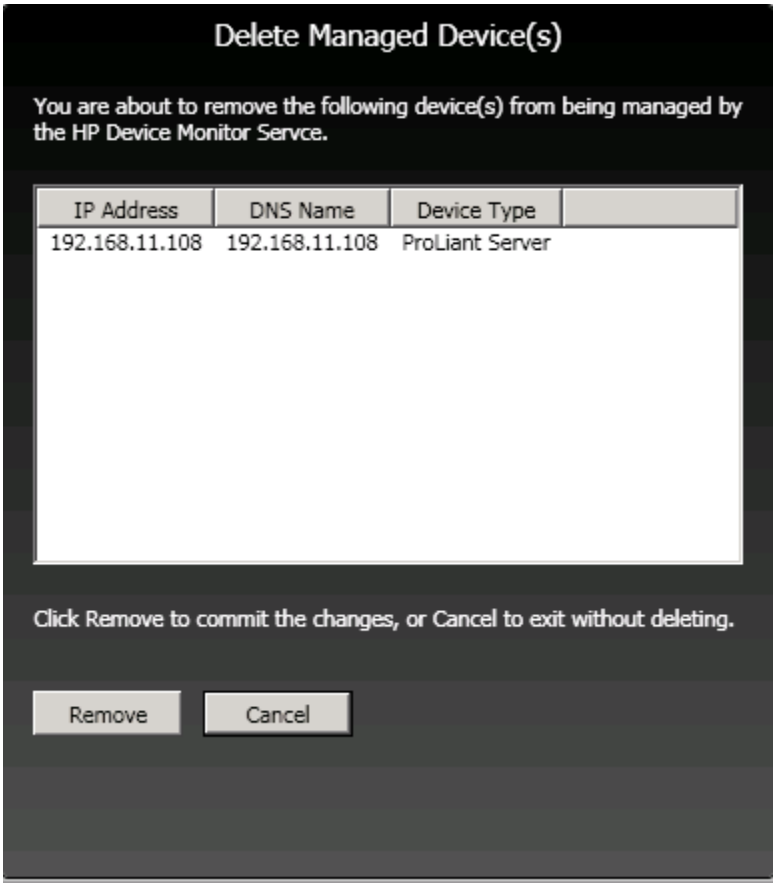
   If the information is valid, the device is added to the Discovered Devices pane.

Deleting devices from the DMS

1. Open the DMC.
2. Select the monitor connection from which you are removing the device.

   The current devices on the connection are displayed in the **Discovered Devices** pane.
3. In the **Discovered Devices** pane, select one or more devices to delete.
4. In the Actions pane, click **Delete Managed Device(s)**.

   The **Delete Managed Device(s)** confirmation window is displayed.



5. Click **Remove**.
   The devices are deleted from the Discovered Devices pane.

TIP: You can also delete a single device by right-clicking on it and selecting the **Delete** menu option.

Updating device configuration

If necessary, you can update the credentials used to access a monitored device.

TIP:

- The Onboard Administrator credentials must be updated in the DMC if the credentials are changed on the managed enclosure's Onboard Administrator.
- The community string must be updated in the DMC if the community string is changed on the managed Linux or VMware server.

1. Open the DMC.
2. Select the monitor connection for the device you are updating.
   The current devices on the connection are displayed in the **Discovered Devices** pane.
3. Right-click the device you are updating and select the **Update** menu option.
4. Enter the appropriate credentials:
   - If you are updating a Linux or VMware ESX Server, enter the **Community String**.
   - If you are updating an Onboard Administrator, enter the credentials.
5. Click **OK**.

Setting up non-administrator account to use the DMC

To connect DMS from the DMC and manage the devices, non-administrator users must be granted the following access permissions to local or remote DMS resources:

- Full Control access to registry key located at `HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\HP SCOM Management Packs\HPDeviceMonitorService`
- Read/write/execute permissions to the HP Device Monitor Service folder located at `%Program Files%\HP SCOM Management Packs\HP Device Monitor Service`. Ensure all files in the HP Device Monitor Service folder have read/write/execute permissions, including `CSDataLayer.dll`.

IMPORTANT: Although it is possible to manage devices using a non-administrator account, it is not recommended you do so. One of the limitations of using a non-administrator account is that no events will be logged in the HP Device Monitor event log if a problem occurs.

When using a non-administrator account, events can be viewed in the device monitor logs generated under `%ProgramFiles%\HP SCOM Management Packs\HP Device Monitor Service`.

Accessing HP Device Monitor help

The **Help** menu provides a **User Guide** option that links to the HP website so you can access the HP Insight Control for Microsoft System Center documentation.

3 Using Windows PowerShell with HP Device Monitor

Many of the tasks performed using the DMC can also be done using Windows PowerShell, the Microsoft command console, and scripting language. PowerShell enables you to create scripts that can automate many of the device monitor tasks.

When the DMS is installed, the PowerShell cmdlets in this chapter are available to add and remove managed devices. If the modules are not available, the following command can be used to load the correct PowerShell snap-in: `Add-PSSnapin HP.Servers.DeviceMonitorCmdLets`

The information in this chapter assumes you are familiar with Windows PowerShell. For more information, access the *Windows PowerShell Owner's Manual* at the following website:

http://technet.microsoft.com/en-us/library/ee221100.aspx

IMPORTANT:

- You must have Administrator rights to use PowerShell with the HP Device Monitor.
- PowerShell must be running on the system on which the DMS is installed.

Add-ProLiantServer

`Add-ProLiantServer` adds the specified ProLiant server to the HP Device Monitor Service. An SNMP community string must be specified. This cmdlet throws an exception if unsuccessful.

Parameters

- `Address`—IP Address or hostname
- `CommunityString`—SNMP community string

Example

```
PS C:\> Add-ProLiantServer

Supply values for the following parameters:
Address: 192.168.21.1
CommunityString: public
PS C:\>
```

Remove-ProLiantServer

`Remove-ProLiantServer` removes the specified ProLiant server from the HP Device Monitor Service. This cmdlet throws an exception if unsuccessful.

Parameters

- `Address`—IP Address or hostname
- `CommunityString`—SNMP community string

Example

```
PS C:\> Remove-ProLiantServer

Supply values for the following parameters:
Address: 192.168.21.1
CommunityString: public
PS C:\>
```

Add-OnboardAdministrator

`Add-OnboardAdministrator` adds the specified Onboard Administrator to the HP Device Monitor Service. A username and password must be specified. This cmdlet throws an exception if unsuccessful.

Parameters

- `Address`—IP Address or hostname
- `Username`—user name
- `Password`—password

Example

```
PS C:\> Add-OnboardAdministrator

Supply values for the following parameters:
Address: 192.168.0.100
Username: public
Password: mypassword
PS C:\>
```

Remove-OnboardAdministrator

`Remove-OnboardAdministrator` removes the specified Onboard Administrator from the HP Device Monitor Service. This cmdlet throws an exception if unsuccessful.

Parameters

- `Address`—IP Address or hostname

Example

```
PS C:\> Remove-OnboardAdministrator

Supply values for the following parameters:
Address: 192.168.0.100
PS C:\>
```

Sample PowerShell Scripts

The following examples illustrate how PowerShell scripts can be created to add multiple devices to the DMS.

Adding multiple ProLiant servers

This sample script uses a CSV file to add two servers to the DMS.

Sample CSV file (servers.csv)

```
Address,CommunityString
192.168.21.37,public
192.168.21.41,public
```

Sample script

```
$items = Import-CSV ".\servers.csv"

foreach ($item in $items)
{
```

```
 "Adding " + $item.Address + " ..."
 Add-ProLiantServer -Address $item.Address -CommunityString $item.CommunityString
}
```

Adding multiple Onboard Administrators

This sample script uses a CSV file to add three Onboard Administrators to the DMS.

Sample CSV file (enclosures.csv)

```
Address,Username,Password
192.168.11.34,vs,password1
192.168.11.35,Administrator,password2
192.168.11.36,vs,password1
```

Sample script

```
$items = Import-CSV ".\enclosures.csv"

foreach ($item in $items)
{
 "Adding " + $item.Address + " ..."
 Add-OnboardAdministrator -Address $item.Address -Username $item.Username -Password $item.Password
}
```

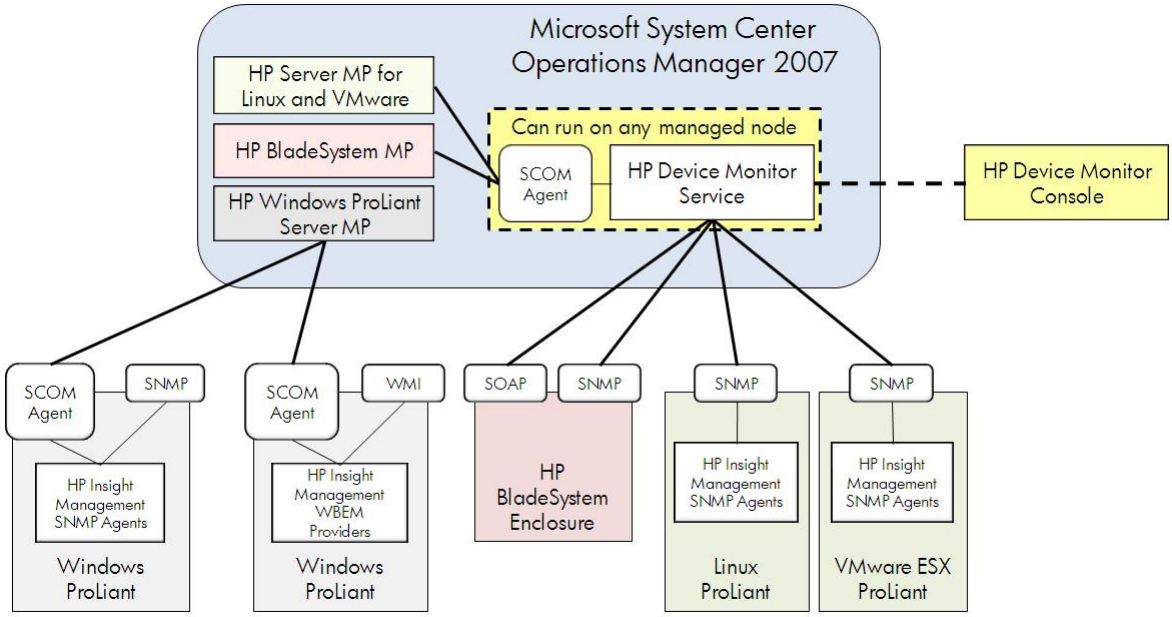
4 More about the HP Device Monitor

This chapter provides supplemental information about the operation of the HP Device Monitor.

HP Device Monitor architecture

The DMS provides a communication link between non-Windows devices that are managed from within Microsoft System Center Operations Manager (SCOM). The Device Monitor Service is built on HP Common Services, which provides the underlying monitoring of the managed devices. On ProLiant servers running Windows, the HP Insight Management Agents (SNMP) or HP Insight Management WBEM Providers communicate directly to the HP ProLiant Server management pack on the SCOM console via a Microsoft SCOM agent that is loaded locally on each managed node. Because non-Windows devices such as HP BladeSystem Enclosures, Linux servers, and VMware servers cannot have Windows-based SCOM agents loaded locally, they must communicate directly with the DMS. Figure 1 (page 16) shows the communication paths.

Figure 1 HP Device Monitor communication paths

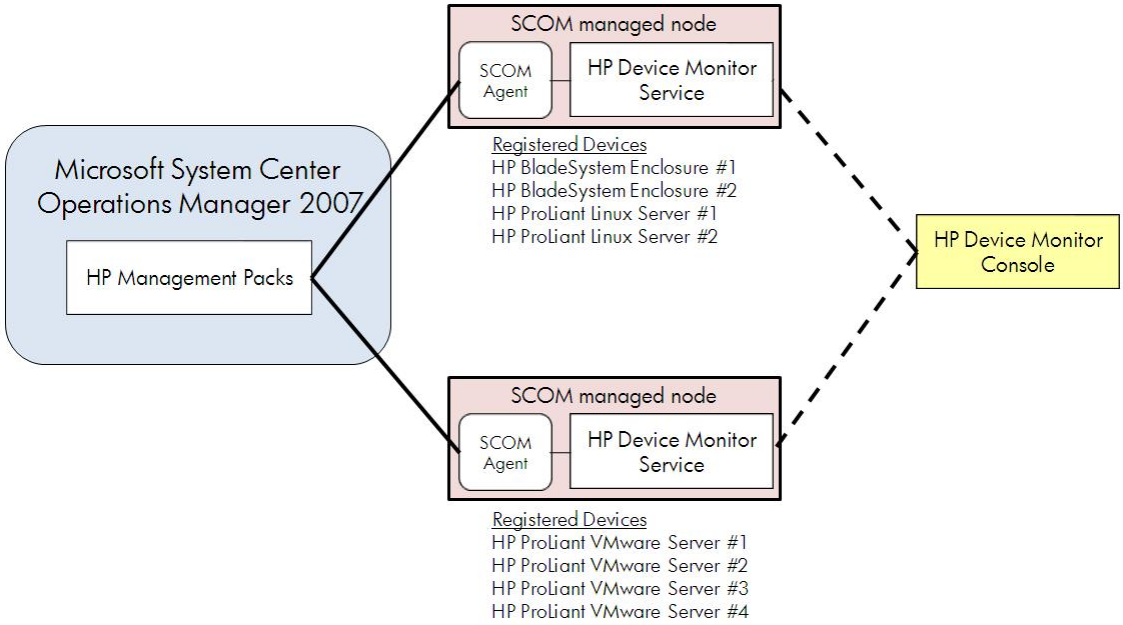


The Device Monitor Service can run on any Windows server managed by SCOM (either a physical or a virtual machine). The DMS uses the SCOM agent of the managed node on which it is installed to communicate with the HP management packs on the SCOM console.

The DMC is an application that communicates directly with instances of the DMS, providing the capability to add or remove non-Windows devices. Non-Windows devices must be registered with an instance of the DMS before they can be managed in the SCOM console. As shown in Figure 2 (page 17), it is possible to run multiple DMS instances. The DMC can communicate with all of the multiple instances simultaneously.

NOTE: Adding the same managed device to multiple DMS instances is not recommended.

Figure 2 Multiple instances of the HP Device Monitor Service



5 Device monitor performance and scalability guidelines

The Device Monitor Service (DMS) acts as a proxy to communicate between the HP Management Packs on the SCOM Server and the non-Windows monitored devices (BladeSystem Onboard Administrator and supported Linux and VMware servers). The DMS requires system and network resources that are shared with Operations Manager server or other applications on the system where it is configured. As the number of monitored devices increases, resource utilization by the DMS may also increase.

This information describes performance characteristics for the DMS and example configurations.

Monitoring process overview

A single DMS instance monitors multiple devices simultaneously. Each monitored device must be registered with the DMS instance via the Device Monitor Console (DMC) or PowerShell cmdlets.

There are four phases involved in the monitoring process:

- **Phase 1. Connection**—establishes connection to device
- **Phase 2. Data collection**—initial collection of inventory and state information of a device
- **Phase 3. Monitoring**—monitoring for changes to inventory or state information of a device
- **Phase 4. Data recollection**—recollection of updated inventory and state information of a device as reported during the monitoring phase (step 3).

The connection and data collection phases occur once in a connection. The data collection phase is the busiest phase and uses a significant amount of system and network resources. After the data collection is done, the management packs can access all enclosure data to produce inventory and state information. The DMS spends most of the time in the monitoring phase and watching for any information change to the monitored device. If a change is found, the data recollection starts and will collect partial data only where a change is reported. After the data recollection is done, the DMS will continue the monitoring phase.

SNMP trap monitoring is performed simultaneously with the above phases. SNMP trap monitoring establishes communication to the SNMP trap service and is not a factor in performance characteristics unless there is significant number of SNMP traps generated into the network.

Factors influencing performance characteristics of the Monitor Service

- Number of registered devices

  The connection, data collection, and monitoring phases are processed on a per device basis. Adding more monitored devices (enclosures, Linux servers, or VMware servers) to a DMS will increase system and network utilization.

- Rate of configuration changes and error events to enclosures

  Any configuration change of a monitored device will trigger the data recollection phase. If a failing component continually changes state between healthy and degraded states, every state change will cause the data recollection phase and cause the DMS additional load while updating the information.

- Connection recovery

  The DMS uses heartbeat monitoring to recover the connection if it is disrupted for 60 seconds or longer. If it observes no heartbeat for a connection, the current connection disconnects and a new connection starts. If there is a network infrastructure issue, which causes instability between the DMS and monitored device, then the DMS will be busy re-establishing connection until it succeeds with the connection to the monitored device.

Best practices based on these factors

- Move the DMS to non-Operations Manager Servers

  If the Operations Manager server is highly utilized, you may not want the DMS to share that same resource. You can move the DMS to any Windows managed node to free up resource sharing from the Operations Manager server.

- Use multiple instances of the DMS

  Multiple DMS instances can be deployed to multiple managed nodes in an Operations Manager domain to divide and reduce the monitoring resource requirements per DMS instance.

- Run the DMS instances in a Hyper-V cluster for high availability

  The DMS can be installed on a Hyper-V virtual machine. If this is part of a Hyper-V cluster, it will provide failover service for the virtual machine. The DMS is not cluster aware, and HP does not recommend running it as a clustered service on its own.

Performance characterization

The DMS performance requirements will vary by environment. Included here are some observed performance characteristics gathered using the following test environment.

Test configuration

- ProLiant DL380 G7, Intel Xeon (2.667 GHz 6 core Processors x2), 20 GB memory, NC382i (1GbE)
- Windows Server 2008 R2 SP1
- Microsoft System Center Operations Manager 2007 R2
- Microsoft SQL Server 2008 SP2
- DMS installed on the system

Table 2 (page 19) shows SCOM, SQL and DMS resource requirements while scaling to 60 monitored servers.

Table 2 SCOM, SQL and DMS resource requirements scaling to 60 servers

	Baseline	15 servers[1]	30 servers[1]	45 servers[1]	60 servers	250 servers[1]	50 encl and 250 servers[1]
CPU (%)	4	4	4	4	6	12	17
Total Memory Utilization (GB)	4.8	4.9	5.0	5.1	5.2	6.4	7.4
DMS Private Bytes (MB)	24.4	24.6	24.9	25.2	25.5	28.9	33.6
HP Common Services Private Bytes (MB)	61.5	64.4	67.3	70.2	73.1	107.9	515.9

1 Estimated

Table 3 (page 20) shows DMS resource requirements for monitoring 60-250 servers and a combination of 50 BladeSystem enclosures and 250 servers after a 72 hour period.

Table 3 DMS resource requirements for 60-250 servers and 50 BladeSystem enclosures

	60 servers	250 servers[1]	50 encl and 250 servers[1]
CPU (%)	6	12	17
DMS Private Bytes (MB)	26.4	29.9	34.9
HP Common Services Private Bytes (MB)	73.5	108.5	518.7

1 Estimated

Table 4 (page 20) shows SCOM, SQL and DMS resource requirements while scaling to an estimated 50 monitored BladeSystem enclosures.

Table 4 SCOM, SQL and DMS resource requirements scaling to 50 BladeSystem enclosures

	Baseline	5 enclosures[1]	10 enclosures	50 enclosures[1]	50 encl and 250 servers[1]
CPU (%)	4	4.5	5	9	17
Total Memory Utilization (GB)	4.8	4.9	5.0	5.8	7.4
DMS Private Bytes (MB)	24.4	24.8	25.3	29.1	33.6
HP Common Services Private Bytes (MB)	61.5	102.3	143.1	469.5	515.9

1 Estimated

Table 5 (page 20) shows DMS resource requirements for monitoring 10-50 BladeSystem enclosures and a combination of 50 BladeSystem enclosures and 250 servers after a 72 hour period.

Table 5 DMS resource requirements for 10-50 BladeSystem enclosures and servers

	10 enclosures	50 enclosures[1]	50 encl and 250 servers[1]
CPU (%)	5	9	17
DMS Private Bytes (MB)	26.3	30.2	34.9
HP Common Services Private Bytes (MB)	143.1	469.5	518.7

1 Estimated

6 Troubleshooting the HP Device Monitor

Introduction

The following information is designed to help resolve some common operating issues that might occur when using the HP Device Monitor.

Device monitor management issues

This section provides troubleshooting information for device monitor management issues with the HP Device Monitor and SCOM.

Same device added to more than one device monitor connection (DMS)

It is possible to add the same device to more than one device monitor connection. If a device is added more than once, SCOM will display multiple instances of the device and duplicate alerts will be generated for each instance.

DMC operational and usage issues

This section provides troubleshooting information for operational and usage issues with the HP Device Monitor and SCOM.

Checking DMS operation

If a problem with the DMS has occurred, first perform the following steps:

1. Launch the DMC to determine if the DMS is working. If it is, you can log in and see the list of managed devices.
2. Check to determine if the DMS has reported an alert. Alerts can be viewed by selecting the **HP Systems→Active Alerts** view in the SCOM console.

SCOM does not discover devices

Every device must be registered with a DMS instance via the DMC. Use DMC to review DMS connections and each of the monitored devices.

The updated registration information appears immediately in the DMS. Any errors are reported in HP Device Monitor Log (in the NT Event Log). However, the SCOM discovery process does not occur immediately. The discovery results do not appear on the management console until after the next discovery cycle. The default discovery cycle time is 60 minutes but can be changed by the administrator.

In addition to registering devices, you must perform the following actions:

- On the HP Onboard Administrator web console, verify that a monitor account exists and that the account has managing permission to each managed device. To see the user settings, select **User/Authentication→Local Users or Directory Groups**, and then select a user or a group.
- Check the HP Device Monitor log (in the NT Event Log). Review the Error and Warning entries that can cause a monitoring issue. Launch the DMC to resolve any registration issues.
- Check all current Active Alerts from the **HP Systems→Active Alerts** view in the SCOM console. Resolve all active alert issues, and then close Active Alerts.
- Check the Operations Manager Log (in the NT Event Log). Review the Error and Warning entries that can cause issues with the system. Report these issues to Microsoft.

SCOM does not alert managed devices

SNMP Settings on the HP BladeSystem Onboard Administrator or Linux/VMware server must be configured to send SNMP Trap-based Alerts to the DMS.

To view and update the SNMP Settings of a BladeSystem Onboard Administrator:

1. Open the Onboard Administrator Web console.
2. Select **SNMP Settings** for the device.
3. Enable SNMP.
4. Verify that the IP address of the system, (where the DMS is running) is registered with a community string.

On OA firmware version 2.10 or later, test SNMP traps can be generated from the same SNMP Settings screen. Click **Send Test Alerts** to send a test trap. If the Management Pack is functioning properly, a test SNMP trap posts in the HP Device Monitor Log (in the NT Event log), and an alert is generated on the SCOM console.

To view and update the SNMP Settings of a Linux/VMware device:

1. Log in to the Linux/VMware device using a root privileged user.
2. Open the SNMP configuration file (`snmpd.conf`) for the device.
3. Verify that the IP address of the system, (where the DMS is running) is registered with a community string.

NOTE: If the `snmpd.conf` file is changed, you must restart the following services:

- snmpd
- hp-snmp-agents

The DMC is unable to connect to the DMS following repair of a management pack

When repairing a management pack, the device monitor services may be stopped. If the services have stopped, the DMC displays an error message indicating that it failed to connect to the DMS. Using the Windows Services Manager, check the following services and start them, if necessary:

- HP Device Monitor Service
- HP Common Services

The DMC is unable to connect to the DMS because of a connection issue

The DMC displays an error message indicating that it failed to connect to the DMS. To verify that the DMC can connect to the DMS through the network:

1. Verify both the DMC and DMS system(s) have network connectivity.
2. Select **Computer Management→Services** from the DMS.
3. Check the following services and start them, if necessary:
   - HP Device Monitor Service
   - HP Common Services
4. Verify that the HP Device Monitor event log does not contain any error messages for the DMS.

The DMC is unable to connect to the DMS because of user credentials

The DMC uses the current user's credentials to access DMS. Verify that the current user has been granted access to the local or remote system hosting DMS. You must have Administrator rights to run the DMC unless an non-administrator account has been created. For more information, see "Setting up non-administrator account to use the DMC" (page 12).

The DMC status line displays failure status

The DMC is configured to periodically connect with the DMS to update its data. The DMC displays a failure status when it fails to connect with the DMS. Ensure that the network connection is working and that the DMS is running.

When adding a Linux or VMware ESX server the process failed and event 440 is entered in the HP Device Monitor event log

Adding a Linux or VMware ESX server caused the following error to be entered in the HP Device Monitor event log:

`The HP Device Monitor Service was unable to discover the device. Please check the connection and configuration for the device and try to discover the device again. Could not discover or identify` *nnnnnnnnn* (IP address or DNS name). `Make sure device is up and connected to the network.`

This error occurs when the device is not up and connected to the network. Make sure the device is connected and available.

This error also occurs if the community string entered for the Linux or VMware ESX server is invalid. Check the community string to determine if it is valid. If it is not, add the server again using a valid community string.

Linux or VMware ESX server not displayed in SCOM console after adding a device with same host name

If a Linux or VMware ESX server is added that has the same host name as an existing server device, the server will be added in DMC but the existing Linux or VMware ESX server will no longer be displayed in the SCOM console. To avoid this situation, do not assign the same host name to multiple devices.

Linux or VMware ESX server not displayed in SCOM console after updating the device

This may occur if an invalid community string is entered when updating a Linux or VMware ESX server. An event 310 is entered in the HP Device Monitor event log if the community string is invalid and the alert can be viewed by selecting the **HP Systems**+**Active Alerts** view in the SCOM console.

Check the community string to determine if it is valid. If it is not, update the server again using a valid community string. Also ensure the device is connected to the network and available.

Events not being logged in the HP Device Monitor event log when using a non-administrator account

This is expected behavior when using the DMC with a non-administrator account. To ensure all events are logged, it is recommended that an administrator account be used when managing devices with the DMC.

When using a non-administrator account, events can be viewed in the device monitor logs generated under `%ProgramFiles%\HP SCOM Management Packs\HP Device Monitor Service`.

Add Onboard Administrator does not add an unverified enclosure

The add Onboard Administrator process verifies the enclosure Onboard Administrator address, login credentials, and the firmware version on Onboard Administrator of the enclosure before adding the Onboard Administrator to the DMS. You can add only valid enclosures to the DMS.

Downgrade of Onboard Administrator firmware is not supported

The supported Onboard Administrator firmware versions are 2.04 and above. Do not downgrade the Onboard Administrator firmware on enclosures that have been added and are currently managed.

Updating the password or community string

If an Onboard Administrator password or Linux/VMware server community string has been changed, you must update the information in the DMC.

Use the update option to update an Onboard Administrator login and password information, or to update a Linux/VMware community string

7 HP Device Monitor Service NT events

Table 6 (page 25) lists the NT events that may be reported when a device connection fails. The events are entered in the HP Device Monitor log file. The event source is the HP Device Monitor Core.

These events can be caused by the following conditions:

- Communication with the device has been lost.
- Device failover has occurred.
- Device information is not yet available because the HP Device Monitor Service is starting.

Table 6 HP Device Monitor Service NT events

NT event	Description	Resolution
300	HP Common Services device state changed to minor.	This event occurs when an Onboard Administrator is no longer visible to the HP Device Monitor Service but a standby Onboard Administrator is available. Once the standby Onboard Administrator becomes active, this event should be resolved automatically.
310	HP Common Services device state changed to major.	This event occurs when a ProLiant Server or an Onboard Administrator (without a standby configured) is no longer visible to the HP Device Monitor Service. To resolve this for a server, ensure the server is running and the SNMP Agents are loaded and configured properly. To resolve this for Onboard Administrator, ensure the Onboard Administrator is visible on the network and properly configured.
320	HP Common Services device state changed to critical.	This event occurs when a ProLiant Server or an Onboard Administrator (without a standby configured) is no longer visible to the HP Device Monitor Service for an extended period of time. To resolve this for a server, ensure the server is running and the SNMP Agents are loaded and configured properly. To resolve this for Onboard Administrator, ensure the Onboard Administrator is visible on the network and properly configured.
400[1]	The HP Device Monitor Service has detected that the device has already been configured for monitoring.	This event occurs when adding a new Server or Onboard Administrator to be managed and the HP Device Monitor service detects the device is already being managed. Insure the IP Address/DNS name does not match a device already being managed. This could also occur if a system has multiple network adapters and a different network adapter was used to access the system.
410[1]	The HP Device Monitor Service was unable to resolve the DNS name to an IP address for the device.	This event occurs when the DMS name or IP address could not be resolved. Check the spelling of the DNS name or IP address for errors to resolve this issue.
420[1]	The HP Device Monitor Service was unable to configure the device for monitoring because credential information already exists.	This event occurs when adding a device and the HP Device Monitor Service detects that credentials already exist for the device. Retry the operation.

Table 6 HP Device Monitor Service NT events *(continued)*

NT event	Description	Resolution
430[1]	The HP Device Monitor Service encountered an error while attempting to process credential information for the device. Check the following: • The device configuration information is correct and the device is up and running on the network. • HP Device Monitor Service is running. • HP Common Service is running.	This event occurs when adding a device and the HP Device Monitor Service and an error occurred when creating the credentials for the device. Retry the operation.
440[1]	The HP Device Monitor Service was unable to discover the device. Check the connection and configuration for the device and try to discover the device again.	This event occurs when the HP Device Monitor Service fails to discover a device. This may be caused by a timeout or other error. Retry the operation.
450[1]	The HP Device Monitor Service was unable to authenticate with the device. Check the credentials for the device and try to discover the device again.	This event occurs when the HP Device Monitor Service fails to authenticate a device. Check the credentials of the device. Update the device credentials if they have changed.

1 This event is not displayed in the SCOM console.

8 Support and other resources

Information to collect before contacting HP

Be sure to have the following information available before you contact HP:

- Software product name
- Hardware product model number
- Operating system type and version
- Applicable error message
- Third-party hardware or software
- Technical support registration number (if applicable)

How to contact HP

Use the following methods to contact HP technical support:

- See the Contact HP worldwide web site:
  http://www.hp.com/go/assistance
- Use the `Contact hp` link on the HP Support Center web site:
  http://www.hp.com/go/hpsc
- In the United States, call +1 800 334 5144 to contact HP by telephone. This service is available 24 hours a day, 7 days a week. For continuous quality improvement, conversations might be recorded or monitored.

Registering for software technical support and update service

Insight Management includes one year of 24 x 7 HP Software Technical Support and Update Service. This service provides access to HP technical resources for assistance in resolving software implementation or operations problems.

The service also provides access to software updates and reference manuals in electronic form as they are made available from HP. Customers who purchase an electronic license are eligible for electronic updates.

With this service, Insight Management customers benefit from expedited problem resolution as well as proactive notification and delivery of software updates. For more information about this service, see the following website:

http://www.hp.com/services/insight

Registration for this service takes place following online redemption of the license certificate.

How to use your software technical support and update service

As HP releases updates to software, the latest versions of the software and documentation are made available to you. The Software Updates and Licensing portal gives you access to software, documentation and license updates for products on your HP software support agreement.

You can access this portal from the HP Support Center:

http://www.hp.com/go/hpsc

After creating your profile and linking your support agreements to your profile, see the Software Updates and Licensing portal at http://www.hp.com/go/hpsoftwareupdatesupport to obtain software, documentation, and license updates.

Warranty information

HP will replace defective delivery media for a period of 90 days from the date of purchase. This warranty applies to all Insight Management products.

HP authorized resellers

For the name of the nearest HP authorized reseller, see the following sources:

- In the United States, see the HP U.S. service locator web site:
  http://www.hp.com/service_locator
- In other locations, see the Contact HP worldwide web site:
  http://www.hp.com/go/assistance

Documentation feedback

HP welcomes your feedback. To make comments and suggestions about product documentation, send a message to:

docsfeedback@hp.com

Include the document title and part number in your message. All submissions become the property of HP.

Related information

- HP Insight Control for Microsoft System Center documentation website: http://www.hp.com/go/icsc/docs
- HP Insight Management WBEM Providers documentation
- HP Insight Management Agents documentation
- HP ProLiant servers:
  - ProLiant BL BladeSystem servers:
    http://www.hp.com/go/blades
  - ProLiant DL series rack mount servers:
    http://www.hp.com/servers/dl
  - ProLiant ML series tower servers:
    http://www.hp.com/servers/ml
  - ProLiant SL series scalable system servers:
    http://h10010.www1.hp.com/wwpc/us/en/sm/WF02a/15351-15351-3896136.html
- HP Integrity servers: http://www.hp.com/go/integrity
- HP NonStop servers: http://www.hp.com/go/nonstop

Typographic conventions

This document uses the following typographical conventions:

Book title	The title of a book. On the web, this can be a hyperlink to the book itself.
`Command`	A command name or command phrase, for example `ls -a`.
`Computer output`	Information displayed by the computer.
Ctrl+x or **Ctrl-x**	A key sequence that indicates you must hold down the keyboard key labeled **Ctrl** while you press the letter `x`.

`ENVIRONMENT VARIABLE`	The name of an environment variable, for example, `PATH`.
Key	The name of a keyboard key. **Return** and **Enter** both refer to the same key.
Term	A term or phrase that is defined in the body text of the document, not in a glossary.
`User input`	Indicates commands and text that you type exactly as shown.
`Replaceable`	The name of a placeholder that you replace with an actual value.
[ ]	In command syntax statements, these characters enclose optional content.
{ }	In command syntax statements, these characters enclose required content.
|	The character that separates items in a linear list of choices.
…	Indicates that the preceding element can be repeated one or more times.
WARNING	An alert that calls attention to important information that, if not understood or followed, results in personal injury.
CAUTION	An alert that calls attention to important information that, if not understood or followed, results in data loss, data corruption, or damage to hardware or software.
IMPORTANT	An alert that calls attention to essential information.
NOTE	An alert that contains additional or supplementary information.
TIP	An alert that provides helpful information.

Index