



# HPE Operations Agent and Infrastructure SPIs

Software Version: 12.03

For Windows®, Linux, HP-UX, Solaris, and AIX operating systems

## Installation Guide

Document Release Date: April 2017

Software Release Date: April 2017



**Hewlett Packard**  
Enterprise

## Legal Notices

### Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

### Restricted Rights Legend

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

### Copyright Notice

© 2012-2017 Hewlett Packard Enterprise Development LP

### Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of the Microsoft group of companies.

UNIX® is a registered trademark of The Open Group.

### Acknowledgements

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

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

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

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

## Documentation Updates

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

This site requires that you register for an HP Passport and to sign in. To register for an HP Passport ID, click **Register** on the HPE Software Support site or click **Create an Account** on the HP Passport login page.

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

## Support

Visit the HPE Software Support site at: <https://softwaresupport.hpe.com/>.

Most of the support areas require that you register as an HP Passport user and to sign in. Many also require a support contract. To register for an HP Passport ID, click **Register** on the HPE Support site or click **Create an Account** on the HP Passport login page.

To find more information about access levels, go to: <https://softwaresupport.hpe.com/web/softwaresupport/access-levels>.

**HPE Software Solutions Now** accesses the HPSW Solution and Integration Portal website. This site enables you to explore HPE Product Solutions to meet your business needs, includes a full list of Integrations between HPE Products, as well as a listing of ITIL Processes. The URL for this website is <https://softwaresupport.hpe.com/km/KM01702731>.

# Contents

Chapter 1: Introduction .....	8
Conventions Used in this Document .....	8
Best Practices for Installing the HPE Operations Agent .....	9
Deploying the HPE Operations Agent .....	9
Installing the HPE Operations Agent in a Single Step .....	10
Single Depot for HP-UX Installation .....	12
Co-existence of HPE Operations Agent with other HPE products .....	13
Installing the HPE Operations Agent on Platforms with Limitation .....	13
Enabling Secure Communication .....	13
Planning the Installation of HPE Operations Agent .....	15
Chapter 2: Connecting the HPE Operations Agent to OMi .....	18
Connecting a New HPE Operations Agent Installation to OMi .....	18
Connecting an Existing HPE Operations Agent to OMi .....	19
Updating the HPE Operations Agent Installation from OMi .....	19
opr-package-manager Command-Line Interface .....	21
Chapter 3: Registering the HPE Operations Agent and Infrastructure SPIs on the HPOM Management Server (and Installing the Infrastructure SPIs) ..	25
Registering the HPOM for Windows Management Server .....	25
Registering the HPOM on UNIX/Linux Management Server .....	32
Uninstalling the HPE Operations Agent and Infrastructure SPIs Deployment Package .....	38
Chapter 4: Prerequisites for Installing the HPE Operations Agent on a Node .....	40
For Windows .....	40
For Linux .....	42
For HP-UX .....	44
For Solaris .....	46
For AIX .....	47
For Debian and Ubuntu .....	48
Upgrade Notes .....	50
Data Collection and Storage with the HPE Operations Agent 12.02 ...	52

Metric Data Store .....	53
Preinstallation Task: Installing the HPE Operations Agent and Infrastructure SPIs on HPOM in Cluster .....	54
Chapter 5: Installing the HPE Operations Agent from HPOM or HPE OMi Console .....	56
Chapter 6: Installing the HPE Operations Agent in a Single Step .....	57
Installing the HPE Operations Agent using Single Step .....	58
Deploying Patches and Hotfixes using Single Step Installer .....	59
Verifying the Installation .....	60
Chapter 7: Installing HPE Operations Agent using Profile File .....	61
Installing HPE Operations Agent using a Profile File .....	70
Installing HPE Operations Agent and Enabling Health Monitoring using Profile File .....	70
Chapter 8: Configuring the Agent User .....	72
Requirements for Using a Non-Default User .....	72
Limitations of Using a Non-Default User .....	73
Configure the Agent User during Installation .....	74
Configuring the Agent User after Installation .....	78
Changing the Default User on Windows .....	78
Alternative Method: Use the ovswitchuser Command .....	78
Changing the Default User on UNIX/Linux .....	81
Use a Profile File .....	81
Alternative Method: Use the ovswitchuser Command .....	83
Chapter 9: Reducing the Installation Time .....	86
Using the removesign option with the zip media .....	86
Using the Profile file .....	87
Using the removesign option while deploying HPE Operations Agent from HPOM and HPE OMi .....	88
Chapter 10: Installing the HPE Operations Agent using Agent Installation Repository .....	89
Standalone Agent Installation Repository .....	89
Agent Installation Repository as a Virtual Appliance .....	92
Deploying HPE Operations Agent Using the Agent Installation Repository .....	93
Chapter 11: Installing the HPE Operations Agent using the Puppet Environment .....	99

Data Flow in a Puppet Environment .....	99
Installing and Configuring the HPE Operations Agent on Linux Using YUM .....	100
Installing and Configuring HPE Operations Agent on Linux Using oarepo.sh .....	103
Installing and Configuring HPE Operations Agent on Windows Using oarepo.ps1 .....	105
Enabling HPE Operations Agent Installation Using Profile File with Puppet .....	107
Configuring HPE Operations Agent Using Puppet Module to Set the XPL Parameters for the Nodes .....	109
Chapter 12: Installing the HPE Operations Agent Using HP Server Automation .....	112
Importing the HPE Operations Agent Software .....	113
Creating a Software Policy .....	114
Attaching the Software Policy to a Device or Server .....	115
Verifying the Installation .....	116
Chapter 13: Installing the HPE Operations Agent using Microsoft System Center 2012 Configuration Manager .....	118
Creating the HPE Operations Agent Package .....	118
Deploying the HPE Operations Agent Package .....	120
Verifying the Installation .....	120
Chapter 14: Installing the HPE Operations Agent Using Red Hat Network Satellite Server .....	122
Downloading and Storing the HPE Operations Agent Depot Files (RPMs) .....	123
Creating the Setup on the Target Node .....	123
Deploying the Packages on the Target Node .....	124
Removing the Packages from the Target Node .....	125
Chapter 15: Installing the HPE Operations Agent RPM based Hotfix Package .....	127
Chapter 16: Installing the HPE Operations Agent on Platforms with Limitations .....	129
Installing the HPE Operations Agent on Platforms with Limitation Remotely from the HPOM for Windows Console .....	129
Installing the HPE Operations Agent on Platforms with Limitation Remotely from the HPOM for UNIX Console .....	130

Installing the HPE Operations Agent on Platforms with Limitation Remotely Using Command Line .....	131
Chapter 17: Installing the HPE Operations Agent Manually on the Node ..	132
Post-Installation Task in a NAT Environment .....	137
Chapter 18: Installing the Infrastructure SPIs on the HPOM Management Server .....	138
Components of the Infrastructure SPI on HPOM for Windows .....	143
Components of the Infrastructure SPIs on HPOM for UNIX .....	146
Chapter 19: Installing the HPE Operations Agent in the Inactive Mode .....	148
Chapter 20: Monitoring the HPE Operations Agent in High Availability Clusters .....	153
Chapter 21: Configuring the HPE Operations Agent in a Secure Environment .....	160
Configuring Proxies .....	161
Organizing the Proxy Configuration File .....	165
Configuring the Communication Broker Port .....	168
Configuring Local Communication Ports .....	171
Configuring Nodes with Multiple IP Addresses .....	172
Configuring HTTPS Communication through Proxies .....	173
Communication in a Highly Secure Environment .....	174
Introduction to the Reverse Channel Proxy .....	176
Secure Communication in an Outbound-Only Environment .....	178
Specifying the RCP Details with a Configuration File .....	181
Configuring a RCP for Multiple Systems .....	182
Verifying the Communication through the RCPs .....	183
Communication through Two Firewalls .....	185
Configuring Amazon Linux VM Outbound Communication with HPOM ..	186
Proxy Configuration and Setup Details .....	187
Troubleshooting .....	190
Chapter 22: Configuring Certificates for the HPE Operations Agent and Infrastructure SPIs .....	194
Requesting Certificates Automatically .....	194
Requesting Certificates with an Installation Key .....	195
Deploying Certificates Manually .....	196
Restoring the Certificates .....	198

Configuring SSL Certificates for the Agent Install Repository Virtual Appliance .....	200
Creating a Certificate .....	200
Creating a Self-Signed Certificate .....	200
Sending a Certificate Signing Request .....	202
Configuring SSL Certificate on the Lighttpd Server .....	202
Importing the SSL Certificate on a Node .....	203
Installing HPE Operations Agent on a Trusted Machine .....	204
Chapter 23: Uninstalling the HPE Operations Agent and Infrastructure SPIs .....	206
Removing the Agent with the oacleanall Script .....	207
Chapter 24: Uninstalling the Infrastructure SPIs .....	209
Chapter 25: Troubleshooting .....	211
Installation .....	211
Certificates .....	219
Coexistence of HP Computesensor Standalone Packages (shipped with vPV) and HPE Operations Agent 12.02 .....	221
Other .....	223
Send documentation feedback .....	224

# Chapter 1: Introduction

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

The *HPE Operations Agent and Infrastructure SPIs 12.02* DVD media provides you with the HPE Operations Smart Plug-ins for Infrastructure (Infrastructure SPIs). If you want to install the Infrastructure SPIs with the electronic media, make sure to download the media for *all* node platforms (and not a platform-specific ISO file). Platform-specific ISO files do not contain the Infrastructure SPIs.

## Conventions Used in this Document

The following conventions are used in this document.

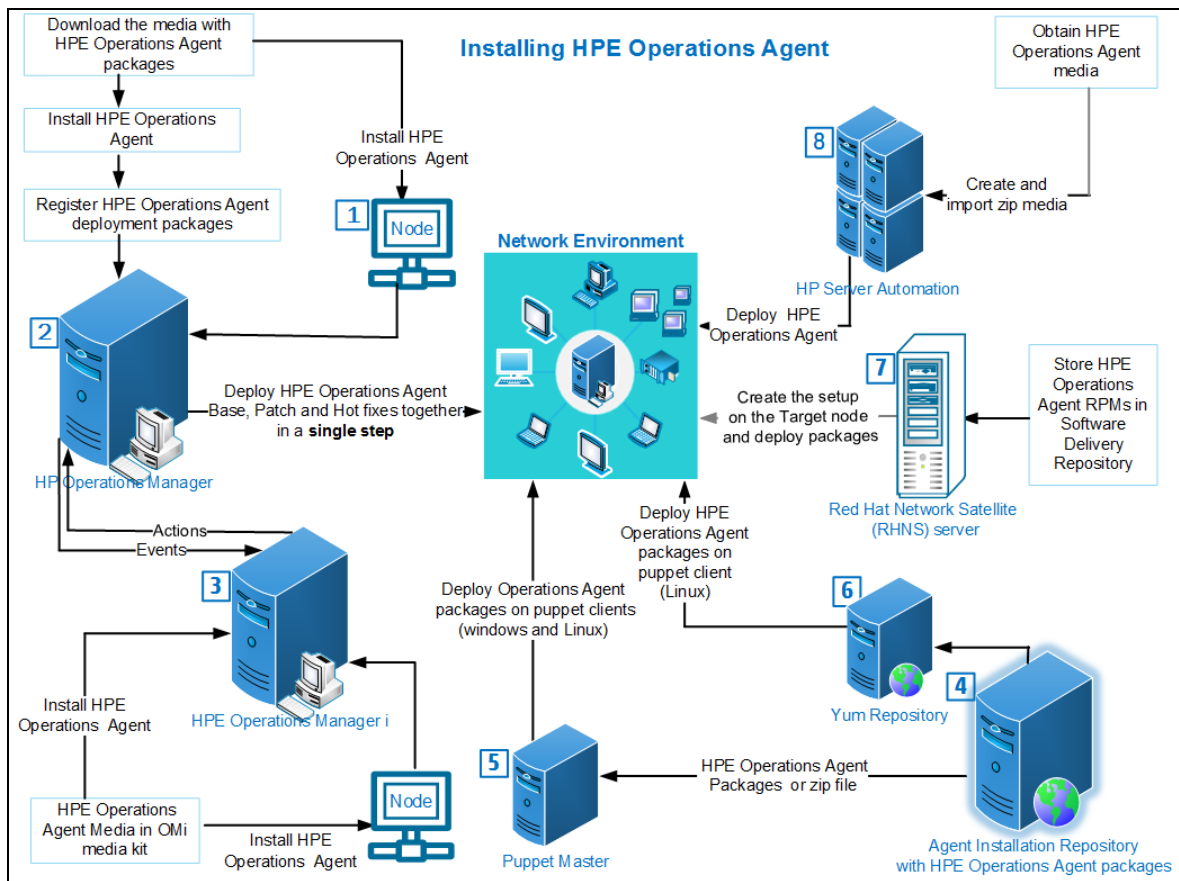
Convention	Description
<OvInstallDir> The installation directory for the HPE Operations Agent.	<b>&lt;OvInstallDir&gt;</b> is used in this document to denote the following location: <ul style="list-style-type: none"><li>• <i>On Windows:</i> %ovinstalldir%</li><li>• <i>On HP-UX/Linux/Solaris:</i> /opt/OV/</li><li>• <i>On AIX:</i> /usr/lpp/OV/</li></ul>
<OvDataDir> The directory for HPE Operations Agent configuration and runtime data files.	<b>&lt;OvDataDir&gt;</b> is used in this document to denote the following location: <ul style="list-style-type: none"><li>• <i>On Windows:</i> %ovdatadir%</li><li>• <i>On HP-UX/Linux/Solaris:</i> /var/opt/OV/</li><li>• <i>On AIX:</i> /var/opt/OV/</li></ul>
<OvInstallBinDir> The bin directory contains all the binaries (executables) of HP Operations Agent.	<b>&lt;OvInstallBinDir&gt;</b> is used in this document to denote the following location: <ul style="list-style-type: none"><li>• <i>On Windows x64:</i> %ovinstalldir%\bin\win64\</li><li>• <i>On Windows x32:</i> %ovinstalldir%\bin\win32\</li><li>• <i>On HP-UX/Linux/Solaris:</i> /opt/OV/bin/</li><li>• <i>On AIX:</i> /usr/lpp/OV/bin/</li></ul>



# Best Practices for Installing the HPE Operations Agent

## Deploying the HPE Operations Agent

You can use one of the following methods to simplify the deployment of HPE Operations Agent in large environments:



For more information see:

1. [Installing the HPE Operations Agent Manually on the Node.](#)
2. [Installing from the HPOM Console and Installing HPE Operations Agent in a Single Step.](#)
3. Installing HPE Operations Agent from HPE OMi. For more information, see the section *Connecting HPE Operations Agents to OMi* in the chapter *Monitored Nodes* in the *OMi Administration Guide*.
4. [Installing HPE Operations Agent using Agent Installation Repository.](#)
5. [Installing HPE Operations Agent using the Puppet Environment](#)
6. [Installing and configuring HPE Operations Agent on Linux using YUM](#)
7. [Installing HPE Operations Agent Using Red Hat Network Satellite Server](#)
8. [Installing HPE Operations Agent Using HP Server Automation](#)

## Installing the HPE Operations Agent in a Single Step

The single step installer enables you to install the base version of HPE Operations Agent along with patches and hotfixes. The prerequisites check occurs only once before the installation.

You can use the `oainstall` script to install the HPE Operations Agent locally on a managed node or use the HPOM console to install HPE Operations Agent remotely.

### Using `oainstall` Script to Install the HPE Operations Agent

1. Log on to the node as a root user or an administrator.
2. Download and extract the media, patches, and hotfix packages to the same directory.
3. Go to the directory where you extracted the bits.
4. Run the following command:

#### On Windows

```
cscript oainstall.vbs -i -a
```

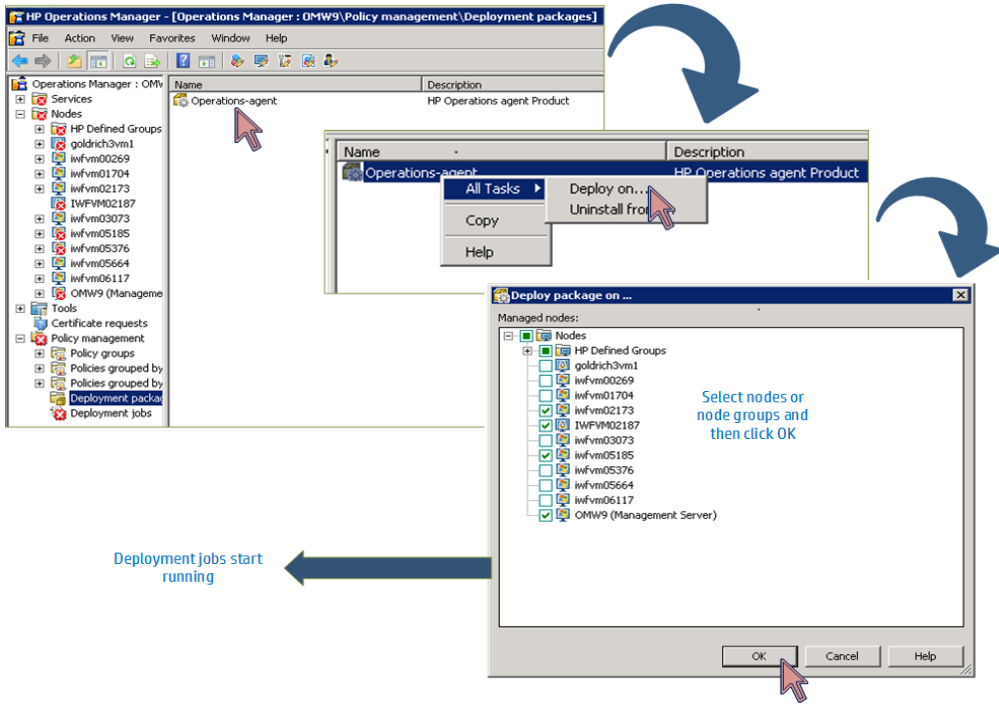
#### On HP-UX/Linux/Solaris

```
./oainstall.sh -i -a
```

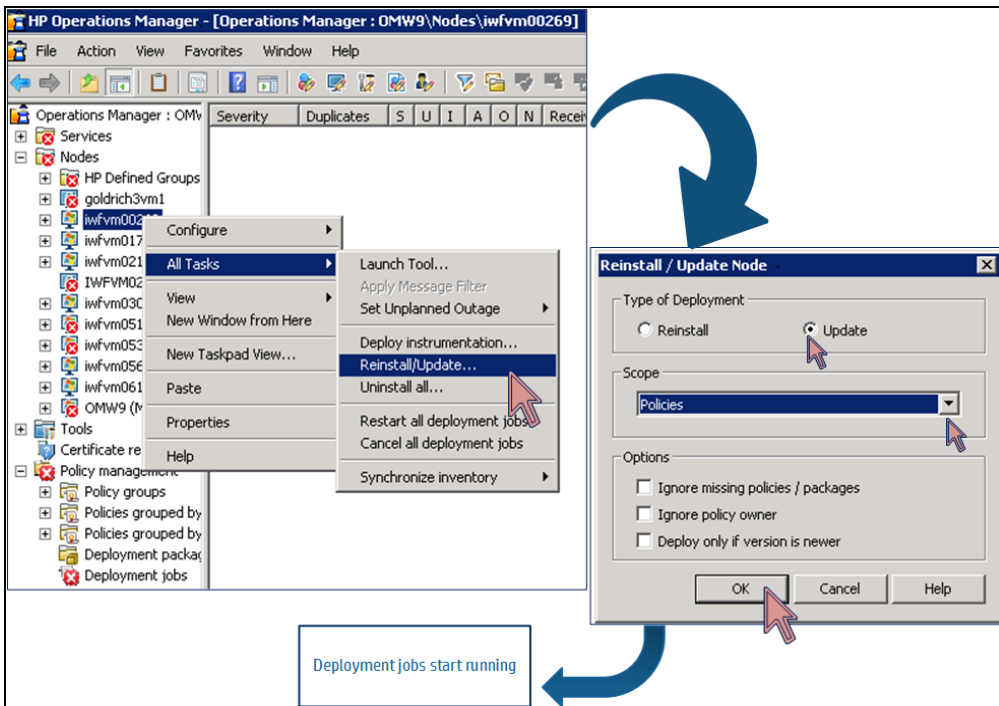
Base version of the HPE Operations Agent along with patches and hotfixes are installed.

### Installing the HPE Operations Agent from HPOM for Windows Management Server

**Scenario 1:** If the HPE Operations Agent 12.02 is not installed on a node, follow the steps to install base version, patches, and hotfixes:

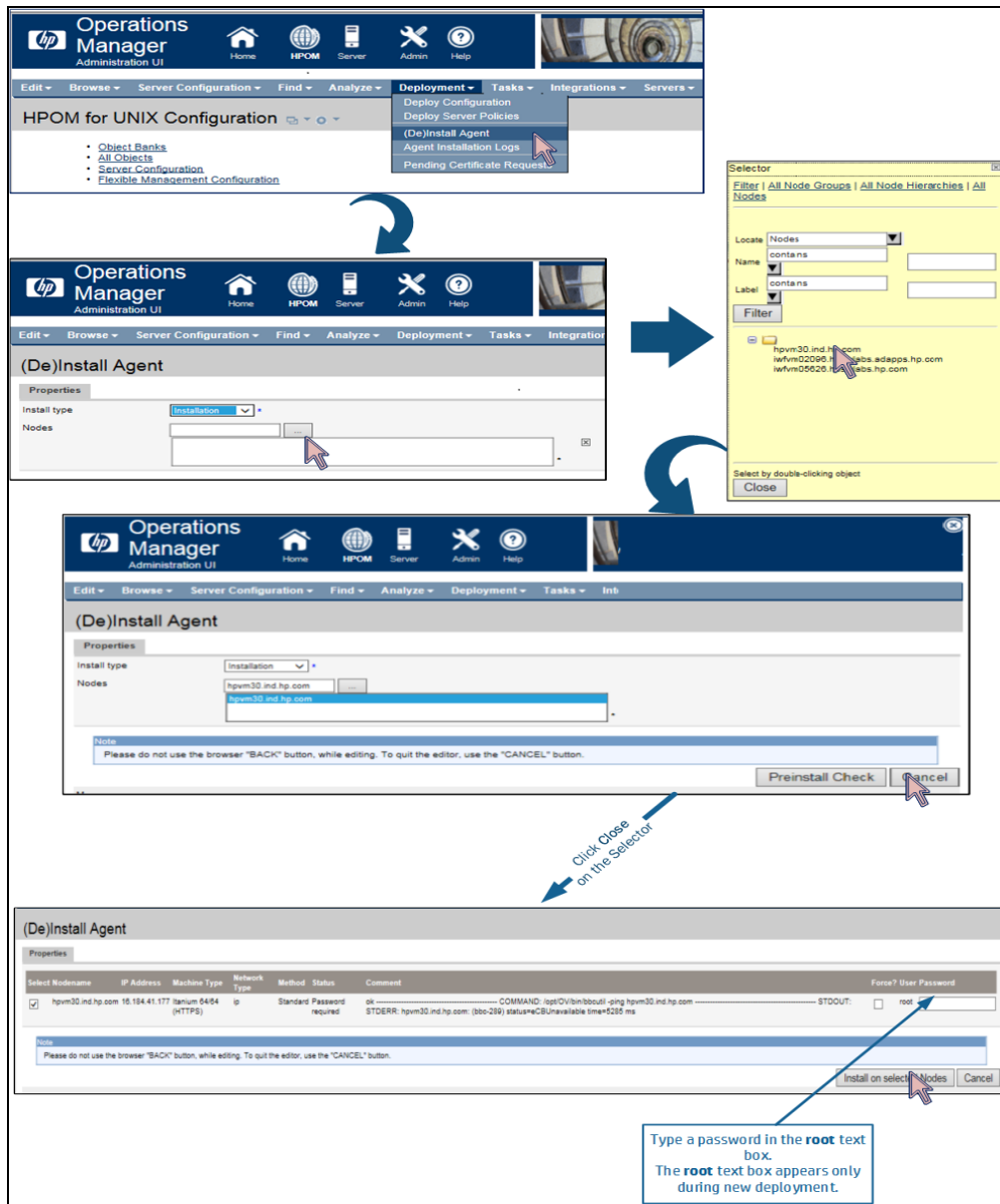


**Scenario 2:** If the HPE Operations Agent 12.02 is already installed on a node, follow the steps to install patches and hotfixes:



**Installing the HPE Operations Agent from HPOM for UNIX Management Server**

**Scenario:** If the HPE Operations Agent 12.02 is not installed on a node, follow the steps to install base version, patches and hotfixes:



## Single Depot for HP-UX Installation

With HPE Operations Agent 12.01 you can use single depot package to install the HPE Operations Agent on HP-UX nodes. Follow the steps:

### Prerequisite

For HP-UX IA, install the following patch on the node: qpkbase for HP-UX B.11.31.1309.397 (or superseding patch). See the [Prerequisites for HP-UX](#) section for more information.

1. Download the single depot package **HPOAConsolidatedpkg.depot** from the media.
2. Use the `swinstall` command to install the HPE Operations Agent.

**For example:**

```
swinstall -x mount_all_filesystems=false -x write_remote_files=true -s  
<single depot directory path>/HPOAConsolidatedpkg.depot
```

## Co-existence of HPE Operations Agent with other HPE products

If you want to install or upgrade HPE Operations Agent on a system where other HPE products are running, make sure you stop all the processes of HPE products before you install or upgrade HPE Operations Agent. Restart the processes only after installation or upgrade is complete.

## Installing the HPE Operations Agent on Platforms with Limitation

To install the HPE Operations Agent 12.02 remotely from the HPOM for Windows or UNIX console on platforms with limitation, you must set the variable `MINPRECHECK` to `True` in the profile file. Add the following content in the profile file:

```
set nonXPL.config:MINPRECHECK=True
```

For more information, see [Installing the HPE Operations Agent on Platforms with Limitation](#).

For more details on platforms with limitation, see the HPE Operations Agent *Support Matrix document*.

## Enabling Secure Communication

To enable secure communication without allowing inbound traffic to the Communication Broker port, you must configure a reverse channel proxy (RCP).

Follow the steps to configure a RCP:

1. On a RCP node set the following configurations to enable RCP on a specific port number:

```
[bbc.rcp]
```

```
SERVER_PORT=<port number>
```

2. On the HPOM Management Server present in the trusted zone, set the following configurations to open an Reverse Admin Channel (RAC):

```
[bbc.cb]
```

```
RC_CHANNELS=<RCP node name>:<port number>
```

```
ENABLE_REVERSE_ADMIN_CHANNELS=True
```

3. On a RCP node, set the following to enable RCP on a specific port number:

```
[bbc.rcp]
```

```
SERVER_PORT=<port number>
```

4. On the HPE Operations Agent nodes present in the untrusted zone, set the following configurations to enable communication through RCP:

```
[bbc.http]
```

```
PROXY=<RCP node name>:<port number>+(<nodes to be included>)-(<Nodes to be excluded>)
```

#### For example:

1. On myserver.serverdomain.com set the following configurations:

```
[bbc.cb]
```

```
RC_CHANNELS=myrcp.mydomain.com:1025
```

```
ENABLE_REVERSE_ADMIN_CHANNELS=True
```

2. On myrcp.mydomain.com set the following:

```
[bbc.rcp]
```

```
SERVER_PORT=1025
```

3. On myagent.mydomain.com set the following:

```
[bbc.http]
```

```
PROXY=myrcp.mydomain.com:1025+(*)-  
(myrcp.mydomain.com,myrcp,myagent.mydomain.com,myagent)
```

In this instance:

- myserver.serverdomain.com is the HPOM Management server
- myrcp.mydomain.com is the Reverse Channel Proxy node
- myagent.mydomain.com is the HP Operations Agent node
- \* specifies that all nodes must be included

For more information, see [Introduction to the Reverse Channel Proxy](#).

On the RCP system, register ovbbcrp with ovc so that this process is started, stopped, and monitored by ovc .

**For example:**

**On Windows**

```
cd "c:\program files\hp openview\newconfig\dataDir\conf\bbc"
"c:\program files\hp openview\bin\ovcreg" -add ovbbcrp.xml
```

**On HP-UX/Linux/Solaris**

```
/opt/OV/bin/ovcreg -add \ /opt/OV/newconfig/DataDir/conf/bbc/ovbbcrp.xml
```

## Planning the Installation of HPE Operations Agent

### Installing the HPE Operations Agent Remotely from the HPOM Management Server

In a centralized monitoring environment with HPOM, you can register the deployment packages for the HPE Operations Agent 12.02 on the Management Server, and then centrally deploy the agent packages on different nodes from the HPOM console.

This process involves:

1. Install the HPE Operations Agent 12.02 on the HPOM management server.
2. Registering the HPE Operations Agent 12.02 deployment packages on the HPOM management server.

**Tip:** A registration process ensures that the HPE Operations Agent deployment package is placed in the appropriate location on the deployment server (a server from which you can deploy the agent on nodes).

The process of registering the HPE Operations Agent deployment packages automatically installs the Infrastructure SPIs on the HPOM server. You can configure the installer to skip the installation of the Infrastructure SPIs.

3. Installing the HPE Operations Agent centrally from the HPOM console.

### **Installing the HPE Operations Agent Manually on the Node**

You can install the HPE Operations Agent from the *HPE Operations Agent and Infrastructure SPIs 12.02* media by manually logging on to the managed node.

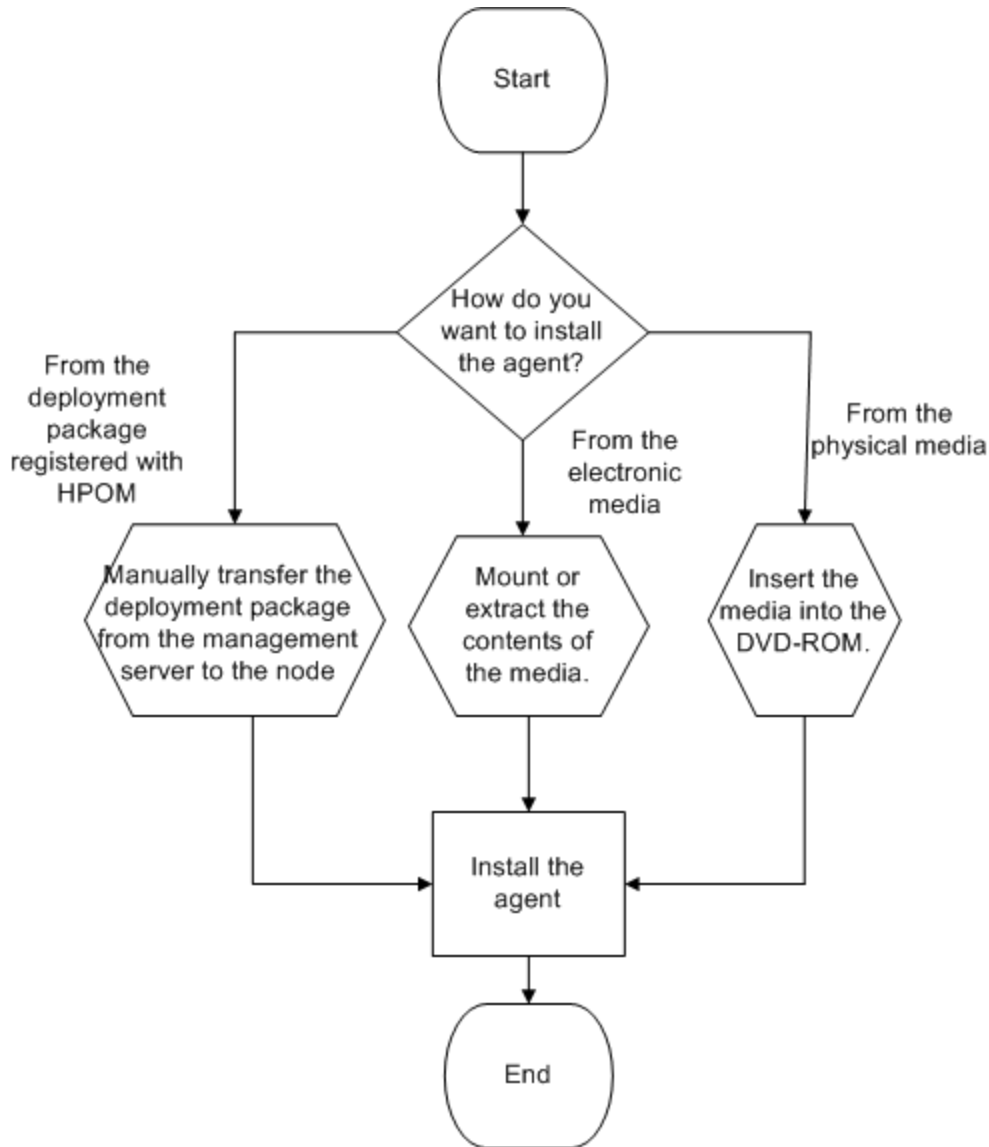
This process involves:

1. Preparing the node

You can prepare a managed node for the agent installation by doing one of the following:

- Insert the *HPE Operations Agent and Infrastructure SPIs 12.02* physical media to the DVD drive.
  - Extract the contents of the *HPE Operations Agent and Infrastructure SPIs 12.02* electronic media into a local directory.
  - Mount the *HPE Operations Agent and Infrastructure SPIs 12.02* physical media.
  - Transfer the deployment package manually from the HPOM management server.
2. Install the agent with the installer program (`oainstall` or `oasetup`) available with the *HPE Operations Agent and Infrastructure SPIs 12.02* media or the deployment package.





### Installing the Infrastructure SPIs

You can install only the Infrastructure SPIs on the HPOM management server by using the *HPE Operations Agent and Infrastructure SPIs 12.02*.

This process involves:

1. Preparing a configuration file on the HPOM management server.
2. Installing the Infrastructure SPIs with the installer program (`oainstall` or `oasetup`) available with the *HPE Operations Agent and Infrastructure SPIs 12.02* media.

## Chapter 2: Connecting the HPE Operations Agent to OMi

HPE Operations Manager i (OMi) is the event management foundation for a complete Business Service Management (BSM) monitoring solution. You can integrate HPE Operations Agent with OMi. HPE Operations Agent can send alerts or events to OMi.

### Connecting a New HPE Operations Agent Installation to OMi

HPE Operations Agent is available on the HPE Operations Agent media DVD, which is included in the OMi media kit. The latest HPE Operations Agent updates can be downloaded from HPE Software Support <http://h20230.www2.hp.com/selfsolve/patches>.

After the installation of the HPE Operations Agent software on the system to be monitored, you must connect the agent to OMi and then grant the agent's certificate request in OMi.

To connect HPE Operations Agent to OMi, follow these steps:

1. Install the HPE Operations Agent on the system that you want to monitor.
2. Run the following command:

**On Windows:** `<OvInstallBinDir>OpC\install cscript opcactivate.vbs -srv <BGateway_Server>`

**On Unix:** `<OvInstallBinDir>OpC/install opcactivate -srv <Gateway_Server>`

3. Log on to OMi server, open the Certificate Requests manager and accept the new certificate request:

**Administration > Setup and Maintenance > Certificate Requests**

4. To verify, check the HTTPS communication in both directions using the following command:

```
bbcutil -ping https://<FQDN>
```

If the connection is successful, the command returns `status=eServiceOK`.

Once the communication between the HPE Operations Agent and the OMi server is established and the HPE Operations Agent processes are running, HPE Operations Agent sends alerts or events to OMi, which you can view in the **Event Browser** of OMi server.

For more information, see *Connecting a New HPE Operations Agent Installation* in the *OMi Administration Guide*.

## Connecting an Existing HPE Operations Agent to OMi

HPE Operations Agents that are already connected to HP Operations Manager (HPOM) can be configured to send events to OMi, run actions, and accept policies from OMi if HPOM is integrated with OMi.

HPOM management server forwards all events (referred to as messages in HPOM) to OMi based on a flexible management policy. Instruction and action execution requests sent from the OMi server are executed on the HPOM server.

You can also connect HPOM managed nodes directly to OMi and configure the agents to accept policies and action execution requests from OMi.

**Note:** You can also switch the HPE Operations Agent management from the OMi server to the HPOM management server.

For more information, see *Connecting an Existing HPE Operations Agent Installation* in the *OMi Administration Guide*.

## Updating the HPE Operations Agent Installation from OMi

You can update the HPE Operations Agent that is currently installed on a monitored node to a hotfix, patch or new base version remotely from the HPE Operations Manager i (OMi) server.

**Note:** After you have updated an HPE Operations Agent, it cannot be reverted to the previous version.

Before you can update the HPE Operations Agent software, you must obtain the updated agent packages and upload them to the OMi database using the `opr-package-manager` [command-line interface](#).

To update the HPE Operations Agent installed on a monitored node from OMi server, follow these steps:

1. Log on to the HPE Operations Manager i (OMi) server.
2. Open the **Monitored Nodes** page on the OMi UI:  
**Administration > Setup and Maintenance > Monitored Nodes.**
3. In the **Node Views** browser in the **Monitored Nodes** page, select the required node.
4. Refresh the agent version of the node by **Synchronizing** the installed packages information with the server to determine whether an update is necessary.
5. Select the node you want to install the update and click **Update Operations Agent** icon. To update multiple nodes in parallel, hold down the `Ctrl` or `Shift` key while selecting them. Then click **Update Operations Agent** icon.

The **Update Operations Agent** dialog box opens.

6. Select the version to which you want to update the agent installation:
  - **Update to Latest Hotfixes** installs the hotfixes that are available on the server and that apply to the agent version installed on the monitored node.
  - **Update to Latest Version** installs the latest patch or base version on the monitored node.
  - **Update to Specific Version** enables you to select the version to install on the monitored node.

If you select the current version, then the hotfixes for that version are installed. This option is only available when the selected monitored nodes can be updated to a common version. If a node already has a later version than the target version, the option is disabled.

OMi creates a deployment job for each update task.

7. You can track the progress of the update by monitoring the corresponding deployment job:

**Administration > Monitoring > Deployment Jobs**

8. In the **Monitored Nodes** page, click **Refresh** to update the information displayed.

For more information, see *Updating HPE Operations Agent Installation* in the *OMi Administration Guide*.

## opr-package-manager Command-Line Interface

You can use the `opr-package-manager` command-line interface (CLI) to upload HPE Operations Agent deployment packages to OMi database.

### Prerequisites

- Obtain the HPE Operations Agent deployment packages.
- To run the `opr-package-manager` successfully, the OMi server processes must be running.

A deployment package usually contains a number of subpackages that make up the agent software. A package is defined by a descriptor file. The descriptor file contains the following information:

- Descriptive information about the package.
- Name of the installer.
- List of files and packages included in the package.

### Location

```
<OMi_HOME>/opr/bin/opr-package-manager[.bat|.sh]
```

You can run `opr-package-manager` on a gateway or a data processing server. The server processes must be running.

### Synopsis

```
opr-package-manager [<authentication>] {<operation> | <target>}
```

- *Syntax for <authentication>*

```
{-username <userName> -password <password>}
```

Option	Description
{-username   -user <username>}	Sets the username to be used to execute the CLI operations on the target gateway server to <username>.
{-password   -pw <password>}	Uses the password <password> for user <username>, which is used to execute the CLI operations on the target gateway server.  Default value of <password>: empty string

- *Syntax for <operation>*

```
{-list_packages [<package_name>] [-format|-f [xml|json]]}
{-upload_packages [<descriptor_file>] [-input <package_directory>] [-platform
<HP-UX/SOL/AIX/LIN/WIN/ALL>]}
{-deploy_package <package_name> -deploy_mode [NEWEST|CURRENT|VERSION -package_ID
<package_ID>|PACKAGE -package_ID <package_ID>]}
{-delete_package <package_name>}
{-delete_package_version <package_name> <package_version>}
```

Option	Description
-list_packages	<p>Lists details of all deployment packages that exist in the OMi database. To list details of a specific package, specify the package name.</p> <p>The output can be in XML or JSON format. The default is XML. To view the output more easily, redirect it to a file and then view the XML content in any of the major browsers.</p>
-upload_packages	<p>Uploads the deployment package specified by the descriptor file. If you do not specify a package, <code>opr -package-</code> manager uploads the default package <code>Operations-agent</code>.</p> <p>The <code>-input</code> option specifies a directory of deployment packages. The tool processes all directories and sub-directories and uploads all deployment packages that contain the specified descriptor file.</p> <p>The <code>-platform</code> option defines a filter to upload deployment packages for a specific platform only (for example, <code>WIN</code> uploads deployment packages for Windows only. Possible values are: <code>HP-UX</code>, <code>SOL</code>, <code>AIX</code>, <code>LIN</code>, <code>WIN</code>, <code>ALL</code>).</p>
-deploy_package	<p>Deploys the deployment package with the specified name.</p> <p>The <code>-deploy_mode</code> option defines how the installed packages are updated; for example, <code>NEWEST</code> deploys the newest version that is available on the server. Possible values are:</p> <ul style="list-style-type: none"> <li>◦ <code>NEWEST</code> updates to latest available version.</li> <li>◦ <code>CURRENT</code> updates to the latest hotfix version of the currently installed version.</li> <li>◦ <code>VERSION</code> updates to the given version.</li> <li>◦ <code>PACKAGE</code> updates to the given package ID.</li> </ul> <p>The <code>-package_ID</code> option is required for the <code>VERSION</code> and <code>PACKAGE</code> deployment modes. It specifies the package identifier. This can be the deployment binary ID or the package version, for example <code>11.14.005</code>.</p> <p><b>Tip:</b> Use the <code>-list_packages</code> option to retrieve the deployment binary ID.</p>

-delete_package	Deletes the deployment package. The package is only deleted from the OMi database, not from any monitored nodes. The package can no longer be deployed after it has been removed.
-delete_package_version	Deletes the deployment package with the specified version. The package is only deleted from the OMi database, not from any monitored nodes. The package can no longer be deployed after it is removed.

- **Syntax for <target>**

-query\_name <query\_name> | -view\_name <view\_name> | -filter\_name <filter\_name> |  
 - node\_list <node\_list> [-dont\_check\_database] | -node\_group <node\_group> | -all

Option	Description
-query_name <query_name>	Performs the operation on monitored nodes selected by the specified TQL query.
-view_name <view_name>	Performs the operation on monitored nodes selected by the specified view.
-filter_name <filter_name>	Performs the operation on a list of monitored nodes with the HPE Operations Agent installed that was obtained by applying the node filter.
- node_list <node_list> [-dont_check_database]	<p>Performs the operation on a list of one or more monitored nodes. The nodes must exist in the RTSM and must be associated with a CI of the type om_operations_agent.</p> <p>Separate multiple nodes with commas (for example, node1.example.com,node2.example.com).</p> <p>If used with the -dont_check_database option, the operation on the nodes is performed without checking if the nodes exist in the RTSM.</p>
-node_group <node_group>	<p>Performs the operation on a group of monitored nodes. A node groups is a CI collection containing hosts. Node groups can be maintained in the Monitoring Automation Node Editor or they can be imported through topology synchronization from HPOM to OMi.</p> <p>The nodes must exist in the RTSM and be associated with a CI of the type om_operations_agent.</p> <p>Specify node groups by their names or their paths (the latter applies to hierarchical node groups imported from HPOM for Windows).</p>
-all	Performs the operation on all monitored nodes that have the HPE Operations Agent installed (that is, nodes that are associated with a CI of the type om_operations_agent).

**Examples**

This section shows a number of examples you can use as a starting point for developing your own `opr-package-manager` commands.

- List all available deployment packages:

```
opr-package-manager -username myU -password myPwd -list_packages > allpkg.xml
```

- Recursively upload the HPE Operations Agent deployment packages for all platforms (starting from the current working directory):

```
opr-package-manager -username myU -password myPwd -upload_packages
```

- Upload the HPE Operations Agent deployment packages for Windows monitored nodes from the file system:

```
opr-package-manager -username myU -password myPwd -upload_packages
c:\Agent\OVOAgent.xml -input c:\Agent\packages\ -platform WIN
```

- Deploy the HPE Operations Agent deployment package version 12.00.078 to the nodes `node1.example.com` and `node2.example.com`:

```
opr-package-manager -username myU -password myPwd -deploy_package
Operationsagent -deploy_mode VERSION -package_ID 12.00.078 -node_list
"node1.example.com,node2.example.com"
```

- Deploy the latest hotfix for the HPE Operations Agent to all nodes selected by the TQL query `All_CIs_with_OM_Agents_Unix`:

```
opr-package-manager -username myU -password myPwd -deploy_package
Operationsagent -deploy_mode CURRENT -query_name All_CIs_with_OM_Agents_Unix
```

- Delete the HPE Operations Agent deployment package from the database:

```
opr-package-manager -username myU -password myPwd -delete_package
Operationsagent
```

- Delete the HPE Operations Agent deployment package version 12.00.078 from the database:

```
opr-package-manager -username myU -password myPwd -delete_package_version
Operationsagent 12.00.078
```

### ***opr-package-manager* Log File**

`opr-package-manager` logs information to the following log file:

```
<OMi_HOME>/log/opr-clis.log
```

For more information on using the `opr-package-manager` command-line interface and uploading the HPE Operations Agent deployment packages to OMi, see the *OMi Administration Guide*.



# Chapter 3: Registering the HPE Operations Agent and Infrastructure SPIs on the HPOM Management Server (and Installing the Infrastructure SPIs)

## Registering the HPOM for Windows Management Server

### *Prerequisites*

No deployment jobs must run at the time of registering the deployment package.

Follow the steps to view the active deployment jobs:

1. In the console tree, expand the Policy Management.
  2. Click **Deployment Jobs**. The details pane shows the list of active deployment jobs. You must make sure that none of the deployment jobs are active at the time of installing the agent deployment packages. You must not start any deployment jobs until the agent deployment package registration is complete.
- If the HP Performance Agent 4.70 deployable for Windows or UNIX/Linux is available on the management server, you must either install the HP Performance Agent 4.72 deployable or remove the HP Performance Agent 4.70 deployable completely before registering the deployment packages for the HPE Operations Agent 12.02. You can remove the deployable packages using the **Control Panel**.
  - Disk space: 1 GB
  - The `oainstall` program installs the Infrastructure SPIs on the management server while registering the deployment package. If you want to install the Infrastructure SPIs, make sure the system meets the following additional requirements:

### **Hardware and Software Requirements**

For a list of supported hardware, operating systems, 12.02 version, and agent version, see the *Support Matrix*.

### Disk Space Requirements

Temporary Directory <sup>a</sup>	Total Disk Space
%tmp% - 15 MB	90 MB

<sup>a</sup>The disk space for the temporary directory/drive is required only during installation. These are approximate values.

### Upgrade Requirements

You can directly upgrade the Infrastructure SPIs version 2.00 or later to the version 12.02.

You must install the HPE Operations Agent 12.02 on the Management Server to be able to register the deployment packages. For more information about upgrading the HPE Operations Agent, see "[Upgrade Notes](#)".

### ***Register the Deployment Package***

In addition to registering the deployment package for the HPE Operations Agent, the `oainstall` script can install the Infrastructure SPIs on the Management Server.

However, the capability to install the Infrastructure SPIs is available only with the physical DVD or the electronic media that contains agent packages for all node platforms. Platform-specific media does not include the Infrastructure SPIs.

Choose one of the following tasks based on your requirement:

- "[Register the HPE Operations Agent deployment packages for all platforms and install the Infrastructure SPIs.](#)" on the next page
- "[Register the HPE Operations Agent deployment package for a specific node platform by using a platform-specific ISO file.](#)" on the next page
- "[Register the HPE Operations Agent deployment packages for all platforms, and install the Infrastructure SPIs, but do not install the graph or report package.](#)" on the next page
- "[Register the HPE Operations Agent deployment packages for all platforms, but do not install the Infrastructure SPIs.](#)" on page 28
- "[Register the HPE Operations Agent deployment packages for selected platforms and install the Infrastructure SPIs](#)" on page 28

## Registering the Deployment Package

Task	Follow these steps
<p>Register the HPE Operations Agent deployment packages for all platforms and install the Infrastructure SPIs.</p>	<ol style="list-style-type: none"> <li>1. Make sure that you have downloaded the ISO file for all platforms or obtained the physical DVD.</li> <li>2. Log on to the management server as administrator.</li> <li>3. Go to the media root.</li> <li>4. Run the following command: <b>cscript oainstall.vbs -i -m</b></li> <li>5. Verify the registration process.</li> </ol>
<p>Register the HPE Operations Agent deployment package for a specific node platform by using a platform-specific ISO file.</p>	<ol style="list-style-type: none"> <li>1. Make sure that you downloaded the .ISO file for the node platform of your choice.</li> <li>2. Log on to the Management Server as administrator.</li> <li>3. Go to the media root.</li> <li>4. Run the following command: <b>cscript oainstall.vbs -i -m</b></li> <li>5. Verify the registration process.</li> </ol>
<p>Register the HPE Operations Agent deployment packages for all platforms, and install the Infrastructure SPIs, but do not install the graph or report package.</p>	<ol style="list-style-type: none"> <li>1. Make sure that you downloaded the .ISO file for all platforms or obtained the physical DVD.</li> <li>2. Log on to the management server as administrator.</li> <li>3. Create a new file using a text editor.</li> <li>4. Add the following content:   <pre>[agent.parameter]  REGISTER_AGENT=YES  [hpinfraspi.parameter]  InfraSPI=YES  InfraSPI_With_Graphs=NO  InfraSPI_With_Reports=NO</pre> <p><b>Note:</b> If you want to install the graph package and report package, set the <code>InfraSPI_With_Graphs</code> and <code>InfraSPI_With_Reports</code> properties to YES else set it to NO.</p> </li> <li>5. Save the file.</li> <li>6. Go to the media root.</li> </ol>

**Registering the Deployment Package, continued**

Task	Follow these steps
	<p>7. From the media root, run the following command:</p> <p><b>cscript oainstall.vbs -i -m -spiconfig &lt;file_name&gt;</b></p> <p>In this instance, &lt;file_name&gt; is the name of the file that you created in <a href="#">step 3</a> (with complete path).</p> <p>The command registers the agent deployment packages for all platforms on the management server and installs the Infrastructure SPIs, but skips the installation of the graphs and reports packages for the Infrastructure SPIs.</p>
<p>Register the HPE Operations Agent deployment packages for all platforms, but do not install the Infrastructure SPIs.</p>	<ol style="list-style-type: none"> <li>1. Make sure that you downloaded the .ISO file for all platforms or obtained the physical DVD.</li> <li>2. Log on to the management server as administrator.</li> <li>3. Create a new file with a text editor.</li> <li>4. Add the following content:           <pre>[agent.parameter]  REGISTER_AGENT=YES  [hpinfraspi.parameter]  InfraSPI=NO  InfraSPI_With_Graphs=NO  InfraSPI_With_Reports=NO</pre> </li> <li>5. Save the file.</li> <li>6. Go to the media root.</li> <li>7. From the media root, run the following command:           <p><b>cscript oainstall.vbs -i -m -spiconfig &lt;file_name with complete path&gt;</b></p> <p>In this instance, &lt;file_name&gt; is the name of the file that you created in <a href="#">step 3</a> (with complete path).</p> <p>The command registers the agent deployment packages for all platforms on the management server, but skips the installation of the Infrastructure SPIs.</p> </li> </ol>
<p>Register the HPE Operations Agent deployment packages for selected platforms and install the Infrastructure SPIs</p>	<ol style="list-style-type: none"> <li>1. Make sure that you downloaded the .ISO file for all platforms or obtained the physical DVD.</li> <li>2. Log on to the management server as administrator.</li> </ol>

## Registering the Deployment Package, continued

Task	Follow these steps
	<ol style="list-style-type: none"> <li>3. Create a new file with a text editor.</li> <li>4. Add the following content:           <pre data-bbox="764 432 1000 464">[agent.parameter]</pre> <pre data-bbox="764 520 1016 552">REGISTER_AGENT=YES</pre> <pre data-bbox="764 573 1068 604">[hpinfraspi.parameter]</pre> <pre data-bbox="764 625 932 657">InfraSPI=YES</pre> <pre data-bbox="764 678 1057 709">InfraSPI_With_Graphs=</pre> <pre data-bbox="764 730 1068 762">InfraSPI_With_Reports=</pre> <div data-bbox="764 789 1357 930" style="border-left: 2px solid black; padding-left: 10px;"> <p><b>Note:</b> Depending on whether you want to skip the installation of the graph or report packages, set the <code>InfraSPI_With_Graphs</code> and <code>InfraSPI_With_Reports</code> properties to YES or NO.</p> </div> </li> <li>5. Save the file.</li> <li>6. Go to the media root.</li> <li>7. From the media root, run the following command:           <pre data-bbox="764 1104 1373 1167"><b>cscript oainstall.vbs -i -m -p &lt;platform&gt; -spiconfig &lt;file_name&gt;</b></pre> <p data-bbox="764 1188 1369 1323">In this instance, <code>&lt;file_name&gt;</code> is the name of the file that you created in <a href="#">step 3</a> (with complete path); <code>&lt;platform&gt;</code> is the node platform for which you want to register the deployment package.</p> <p data-bbox="764 1344 1219 1375">Use the following values for <code>&lt;platform&gt;</code>:</p> <p data-bbox="764 1396 984 1428"><i>For Windows:</i> WIN</p> <p data-bbox="764 1449 992 1480"><i>For HP-UX:</i> HP-UX</p> <p data-bbox="764 1501 927 1533"><i>For Linux:</i> LIN</p> <p data-bbox="764 1554 954 1585"><i>For Solaris:</i> SOL</p> <p data-bbox="764 1606 911 1638"><i>For AIX:</i> AIX</p> <p data-bbox="764 1659 1330 1793">The command registers the agent deployment packages for the specific platforms on the management server and installs the Infrastructure SPIs.</p> <p data-bbox="764 1814 1330 1877">You can specify multiple platforms in a single command line. For example, to install deployment</p> </li> </ol>

**Registering the Deployment Package, continued**

Task	Follow these steps
	packages for AIX and Solaris: <b>cscript oainstall.vbs -i -m -p AIX -p SOL</b>

**Note:** After installation, see [Install Report and Graph Packages on a Remote Server](#) if you want to install report or graph packages on a remote server.

*When HPOM is in a High-Availability (HA) Cluster*

Follow the above steps on the active node in the HPOM High-Availability (HA) cluster:

After completing the steps, perform the following steps:

1. Fail over to the active node.
2. Go to the %OvShareDir%server\installation directory.
3. Run the following command:

**cscript oainstall\_sync.vbs**

After you run the installation command, the registration procedure begins. Depending on number of selected packages, the registration process may take up to 20 minutes to complete.

**Verification**

1. On the Management Server, go to the following location:

On HPOM for Windows Management Server version 8.xx:

```
%ovinstalldir%bin\OpC\agtinstall
```

On HPOM for Windows Management Server version 9.xx:

```
%ovinstalldir%bin\win64\OpC\agtinstall
```

2. Run the following command:

**cscript oainstall.vbs -inv -listall**

The command shows the list of available (active) deployment packages on the management server.

To check that the Infrastructure SPIs are installed, run the command with the `-includespi` option.

**cscript oainstall.vbs -inv -includespi -listall**

3. Locate the platform for which you installed the deployment package. If the active version is displayed as 12.02, as in the following figure, the registration is successful.

### Log File

The registration log file (oainstall.log) is available in the following directory:

```
%OvDataDir%shared\server\log
```

### Placement of Packages

When you register the HPE Operations Agent packages on the management server, the oainstall program places all necessary deployment packages into the following directory:

```
%OvDataDir%shared\Packages\HTTPS
```

### Backup of Deployment Packages

When you register the deployment packages on the management server, the oainstall script saves a copy of the older deployment packages into the following local directory:

```
%OvShareDir%server\installation\backup\HPOpsAgt\<OS>\<OA_Version>\<ARCH>
```

To view the active deployment packages, run the following command:

```
cscript oainstall.vbs -inv
```

To view all deployment packages (active and backed-up) on the system, run the following command:

```
cscript oainstall.vbs -inv -listall
```

To check that the Infrastructure SPIs are installed, run the command with the **-includespi** option.

```
cscript oainstall.vbs -inv -includespi -listall
```

### Alternate Backup Location

When the default backup location does not have sufficient space to accommodate the backed up deployment packages, you can configure the system to use an alternate backup location.

Run the following command on the management server to use a non-default location to back up the old deployment package:

```
ovconfchg -ovrg server -ns eaagt.server -set OPC_BACKUP_DIR <directory>
```

In this instance, <directory> is the location on your system where you can back up the old deployment packages.

The log file (oainstall.log) created during the installation of deployment packages, is placed inside the backup directory.

# Registering the HPOM on UNIX/Linux Management Server

## Register the Deployment Package on the HPOM Management Server

### Prerequisites

- Disk space: 1 GB
- The `oainstall` program installs the Infrastructure SPIs on the management server while registering the deployment package. If you want to install the Infrastructure SPIs, make sure the system meets the following additional requirements:

### Hardware and Software Requirements

For a list of supported hardware, operating systems, HPOM version, and agent version, see the *Support Matrix*.

### Disk Space Requirements

Operating System on the HPOM Management Server	Temporary Directory <sup>a</sup>	Total Disk Space
Linux	/tmp - 35 MB	90 MB
HP-UX	/tmp - 17 MB	240 MB
Solaris	/tmp - 35 MB	80 MB

<sup>a</sup>The disk space for the temporary directory/drive is required only during installation. These are approximate values.

### Upgrade Requirements

You can directly upgrade the Infrastructure SPIs version 2.00 or above to the version 12.02.

You must install the HPE Operations Agent 12.02 on the management server to be able to register the deployment packages.

### Register the Deployment Package

In addition to registering the deployment package for the HPE Operations Agent, the `oainstall` script can install the Infrastructure SPIs on the management server.



However, the capability to install the Infrastructure SPIs is available only with the physical DVD or the electronic media that contains agent packages for all node platforms. Platform-specific media does not include the Infrastructure SPIs.

Choose one of the following tasks based on your requirement:

- Register deployment packages for all platforms and install the Infrastructure SPIs
- Register the deployment package for a specific node platform by using a platform-specific .ISO file
- Register deployment packages for all platforms and install the Infrastructure SPIs without the graph or report package
- Register deployment packages for all platforms, but do not install the Infrastructure SPIs
- Register the HPE Operations Agent deployment packages for select platforms and install the Infrastructure SPIs
- "Register the deployment packages and install the health view package."

### Registering the Deployment Package

Task	Follow these steps
Register the HPE Operations Agent deployment packages for all platforms and install the Infrastructure SPIs.	<ol style="list-style-type: none"> <li>1. Make sure that you downloaded the .ISO file for all platforms or obtained the physical DVD.</li> <li>2. Log on to the management server as root.</li> <li>3. Go to the media root.</li> <li>4. Run the following command: <code>./oainstall.sh -i -m</code></li> <li>5. Verify the registration process.</li> </ol>
Register the HPE Operations Agent deployment package for a specific node platform by using a platform-specific ISO file.	<ol style="list-style-type: none"> <li>1. Make sure that you downloaded the .ISO file for the node platform of your choice.</li> <li>2. Log on to the management server as root.</li> <li>3. Go to the media root.</li> <li>4. Run the following command: <code>./oainstall.sh -i -m</code></li> <li>5. Verify the registration process.</li> </ol>
Register the HPE Operations Agent deployment packages for all platforms, and install the Infrastructure SPIs, but do not install the graph package.	<ol style="list-style-type: none"> <li>1. Make sure that you downloaded the .ISO file for all platforms or obtained the physical DVD.</li> <li>2. Log on to the management server as root.</li> <li>3. Create a new file with a text editor.</li> <li>4. Add the following content:</li> </ol>

**Registering the Deployment Package, continued**

Task	Follow these steps
	<pre data-bbox="771 325 1006 357">[agent.parameter]</pre> <pre data-bbox="771 415 1023 447">REGISTER_AGENT=YES</pre> <pre data-bbox="771 468 1076 499">[hpinfraspi.parameter]</pre> <pre data-bbox="771 520 938 552">InfraSPI=Yes</pre> <pre data-bbox="771 573 1092 604">InfraSPI_With_Graphs=NO</pre> <ol data-bbox="727 625 1323 751" style="list-style-type: none"> <li>5. Save the file.</li> <li>6. Go to the media root.</li> <li>7. From the media root, run the following command:</li> </ol> <pre data-bbox="771 772 1372 804">./oainstall.sh -i -m -spiconfig &lt;file_name&gt;</pre> <p data-bbox="771 825 1356 888">In this instance, <i>&lt;file_name&gt;</i> is the name of the file that you created in <a href="#">step 3</a> (with complete path).</p> <p data-bbox="771 909 1372 1077">The command registers the agent deployment packages for all platforms on the management server and installs the Infrastructure SPIs, but skips the installation of the graph package for Infrastructure SPIs.</p>
Register the HPE Operations Agent deployment packages for all platforms, but do not install the Infrastructure SPIs.	<ol data-bbox="727 1102 1339 1312" style="list-style-type: none"> <li>1. Make sure that you downloaded the .ISO file for all platforms or obtained the physical DVD.</li> <li>2. Log on to the management server as root.</li> <li>3. Create a new file with a text editor.</li> <li>4. Add the following content:</li> </ol> <pre data-bbox="771 1333 1006 1365">[agent.parameter]</pre> <pre data-bbox="771 1423 1023 1455">REGISTER_AGENT=YES</pre> <pre data-bbox="771 1476 1076 1507">[hpinfraspi.parameter]</pre> <pre data-bbox="771 1528 925 1560">InfraSPI=NO</pre> <pre data-bbox="771 1581 1109 1612">InfraSPI_With_Reports=NO</pre> <pre data-bbox="771 1633 1092 1665">InfraSPI_With_Graphs=NO</pre> <ol data-bbox="727 1686 1323 1812" style="list-style-type: none"> <li>5. Save the file.</li> <li>6. Go to the media root.</li> <li>7. From the media root, run the following command:</li> </ol> <pre data-bbox="771 1833 1356 1864">./oainstall.sh -i -m -spiconfig &lt;file_name</pre>

## Registering the Deployment Package, continued

Task	Follow these steps
	<p>with complete path&gt;</p> <p>In this instance, <i>&lt;file_name&gt;</i> is the name of the file that you created in <a href="#">step 3</a> (with complete path).</p> <p>The command registers the agent deployment packages for all platforms on the management server, but skips the installation of the Infrastructure SPIs.</p>
<p>Register the HPE Operations Agent deployment packages for select platforms and install the Infrastructure SPIs</p>	<ol style="list-style-type: none"> <li>1. Make sure that you downloaded the .ISO file for all platforms or obtained the physical DVD.</li> <li>2. Log on to the management server as root.</li> <li>3. Create a new file with a text editor.</li> <li>4. Add the following content: <p>[agent.parameter]</p> <p>REGISTER_AGENT=YES</p> <p>[hpinfraspi.parameter]</p> <p>InfraSPI=YES</p> <p>InfraSPI_With_Graphs=</p> <p><b>Note:</b> If you want to skip the installation of the graph packages, set the <code>InfraSPI_With_Graphs</code> property to NO else set it to YES.</p> </li> <li>5. Set the <code>InfraSPI_With_Graphs</code> property to YES or NO depending on whether you want to skip the installation of the graph packages.</li> <li>6. Save the file.</li> <li>7. Go to the media root.</li> <li>8. From the media root, run the following command: <pre>./oainstall.sh -i -m -p &lt;platform&gt; -spiconfig &lt;file_name&gt;</pre> <p>In this instance, <i>&lt;file_name&gt;</i> is the name of the file that you created in <a href="#">step 3</a> (with complete path); <i>&lt;platform&gt;</i> is the node platform for which you want to register the deployment package.</p> <p>Use the following values for <i>&lt;platform&gt;</i>:</p> <p><i>For Windows:</i> WIN</p> </li> </ol>

## Registering the Deployment Package, continued

Task	Follow these steps
	<p><i>For HP-UX:</i> HP-UX</p> <p><i>For Linux:</i> LIN</p> <p><i>For Solaris:</i> SOL</p> <p><i>For AIX:</i> AIX</p> <p>The command registers the agent deployment packages for specified platforms on the management server and installs the Infrastructure SPIs.</p> <p>You can specify multiple platforms in a single command line. For example, to install deployment packages for AIX and Solaris:</p> <pre>./oainstall.sh -i -m -p AIX -p SOL</pre>
<p>Register the HPE Operations Agent deployment packages and install the health view package.</p>	<ol style="list-style-type: none"> <li>1. Make sure that you have downloaded the .ISO file or obtained the physical DVD of the HPE Operations Agent 12.02.</li> <li>2. Log on to the server as an administrator.</li> <li>3. Extract the contents of the .ISO file into a local directory on the server or mount the .ISO file.</li> <li>4. Go to the media root and run the following command to register the agent deployment packages and install the health view package:</li> </ol> <pre>./oainstall.sh -i -m -hv -healthview</pre> <p>For more information on Health View, see <i>HPE Operations Agent User Guide: Health View</i>. To install HPE Operations Agent and enable health monitoring using profile file see <a href="#">profile file</a>.</p>

**Note:** Since HP Reporter is not supported on UNIX/Linux, you cannot install report packages on the management server and you must set the `InfraSPI_With_Reports` property to NO.

After installation, see [Install Report and Graph Packages on a Remote Server](#) to install report or graph packages on a remote server.

#### When HPOM is in a High-Availability (HA) Cluster

Follow the above steps on the active node in the HPOM High-Availability (HA) cluster:

After completing the steps, fail over to the passive node, go to the `/var/opt/OV/shared/server/installation` directory on the passive node, and then run the following command:

```
./oainstall_sync.sh
```

After you run the command with necessary options and arguments, the registration procedure begins. Depending on number of selected packages, the registration process may take up to 20 minutes to complete.

### Verification

1. On the management server, go to the following location:

```
/opt/OV/bin/OpC/agtinstall
```

2. Run the following command:

```
./oainstall.sh -inv -listall
```

The command shows the list of available (active and backed-up) deployment packages on the management server.

To check if the Infrastructure SPIs are installed, run the command with the `-includespi` option.

```
./oainstall.sh -inv -includespi -listall
```

3. Locate the platform for which you installed the deployment package. If the active version is displayed as 12.02, the registration is successful.

### Log File

The registration log file (`oainstall.log`) is available in the following directory:

```
/var/opt/OV/shared/server/log
```

### Placement of Packages

When you register the HPE Operations Agent packages on the management server, the `oainstall` program places all necessary deployment packages into the following directory:

```
/var/opt/OV/share/databases/OpC/mgd_node/vendor
```

### Backup of Deployment Packages

When you register the deployment packages on the management server, the `oainstall` script saves a copy of the older deployment packages into the following local directory:

```
/var/opt/OV/shared/server/installation/backup/HP0psAgt/<OS>/<OA_Version>/<ARCH>
```

To view the active deployment packages, run the following command:

```
./oainstall.sh -inv
```

### Alternate Backup Location

When the default backup location does not have sufficient space to accommodate the backed up deployment packages, you can configure the system to use an alternate backup location.

Run the following command on the management server to use a non-default location to back up the old deployment package:

```
ovconfchg -ovrg server -ns eaagt.server -set OPC_BACKUP_DIR <directory>
```

In this instance, *<directory>* is the location on your system where you can back up the old deployment packages.

The log file (oainstall.log) created during the installation of deployment packages, is placed inside the backup directory.

## Uninstalling the HPE Operations Agent and Infrastructure SPIs Deployment Package

1. On Windows: Log on to the Management Server as an administrator and go to the %ovinstalldir%bin\OpC\agtinstall directory.

On UNIX/Linux: Log on to the Management Server as root and go to the /opt/OV/bin/OpC/agtinstall directory.

2. Run the following command to note down the correct version number of the deployment package that you want to remove.

### On Windows

```
cscript oainstall.vbs -inv -listall
```

### On UNIX/Linux

```
./oainstall.sh -inv -listall
```

3. Run the following command:

### On Windows

```
cscript oainstall.vbs -r -m -v <version> -p <platform>
```

### On UNIX/Linux

```
./oainstall.sh -r -m -v <version> -p <platform>
```

In this instance, *<version>* the version of the agent deployment package that you want to

remove.

The **-p** option specifies the platform-specific package of the HPE Operations Agent that you want to remove from the management server. Use the following list to specify the platform information in the form of arguments to this option:

- Linux: LIN
- Solaris: SOL
- HP-UX: HP-UX
- AIX: AIX
- Windows: WIN
- All platforms: ALL

For example, to remove a Solaris HPE Operations Agent package, use the command:

```
./oainstall.sh -r -m -v 12.01.XXX -p SOL
```

The options and arguments are case-sensitive.

To remove the Infrastructure SPIs along with deployment packages, run the following command:

#### **On Windows**

```
cscript oainstall.vbs -r -m -v <version> -p <platform> -spiconfig
```

#### **On UNIX/Linux**

```
./oainstall.sh -r -m -v <version> -p <platform> -spiconfig
```

When you remove the HPE Operations Agent 12.02 deployment packages, the installer program reinstates the highest backed-up version of deployment packages (if available) on the Management Server.

# Chapter 4: Prerequisites for Installing the HPE Operations Agent on a Node

## For Windows

### *User*

To install the HPE Operations Agent on a Windows node remotely, you must use a user with the administrative privileges. The user must have access to the default system share (the disk on which the **Programs Files** folder is configured) with the following additional privileges:

- Membership of the Local Administrators group
- *<only for remote deployment>* Write access to the admin\$ share
- Read and write access to the registry
- *<only for remote deployment>* Permission to log on as a service
- Permission to start and stop services

### *Necessary Software*

**Windows Installer 4.5 or later:** The Windows Installer software is packaged with the Microsoft Windows operating system. The installer program of the HPE Operations Agent requires the version 4.5 of this software component to be present on the system. To check if the Windows Installer 4.5 or later is present, follow these steps:

1. Log on to the Windows system.
2. From the **Start** menu, open the **Run** prompt.
3. At the **Run** prompt, type **regedit** and then press **Enter**. The Registry Editor window opens.
4. In the Registry Editor window, expand **HKEY\_LOCAL\_MACHINE > SOFTWARE > Microsoft**, and then click **DataAccess**.
5. In the right pane, double-click **FullInstallVer**. The **Edit String** dialog box opens.
6. In the **Edit String** dialog box, check if the version string is set to 4.5 or higher.

**Windows Script Host:** The Windows Script Host must be enabled on the system. The installer program of the HPE Operations Agent requires the Windows Script Host to be enabled. To check if the Windows Script Host is enabled, follow these steps:



1. Log on to the Windows system.
2. From the **Start** menu, open the **Run** prompt.
3. At the Run prompt, type **regedit** and then press **Enter**. The Registry Editor window opens.
4. In the **Registry Editor** window, expand **HKEY\_LOCAL\_MACHINE > SOFTWARE > Microsoft**, and then click **Windows Script Host**.
5. In the right pane, search for the key **Enabled**:
6. If the key **Enabled** is present, double-click the key and make sure the Value Data is set to 1. The **Windows Script Host** is disabled if the Value Data for the **Enabled** key is set to 0.
7. If the key **Enabled** is not present, you can assume that the **Windows Script Host** is enabled.

### ***Necessary Services***

Before installing the agent, make sure the following services are running:

- Event Log
- Remote Procedure Call
- Plug and Play
- Security Accounts Manager
- Net Logon
- <only for remote deployment> Remote Registry
- Server
- Workstation

To verify that the above services are running, follow these steps:

1. Log on to the system as an administrator.
2. From the **Start** menu, open the **Run** prompt.
3. At the **Run** prompt, type **services.msc**, and then press **Enter**. The **Services** window opens.
4. Check if the status of each of the above services is **Started**. If the status of one of the services is other than **Started**, right-click the service, and then click **Start**.

### ***Disk Space***

#### **For new installation**

For the installation directory: 350 MB

For the data directory: 50 MB

### **For upgrade from old agent software**

For the installation directory: 100 MB

For the data directory: 50 MB

### **Recommended Software and Services**

**For WMI Interceptor policies:** The Windows Management Instrumentation service must be available on the system if you want to:

- Deploy the WMI Interceptor policies or measurement threshold policies to monitor WMI events and classes.
- Perform automatic service discovery on the node.

**For SNMP MIB monitoring:** If you want to monitor objects in an SNMP Management Information Base (MIB) on the agent system, make sure the SNMP agent (compliant with MIB-I and MIB-II) is installed on the system.

**For HPOM actions and tools:** For launching HPOM actions and tools on the node, the NT LM Security Support Provider service must be running.

## For Linux

### **User**

To install the HPE Operations Agent on a Linux node, you must be a user with root privileges.

### **Necessary Software**

To install the HPE Operations Agent, the following runtime libraries and packages are required:

- On x64 systems:
  - To check for the packages, use the following command:

```
rpm -qa | grep -i <packagename>
```

In this instance, <packagename> is the name of the package to be checked.

- libstdc++33-32bit-3.3.3-7.8.1.x86\_64.rpm and above

**Note:** Make sure that libstdc++33-32bit-3.3.3-7.8.1.x86\_64.rpm is installed before you install HPE Operations Agent 12.02 on SLES10 SP4 x64 system. This rpm is applicable only for SUSE Linux Enterprise Server 10 and later.

- C++ runtime:
  - For systems with kernel version 2.6:  
libstdc++.so.5
- Only required for Glance- Curses runtime library:  
libncurses.so.5

**Note:** Make sure that the libncurses.so.5 library is present at the following path:

**On Linux (64-bit systems)**

/usr/lib64/libncurses.so.5 or /lib64/libncurses.so.5

**On Linux (32-bit systems)**

/usr/lib/libncurses.so.5 or /lib/libncurses.so.5

- Make sure that the m4 utility is installed at the path /usr/bin/m4.
- Set the executable (x) bit for the libvirt library at one of the following paths as appropriate:
  - /usr/lib64/libvirt.so
  - /usr/lib64/libvirt.so.0
  - /usr/lib/libvirt.so
  - /usr/lib/libvirt.so.0

If these paths contain softlinks, make sure that the library pointed by the link has the executable bit set.

If you want to remotely install the agent from the HPOM for Windows console, make sure OpenSSH 5.2 or later is installed on the system.

### **Disk Space**

#### **For new installation**

For the installation directories (/opt/OV and /opt/perf): 350 MB

For the data directories (/var/opt/OV and /var/opt/perf): 350 MB

#### **For upgrade**

For the installation directories (/opt/OV and /opt/perf): 100 MB

For the data directories (/var/opt/OV and /var/opt/perf): 350 MB

**Note:** If you do not have sufficient space in the installation or data directory, you can symbolically

link the install or data directory to another location on the same system by using the `ln -s` command.

For example, to symbolically link the `/opt/OV` directory to the `/new` directory, run the following command:

```
ln -s /new /opt/OV
```

### **Recommended Software and Services**

**For SNMP MIB monitoring:** If you want to monitor objects in an SNMP Management Information Base (MIB) on the agent system, make sure the SNMP agent (compliant with MIB-I and MIB-II) is installed on the system.

**For xglance:** To use the **xglance** utility, make sure the following components are available on the system:

Open motif toolkit 2.2.3 (On Linux platforms other than Red Hat Enterprise Linux 5.x and SUSE Linux Enterprise Server 10.x on x86\_64 and Itanium, the 32-bit version of the Open motif toolkit and associated libraries must be present.)

## For HP-UX

### **User**

To install the HPE Operations Agent on an HP-UX node, you must be user with root privileges.

### **Necessary Software**

On HP-UX, make sure that the following patches are installed:

- *For HP-UX 11.31.* qpkbase package September 2013 (or superseding patch)
- *For HP-UX 11.23.* PHKL\_36853, PHCO\_38149 (or superseding patch)
- *For HP-UX 11i v1.* PHNE\_27063 (or superseding patch)
- *For HP-UX 11i v1.* PHCO\_24400 s700\_800 11.11 libc cumulative patch (or superseding patch)
- *For HP-UX 11.11 PA-RISC.* PHCO\_38226 (or superseding patch)
- *For HP-UX 11i v1.* The following patches are required for the performance tools to function with VERITAS Volume Manager 3.2:
  - PHKL\_26419 for HP-UX B.11.11 (11.11) (or superseding patch)
  - PHCO\_26420 for HP-UX B.11.11 (11.11) (or superseding patch)

On HP-UX systems running on Itanium, the `libunwind` library must be available.

If multiple processor sets are configured on an HP-UX 11i v1 system and you are using the `log application=prm` switch in the `parm` file to log APP\_ metrics by the PRM Group, you must install the following patch:

PHKL\_28052 (or superseding patch)

On HP-UX 11i v1 and higher, the performance tools work with Instant Capacity on Demand (iCOD). The following kernel `pstat` patch should be installed to correctly report iCOD data (If iCOD is not installed on your system, do not install the kernel patch.):

PHKL\_22987 for HP-UX B.11.11 (11.11) (or superseding patch)

Make sure that the `m4` utility is installed at the path `/usr/bin/m4`.

HP GlancePlus, included in this version of the HPE Operations Agent, works with Process Resource Manager (PRM) version C.03.02.

HP-UX 11.11 and higher running EMC PowerPath v2.1.2 or v3.0.0 must have the latest EMC patches installed.

- For the EMC PowerPath v2.1.2 release, use the following patch:  
EMCpower\_patch213 HP.2.1.3\_b002 (or superseding patch)
- For the EMC PowerPath v3.0.0 release, use the following patch:  
EMCpower\_patch301 HP.3.0.1\_b002 (or superseding patch)

To install HPE Operations Agent using the single depot package on HP-UX IA nodes, you must install the following patch:

qpkbase for HP-UX B.11.31.1309.397 (or superseding patch)

**Note:** To install HPE Operations Agent 12.01 on HP-UX nodes from the HP Operations Manager for Linux or HP Operations Manager for Unix version 9.xx, you must install the following hotfix on the management server:

**QCCR1A184835**

Contact HPE Support to obtain the hotfix.

### **Disk Space**

#### **For new installation**

For the installation directories (`/opt/OV` and `/opt/perf`): 830 MB

For the data directories (`/var/opt/OV` and `/var/opt/perf`): 800 MB

#### **For upgrade**

For the installation directories (/opt/OV and /opt/perf): 830 MB

For the data directories (/var/opt/OV and /var/opt/perf): 800 MB

**Note:** If you do not have sufficient space in the installation or data directory, you can symbolically link the install or data directory to another location on the same system by using the `ln -s` command.

For example, to symbolically link the /opt/OV directory to the /new directory, run the following command:

```
ln -s /new /opt/OV
```

### **Recommended Software and Services**

**For SNMP MIB monitoring:** If you want to monitor objects in an SNMP Management Information Base (MIB) on the agent system, make sure the SNMP agent (compliant with MIB-I and MIB-II) is installed on the system.

## For Solaris

### **User**

To install the HPE Operations Agent on a Solaris node, you must use a user with the root privileges.

### **Necessary Software**

- *For all supported Solaris versions.* Make sure the following packages are available:
  - SUNWlibC
  - SUNWlibms

To check for packages, use the following command:

```
pkginfo <packagename>
```

In this instance, <packagename> is the name of the package.

- Make sure that the m4 utility is installed at the path /usr/xpg4/bin/m4 or /usr/ccs/bin/m4.

### **Disk Space**

#### **For new installation**

For the installation directories (/opt/OV and /opt/perf): 350 MB

For the data directories (/var/opt/OV and /var/opt/perf): 350 MB

**For upgrade**

For the installation directories (/opt/OV and /opt/perf): 100 MB

For the data directories (/var/opt/OV and /var/opt/perf): 350 MB

**Note:** If you do not have sufficient space in the installation or data directory, you can symbolically link the install or data directory to another location on the same system by using the `ln -s` command.

For example, to symbolically link the /opt/OV directory to the /new directory, run the following command:

```
ln -s /new /opt/OV
```

**Recommended Software and Services**

**For SNMP MIB monitoring:** If you want to monitor objects in an SNMP Management Information Base (MIB) on the agent system, make sure the SNMP agent (compliant with MIB-I and MIB-II) is installed on the system.

**For xglance:** To use the **xglance** utility, make sure the following components are available on the system:

- SUNWmfrun
- SUNWxwplt

## For AIX

**User**

To install the HPE Operations Agent on an AIX node, you must use a user with the root privileges.

To check for specific packages on the AIX node, use the following command:

```
lsLpp -l | grep -i <packagename>
```

In this instance, <packagename> is the name of the package.

**Necessary Software**

- The `libC.a` library is required for the HP GlancePlus to function correctly. The library is bundled within the `xIC.rte` package, which is available from your AIX Operating System optical media.
- The `bos.perf.libperfstat` package is required for the communication daemon.
- If you want to remotely install the agent from the HPOM for Windows console, make sure

OpenSSH 5.2 or higher is installed on the system.

- Make sure that the m4 utility is installed at the path `/usr/bin/m4`.

### **Disk Space**

#### **For new installation**

For the installation directory (`/usr/lpp/0V` and `/usr/lpp/perf`): 350 MB

For the data directory (`/var/opt/0V` and `/var/opt/perf`): 350 MB

#### **For upgrade**

For the installation directory (`/usr/lpp/0V` and `/usr/lpp/perf`): 350 MB

For the data directory (`/var/opt/0V` and `/var/opt/perf`): 350 MB

**Note:** If you do not have sufficient space in the installation or data directory, you can symbolically link the install or data directory to another location on the same system by using the `ln -s` command.

For example, to symbolically link the `/usr/lpp/0V` directory to the `/new` directory, run the following command:

```
ln -s /new /usr/lpp/0V
```

### **Recommended Software and Services**

**For SNMP MIB monitoring:** If you want to monitor objects in an SNMP Management Information Base (MIB) on the agent system, make sure the SNMP agent (compliant with MIB-I and MIB-II) is installed on the system.

**For xglance:** To use the **xglance** utility, make sure the following components are available on the system:

- Open Motif 2.1 or higher
- X11 Revision 6 (X11R6)

To collect and log cross-partition metrics, the `xmservd` or `xmtopas` daemon must be available. `xmtopas` is a part of `perf-agent.tools` file set and `xmservd` is bundled with the Performance Toolbox for AIX component (a licensed software program).

## For Debian and Ubuntu

### **User**



To install the HPE Operations Agent on a Debian or Ubuntu node, you must log on with the root privileges.

### **Necessary Software**

To install the HPE Operations Agent, the following runtime libraries and packages are required. You can run the following command to list the packages:

```
dpkg -l | grep -i <package_name>
```

- C++ runtime:
  - For systems with kernel version 2.6:  
/lib/libstdc++.so.5
  - For systems with kernel version 2.6 on Itanium :  
/lib/libstdc++.so.6
- **Only required for Glance-** Curses runtime library:  
/lib/libncurses.so.5
- Make sure that the m4 utility is installed at the path /usr/bin/m4.
- Debian libraries:
  - libgcc 4.7.2 and above
  - libstdc++6 4.7.2 and above
  - libc 2.13 and above
  - libncurses5 5.9 and above
- Ubuntu libraries:
  - libc 2.19 and above
  - libstdc++6 4.8.2 and above
  - libgcc 4.8.2 and above
  - libncurses5 5.9 and above

### **Disk Space**

#### **For new installation**

For the installation directories (/opt/OV and /opt/perf): 350 MB

For the data directories (/var/opt/OV and /var/opt/perf): 350 MB

#### **For upgrade**

For the installation directories (/opt/OV and /opt/perf): 100 MB

For the data directories (`/var/opt/OV` and `/var/opt/perf`): 350 MB

**Note:** If you do not have sufficient space in the installation or data directory, you can symbolically link the install or data directory to another location on the same system by using the `ln -s` command.

For example, to symbolically link the `/opt/OV` directory to the `/new` directory, run the following command:

```
ln -s /new /opt/OV
```

To remotely install the HPE Operations Agent from the HPOM for Windows console, make sure that the OpenSSH 5.2 or higher is installed on the system.

## Upgrade Notes

You can upgrade an older version of the HPE Operations Agent, HP Performance Agent or HP GlancePlus to the HPE Operations Agent. The following version can be directly upgraded to the HPE Operations Agent 12.02:

- HP Operations Agent 11.xx
- HP Performance Agent 11.xx
- HP GlancePlus 11.xx

The installation of the HPE Operations Agent 12.02 fails if any agent software older than 11.xx is installed. Before installing the HPE Operations Agent 12.02 on nodes with the HPE Operations Agent older than 11.xx, the HP Performance Agent older than 11.xx or HP GlancePlus older than 11.xx, do one of the following:

- Upgrade the agent software to the version 11.xx and then upgrade to the HPE Operations Agent 12.02.

This is the preferred method of upgrade. This method ensures necessary packages and policies are retained on the node.

- Remove the agent software completely and then install the HPE Operations Agent 12.02.

This may result in removal of policies and instrumentation files from the node. After upgrading to the HPE Operations Agent 12.02, make sure necessary policies and instrumentation files are deployed on the node again.

### Check the Version of the Existing Agent

#### On Windows

1. Log on to the node as an administrator.
2. Open a command prompt.
3. Run the following command:

```
opcagt -version
```

If the command output shows that the version of the existing HPE Operations Agent is lower than 11.xx, you must do one of the following:

- Upgrade the HP Operations Agent to the version 11.xx and then upgrade to the HPE Operations Agent 12.02.
  - Remove the installed version of the HP Operations Agent completely and then install the HPE Operations Agent 12.02.
4. Check the version of the HP Performance Agent:
    - a. Open a command prompt.
    - b. Run the following command:

```
perfstat -v
```

The command output shows the versions of different components of the HP Performance Agent. If the version of the component **ovpa.exe** is lower than 11.xx, you must upgrade to the version 11.xx or completely remove the installed version of the HP Performance Agent and then upgrade to the HPE Operations Agent 12.02.

### On UNIX/Linux

1. Log on to the node as an administrator.
2. Open a command prompt.
3. Run the following command:

```
opcagt -version
```

If the command output shows that the version of the existing HPE Operations Agent is lower than 11.xx, you must do one of the following:

- Upgrade the HP Operations Agent to the version 11.xx and then upgrade to the HPE Operations Agent 12.02.
  - Remove the installed version of the HP Operations Agent completely and then install the HPE Operations Agent 12.02.
4. Check the version of the HP Performance Agent:

- a. Open a command prompt.
- b. Run the following command:

```
perfstat -v
```

The command output shows the versions of different components of the HP Performance Agent. If the version of the component **ovpa** is lower than 11.xx, you must upgrade to the version 11.xx or completely remove the installed version of the HP Performance Agent and then upgrade to the HPE Operations Agent 12.02.

5. Check the version of HP GlancePlus:

- a. Open a command prompt.
- b. Run the following command:

```
perfstat -v
```

The command output shows the versions of different components of the HP Performance Agent and HP GlancePlus. If the version of the component **glance** is lower than 11.xx, you must upgrade to the version 11.xx or completely remove the installed version of HP GlancePlus and then upgrade to the HPE Operations Agent 12.02.

## Data Collection and Storage with the HPE Operations Agent 12.02

With the HPE Operations Agent version 12.02, the CODA and scope processes (Scopeux on UNIX and Linux nodes and Scopent on Windows nodes) are consolidated into a single process called **oacore**. The **oacore** process provides both read and write interface for system performance and custom data.

The data collector **oacore** captures the following information:

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

The Collection Parameters file or the **parm** file contains the instructions for the data collector to collect specific types of data and defines the data collection interval. This is an ASCII file that you can use to

customize the default data collection mechanism. For more information, see the *HPE Operations Agent User Guide*.

The data collector gathers a large set of system performance metrics, which presents a wide view of the health and performance of the system. The collected information is stored in the **Metric Data Store**.

## Metric Data Store

With the HPE Operations Agent version 12.02, Metric Data Store replaces the log file based data store. Multiple data stores such as CODA, SCOPE, and DSI log files have been consolidated into a single Relational Database Management System (RDBMS) based data store. The RDBMS used is SQLite. Data stored in the Metric Data Store is available on the system for analysis and use with tools like **HP Performance Manager** and **HP Reporter**.

Old data stored in the CODA database files, SCOPE log files and the DSI log files are retained in read-only mode. You can access the old data through utilities such as `ovcodautl`, `extract`, or through reporting tools such as **HP Performance Manager** and **HP Reporter**.

Despite the change in the data collection and data storing mechanism, threshold comparison process through policies remains the same.

### ***Upgrading on a Solaris SPARC Management Server with Solaris SPARC Managed Nodes***

If you are using a Solaris SPARC HPOM management server with HP Operations Agent 8.60; follow the steps to ensure the SPARC nodes communicate with SPARC management server:

1. Log on to the Management Server as an administrator.
2. Run the following command to check the version of the HP Software Security Core (OvSecCo) component:

```
strings /opt/OV/lib/libOvSecCore.so | grep FileV
```

- If the version of the HP Software Security Core (OvSecCo) component is 06.20.077 (or higher), then upgrade the HPE Operations Agent to the version 12.02 on the Solaris SPARC HPOM management server.
- If the version of the HP Software Security Core (OvSecCo) component is 06.20.050 then follow the steps:
  - i. On the Solaris SPARC node, upgrade to the HPE Operations Agent version 12.02.
  - ii. Apply the hotfix QCCR1A97520 on the Management Server (contact HPE Support to obtain this hotfix).

**Note:** Run the following command on the management server to verify if the version of the HPOvSecCo component is upgraded to 06.20.077

```
strings /opt/0V/lib/libOvSecCore.so | grep FileV
```

- iii. On the Solaris SPARC HPOM management server, upgrade the HPE Operations Agent to version 12.02.

This hotfix ensures that the SPARC nodes with the HPE Operations Agent 12.02 can communicate with the SPARC management server that includes the HPOvSecCo component, version 06.20.050. If you do not install this hotfix on the SPARC management server, the SPARC nodes with the HPE Operations Agent 12.02 cannot communicate with the SPARC management server.

## Preinstallation Task: Installing the HPE Operations Agent and Infrastructure SPIs on HPOM in Cluster

If installed in a high-availability (HA) cluster environment, the HPE Operations Agent does not fail over when the active system in the cluster fails over to another system. However, the HPE Operations Agent can help you monitor cluster-aware applications running in a cluster.

You must install the HPE Operations Agent on every node that belongs to the cluster. Installing the agent in a cluster does not involve any additional steps or any special configuration. However, to install the agent on an HPOM management server that runs in a cluster requires additional configuration steps.

### For HPOM for Windows

1. Make sure the HPOM database is up and running.
2. Log on to the active management server as an administrator.
3. Set the active node to the maintenance outage mode by running the following command:  

```
ovownodeutil -outage_node -unplanned -node_name <FQDN_of_node> -on
```
4. Install the agent on the active server by following instructions in "[Installing from the HPOM Console](#)" or "[Installing the HPE Operations Agent and Infrastructure SPIs Manually on the Node](#)".
5. Perform step 3 and 4 on each node in the cluster.

In this instance:

<FQDN\_of\_node> is the fully-qualified domain name of the active node.

### For HPOM on UNIX/Linux

1. Log on to the active management server as an administrator.
2. Disable monitoring of the HA resource group on the active node by setting the maintenance mode for the node:

Run the following command on the active node:

```
/opt/OV/sbin/ovharg -monitor <HA_resource_group_name> disable
```

In this instance:

<HA\_resource\_group\_name> is the HA resource group for HPOM on the management server.

3. Install the agent on the active server by following instructions in "[Installing from the HPOM Console](#)" or "[Installing the HPE Operations Agent and Infrastructure SPIs Manually on the Node](#)".

Make sure the shared disk is mounted at the time of installation.

4. Perform step 3 on each node in the cluster.
5. Once installation is completed, server resource group monitoring should be enabled again.

# Chapter 5: Installing the HPE Operations Agent from HPOM or HPE OMi Console

**Note:** If the node hosts another HP Software product, make sure to stop all the processes of the product prior to the agent installation. You can start the processes after the agent installation is complete.

## From HPOM for Windows

To install the HPE Operations Agent on managed nodes from the HPOM console, follow the *Remote agent installation* section in the *HP Operations Manager for Windows Online Help*.

For information on installing agent from the management server to a remote node, see "[Configure the Agent Remotely from an HPOM for Windows Management Server](#)" on page 149.

## From HPOM on UNIX/Linux

To install the HPE Operations Agent on managed nodes from the HPOM on UNIX/Linux console, follow the *HPOM for UNIX: New Agent Installation* topic in the *HPOM on UNIX/Linux Online Help*.

**Note:** When you are installing HPE Operations Agent for the first time, remotely from the HPOM UNIX/Linux console on the Linux (Debian) Operating system, do not select the `force` option. This installs the HPE Operations Agent twice.

**Note:** You can install the HPE Operations Agent 12.01 only on HP-UX IA64 systems with the patch level `qpkbase` package September 2013 or superseding patches. Remote installation of HPE Operations Agent 12.01 from the HPOM management server to a HP-UX IPF32 node will fail as the required agent binary format for HPE Operations Agent 12.01 is HP-UX IPF64.

## From HPE OMi

HPE Operations Manager i (OMi) is the event management foundation for a complete Business Service Management (BSM) monitoring solution. You can integrate HPE Operations Agent with OMi. After the installation of the HPE Operations Agent on a node, you must connect the HPE Operations Agent to OMi and then grant the agent's certificate request in OMi.

For more information about integrating HPE Operations Agent with OMi, see the section *Connecting HP Operations Agents to OMi* in the chapter *Monitored Nodes* in the *OMi Administration Guide*.



# Chapter 6: Installing the HPE Operations Agent in a Single Step

The HPE Operations Agent 12.02 single step installer enables you to install the base version of HPE Operations Agent along with patches and hotfixes. The installer first installs the base version of the HPE Operations Agent on the system, and then installs any updates if available with the patches, followed by any available hotfix.

You can use the `oainstall` script to install HPE Operations Agent locally on a managed node or you can use the `ovdeploy` command to remotely install the HPE Operations Agent on a managed node from the management server.

If you use the single step installer to install the HPE Operations Agent, the time taken for installation is reduced on all platforms. The following table lists all the changes in the installation process for HPE Operations Agent 12.02:

### Comparing previous versions of HPE Operations Agent with version 12.02

Previous versions of HP Operations agent	HPE Operations Agent 12.02
<p>The pre-requisite check occurs thrice during the installation process of HP Operations Agent. Each before installation of the base version of agent, patch, and hotfix.</p> <pre>INFO: Validating pre-requisites for installation on &lt;system_name&gt; ..... STATUS: All checked prerequisites are OK. INFO: &lt;system_name&gt; meets all pre-requisites</pre>	<p>The pre-requisites check occurs only once before the installation of the HPE Operations Agent 12.02 along with the patch and hotfix in a single step.</p> <pre>INFO: HP Operations-agent install options are: -install INFO: Validating pre-requisites for installation on &lt;system_name&gt; Requirements:</pre>
<pre>INFO: HP Operations agent installation started ===== INFO: Validating pre-requisites for installation on &lt;system_name&gt; ..... STATUS: All checked prerequisites are OK. INFO: &lt;system_name&gt; meets all pre-requisites</pre>	<pre>[ PASS ] Is user root ..... [ PASS ] Check if m4 is installed STATUS: All checked prerequisites are OK. INFO: &lt;system_name&gt; meets all pre- requisites =====</pre>

**Comparing previous versions of HPE Operations Agent with version 12.02, continued**

<pre> INFO: HP Operations agent Patch: OAHPUX_ 00031 installation started  =====  INFO: Validating pre-requisites for installation on &lt;system_name&gt;  .....  STATUS: All checked prerequisites are OK.  INFO: &lt;system_name&gt; meets all pre-requisites  INFO: HP Operations agent Hotfix: HFHPUX_ 13018 installation started  =====                 </pre>	<pre> INFO: HP Operations agent installation started  =====                 </pre>
<p>Configuration of the HP Operations Agent occurs multiple times during the installation process.</p>	<p>Configuration of the HPE Operations Agent occurs only once during the installation process of HPE Operations Agent 12.02, patch, and hotfix in a single step.</p>
<p>The activation of the HP Operations Agent occurs thrice during the installation process. Each after the installation of the base version of agent, patch, and hotfix.</p>	<p>The activation of the HPE Operations Agent occurs only once at the end of the installation of HPE Operations Agent 12.02, patch, and hotfix.</p>
<p>The installer pauses the installation process of the HP Operations Agent if the certificate is not auto granted.</p>	<p>The installer does not pause the installation of the HPE Operations Agent 12.02 in case the certificate is not auto granted.</p>

## Installing the HPE Operations Agent using Single Step

Follow the steps:

1. Log on to the node as an administrator.
2. Download and extract the media, patches, and hotfix packages to the same directory.
3. Go to the directory where you extracted the bits.
4. Run the following command:

**On Windows**

```
cscript oainstall.vbs -i -a
```

**On UNIX**

```
./oainstall.sh -i -a
```

## Deploying Patches and Hotfixes using Single Step Installer

**From HPOM for Windows Management Server**

If the HPE Operations Agent 12.02 is already installed on a node, follow the steps to install patches and hotfixes:

**Note:** Before installing patches and hotfixes, you must apply the hotfix QCCR1A174773. Contact HPE Support to obtain the hotfix.

1. In the console tree, right-click the node (where you want to install the patches and hotfixes), and then click **All Tasks > Reinstall/Update**. The **Reinstall/Update Node** dialog box appears.
2. Select **Update**, select **Packages** in the **Scope** section, clear the **Deploy only if version is newer** check box, and then click **OK**.
3. After the installation is complete, go to the console tree on the HPOM console, right-click the node, and then click **All Tasks > Synchronize inventory> Packages**.

All available patches and hotfixes are installed on the node.

**Note:** On a node with HPE Operations Agent 12.02, if you upgrade a patch or hotfix, only those patches and hotfixes that are not available on the node are transferred and installed. Thus the installation time is reduced.

For more information, see [Installing from the HPOM Console](#).

**From HPOM for Linux Management Server**

Follow the steps to install patches and hotfixes:

1. On the console, select the option **(De) Install Agent** from the **Deployment** drop-down.
2. From the **Install Type** drop-down, select **Installation**.

3. Select a node and then click the **Preinstall Check** button. The **Install Agent** window appears.
4. In the **Install Agent** window, ensure that the node is selected. Depending on the original state of the node, perform one of the following:
  - If the node does not have any version of the HPE Operations Agent installed, select the **Force** check box in the **Install Agent** window and then click the **Install On Selected Nodes** button. HPOM installs the HPE Operations Agent versions 12.02, patch and hotfix.
  - If the HPE Operations Agent 12.02 is already installed on the node, select the **Force** check box in the **Install Agent** window and then click the **Install On Selected Nodes** button. All available patches and hotfixes are installed on the node.

**Note:** If the node has older version of HPE Operations Agent that cannot be upgraded to the version 12.02 then the installation fails.

If the node has a version of HPE Operations Agent that can be upgraded to the version 12.02, the existing HPE Operations Agent is upgraded to the version 12.02, and then the patches and hotfixes are installed (this two-step upgrade takes place automatically and no additional steps are involved).

For more information, see [Installing from the HPOM Console](#).

## Verifying the Installation

Run the following command:

```
ovdeploy -inv -includeupdates.
```

The command lists the version of the base, patch, and hotfix components.

## Chapter 7: Installing HPE Operations Agent using Profile File

You can use a *profile* file during the installation (manual installation) to program the agent to run with non-default configuration settings (such as the communication port, event interceptor port or the license type).

### Note:

- With HPE Operations Agent version 12.02, all install time configurable values must be added in the profile file under the new namespace `nonXPL.config`. The configurable values added under the namespace `nonXPL.config` will not be uploaded on the `xpl.config` settings.
- HPE Operations Agent does not support comments in profile file.

You can modify the default profile file available on the HP Operations Manager or manually create a profile file on the HPE Operations Agent node.

### Modifying the Default Profile file on the HPOM for Windows Console

Follow the steps:

1. Log on to the Management Server as an administrator.
2. Go to the directory `%ovdatadir%shared\conf\PMAD`.
3. Rename the `agent_install_defaults.cfg.sample` file to `agent_install_defaults.cfg`.

**Tip:** Take a backup of the `agent_install_defaults.cfg.sample` file.

4. Open the `agent_install_defaults.cfg` file with a text editor and use the following syntax to configure non-default values for agent variables:

```
[<namespace>]
<variable>=<value>
```

In this instance:

`<namespace>` is the configuration variable namespace.

`<variable>` is the variable that you want to configure.

`<value>` is the value you want to assign to the variable.

5. Save the file and then follow the steps to install the [HPE Operations Agent using a Profile File](#).

## Modifying the Default Profile file on the HPOM for UNIX Console

Follow the steps:

1. Log on to the management server with the root privileges.
2. Go to the directory `/etc/opt/OV/share/conf/OpC/mgmt_sv`.
3. Rename the file `bbc_inst_defaults.sample` to `bbc_inst_defaults`.
4. Open the file `bbc_inst_defaults` with a text editor and use the following syntax to configure non-default values for agent variables:

```
[<namespace>]
```

```
<variable>=<value>
```

In this instance:

`<namespace>` is the configuration variable namespace

`<variable>` is the variable that you want to configure

`<value>` is the value you want to assign to the variable

5. Save the file and then follow the steps to install the [HPE Operations Agent using a Profile File](#).

## Creating the Profile File Manually on the Node:

Follow the steps :

1. On the system where you want to install the agent, create a new file and open the file with a text editor.
2. Type the following syntax to configure agent variables to use a non-default value:

```
set<namespace>:<variable>=<value>
```

In this instance:

`<namespace>` is the configuration variable namespace

`<variable>` is the variable that you want to configure

`<value>` is the value you want to assign to the variable

3. Save the file into a local directory.

**Key features that you can configure during installation**

Feature	Modifying Profile File on HPOM	Creating Profile File Manually
<p><b>MODE:</b> At the time of installation, you can configure the user that the agent runs under. The <code>MODE</code> variable enables to choose a non-default user that can be used by the agent while running on the system.</p>	<p>To configure the agent to run under a non-root/non-privileged user, add the following content:</p> <pre>[eaagt] MODE=NPU SNMP_TRAP_PORT=1162 OPC_RPC_ONLY=TRUE [bbc.cb] SERVER_PORT=&lt;Port number &gt; [ctrl.sudo] OV_SUDO_USER=&lt;NPU user name&gt; OV_SUDO_GROUP=&lt;NPU group name&gt;</pre> <p>To configure the agent to run only the Operations Monitoring Component under a non-root/non-privileged user, add the following content (the rest of the agent runs with root/Local System):</p> <pre>[eaagt] MODE=MIXED NPU_TASK_SET=EVENT_ACTION [bbc.cb] SERVER_PORT=&lt;Port number &gt; 1024 &gt; [ctrl.sudo] OV_SUDO_USER=&lt;NPU user name&gt; OV_SUDO_GROUP=&lt;NPU</pre>	<p>To configure the agent to run under a non-root/non-privileged user, add the following content:</p> <pre>set eaagt:MODE=NPU set eaagt:SNMP_TRAP_PORT=1162 set eaagt:OPC_RPC_ONLY=TRUE set bbc.cb:SERVER_PORT=&lt;Port number &gt; set ctrl.sudo:OV_SUDO_USER=&lt;NPU user name&gt; set ctrl.sudo:OV_SUDO_GROUP=&lt;NPU group name&gt;</pre> <p>To configure the agent to run only the Operations Monitoring Component under a non-root/non-privileged user, add the following content (the rest of the agent runs with root/Local System):</p> <pre>set eaagt:MODE=MIXED set eaagt:NPU_TASK_SET=EVENT_ACTION set bbc.cb:SERVER_PORT=&lt;Port number &gt; 1024 &gt; set ctrl.sudo:OV_SUDO_USER=&lt;NPU user name&gt; set ctrl.sudo:OV_SUDO_GROUP=&lt;NPU group name&gt;</pre> <p>In addition, you must configure a set of variables in the similar fashion to enable the agent to run under a non-default user. See the <i>Configure the Agent User During Installation</i> section in the <i>HPE Operations Agent User Guide</i> for detailed information.</p> <p><b>Note:</b> On a windows system, to install HPE Operations Agent in NPU mode you must run the following command:</p> <pre>%OvInstallDir%bin\win64\OpC\install\cscript oainstall.vbs -i -a -agent_profile &lt;path&gt;\&lt;profile_file&gt; -npu_</pre>

**Key features that you can configure during installation, continued**

Feature	Modifying Profile File on HPOM	Creating Profile File Manually
	<p><b>group name&gt;</b></p> <p>In addition, you must configure a set of variables in the similar fashion to enable the agent to run under a non-default user. See the <i>Configure the Agent User During Installation</i> section in the <i>HPE Operations Agent User Guide</i> for detailed information.</p>	<pre>password &lt;password&gt;</pre> <p>On a windows system if the HPE Operations Agent is in NPU mode, you must provide the NPU password in the command line to remove patches or hotfixes.</p> <pre>%vInstallDir%bin\win64\OpC\install\cscript oainstall.vbs -r -a -npu_password &lt;password&gt;</pre>
<p><b>CREATE_DEFAULT_USER:</b> At the time of installation, the <i>opc_op</i> user is created as a default behavior. You can disable the option by using <b>CREATE_DEFAULT_USER</b> variable.</p>	<p>Add the following content in the profile file to disable the creation of <i>opc_op</i> user:</p> <pre>[nonXPL.config] CREATE_DEFAULT_USER=FALSE</pre>	<p>Add the following content in the profile file to disable the creation of <i>opc_op</i> user:</p> <pre>set nonXPL.config:CREATE_DEFAULT_USER=FALSE</pre>
<p><b>DISBALE_REALTIME:</b> At the time of installation, use the <b>DISBALE_REALTIME</b> variable to disable the real-time monitoring component .</p>	<p>Add the following content in the profile file to disable the real-time monitoring component:</p> <pre>[nonXPL.config] DISABLE_REALTIME=TRUE</pre>	<p>Add the following content in the profile file to disable the real-time monitoring component:</p> <pre>set install.config:DISABLE_REALTIME=TRUE</pre>
<p><b>ENABLE_DNSCHK and ENABLE_PORTCHK:</b> <i>Only for UNIX machines:</i> At the time of</p>	<p>Add the following content in the profile file to enable the pre-requisite check for DNS validation:</p> <pre>[nonXPL.config] ENABLE_DNSCHK=TRUE</pre>	<p>Add the following content in the profile file to enable the pre-requisite check for DNS validation:</p> <pre>set nonXPL.config:ENABLE_DNSCHK=TRUE</pre> <p>Add the following content in the profile file to enable the pre-requisite check for port validation:</p>



**Key features that you can configure during installation, continued**

Feature	Modifying Profile File on HPOM	Creating Profile File Manually
<p>installation, you can enable or disable the pre-requisite check for DNS validation and availability of port 383 of the management and certificate server by using ENABLE_DNSCHK variable and ENABLE_PORTCHK variable respectively.</p>	<p>Add the following content in the profile file to enable the pre-requisite check for port validation:</p> <p><b>[nonXPL.config]</b></p> <p><b>ENABLE_PORTCHK=TRUE</b></p> <p>These prerequisite checks are only enabled if the values are set as TRUE in the profile file.</p>	<p><b>set nonXPL.config:ENABLE_PORTCHK=TRUE</b></p> <p>These prerequisite checks are only enabled if the values are set as TRUE in the profile file.</p>
<p><b>INSTALL_REMOVESIGN</b> You can disable the signature checks to reduce the installation time in Windows. You can disable the option by using INSTALL_REMOVESIGN variable.</p>	<p>Add the following content in the profile file to disable the signature checks at the installation time:</p> <p><b>[nonXPL.config]</b></p> <p><b>INSTALL_REMOVESIGN=True</b></p>	<p>Add the following content in the profile file to disable the signature checks at the installation time:</p> <p><b>set nonXPL.config:INSTALL_REMOVESIGN=True</b></p>
<p><b>Licensing:</b> If you install the agent manually on a node (that is, without using the HPOM console), no evaluation licenses are enabled automatically after installation.</p>	<p>For example, if you want to apply the HP Operations OS Inst Adv SW LTU permanently, add the following content:</p> <p><b>[eaagt.license]</b></p> <p><b>HP_Operations_OS_Inst_Adv_SW_LTU=PERMANENT</b></p>	<p>For example, if you want to apply the HP Operations OS Inst Adv SW LTU permanently, add the following content:</p> <p><b>set eaagt.license:HP_Operations_OS_Inst_Adv_SW_LTU=PERMANENT</b></p>

**Key features that you can configure during installation, continued**

Feature	Modifying Profile File on HPOM	Creating Profile File Manually
<p>You can configure license-specific variable in the profile file to apply a license-to-use (LTU) of your choice at the time of installation.</p> <p>For detailed information on applying licenses at the time of installation with a profile file, see the <i>HPE Operations Agent License Guide</i>.</p>		
<p><b>Perfd and ttd variables</b> At the time of installation, you can set the options for <b>perfd</b> and <b>ttd</b> component.</p>	<p>Add the following content in the profile file for <b>perfd</b> component:</p> <p><b>[nonXPL.config.perfd]</b></p> <p><b>interval=value</b></p> <p>Set the interval to any value.</p> <p><b>[nonXPL.config.perfd]</b></p> <p><b>ipv4=TRUE</b></p> <p>Set the IPv4 connection.</p> <p><b>[nonXPL.config.perfd]</b></p> <p><b>add="gbl,fs,dsk" -</b></p> <p>Add the data formats and file extensions.</p> <p>Add the following content in the profile file for <b>ttd</b> component:</p>	<p>Add the following content in the profile file for <b>perfd</b> component:</p> <p><b>set nonXPL.config.perfd:interval=value-</b> set the interval to any value.</p> <p><b>set nonXPL.config.perfd:ipv4=TRUE</b> - set the IPv4 connection.</p> <p><b>set nonXPL.config.perfd:add="gbl,fs,dsk" -</b> add the data formats and file extensions.</p> <p>Add the following content in the profile file for <b>ttd</b> component:</p> <p><b>set nonXPL.config.ttd:SEM_KEY_PATH=/var/opt/perf/datafiles</b></p> <p><b>set nonXPL.config.ttd:tran=* range=1,2,3,5,10,30,120,300 slo=15.0</b></p> <p><b>set nonXPL.config.ttd:app=[HP Perf Tools] tran=Scope_Get_Global_Metrics range=0.5,1.0,1.5,2,3,5,8,10,15 slo=5</b></p> <p><b>set nonXPL.config.ttd:app=[&lt;user_defined</b></p>

Key features that you can configure during installation, continued

Feature	Modifying Profile File on HPOM	Creating Profile File Manually
	<pre>[nonXPL.config.ttd] SEM_KEY_ PATH=/var/opt/perf/datafiles tran=* range=1,2,3,5,10,30,120,300 slo=15.0  app=[HP Perf Tools] tran=Scope_Get_Global_Metrics range=0.5,1.0,1.5,2,3,5,8,10,15 slo=5  app=[&lt;user_defined name&gt; Perf Tools] tran=Navin_Get_Process_Metrics range=0.5,1.0,1.5,2,3,5,8,10,15 slo=10  app=[HP Perf Tools1] tran=Scope_Get_Process_Metrics range=0.5,1.0,1.5,2,3,5,8,10,15 slo=25  app=[HP Perf Tools] tran=Navin_Get_Process_Metrics range=0.5,1.0,1.5,2,3,5,8,10,15 slo=10</pre>	<pre>name&gt; Perf Tools] tran=Navin_Get_Process_Metrics range=0.5,1.0,1.5,2,3,5,8,10,15 slo=10  set nonXPL.config.ttd:app=[HP Perf Tools1] tran=Scope_Get_Process_Metrics range=0.5,1.0,1.5,2,3,5,8,10,15 slo=25  set nonXPL.config.ttd:app=[HP Perf Tools] tran=Navin_Get_Process_Metrics range=0.5,1.0,1.5,2,3,5,8,10,15 slo=10</pre>
<p><b>IGNORE_LOCALE:</b> At the time of installation, all localization packages (Japanese, Korean, Spanish, and Chinese) are installed along with English. You can set the</p>	<p>Add the following content in the profile file to set the user interface to English:</p> <pre>[xpl.locale] IGNORE_LOCALE=True</pre> <p>Once the configuration variable is set to True, the user interface appears in English but the node communicates with the OM server with the set system locale language.</p>	<p>Add the following content in the profile file to set the user interface to English:</p> <pre>set xpl.locale:IGNORE_LOCALE=True</pre> <p>Once the configuration variable is set to True, the user interface appears in English but the node communicates with the OM server with the set system locale language.</p>

**Key features that you can configure during installation, continued**

Feature	Modifying Profile File on HPOM	Creating Profile File Manually
<p>user interface to English using IGNORE_LOCALE variable.</p>		
<p><b>ENABLE_PERFALARM:</b> On fresh installation of HPE Operations Agent 12.02, the alarm generator server (perfalarm) is disabled by default. To enable perfalarm, set the variable ENABLE_PERFALARM to True in the profile file.</p> <p>You can also enable perfalarm after installing HPE Operations Agent. For more information see the section <i>Enabling perfalarm</i> in the chapter <i>Performance Alarms</i> in the <i>HPE Operations Agent User Guide</i>.</p>	<p>Add the following content in the profile file to enable perfalarm:</p> <pre>[nonXPL.config] ENABLE_PERFALARM=TRUE</pre>	<p>Add the following content in the profile file to enable perfalarm:</p> <pre>set nonXPL.config:ENABLE_PERFALARM=TRUE</pre>
<p><b>MINPRECHECK:</b> To install the HPE Operations Agent 12.02</p>	<p>Add the following content in the profile file:</p> <pre>[nonXPL.config] MINPRECHECK=true</pre>	<p>Add the following content in the profile file:</p> <pre>set nonXPL.config:MINPRECHECK=true</pre>

**Key features that you can configure during installation, continued**

Feature	Modifying Profile File on HPOM	Creating Profile File Manually
<p>remotely from the HPOM for Windows or UNIX console on platforms supported with limitation, you must set the variable <code>MINPRECHECK</code> to True in the profile file.</p>		
<p><b>ENABLE_HPSENSOR:</b> On a system with only Glance license, <b>hpsensor</b> is not started automatically. You can use the <code>ENABLE_HPSENSOR</code> option to start <b>hpsensor</b> on a system where only Glance license is installed.</p> <p>This variable is not applicable on Windows systems as there is no Glance on Windows systems.</p>	<p>Add the following content in the profile file:</p> <pre>[nonXPL.config] ENABLE_HPSENSOR=True</pre>	<p>Add the following content in the profile file:</p> <pre>set nonXPL.config:ENABLE_HPSENSOR=True</pre>

## Installing HPE Operations Agent using a Profile File

After creating the profile file, run the following command to install the HPE Operations Agent with a profile file:

### On Windows

```
cscript oainstall.vbs -i -a -agent_profile <path>\<profile_file> -s <management_server> [-cs <certificate_server>] [-install_dir <install_directory> -data_dir <data_directory>]
```

### On UNIX/Linux

```
./oainstall.sh -i -a -agent_profile <path>/<profile_file> -s <management_server> [-cs <certificate_server>]
```

In this instance:

<path> is the path to the profile file.

<profile\_file> is the name of the profile file.

<management\_server>: FQDN of the management server

<certificate\_server>: FQDN of the certificate server

<install\_directory>: Path to place all packages and binary files on the node.

<data\_directory>: Path to place all data and configuration files on the node.

## Installing HPE Operations Agent and Enabling Health Monitoring using Profile File

HPE Operations Agent Health View is a health monitoring tool that provides a overview of the health of the HPE Operations Agent. Follow these steps to update default configuration settings for the HPE Operations Agent health monitoring on the node using the profile file during installation:

1. Log on to the node as an administrator where you want to install the HPE Operations Agent 12.02.
2. Open the profile file with a text editor.

3. You can edit the following variables:

```
set agent.health:OPC_SELFMON_ENABLE=<TRUE/FALSE>
```

```
set agent.health:OPC_SELFMON_SERVER=<health view server IP address>
```

```
set agent.health:OPC_SELFMON_INTERVAL=<time_interval>
```

```
set agent.health:OPC_SELFMON_HBP=<TRUE/FALSE>
```

In this instance,

`<health view server IP address>` is the IP address or the host name of the Health View Server. By default, the HP Operations Manager Management Server is configured as the Health View Server.

`<time_interval>` defines the frequency at which the system health information is collected. The default value is 300 seconds and the minimum value recommended is 60 seconds.

4. Install HPE Operations Agent 12.02 and include the agent profile file. Run the following command to install HPE Operations Agent 12.02 with a profile file:

#### **On Windows**

```
cscript oainstall.vbs -i -a -agent_profile <path>\<profile_file> -s <health view server IP address>
```

#### **On UNIX/Linux**

```
./oainstall.sh -i -a -agent_profile <path>/<profile_file> -s <health view server IP address>
```

In this instance,

`<health view server IP address>` is the IP address or the host name of the Health View Server. By default, the HPOM Management Server is configured as the Health View Server.

## Chapter 8: Configuring the Agent User

HPE Operations Agent, after installation, starts running with the Local System account on Windows nodes and with the root account on the UNIX/Linux nodes. You can, however, configure the HPE Operations Agent to run with a non-default user that has fewer privileges than the root or Local System user.

You can run only the Operations Monitoring Component with a non-root/non-Local System user and the remaining components with the default root/Local System user.

Based on the user account used, you can configure the following modes of operation of the agent:

- **Non-privileged:** All components of the HPE Operations Agent run with a non-default user account that has fewer privileges than root or Local System.

**Note:** You cannot run the HPE Operations Agent in the non-privileged mode on HP-UX.

You must not run HPE Operations Agent in a non-privileged user mode when both the HPE Operations Agent and NNMi coexist on a system.

- **Root:** All components of the HPE Operations Agent run with the default user (root or Local System). This is the default mode of operation of the agent.
- **Mixed:** The Performance Collection Component runs with the root user and the Operations Monitoring Component runs with the local user account.

**Note:** While running in the mixed mode, it is recommended that the root or privileged user start the agent processes.

When the agent is configured to run under a non-default user on a system where the HP Performance Manager is installed, the `OvTomCatB` service of HP Performance Manager starts running under the non-default agent user.

In an HPOM-managed environment, you can also configure the agent to perform automatic or operator-initiated commands with a user different from the user it runs under.

## Requirements for Using a Non-Default User

The non-default agent user that you want to use must satisfy the following requirements:



- **Windows-only requirements:**

- The user must have full control of the registry key HKEY\_LOCAL\_MACHINE/Software/Hewlett-Packard/OpenView
- The user must have read access to the registry key HKEY\_LOCAL\_MACHINE/Software/Microsoft/WindowsNT/CurrentVersion/Perflib
- The user must have rights to:
  - Log on as service — To start and stop the Performance Collection Component services.
  - Manage auditing and security logs — The user can view audited events in the security log of the event viewer. A user with this privilege can view and clear the security log.
  - Act as part of the operating system — To control the agent processes
  - Replace a process-level token — To create the agent processes as the non-root user.
- To monitor a log file using a policy, the agent user must have the permission to read that log file.
 

**Note:** On Windows, the agent user cannot read the log file since the user does not have permission.
- To start a program using an automatic command, operator-initiated command, tool, or scheduled task, the agent user must have permission to start that program.
- Some Smart Plug-ins may require additional configuration or user rights when the agent runs under an alternative user. For more details, see the documentation for individual Smart Plug-ins.

## Limitations of Using a Non-Default User

The non-default (non-root or non-privileged) agent user that you want to use has the following limitations:

- The non-privileged user mode is not supported on HP-UX platforms.
- The non-privileged user mode is not supported on the HPOM management server but mixed user mode is supported on the HP Operations Manager for UNIX, Linux and Solaris from version 9.20.
- The non-privileged user and mixed modes are not supported on AIX WPAR.
- The BYLS metrics data cannot be collected for Xen, KVM, VMware vSphere, Hyper-V and other virtualization domains.
- By default, the agent user with non-privileged and mixed user modes will not have permission to read the monitored log file.

- By default, the agent user with non-privileged and mixed user modes will not have permission to start a program using an automatic command, operator-initiated command, tool, or scheduled task.
- HP Operations Smart Plug-ins may require additional configuration or user rights if the agent user with non-privileged and mixed modes does not have administrative rights.
- The HPE Operations Agent cannot collect metrics starting with `PROC_REGION_*` or `PROC_FILE_*` for all instances of processes owned by non-privileged users. Also, depending on the operating system, processes running with higher privileges such as **ovbbccb** and `sshd` will be either available or unavailable in the non-privileged mode.
- On Windows, the metric `PROC_USER_NAME` is displayed as `Unknown` for processes owned by users other than the agent user.
- On AIX, you may see the following error message in the command line console (or in the `oainstall.log` file in the `/var/opt/OV/log` directory) after you configure the agent to use the non-default user:
 

```
Product activation failure. Refer to the log file for more details.

Ignore this error.
```
- On Solaris, HPE Operations Agent gets the process details only up to 80 characters, which is a limitation of Solaris. **opcmona** reads the `/proc/pid/psinfo` file and stores the results in a structure. If extended information is required later, the system reads `/proc/pid/as` file. If the agent is running as a non-root user and does not have permission to open `/proc/pid/as` file, then it compares the process details with the limited information available in `psinfo`.

## Configure the Agent User during Installation

At the time of installation, you can configure the HPE Operations Agent to run under a non-default user (other than root or Local System) on the system. For this purpose, you must install the agent with the help of the profile file for manual installation or the defaults file for HPOM-assisted remote installation. If you cannot configure this at the time of installation, perform the post-installation configuration steps to change the default agent user (see ["Configuring the Agent User after Installation" on page 78](#)).

**Note:** You cannot use this procedure if you want to install the agent on Windows nodes remotely from the HPOM console. While installing the agent on Windows nodes from the HPOM console, install the agent in the *inactive* mode, and then use one of the post-installation configuration procedures to configure the agent to run with a non-default user.

To configure the agent during installation to run under a non-default user, follow these steps:

1. Make sure the user is created on the system and the user meets all the requirements.
2. If you want to install the HPE Operations Agent manually on the node, create a **profile** file.
  - a. On the system where you want to install the agent, create a new file and open the file with a text editor.
  - b. Type one of the following statements to specify the mode of agent's mode of operation:

To run the agent under a non-root or non-Local System account, type:

```
set eaagt:MODE= NPU
```

```
set eaagt:OPC_RPC_ONLY=TRUE
```

To run only the Operations Monitoring Component with a non-root or non-Local System account, type:

```
set eaagt:MODE= MIXED
```

```
set eaagt:NPU_TASK_SET=EVENT_ACTION
```

- c. *On Windows only.* Type the following statement:

```
set eaagt:OPC_PROC_ALWAYS_INTERACTIVE=NEVER
```

**Note:** This step is required to successfully run automatic and operator-initiated actions on the node from HPOM when the agent runs in the NPU or MIXED mode.

- d. Type the following statement:

**Note:** This is a mandatory step for UNIX/Linux nodes. You can skip this step for Windows nodes, but it is recommended that you configure these settings for Windows nodes as well.

```
set bbc.cb:SERVER_PORT=<Comm_Port>
```

```
set eaagt:SNMP_TRAP_PORT=<SNMP_Port>
```

**Note:** Since the default communication port for the agent is 383 and the non-root user on UNIX/Linux does not have the permission to access ports below 1024, you must perform this step to assign a non-default communication port to the agent.

In this instance,

*<Comm\_Port>* is the communication port number of your choice.

*<SNMP\_Port>* is the port at which the HPE Operations Agent receives SNMP traps.

These ports must be higher than 1024 since a non-root user on UNIX/Linux cannot access ports below 1024.

- e. Type the following statements:

```
set ctrl.sudo:OV_SUDO_USER=<User_Name>
```

```
set ctrl.sudo:OV_SUDO_GROUP=<User_Group>
```

In this instance, *<User\_Name>* is the name of the non-default user; *<User\_Group>* is the group where the non-default user belongs.

If you want to install the agent remotely from the HPOM console, configure installation defaults:

**Note:** You cannot use this procedure if you want to install the agent on Windows nodes. For Windows nodes, configure the agent user by manually installing the agent on the node or by performing the post-installation configuration.

- a. Go to the following directory:

**On HPOM for Windows:**

```
<share_dir>\conf\PMAD
```

**On HPOM for HP-UX/Linux/Solaris:**

```
/etc/opt/OV/share/conf/OpC/mgmt_sv
```

- b. Save the following file:

**On HPOM for Windows:**

Save the `agent_install_defaults.cfg.sample` file as `agent_install_defaults.cfg`.

**On HPOM for HP-UX/Linux/Solaris:**

Save the `bbc_inst_defaults.sample` file as the `bbc_inst_defaults` file.

- c. Open the file with a text editor.

- d. Add the following content:

```
[eaagt]
<node_details> : MODE=<MODE>
<node_details> : OPC_RPC_ONLY=TRUE
<node_details>: NPU_TASK_SET=EVENT_ACTION
<node_details>: SNMP_TRAP_PORT=<SNMP_Port>
```

```
[ctrl.sudo]
<node_details> : OV_SUDO_USER=<User_Name>
<node_details> : OV_SUDO_GROUP=<User_Group>
[bbc.cb]
<node_details>: SERVER_PORT=<Comm_Port>
```

In this instance:

`<node_details>` is a pattern that matches one or more node names or IP addresses. Use standard HPOM pattern syntax. For example:

- `node1.example.com` matches any node with a name that contains the string `node1.example.com`
- `example.com$` matches any node with a name that ends with `example.com`
- `^192.168.<<#> -lt 10>` matches any node with an IP address in the range 192.168.0.0 to 192.168.9.255

`<MODE>` is the mode of operation of the agent (NPU or MIXED)

`<User_Name>` is the name of the non-default user

`<User_Group>` is the group where the non-default user belongs

`<Comm_Port>` is the communication port number of your choice. This must be higher than 1024. You must also configure the management server so that it connects to `<Comm_Port>` when it communicates with this node. For more information, see *Configuring the Communication Broker Port* in the *HPE Operations Agent and HPE Operations Smart Plugins for Infrastructure Installation Guide*.

`<SNMP_Port>` is the port at which the HPE Operations Agent receives SNMP traps. This must be higher than 1024 so that all the SNMP traps from various sources can be sent to the `<SNMP_Port>`.

e. Save the file.

3. If you want to configure the agent during installation to run under NPU to root mode, then add the following text in the profile file:

**set eaagt:MODE=**

**For example:**

```
set eaagt:MODE=
```

```
set eaagt:SNMP_TRAP_PORT=<SNMP_Port>
set eaagt:OPC_RPC_ONLY=TRUE
set bbc.cb:SERVER_PORT=<Comm_Port>
set ctrl.sudo:OV_SUDO_USER=root
set ctrl.sudo:OV_SUDO_GROUP=root
```

4. Install the HPE Operations Agent.

## Configuring the Agent User after Installation

If you are not able to configure the HPE Operations Agent to use a non-default user at the time of installation, you can use the `-configure` option of the `oainstall` script (which is available on the agent node) or the `ovswitchuser` command after installation to complete this configuration.

## Changing the Default User on Windows

If you are not able to configure the agent to run with a non-default user at the time of installation, it is recommended that you install the HPE Operations Agent in the *inactive* mode. For more information, see the *HPE Operations Agent and HPE Operations Smart Plug-ins for Infrastructure Installation Guide*.

You can use one of the following methods to configure the agent to use a non-default user:

- [Use a Profile File](#)
- [Use the ovswitchuser Command](#)

## Alternative Method: Use the ovswitchuser Command

**Note:** Make sure to stop all the Operations Agent processes before you start using the `ovswitchuser.vbs` command.

If you do not want to use a profile file, follow these steps:

**Note:** Configuration with the profile file is the recommended configuration procedure.

1. Stop the agent:

**On Windows 64-bit nodes:**

```
%ovinstalldir%bin\win64\opcagt -kill
```

**On other Windows nodes:**

```
%ovinstalldir%bin\opcagt -kill
```

2. Run the following command to configure the agent to run with a non-default user:

```
cscript "%ovinstalldir%bin\ovswitchuser.vbs" -existinguser<DOMAIN\USER>-existinggroup<GROUP>-passwd<PASSWORD>
```

In this instance:

<DOMAIN\USER> is the domain and user name.

<GROUP> is the name of the group that the user belongs to, for example AgentGroup.

<PASSWORD> is the user's password.

**Note:** The command assigns the user rights required for basic agent functionality at group level, not to the individual user. Therefore, take care when you select the group to use. It is advisable to create a new group specifically for the agent user, and add the agent user as a member.

3. Run the following command to set necessary permissions to the non-default user:

```
cscript %ovinstalldir%\bin\xpl\ovsetscmpermissions.vbs -user<User_Name> -f
```

In this instance, <User\_Name> is the name of the non-default user.

4. Run one of the following commands:

To run all components of the agent under a non-Local System account:

**On Windows 64-bit nodes:**

```
%OvInstallDir%bin\win64\ovconfchg -ns eaagt -set MODE NPU
```

**On all other Windows nodes:**

```
%OvInstallDir%bin\ovconfchg -ns eaagt -set MODE NPU
```

To run only the Operations Monitoring Component with a non-Local System account:

**On Windows 64-bit nodes:**

```
%OvInstallDir%bin\win64\ovconfchg -ns eaagt -set MODE MIXED
```

**On all other Windows nodes:**

```
%OvInstallDir%bin\ovconfchg -ns eaagt -set MODE MIXED
```

5. Run the following commands:

**On Windows 64-bit nodes:**

```
%OvInstallDir%bin\win64\ovconfchg -ns ctrl.sudo -set OV_SUDO_USER<User_Name>
```

```
%OvInstallDir%bin\win64\ovconfchg -ns ctrl.sudo -set OV_SUDO_GROUP<Group_Name>
```

```
%OvInstallDir%bin\win64\ovconfchg -ns eaagt -set OPC_PROC_ALWAYS_INTERACTIVE  
NEVER
```

**On all other Windows nodes:**

```
%OvInstallDir%bin\ovconfchg -ns ctrl.sudo -set OV_SUDO_USER<User_Name>
```

```
%OvInstallDir%bin\ovconfchg -ns ctrl.sudo -set OV_SUDO_GROUP<Group_Name>
```

```
%OvInstallDir%bin\ovconfchg -ns eaagt -set OPC_PROC_ALWAYS_INTERACTIVE NEVER
```

In this instance, <User\_Name> is the name of the non-default user; <Group\_Name> is the group where the non-default user belongs.

6. If you have chosen the non-privileged mode of operation, run the following command:

**On Windows 64-bit nodes:**

```
%OvInstallDir%bin\win64\ovconfchg -ns eaagt -set OPC_RPC_ONLY TRUE
```

**On all other Windows nodes:**

```
%OvInstallDir%bin\ovconfchg -ns eaagt -set OPC_RPC_ONLY TRUE
```

7. If you have chosen the mixed mode of operation, run the following command:

**On Windows 64-bit nodes:**

```
%OvInstallDir%bin\win64\ovconfchg -ns eaagt -set NPU_TASK_SET EVENT_ACTION
```

**On all other Windows nodes:**

```
%OvInstallDir%bin\ovconfchg -ns eaagt -set NPU_TASK_SET EVENT_ACTION
```

8. Run the following command:

**Note:** This is a requirement for UNIX/Linux nodes and not a mandatory step on Windows nodes. However, it is recommended that you complete this step on Windows nodes as well.

**On Windows 64-bit nodes:**



```
%OvInstallDir%bin\win64\ovconfchg -ns eaagt -set SNMP_TRAP_PORT <SNMP_Port>
```

```
%OvInstallDir%bin\win64\ovconfchg -ns bbc.cb -set SERVER_PORT<Comm_Port>
```

**On all other Windows nodes:**

```
%OvInstallDir%bin\ovconfchg -ns eaagt -set SNMP_TRAP_PORT <SNMP_Port>
```

```
%OvInstallDir%bin\ovconfchg -ns bbc.cb -set SERVER_PORT<Comm_Port>
```

In this instance,

<Comm\_Port> is the communication port number of your choice. If you set SERVER\_PORT to 383, no additional configuration is required. If you do not set the port value to 383, make sure to configure the port on the HPOM management server.

<SNMP\_Port> is the port at which the HPE Operations Agent receives SNMP traps.

These ports must be higher than 1024.

- Restart the agent:

**On Windows 64-bit nodes:**

```
%ovinstalldir%bin\win64\opcagt -start
```

**On all other Windows nodes:**

```
%ovinstalldir%bin\opcagt -start
```

## Changing the Default User on UNIX/Linux

If you are not able to configure the agent to run with a non-default user at the time of installation, it is recommended that you install the HPE Operations Agent in the *inactive* mode. For more information, see the *HPE Operations Agent and HPE Operations Smart Plug-ins for Infrastructure Installation Guide*.

You can use one of the following methods to configure the agent to use a non-default user:

- [Use a Profile File](#)
- [Use the ovswitchuser Command](#)

### Use a Profile File

To change the default agent user with the help of a profile file, follow these steps:

1. On the system where you want to install the agent, create a new file and open the file with a text editor.

2. Type one of the following statements to specify the mode of agent's mode of operation:

To run the agent under a non-Local System account, type:

**set eaagt:MODE=NPU**

To run only the Operations Monitoring Component with a non-Local System account, type:

**set eaagt:MODE=MIXED**

3. If you have selected the non-privileged mode (that is, if you typed `set eaagt:MODE=NPU` in the previous step), type the following statement:

**set eaagt:OPC\_RPC\_ONLY=TRUE**

4. If you have selected the non-privileged mode (that is, if you typed `set eaagt:MODE=NPU` in the previous step), type the following statements:

**set eaagt:SNMP\_TRAP\_PORT=<SNMP\_port\_number>**

**set bbc.cb:SERVER\_PORT=<Comm\_port\_number>**

**Note:** This is a requirement for UNIX/Linux nodes since the non-root user on UNIX/Linux does not have the permission to access ports below 1024.

In this instance,

*<Comm\_Port>* is the communication port number of your choice.

*<SNMP\_Port>* is the port at which the HPE Operations Agent receives SNMP traps.

These ports must be higher than 1024.

5. If you have selected the mixed mode (that is, if you typed `set eaagt:MODE=MIXED` in [step 2](#)), type the following statement:

**set eaagt:NPU\_TASK\_SET=EVENT\_ACTION**

6. Type the following statements:

**set ctrl.sudo:OV\_SUDO\_USER=<User\_Name>**

**set ctrl.sudo:OV\_SUDO\_GROUP=<Group\_Name>**

In this instance, *<User\_Name>* is the name of the non-default user; *<Group\_Name>* is the group where the non-default user belongs.

7. Save the file into a local directory on the system.

8. Reconfigure the agent to run with the user specified in the profile file:
  - a. Go to the following location on the node:

```
/opt/OV/bin/OpC/install
```

- b. Run the following command:

```
./oainstall.sh -a -configure -agent_profile<path>/<profile_file>
```

In this instance, *<profile\_file>* is the name of the profile file; *<path>* is the complete path to the profile file.

## Alternative Method: Use the ovswitchuser Command

**Note:** Make sure to stop all the Operations agent processes before you start using **ovswitchuser.sh** command.

If you do not want to use a profile file, follow these steps:

**Note:** Configuring with the profile file is the recommended configuration procedure.

1. Go to the following directory:

**On HP-UX/Linux/Solaris:**

```
/opt/OV/bin
```

**On AIX:**

```
/usr/lpp/OV/bin
```

2. Run the following command to stop the agent:

```
./opcagt -kill
```

3. Run the following command to configure the agent to run with a non-default user:

```
./ovswitchuser.sh -existinguser<User_Name>-existinggroup<Group_Name>
```

In this instance:

*<User\_Name>* is the name of the user that the agent runs under.

*<Group\_Name>* is the name of the group that the user belongs to, for example AgentGroup. The command gives this group full control of all files in the agent data directory, and also full control of

all installed packages. If you previously started the command and specified a different group, the command removes control of the files for the previous group.

The group ID flag is set on the agent's data directories. This flag means that the group that you specify will also own any new files and subdirectories in the agent's base directories.

**Note:** The command assigns the user rights required for basic agent functionality at group level, not to the individual user. Therefore, take care when you select the group to use. It is advisable to create a new group specifically for the agent user, and add the agent user as a member.

4. Run one of the following commands:

To run all components of the agent under a non-root user:

```
./ovconfchg -ns eaagt -set MODE NPU
```

To run only the Operations Monitoring Component with a non-root user:

```
./ovconfchg -ns eaagt -set MODE MIXED
```

5. Run the following command:

**Note:** This is a requirement for UNIX/Linux nodes since the non-root user on UNIX/Linux does not have the permission to access ports below 1024.

```
./ovconfchg -ns eaagt -set SNMP_TRAP_PORT <SNMP_Port>
```

```
./ovconfchg -ns bbc.cb -set SERVER_PORT<Comm_Port>
```

In this instance,

<Comm\_Port> is the communication port number of your choice. If you set SERVER\_PORT to 383, no additional configuration is required. If you do not set the port value to 383, make sure to configure the port on the HPOM management server.

<SNMP\_Port> is the port at which the HPE Operations Agent receives SNMP traps.

These ports must be higher than 1024.

6. Run the following commands to start the agent:

```
./opcagt -start
```

After you configure the agent to run as a non-root user, the following error message may appear in the **System.txt** file:

```
ovbbccb (22461/1): (bbc-188) Cannot change the root directory for the current process.
```

Ignore this error.

## Chapter 9: Reducing the Installation Time

In previous versions of the HPE Operations Agent, the installer program used to take a significant time to validate the signatures when installing HPE Operations Agent media on Windows nodes without internet due to Certificate Revocation List (CRL) checks.

With HPE Operations Agent 12.02, you can reduce the installation time on Windows node by removing the signatures from the packages and MSI scripts. Use one of the following methods to remove the signatures:

- Use the `removesign` option with the zip media
- Use the Profile File

### Using the `removesign` option with the zip media

**Note:** The `removesign` option will work with MSI package only and is not supported with hotfix or patch installation.

To create a ZIP of the product media without the digital signatures from msi packages and vbscripts, follow the steps:

1. Log on to the node as an administrator.
2. Go to the media root.
3. Run the following command:

#### **On Windows**

```
cscript oainstall.vbs -createzip -p WIN -removesign
```

After the command is executed, a zip file containing the updated media (without signatures) is available at the location `-%TEMP%/OA_ZIP_MEDIA` folder.

Copy the zip media to another folder. To use the zip media, unzip the media at the location where the agent must be installed and then start installing the HPE Operations Agent.

Installation time is significantly reduced to less than 4 minutes when you use the `removesign` option.

## Using the Profile file

You can use the profile file option to remove the digital signatures from vbscripts while installing the HPE Operations Agent.

Follow the steps:

1. On the system where you want to install the agent, create a new file and open the file using a text editor.
2. Add the following content in the profile file to disable the signature checks at the time of installation: **set eaagt:INSTALL\_REMOVESIGN=True**
3. Save the file in a local directory.
4. Run the following command to install the HPE Operations Agent with a profile file:

### On Windows

```
cscript oainstall.vbs -i -a -agent_profile <path>\<profile_file> -s
<management_server> [-cs <certificate_server>] [-install_dir <install_
directory> -data_dir <data_directory>]
```

In this instance:

<path> is the path to the profile file.

<profile\_file> is the name of the profile file.

<management\_server>: FQDN of the management server.

<certificate\_server>: FQDN of the certificate server.

<install\_directory>: Path to place all packages and binary files on the node.

<data\_directory>: Path to place all data and configuration files on the node.

For more information, see [Installing HPE Operations Agent using Profile File](#).

Installation time is significantly reduced to less than 8 minutes when you use the profile file option to install the HPE Operations Agent.

# Using the `removesign` option while deploying HPE Operations Agent from HPOM and HPE OMi

Use one of the following methods:

## Method 1

1. Create zip media on any Windows system. For more information, see [Using the `removesign` option with the zip media](#).
2. Copy the zip media to another folder on the management server. To use the zip media, unzip the media at the location from where the Agent is registered.
3. Use the unzipped folder location to register the HPE Operations Agent on HPOM or HPE OMi.

To register HPE Operations Agent on HPOM, see [Registering the HPE Operations Agent and Infrastructure SPIs on the HPOM Management Server](#).

To register the HPE Operations Agent on HPE OMi, see the section `opr-package-manager` Command-Line Interface in the chapter *Command-Line Interfaces* in the *OMi Administration Guide*.

**Note:** If you use this method to remove signatures, then the Agents without signatures are deployed on all the nodes.

## Method 2

You can also use the `removesign` option with the profile file to deploy HPE Operations Agent from HPOM or HPE OMi. For more information, see [Installing HPE Operations Agent using Profile File](#).



# Chapter 10: Installing the HPE Operations Agent using Agent Installation Repository

In a typical environment, there are multiple versions of HPE Operations Agent deployed in a combination of different operating systems. You can install the **Agent Installation Repository** on a Linux operating system and deploy different versions of HPE Operations Agent available in the repository on Windows and Linux operating systems.

The Agent Installation Repository can be hosted in your environment by using any one of the following:

- [Standalone Agent Installation Repository](#)
- [Agent Installation Repository as a Virtual Appliance](#)

## Standalone Agent Installation Repository

Agent Installation Repository can be installed on a Linux machine using the standalone TAR file provided to set up standalone repository. The same repository can act as a **Yum repository** for the HPE Operations Agent and LCore packages. For more information about Yum repository, see [Data Flow in Yum Repository](#).

**Note:** The Standalone Agent Installation Repository is supported *only* on Linux x64 and x86 architecture.

### Prerequisites

1. The **createrepo** utility should be available and running on the system.

**Note:** **createrepo** is a OS utility. If it is not installed, then you can install it using the following command:

```
yum install createrepo
```

2. Make sure that a web server is running on the system.

**For example:** For RHEL machine, you can deploy on Apache Web Server.

- To start the web service, run the following command:

```
service httpd start
```

## Installing the Standalone Agent Installation Repository on a Linux server or on the HP Operations Manager for Linux 9.x

Follow the steps:

1. Log on to the server where you want to install the repository.
2. Open the Standalone Agent Installation Repository (**HPOvOpsAgt-12.xx.xxx-AIR.tar**) media and extract the contents.

The **HPOvOpsAgt-12.xx.xxx-AIR.tar** file contains the **RPMs** and a wrapper script (**oainstall\_air.sh**) to install the RPMs.

3. You can install the Standalone Agent Installation Repository on a Linux server or on the HP Operations Manager for Linux 9.x.
  - a. Run the following command to install the Standalone Agent Installation Repository on a Linux server:

```
./oainstall_air.sh -i -wu <webURL> -wr <web root path>
```

**For Example:** `./oainstall_air.sh -i -wu https://hostname:portnumber -wr /var/www/html`

In this instance,

<wu>	specifies the webURL of the web server
<https://hostname:portnumber>	specifies the URL of the web server where portnumber is the port on which this instance of the web server is running.
<wr>	specifies the web root path on the system. For Example: /var/www/html in RHEL for Apache web server.

- b. Run the following command to install the Standalone Agent Installation Repository on the HP Operations Manager for Linux 9.x:

```
oainstall_air.sh -i
```

This command helps you install the Standalone Agent Installation Repository on the OVTomcat web server. The console displays the home page URL for the Agent Installation Repository after installation.

```
Refer to the logs for details : /var/tmp/oainstall_air.log
INFO: Checking for OM Server.
INFO: HOME page url : http://Host Name:8081/oarepo
INFO: Check ARCH supported for Standalone Repository installation
INFO: Standalone installation repository supported for : x86_64. Proceeding
INFO: with installation
INFO: Found package to install: HPOA_AIRVA_WEBAPP-1
INFO: Installing the packages: ./HPOA_AIRVA_WEBAPP_1.00.00-1.00.00_i386.rpm
INFO: Installed package successfully
INFO: Found package to install: HPOA_AIRVA_MEDIA_12_00-1
INFO: Installing the packages:
INFO: ./HPOA_AIRVA_MEDIA_12_00_1.00.00-1.00.00_i386.rpm
INFO: Installed package successfully
INFO: Found package to install: HPOA_AIRVA_MEDIA_11_14-1
INFO: Installing the packages:
INFO: ./HPOA_AIRVA_MEDIA_11_14_1.00.00-1.00.00_i386.rpm
INFO: Installed package successfully
You have new mail in /var/spool/mail/root
```

**Note:** On the HP Operations Manager for Linux, `oainstall_air.sh` runs without parameters (webURL and web root path). The media on the HP Operations Manager for Linux is available in the following location for Agent Installation Repository:

`/opt/OV/nonOV/tomcat/b/www/webapps/AIRVA/media`

### Verification


Follow the steps:

1. Restart the web server using the following command:  

```
service httpd restart
```
2. Go to the browser and type `https://hostname:portnumber/oarepo/` to open the Agent Installation Repository home page.

## Operations Agent

This repository serves as a central installation and deployment station for Operations Agent software. The Operations Agent software can be installed on your servers from this repository, for the purposes of centralized monitoring via HP Operations Manager or for performance data collection.



**Packages download**

The main way of interacting with the repository is using the oarepo script available here for [Linux](#) and here for [Windows](#).

- oarepo -ll-install -sl-server <server name> [-vl-version <version no.>] [-oml-om\_server <OM server name>] [-pel-profile\_enable] [<[-unsecl-unsafe]>][<[-secl-secure]>]
- oarepo -dl-download -sl-server <server name> [-vl-version <version no.>] [-pfl-platform <LINUX|WIN>]
- oarepo -ll-list [-sl-server <server name>] [-pfl-platform <LINUX|WIN>]
- oarepo -hl-help

**Versions Available**

- 11.14.12.00

3. Check the log file: `/var/tmp/oainstall_air.log`
4. Run the following command to check the list of RPMs installed or removed:

```
rpm -qa | grep -i hpoa*
```

In this instance,

\* displays the list of RPMs starting with **hpoa**.

## Removing the Standalone Agent Installation Repository

To remove the standalone repository, follow the steps:

1. Log on to the node.
2. Run the following command:

```
./oainstall_air.sh -r
```

# Agent Installation Repository as a Virtual Appliance

Agent Installation repository is available as a Virtual Appliance and can be deployed in VMware environment.

### Prerequisite

Agent Installation Repository Virtual Appliance for VMware vSphere 4.x and 5.x.

### Deploying Agent Installation Repository Virtual Appliance

To deploy the virtual appliance with the HPE Operations Agent from the vSphere console:

1. Log on to vCenter using vSphere client.
2. Click **File > Deploy OVF Template**. The **Deploy OVF Template** window opens.
3. Provide the source location to download and install the **OVF Package** and then click **Next**.
4. Verify the **OVF Template** details and click **Next**.
5. Accept the end user license agreement and click **Next**.
6. Specify a name and location for the deployed template and click **Next**.
7. Select a destination storage for the virtual machine files and click **Next**.
8. Provide the details of network properties such as **Default Gateway**, **DNS**, **Interface IP Address**, and the **Netmask** and then click **Next**.
9. Click **Finish** to start the deployment.

### Verifying the Deployment

1. Go to the repository home page URL using the IP or FQDN of the VA instance that is deployed:

```
https://<system_name or ip>:5480/oarepo/
```

**Note:** The Default login credentials are:

User name: *root*

Password: *password*

2. Go to the browser and use the repository home page URL to open the Agent Installation Repository.

## Deploying HPE Operations Agent Using the Agent Installation Repository

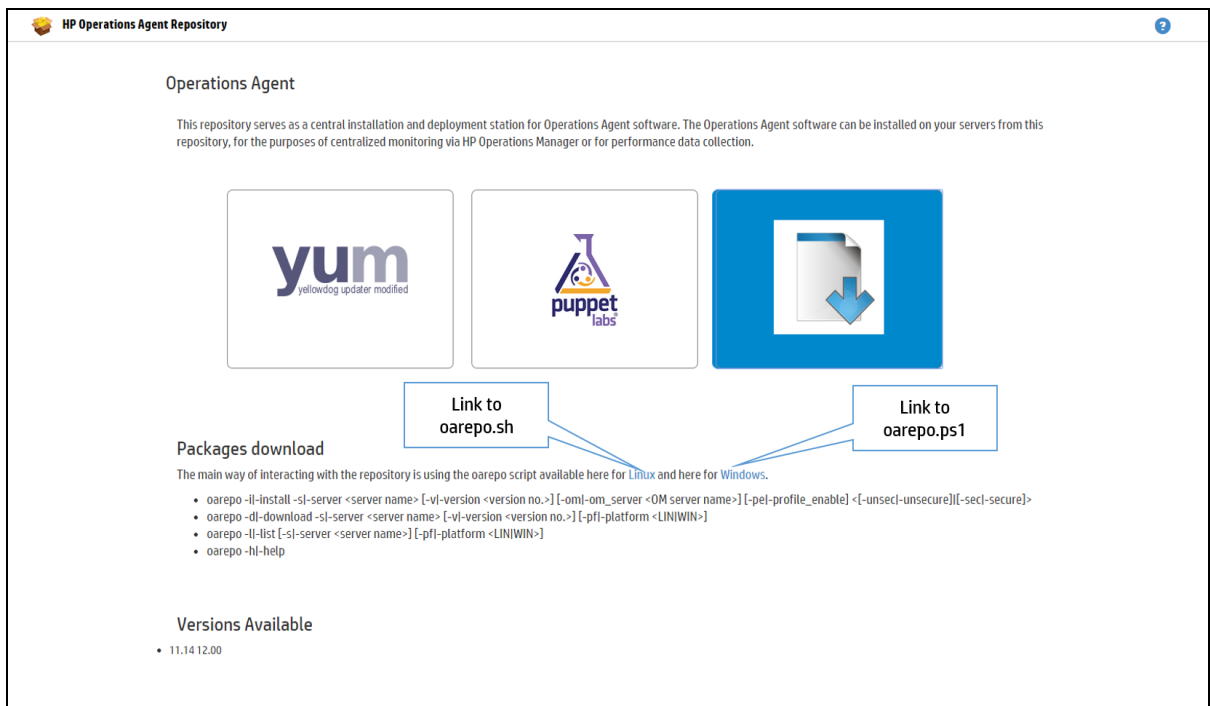
HPE Operations Agent can be installed using the Agent Installation Repository using any of the following options:

- Using the **oarepo** scripts
- Using the Yum repository
- Using the Puppet modules

### Installing the HPE Operations Agent using the oarepo scripts

To install the HPE Operations Agent using the oarepo scripts, follow the steps:

1. Log on to the node where you want to install the HPE Operations Agent.
2. Download the **oarepo.sh** or **oarepo.ps1** script for Linux or Windows respectively on the systems where you need the HPE Operations Agent to be installed using the Agent Installation Repository landing page.



3. Install the HPE Operations Agent on the server. Run the following command:

```
oarepo -i|-install -s|-server <server url> [-v|-version <"version no.">] [-om|-om_server <OM server name>] [-pe|-profile_enable] <[-unsec|-unsecure] <[-sec|-secure]>
```

For example:

#### On Windows

```
./oarepo.ps1 -i -s https://myhostname:5480 -v "12.01" -om <omservername> -sec
```

**On Linux**

```
./oarepo.sh -i -s https://myhostname:5480 -v "12.01" -om <omservername> -unsec
```

In this instance,

- i Is used to install and download the HPE Operations Agent packages.
- s Specifies the server URL along with the port number where the agent installation repository is hosted.
- v Specifies the version of the HPE Operations Agent.

**For example:** "12.01"

You can get the version from the Agent Installation Repository page.

- om Specifies the OM server name to which the HPE Operations Agent has to be activated.
- pe If you specify `-pe`, then the default profile file settings are applied. If you don't specify `-pe`, then none of the profile file settings are applied. The profile file is available in the following location:

```
<web root path>/AIRVA/media
```

The file name is: **profile\_file\_default**

**Note:** All profile file options are applicable. For more information, see [Installing HPE Operations Agent using Profile File](#).

- sec Is used if SSL certificate is imported and installed on the client.
- Is used if SSL certificate is not imported.
- unsec

**Note:** If the version is not mentioned in the command, then by default latest version of HPE Operations Agent is downloaded. Also, option `-d` can be used *only* to download the HPE Operations Agent packages.

**Verifying the Version of the HPE Operations Agent**

To check the version of HPE Operations Agent installed, run the following command:

**On Windows:** %ovinstalldir%/bin/opcagt -version

**On Linux:** /opt/OV/bin/opcagt -version

**Installing the HPE Operations Agent using the Yum Repository**

Yum is a utility which checks for the repository details mentioned in the configuration file and installs the HPE Operations Agent packages on those nodes. The Yum repository for the HPE Operations Agent is provided along with the Agent Installation Repository.

You can access the Yum repository on the Virtual Appliance using the following URL:

`https://hostname:portnumber/oa/yum_oa_all.repo`

In this instance,

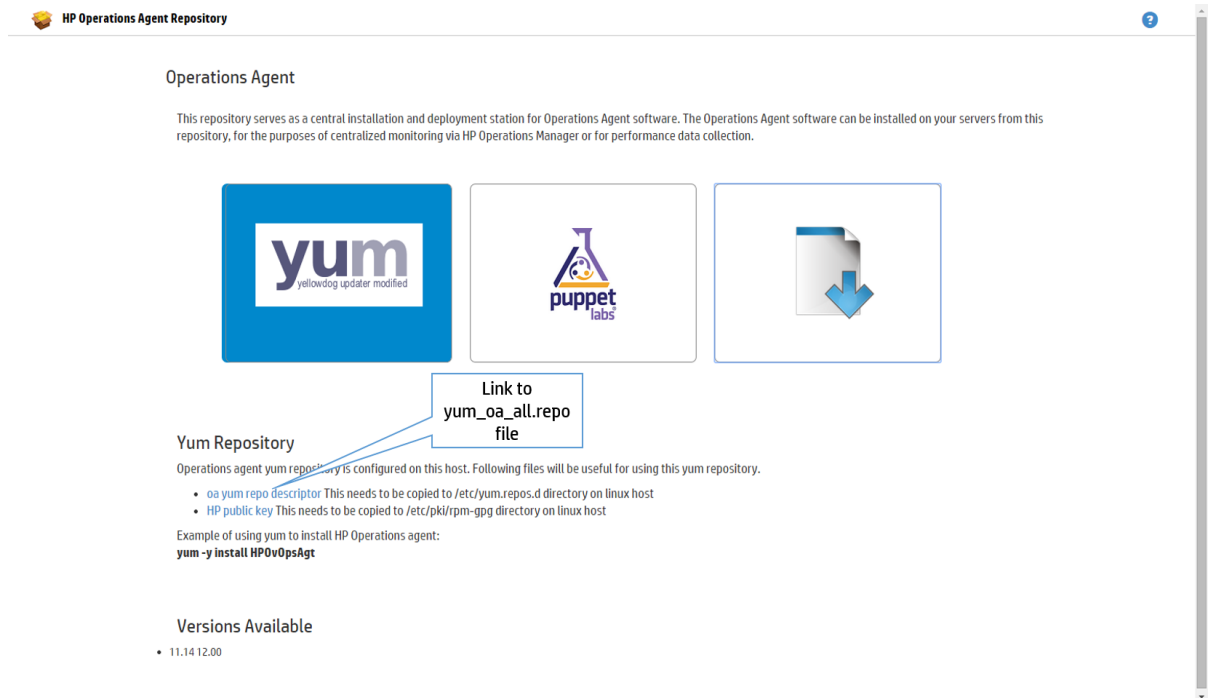
`hostname` is the IP address of the VM.

`portnumber` is the default port of the VM or it can be any other port if set.

To install the HPE Operations Agent using Yum repository, follow the steps:

**Note:** For information on prerequisites to install the HPE Operations Agent, see the chapter [Prerequisites to Install the HP Operations Agent on a Node](#).

1. Log on to the target node.
2. Download and copy the `yum_oa_all.repo` file from `https://hostname:portnumber/oa/yum_oa_all.repo` to `/etc/yum.repos.d/`.



In this instance,

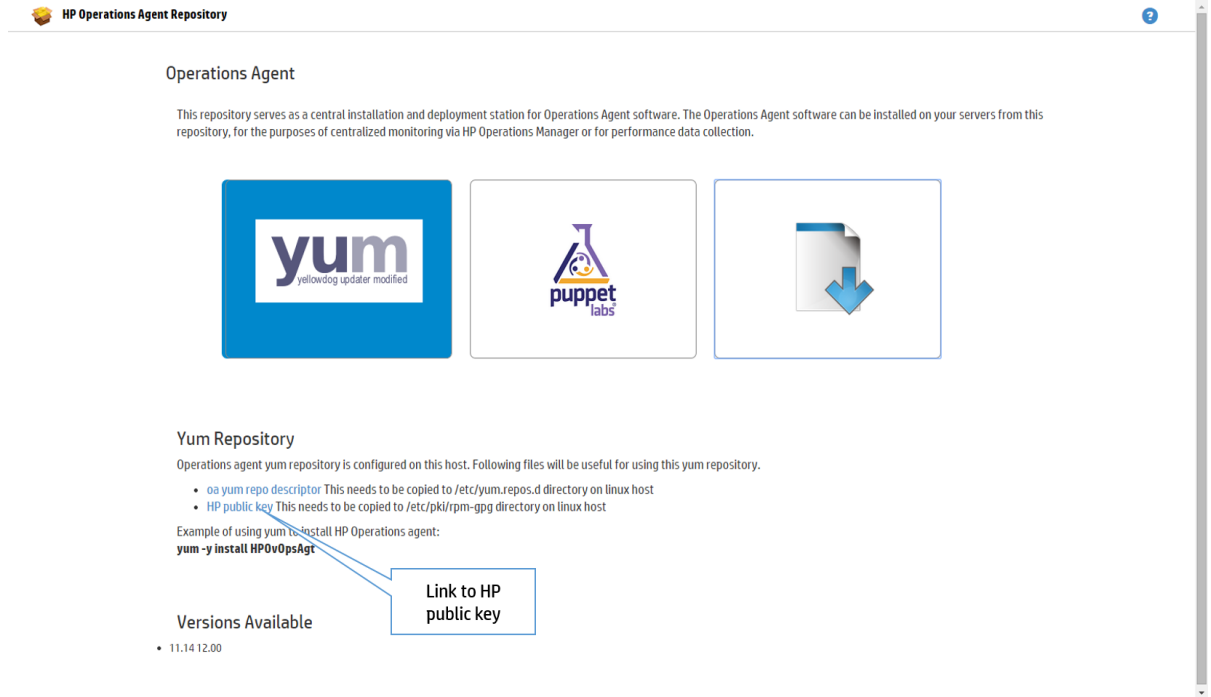


hostname is the IP address of the VM.

portnumber is the default port of the VM or it can be any other port if set.

3. Download and copy the HP public key from

https://hostname:portnumber/oarepo/hpPublicKey2048.pub to /etc/pki/rpm-gpg/hpPublicKey2048.



4. Run the following command to install specific versions of the HPE Operations Agent:

To install the latest version:

```
yum install HPOvOpsAgt
```

To install previous versions 11.11 and 11.14 together:

```
yum --disablerepo=oa_12.01 install HPOvOpsAgt
```

In this instance,

disablerepo is used to disable the HPE Operations Agent version you do not want to install.

5. Configure the management server by performing the following steps:

- a. Go to the following directory on the Linux node: /opt/OV/bin/OpC/install
- b. Run the following command: opcactivate -srv <management\_server> -cert\_srv <management\_server> -f

In this instance,

`<management_server>` is the FQDN of the HPOM management server.

### **Verification**

- To verify if HPE Operations Agent packages are installed, run the following command:

```
rpm -qa | grep <packagename>
```

In this instance,

`<packagename>` is the name of the HPE Operations Agent package.

**For Example:** `rpm -qa | grep <HPOvBbc>`

- To check the version of HPE Operations Agent on the node, run the following command:

**On Linux:** `/opt/OV/bin/opcagt -version`

- To check the inventory, run the following command:

**On Linux:** `/opt/OV/bin/ovdeploy -inv -includeupdates`

To remove the packages from the Target Node, see "[Removing the Packages from the Target Node](#)" on page 125.

# Chapter 11: Installing the HPE Operations Agent using the Puppet Environment

You can install the HPE Operations Agent using **Puppet** in an environment where **Puppet Master** and **Puppet Clients** are configured.

HPE Operations Agent packages are stored in the Agent Installation Repository. The puppet module available on the puppet master fetches the HPE Operations Agent packages or zip file from Agent Installation Repository and deploys the HPE Operations Agent packages on the puppet client (Linux nodes).

You can use puppet open source or puppet enterprise to deploy HPE Operations Agent on the node. For the puppet open source, you can use the OA modules and install HPE Operations Agent by using the following options:

## On Linux

- [Using Yum](#)

Or

- [Using oarepo.sh](#)

## On Windows

- [Using oarepo.ps1](#)

You can also [configure the XPL parameters by using the puppet module](#).

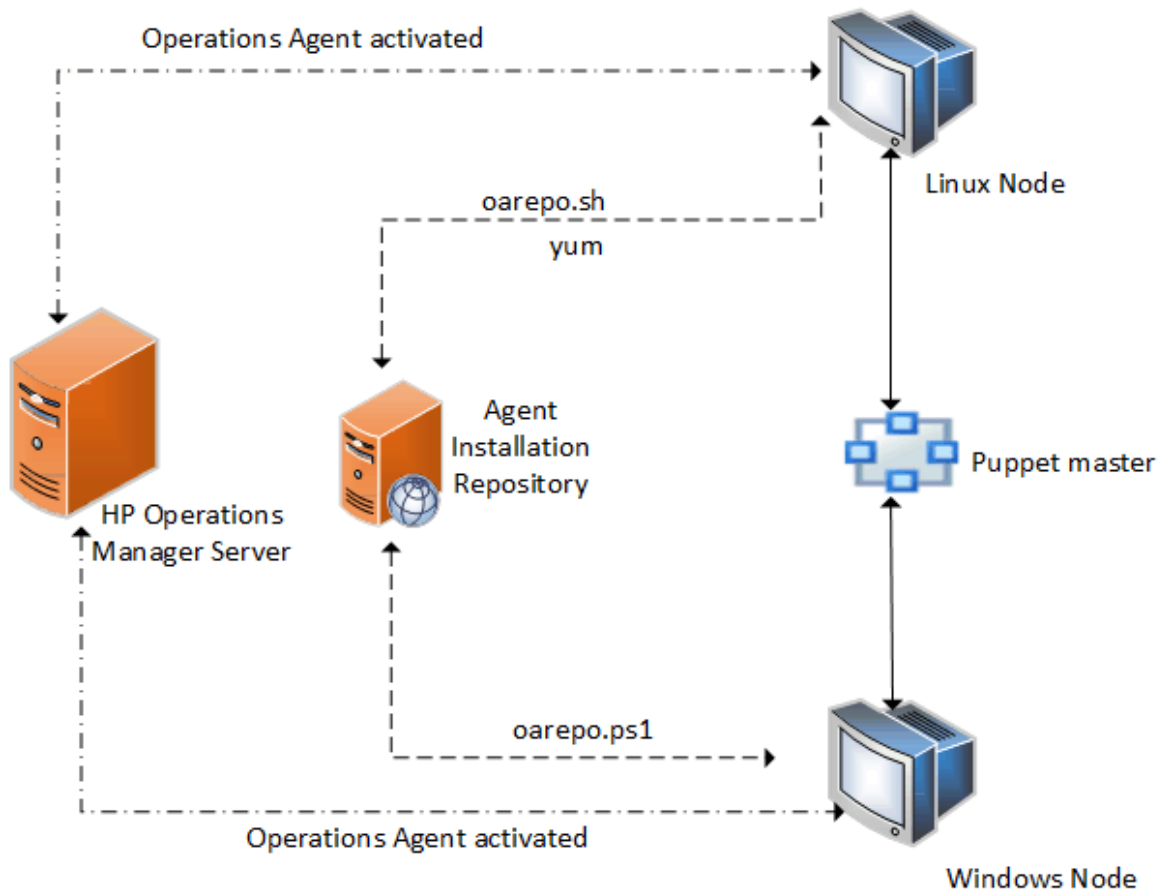
**Note:** HPE Operations Agent supports Puppet Enterprise 3.8 and 3.9 versions.

## Prerequisites

- Enable PowerShell (version 2.0 and later) on Windows
- Configure Puppet environment: puppet master and puppet clients

## Data Flow in a Puppet Environment

The following illustration shows the data flow in a puppet environment for deployment.



## Installing and Configuring the HPE Operations Agent on Linux Using YUM

To deploy the HPE Operations Agent, follow the steps:

**Note:** For information about prerequisites required to install the HPE Operations Agent, see the chapter [Prerequisites to Install the HPE Operations Agent on a Node](#).

1. Log on to the puppet master.
2. The **puppet\_modules.tar** is available on the Agent Installation Repository landing page [https://hostname:portnumber/oarepo/puppet\\_modules.tar](https://hostname:portnumber/oarepo/puppet_modules.tar). Download, copy and untar the **puppet\_modules.tar** file in the puppet modules directory.

## Operations Agent

This repository serves as a central installation and deployment station for Operations Agent software. The Operations Agent software can be installed on your servers from this repository, for the purposes of centralized monitoring via HP Operations Manager or for performance data collection.



## Puppet modules

A set of Puppet modules are created which can be useful for installing and configuring HP Operations agent on Windows and Linux puppet agent nodes. These puppet modules can be downloaded from: [hp\\_om\\_config\\_install](#). Information about how to use these puppet modules can be located in the InstallGuide.

### Versions Available

- 11.14.12.00

Link to puppet modules

<https://16.184.45.246:5480/oarepo/#tabs-3>

**For Example:** You can download the **puppet\_modules.tar** file from `/etc/puppet/modules/` on puppet master.

- For configuring the HPE Operations Agent deployment using YUM, open the `init.pp` class file from `hpoa_install_config/manifests/init.pp` on puppet module and define the modules to be deployed on the puppet client:

```
class { 'hpoa_install_config::pkginstall':
  reposerver => "$repo_server",
  version    => "$version_yum",
}

class { 'hpoa_install_config::activate':
  om_server => "$om_server",
  profile_enable => $profile_enable,
  require    => Class['hpoa_install_config::pkginstall']
}

service { 'OVCtrl':
  ensure => running,
  enable => true,
```

```
require => Class['hpoa_install_config::activate']
}
```

4. Open the `site.pp` class file from `/<puppet modules directory>/manifests/site.pp` on puppet master and define the modules to be deployed on the puppet client:

**Example: For Linux nodes:**

```
class { 'hpoa_install_config':
  om_server => "om_server",
  profile_enable => "yes",
  repo_server => "repo_server",
  secured => "-unsec",
  version => "version",
}
```

In this instance,

<code>version</code>	specifies the HPE Operations Agent version. For example, version can be 11.14.014.
<code>repo_server</code>	specifies the system name where Agent Installation Repository (VA or Standalone) is available.
<code>om_server</code>	specifies the server name to which the HPE Operations Agent has to be activated.

**Note:** Profile file based installation is enabled by default. To disable profile file based installation, set `profile_enable => "no"`. To enable profile file based installation, set `profile_enable => "yes"` or `""`. Make sure that profile file configuration settings are updated as mentioned in ["Enabling HPE Operations Agent Installation Using Profile File with Puppet" on page 107](#).

5. To test the deployment, log on to the puppet client and run the following command:

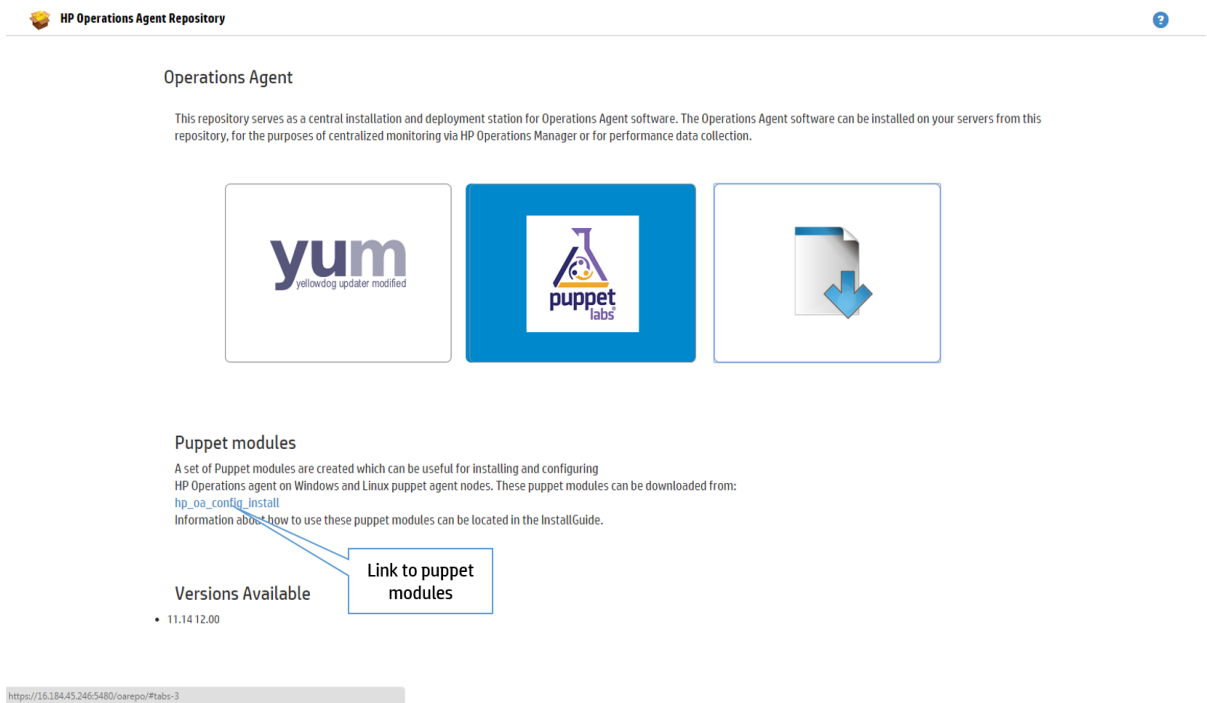
```
puppet agent --test
```

**Note:** You can verify the HPE Operations Agent version installed by using the command:  
`/opt/OV/bin/opcagt -version`

# Installing and Configuring HPE Operations Agent on Linux Using **oarepo.sh**

To deploy HPE Operations Agent, follow the steps:

1. Log on to the puppet master.
2. The **puppet\_modules.tar** is available on the Agent Installation Repository landing page [https://hostname:portnumber/oarepo/puppet\\_modules.tar](https://hostname:portnumber/oarepo/puppet_modules.tar). Download, copy and untar the **puppet\_modules.tar** file in the puppet modules directory.



**For Example:** You can download the **puppet\_modules.tar** file at `/etc/puppet/modules/` on puppet master.

3. Open the `init.pp` class file from `hpoa_install_config/manifests/init.pp` on puppet module. The `hpoa_install_config` puppet module uses the **oarepo.sh** script to download, install or configure the HPE Operations Agent from the Agent Installation Repository server. Check the **version**, **repo\_server**, and the **om\_server** details.

```
class {'hpoa_install_config':air_linux'
```

```

repo_server => $repo_server,
version     => $oarepo_version,
om_server   => $om_server
profile_enable => $profile_enable
}

```

4. Open the `site.pp` class file from `<puppet modules directory>/manifests/site.pp` on puppet master and define the modules to be deployed on the puppet client:

```

class { 'hpoa_install_config' :
repo_server => $repo_server,
version     => $oarepo_version,
om_server   => $om_server
profile_file => "yes"
secured => "-sec"
}

```

In this instance,

<code>version</code>	specifies the HPE Operations Agent version. For example, version can be 11.14.014.
<code>repo_server</code>	specifies the system name where Agent Installation Repository (VA or Standalone) is available.
<code>om_server</code>	specifies the server name to which the HPE Operations Agent has to be activated.
<code>secured</code>	use <code>-sec</code> if SSL certificate is imported and installed on the client. If SSL certificate is not imported, use <code>-unsec</code> .

**Note:** Profile file based installation is enabled by default. To disable profile file based installation, set `profile_enable => "no"`. To enable profile file based installation, set `profile_enable => "yes"` or `""`. Make sure that profile file configuration settings are updated as mentioned in ["Enabling HPE Operations Agent Installation Using Profile File with Puppet" on page 107](#).

5. To test the deployment, log on to the puppet client and run the following command:

```
puppet agent --test
```

**Note:** You can verify the HPE Operations Agent version installed by using the command:



```
| /opt/OV/bin/opcagt -version
```

## Installing and Configuring HPE Operations Agent on Windows Using **oarepo.ps1**

### **Prerequisite**

Enable PowerShell (version 2.0 and above) script execution by setting the remote signed policy. To check the policy, run the following command in PowerShell:

```
PS C:\> Get-ExecutionPolicy
```

If the policy is not specified as RemoteSigned, set it to RemoteSigned by running the following command in PowerShell:

```
PS C:\> Set-ExecutionPolicy RemoteSigned
```

In this instance,

RemoteSigned specifies that downloaded scripts must be signed by a trusted publisher before they can be run.

**Note:** RemoteSigned is the threshold level of permission required, you can also set policy as AllSigned or Unrestricted.

In this instance,

AllSigned specifies that scripts signed by a trusted publisher *only* can be run.

Unrestricted means all Windows PowerShell scripts can be run.

### **Installation**

To install HPE Operations Agent on Windows using oarepo.ps1, follow the steps:

1. Log on to the puppet master.

The **puppet\_modules.tar** is available on the Agent Installation Repository landing page [https://hostname:portnumber/oarepo/puppet\\_modules.tar](https://hostname:portnumber/oarepo/puppet_modules.tar).

2. Download, copy and untar the **puppet\_modules.tar** file in the puppet modules directory.

## Operations Agent

This repository serves as a central installation and deployment station for Operations Agent software. The Operations Agent software can be installed on your servers from this repository, for the purposes of centralized monitoring via HP Operations Manager or for performance data collection.



## Puppet modules

A set of Puppet modules are created which can be useful for installing and configuring HP Operations agent on Windows and Linux puppet agent nodes. These puppet modules can be downloaded from: [hp\\_ua\\_config\\_install](#). Information about how to use these puppet modules can be located in the InstallGuide.

### Versions Available

- 11.14.12.00

Link to puppet modules

<https://16.184.45.246:5480/oarepo/#tabs-3>

**For example:** You can download the **puppet\_modules.tar** file at `/etc/puppet/modules/` on puppet master.

3. Open the **init.pp** class file from `hpoa_install_config/manifests/init.pp` on puppet module. The **hpoa\_install\_config** puppet module uses the **oarepo.ps1** script to download, install or configure the HPE Operations Agent from the Agent Installation Repository server. Check the **version**, **repo\_server**, and the **om\_server** details.

```
class { 'hpoa_install_config::air_windows':
  repo_server => $repo_server,
  version => $oarepo_version,
  om_server => $om_server,
  profile_enable => $profile_enable
}
```

4. Open the **site.pp** class file from `/<puppet modules directory>/manifests/site.pp` on puppet master and define the modules to be deployed on the puppet client:

```
class { 'hpoa_install_config' :
  repo_server => $repo_server,
  version => $oarepo_version,
```

```

om_server    => $om_server
profile_file => "yes"
secured     => "-sec"
}

```

In this instance,

<code>version</code>	specifies the HPE Operations Agent version. For example, version can be 11.14.014.
<code>repo_server</code>	specifies the system name where Agent Installation Repository (VA or Standalone) is available.
<code>om_server</code>	specifies the server name to which the HPE Operations Agent has to be activated.
<code>secured</code>	use <code>-sec</code> if SSL certificate is imported and installed on the client. If SSL certificate is not imported, use <code>-unsec</code> .

**Note:** Profile file based installation is enabled by default. To disable profile file based installation, set `profile_enable => "no"`. To enable profile file based installation, set `profile_enable => "yes" or ""`. Make sure that profile file configuration settings are updated as mentioned in ["Enabling HPE Operations Agent Installation Using Profile File with Puppet" below](#).

- To test the deployment, log on to the puppet client and run the following command:

```
puppet agent --test
```

**Note:** You can verify the HPE Operations Agent version installed by using the command:


```
<OvInstallDir>/opcagt -version
```

## Enabling HPE Operations Agent Installation Using Profile File with Puppet

You can use the profile file option during installation to enable HPE Operations Agent to run with non-default configuration settings. For example, you can update the configuration settings such as the communication port, event interceptor port, or the license type using the profile file.

In the puppet environment, profile file is available as a template `profile_file_default.erb` with the default configuration settings for `MANAGER`, `CERTIFICATE_SERVER` and `INSTALL_OPCAUTH`.



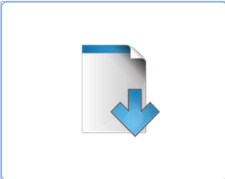
The template is available in the **puppet\_modules.tar** on the Agent Installation Repository landing page. You can download the **puppet\_modules.tar** from [https://hostname:portnumber/oarepo/puppet\\_modules.tar](https://hostname:portnumber/oarepo/puppet_modules.tar)

 HP Operations Agent Repository 2

---

**Operations Agent**

This repository serves as a central installation and deployment station for Operations Agent software. The Operations Agent software can be installed on your servers from this repository, for the purposes of centralized monitoring via HP Operations Manager or for performance data collection.

**Puppet modules**

A set of Puppet modules are created which can be useful for installing and configuring HP Operations agent on Windows and Linux puppet agent nodes. These puppet modules can be downloaded from: [hp\\_oo\\_config\\_install](#)  
 Information about how to use these puppet modules can be located in the InstallGuide.

[Link to puppet modules](#)

**Versions Available**

- 11.14.12.00

<https://16.184.45.246:5480/oarepo/#tabs-3>

The profile file is available under `hpoa_install_config/templates`.

You can configure the profile file in the following ways:

- Define the required configuration settings in the template `profile_file_default.erb`.

**For example:**

To set the custom Health View Server using the profile file during installation:

Add the following in the template `profile_file_default.erb`:

```
set agent.health:OPC_SELFMON_SERVER=hostname
```

In this instance,

*agent.health* is the configuration variable namespace.

*OPC\_SELFMON\_SERVER* is the configuration variable.

*hostname* is the value for the configuration variable. This value will be fetched during the run-time from the puppet module.

**Note:** All profile file options are applicable. For more information see, [Installing HPE Operations Agent using Profile File](#).

- Set the configuration variable in the template `profile_file_default.erb` and define the value in the `profile.pp` class file which is available under `/hpoa_install_config/manifests/profile.pp` in the puppet modules directory.

**For example:**

To set custom Health View Server using profile file during installation:

Configure the profile file, follow the steps:

- a. Set the configuration variable in the template `profile_file_default.erb` as:

```
set agent.health:OPC_SELFMON_SERVER=<%=@selfmonserver%>
```

- b. Define the value in `profile.pp` class file as:

```
$selfmonserver = "hostname"
```

In this instance,

`agent.health` is the configuration variable namespace

`OPC_SELFMON_SERVER` is the configuration variable

`<%=@selfmonserver%>` is the representation for the value

`hostname` is the value for the configuration variable. This value is fetched during run-time from the puppet module.

Profile file configuration for YUM and oarepo is provided in their respective sections.


## Configuring HPE Operations Agent Using Puppet Module to Set the XPL Parameters for the Nodes

The puppet module uses the `oa_config` custom resource to set the xpl parameters.

Follow these steps:

1. Log on to the puppet master.
2. The `puppet_modules.tar` is available on the Agent Installation Repository landing page

`https://hostname:portnumber/oarepo/puppet_modules.tar`. Download, copy, and untar the **puppet\_modules.tar** file in the puppet modules directory.

 HP Operations Agent Repository



## Operations Agent

This repository serves as a central installation and deployment station for Operations Agent software. The Operations Agent software can be installed on your servers from this repository, for the purposes of centralized monitoring via HP Operations Manager or for performance data collection.



## Puppet modules

A set of Puppet modules are created which can be useful for installing and configuring HP Operations agent on Windows and Linux puppet agent nodes. These puppet modules can be downloaded from: [hp\\_oa\\_config\\_install](#)  
Information about how to use these puppet modules can be located in the InstallGuide.

## Versions Available

- 11.14.12.00

Link to puppet modules

<https://16.184.45.246:5480/oarepo/#tabs-3>

**For Example:** You can download the **puppet\_modules.tar** file at `/etc/puppet/modules` on puppet master.

- The puppet module uses the **oa\_config** custom resource to complete the configuration. Edit the **init.pp** class file for XPL parameters:

```
oa_config
{
  ensure => present,
  notify => Service['OVCtrl'],
}
oa_config { 'coda.comm/SERVER_BIND_ADDR': value => 'localhost6', }
oa_config { 'eaagt/Dummy12': value => '12', }
oa_config { 'new_namespace/Dummy2': value => '12', }
```

In this instance,

`coda.comm` is the namespace.

`SERVER_BIND_ADDR` is the configuration variable.

`value` specifies the configuration variable value you want to update.

**Note:** The `ensure` parameter is used to set or clear the variable. By default **present** is used to set and **clear** is used to clear the configuration variable

### **Verification**

Run the following command to verify the configuration changes made through puppet provider:

**On Linux:** `/opt/OV/ovconfget <namespace>`

**On Windows:** `%ovinstalldir%bin\ovconfget <namespace>`

## Chapter 12: Installing the HPE Operations Agent Using HP Server Automation

HP Server Automation (SA) helps in automated application deployment. You can use the HP Server Automation to deploy the HPE Operations Agent. For more information on the prerequisites for installing the HPE Operations Agent, see [Prerequisites for Installing the HPE Operations Agent](#). The target where you are installing the HPE Operations Agent must always have SA agent installed on it.

To obtain the platform-specific media zip from the HPE Operations Agent media, run the following command. The command creates zip media that can be imported into HP Server Automation.

```
cscript oainstall.vbs -createzip
```

or

```
./oainstall.sh -createzip
```

This creates a .zip file for each platform package in the media. To download a platform-specific .zip file from a specific location, run the following command:

```
cscript oainstall.vbs -createzip -out_dir c:\temp -p <OS name>
```

In this instance:

<OS name> is the name of the operating system

Use the following values for <OS name>:

For Windows: WIN

For Linux: LIN

### **For example:**

To obtain a .zip file for Windows operating system from a specific location, run the following command:

```
cscript oainstall.vbs -createzip -out_dir c:\temp -p win
```

To install HPE Operations Agent using the SA console, perform the following tasks:

- ["Importing the HPE Operations Agent Software" on the next page](#)
- ["Creating a Software Policy " on page 114](#)
- ["Attaching the Software Policy to a Device or Server" on page 115](#)



Before starting the tasks to install HPE Operations Agent using the SA console, make sure that SA agent is installed on the node. For more information, see *Installing Server Agent* section in the *HP Server Automation User Guide*.

## Importing the HPE Operations Agent Software

To import the HPE Operations Agent software, follow these steps:

1. Download the HPE Operations Agent media.

The HPE Operations Agent media is in the **.tar** file format. To extract the contents of the **.tar** file containing the HPE Operations Agent media, use the command `tar -xvf <filename>.tar` on the UNIX/Linux systems.

2. After you untar the HPE Operations Agent media, run the following command to create the zip media:

```
cscript oainstall.vbs -createzip -p <OS name>
```

3. Log on to the HP Server Automation Client console.
4. In the navigation pane, select **Library**.
5. Select the **By Folder** tab, and the required folder.
6. Click **Actions > Import Software**. The **Import Software** dialog box opens.
7. Browse and select the zip file that you created and select **ZIP Archive (.zip)** as the package type.
8. Browse and select the appropriate folder and platform.
9. Click **Import**.
10. Click **Close** when the import is successful. Double click the uploaded package to change the following properties:

### On Windows:

- Default install path:  
`%temp%\oa_media_Windows_X64`
- Install Scripts - Post-install script:  
`%temp%\oa_media_Windows_X64\oainstall.bat`
- Uninstall Scripts - Pre-uninstall script:  
`%temp%\oa_media_Windows_X64\oaremove.bat`

**On Linux:**

- Default install path:

```
/usr/local/oa_media_Linux2.6_X64
```

- Install Scripts - Post-install script:

```
cd /usr/local/oa_media_Linux2.6_X64
```

```
find . -print | xargs chmod +x
```


```
/usr/local/oa_media_Linux2.6_X64/oainstall.sh -i -a
```

- Uninstall Scripts - Pre-uninstall script:

```
/usr/local/oa_media_Linux2.6_X64/oainstall.sh -r -a
```

The package appears in the contents pane.

You can also install the imported software without creating and attaching a software policy by performing the following tasks:


1. In the navigation pane, select **Library**, expand **Packages**, and select the platform on which you imported the software **zip** file. The contents pane displays the imported software package.
2. Select **Actions > Install Software...** The **Install Software** window opens.
3. Click  and select the required device or server from the list and click **Select**.
4. Click **Start Job**.
5. Click **Close** when the processes are successfully completed. To verify if the package is successfully installed, see ["Verifying the Installation" on page 116](#).

## Creating a Software Policy

To create a software policy, follow these steps:

1. In the navigation pane, select **Library**.
2. In the **By Type** tab, expand **Software Policies** and select the required platform from the list. The Contents pane displays the existing software policies for the selected platform.
3. Click **Actions > New...**

The **Software Policy** window opens.

4. Type a name for the policy in the **Name** field.
5. Click **Select** to select the appropriate folder.
6. Click **Policy Items** in the **Views** pane.
7. Click  in the **Policy Items** pane. The Select Library Item window opens.
8. Select **Package** from the **Browse Types** tab. The right pane displays all the available packages.

Alternatively, you can also select **Browse Folders**, and select the folder where you imported the package.

9. Select the required package to attach the software policy.
10. Click **Select**. The package details appear in the Software Policy window.
11. In the left pane, click **Contents** to view the contents of the package.
12. Click **File > Save**. Close the window. The policy details appear on the contents pane.

## Attaching the Software Policy to a Device or Server

To attach a Software Policy, do one of the following:

- ["Attaching the Software Policy from the Software Policy list" below](#)
- ["Attaching the Software Policy from the Devices list" below](#)

### Attaching the Software Policy from the Software Policy list

1. In the navigation pane, select **Library**.
2. In the **By Type** tab, expand **Software Policies** and select the required platform from the list. The contents pane displays the existing software policies for the selected platform.
3. Select the required software policy. Click **Actions > Attach**. The **Attach Server** window opens.
4. Select the required device from the **Devices** list and click **Attach**. The **Remediate** window opens.
5. Click **Start Job**. Wait till the installation process is complete.
6. Click **Close** after all requests are successfully completed.

### Attaching the Software Policy from the Devices list

1. In the navigation pane, select **Devices**.
2. Select the required device or server from the **Devices** list. The contents pane displays the associated devices or servers.
3. Select the required device or server. Click **Actions > Attach > Software Policy**. The **Attach Software Policy** window opens.
4. Select the software policy and click **Attach**. The **Remediate** window opens.
5. Click **Start Job**. Wait till the installation process is complete.
6. Click **Close** after all requests are successfully completed.

To verify that the policy is attached to the device or server successfully, select the device or server from the devices list and select **Software Policies** from the **View** drop down list. The policies attached to the device or server are listed at the bottom of the contents pane.

## Verifying the Installation

To verify that HPE Operations Agent is successfully installed, follow these steps:

1. In the navigation pane, select **Devices**.
2. Select the required device or server from the **Devices** list. The contents pane displays the associated devices or servers.
3. Select the required device or server.
4. Select **Installed Packages** from the **Views** drop down list in the contents pane. The list of packages installed on the selected server or devices appears at the bottom of the pane.
5. Check if the HPE Operations Agent package is available.


**Note:** You can also check the contents of the *oainstall.log* file on the target system and verify that HP Operations agent is installed.

### Uninstalling HPE Operations Agent using SA console

To uninstall HPE Operations Agent using the SA console, follow these steps:

1. In the navigation pane, select **Devices**.
2. Select the required device or server from the **Devices** list. The contents pane displays the

associated devices or servers.

3. Select the required device or server. Click **Actions > Uninstall > Software**. The **Uninstall Software** window opens and the contents pane displays the selected device or server.
4. Click **Software** from the list on the left pane.
5. Click  to specify the software policy. The **Select Library Item** window opens.
6. Select the required software policy attached to the HPE Operations Agent package to be uninstalled.
7. Click **Select** and then **Start Job**. The Job Status appears and uninstalls the HPE Operations Agent package.
8. Click **Close** after the job is completed.

To verify that package is uninstalled from the device or server successfully, select the device or server from the devices list and select **Software Policies** from the **View** drop down list. The policies attached to the device or server are listed at the bottom of the contents pane. The list does not contain the HPE Operations Agent package after successful uninstallation.

## Chapter 13: Installing the HPE Operations Agent using Microsoft System Center 2012 Configuration Manager

The Microsoft System Center 2012 Configuration Manager is a systems management software product. You can use Microsoft System Center 2012 Configuration Manager to install HPE Operations Agent on the required Windows nodes and servers. For more information on the prerequisites for installing HPE Operations Agent, see ["Prerequisites for Installing the HPE Operations Agent on a Node" on page 40](#).

For more information, see the *Microsoft System Center documentation*. After adding the node or server, navigate to **Assets and Compliance > Overview > Devices** and check if the details appear in the devices list.

To install the Microsoft System Center 2012 Configuration Manager client on the required node, select

the node from the devices list and click **Install Client** .

To install HP Operations Agent using the Microsoft System Center 2012 Configuration Manager console, perform the following tasks:

1. ["Creating the HPE Operations Agent Package" below](#)
2. ["Deploying the HPE Operations Agent Package" on page 120](#)


### Creating the HPE Operations Agent Package

To create an HPE Operations Agent deployment package, follow these steps:

1. Download the HPE Operations Agent media.
2. Browse to the **packages** folder and select the required Operating System.

For example, to obtain the Windows 64-bit packages, browse to **packages > WIN > Windows\_X64**.

3. Extract the contents of the media.
4. Log on to the Microsoft System Center 2012 Configuration Manager console.

5. In the left Navigation Pane, select **Software Library**.
6. Expand **Overview > Application Management** and select **Packages**.
7. Click **Create Package**  to create the HPE Operations Agent deployment package.  
The **Create Package and Program Wizard** window opens.
8. Type a name for the package in the **Name** field.
9. Type a description in the **Description** field.
10. Select the **This package contains source files** checkbox and click **Browse**.  
The **Set Source Folder** dialog box opens.
11. Select **Network path (UNC name)**.
12. Click **Browse** and navigate to the location where the HPE Operations Agent package is available.
13. Click **OK** and then click **Next**.
14. Select the program type you want to create and click **Next**.
15. Type a name for the program in the **Name** field.
16. Click **Browse** corresponding to the **Command line** field and navigate to the folder where the **oasetup.exe** is available.  
To start the installation on the node automatically with **oasetup.exe**, type  

```
oasetup.exe -install.
```

  
For example, you can also type `cscript.exe oainstall.vbs -i -a -agent_profile <absolute path of profile text file>`, if you want to specify an agent profile. Make sure that the `.txt` file is placed at the same location where the **oainstall.vbs** file is present.  
For example, you can also use the command `cscript.exe oainstall.vbs -i -a -srv <management_server_hostname> -cert_srv <management_server_hostname> -f`  
You can mention any agent installation command to perform an appropriate action during deployment.
17. Select and provide values in the required fields.
18. Click **Next** until the completion status window appears.
19. Click **Close** to close the dialog box.

The created package appears in the right pane of the console.

## Deploying the HPE Operations Agent Package

To deploy the HPE Operations Agent package on the node or server, follow the steps:

1. Select the HPE Operations Agent package.

2. Click **Deploy** .

The Deploy Software Wizard window opens.

3. Verify that the **Software** field contains the package name.

If you need to select a different package, click the corresponding **Browse** button and select the required package.

4. Click **Browse** corresponding to the **Collection** field.

The Select Collection window opens.

5. Select the required node or server on which you want to deploy the HPE Operations Agent. Click **OK**.

6. Click **Next**.

7. Click **Add**. Select **Distribution Point** or **Distribution Point Group**.

A window opens that displays the distribution points or the distribution point groups.

8. Select the required value and click **OK**.

9. Click **Next**. Specify the required Deployment Settings in the settings screen.

10. In the Summary screen, click **Next**. The window shows the progress of the deployment.

11. Click **Close** in the Completion screen after the wizard displays the message that the software is successfully deployed.

## Verifying the Installation

To verify if the HPE Operations Agent is successfully installed, follow the steps:



1. In the left navigation pane, select **Monitoring**.
2. Navigate to **Overview > Deployments**. The right pane displays all the deployments with the name of the package.

3. Select the appropriate deployment and click **View Status** (  ).

Alternatively, you can also double-click the deployment to view the status.

The right pane displays the deployment status. You can check the different tabs to view the status of the deployment.

# Chapter 14: Installing the HPE Operations Agent Using Red Hat Network Satellite Server

You can use the Red Hat Network Satellite server to deploy the HPE Operations Agent on all the Linux nodes. For more information about the prerequisites for installing HPE Operations Agent, see ["Prerequisites for Installing the HPE Operations Agent on a Node" on page 40](#). The target node where you are installing HPE Operations Agent must always be added to communicate with Red Hat Network Satellite (RHNS) server.

**Note:** When you upgrade from the HP Operations Agent 8.60 to HPE Operations Agent 12.03, ensure that you uninstall HP Operations Agent 8.60 using the `opc_inst.sh -r` command and then install the HPE Operations Agent 12.03 using the Red Hat Network Satellite server.

To download platform specific packages from the HPE Operations Agent media, browse the media to the specific package location. The following table lists the platform-specific packages to be obtained from the media.

Operating System	Architecture	Packages
Linux	Linux2.6 x64	packages/LIN/Linux2.6_X64
	Linux2.6 x86	packages/LIN/Linux2.6_X86
	Linux2.6 PPC64	packages/LIN/Linux2.6_PPC64

To install HPE Operations Agent using RHNS server, perform the following tasks:

1. ["Downloading and Storing the HPE Operations Agent Depot Files \(RPMs\)" on the next page](#)
2. ["Creating the Setup on the Target Node" on the next page](#)
3. ["Deploying the Packages on the Target Node" on page 124](#)

To remove the packages from the target node, see ["Removing the Packages from the Target Node" on page 125](#)

## Downloading and Storing the HPE Operations Agent Depot Files (RPMs)

To download and store the HPE Operations Agent software in Software Delivery Repository, follow these steps:

1. Obtain the HPE Operations Agent media and mount it to your desired location.
2. To obtain the Linux packages, browse to the **packages** folder and select **Lin**.
3. Select and unzip all the **gzip** files from the media using the `- N` option.
4. Upload the HPE Operations Agent RPMs to Software Delivery Repository location of the RHNS server.

## Creating the Setup on the Target Node

To create the setup on the target node, follow these steps:

1. Add the node to RHNS server. The node is known as the target node.
2. On the target node, create a file and provide the location on the system where HPE Operations Agent package must create the **Default Agent File (oa.repo)**.

For example, create a file `/etc/yum.repos.d/<oa.repo>`.

**Note:** The agent depot files must be available in the **repos.d** location.

3. Update the contents of the file and specify the location (*baseurl*) where HPE Operations Agent depot files are available.

**Note:** The content of the file:

```
[oa]
```

```
Name=Operations Agent
```

```
baseurl=System_name/SDR/downloads/Extras/RedHat/6Server/x86_64/current/operation-agent/<Agent RPMs location>
```

```
gpgcheck=0
```

In this instance:

*<Name>* is the product name.

*<baseurl>* is the location where HPE Operations Agent package is available.

*gpgcheck* is the additional check to verify the RPMs. To disable this additional check, set the value as 0.

### **OR**

Use the content to verify the RPMs with the public key.

[oa]

Name=**Operations Agent**

baseurl=System\_name/SDR/downloads/Extras/RedHat/6Server/x86\_64/current/operation-agent/*<Agent RPMs location>*

gpgcheck=1

gpgkey=file://<path of hpPublicKey.pub>

In this instance:

*<Name>* is the product name.

*<baseurl>* is the location where agent package is available.

*gpgcheck* is the additional check to verify the RPMs. To enable this additional check, set the value as **1**.

*gpgkey* is the path to get the HP public key. This key is only required if you need additional security.

## Deploying the Packages on the Target Node

To deploy the packages on the target node, follow these steps:

1. Run the command to install the required RPMs:

```
# yum install <HPOvOpsAgt>
```

**Note:** All the dependent HPE Operations Agent RPMs are installed.

```

=====
Package                                     Arch
=====
Installing:
HPOvOpsAgt                                 x86_64
Installing for dependencies:
HPOvAgtLc                                  x86_64
HPOvBbc                                    x86_64
HPOvConf                                   x86_64
HPOvCtrl                                   x86_64
HPOvDepl                                   x86_64
HPOvEaAgt                                  x86_64
HPOvGlanc                                  x86_64
HPOvPacc                                   x86_64
HPOvPerfAgt                                x86_64
HPOvPerfMI                                 x86_64
HPOvPerfIA                                 x86_64
HPOvSecCC                                  x86_64
HPOvSecCo                                  x86_64
HPOvXpl                                    x86_64
=====

```

2. Run the following command to verify if HPE Operations Agent packages are installed:

```
rpm -qa | grep <packagename>
```

In this instance, <packagename> is name of the agent package.

For example, `rpm -qa | grep <HPOvBbc>`

After performing all the steps, HPE Operations Agent RPMs are available on the node. Configure the management server by performing the following steps:

1. Go to the following directory on the Linux node:

```
/opt/OV/bin/OpC/install
```

2. Run the following command:

```
opcactivate -srv <management_server> -cert_srv <management_server> -f
```

In this instance:

<management\_server> is the FQDN of the HPOM management server.

## Removing the Packages from the Target Node

You can remove the packages by using either the *YUM* command or *oainstall.sh* program.

### Using YUM Commands to remove the packages

- Run the following command to remove the package or *only* the specific RPMs:

```
yum remove <package name>
```

**Note:** Make sure that you install *yum-plugin-remove-with-leaves* to remove all the Operations agent packages by using a single command.

- Run the following command to remove the HPE Operations Agent completely:

```
yum remove --remove-leaves HPOvOpsAgt HPOvSecCo
```

### Using oainstall.sh program to remove the packages

To remove the packages, run the following command:

```
/opt/OV/bin/OpC/install/oainstall.sh -r -a
```

# Chapter 15: Installing the HPE Operations Agent RPM based Hotfix Package

The HPE Operations Agent 12.02 enables you to install RPM based hotfix package on a Linux system. This RPM hotfix packages are placed in the hotfix media.

The RPM hotfix package is available at the following folder location:

```
hotfixes/<hotfixID>/<platform>/
```

For example, in this hotfix, the XPL hotfix RPM package is available at the following location:

```
hotfixes/HFLIN_XXXXX/Linux2.6_X64/HPOvXp1-12.01.xxx.rpm.gz
```

**Note:** During the registration and deployment of HPOM or HPE OMi the RPM based hotfixes are not deployed instead only the tar based hotfix packages are deployed. Hence, there is no change in the existing behavior of the deployment scenarios.

To install RPM hotfix package on the Linux system, follow these steps:

1. Go to the directory:

```
<root directory>/hotfixes/<hotfixID>/<platform>/
```

For example, <root directory>/hotfixes/HFLIN\_XXXXX/Linux2.6\_X64/

2. Run the following command to unzip the RPM hotfix package:

```
gzip -d <rpm package>.gz
```

For example, `gzip -d HPOvXp1-12.01.xxx.rpm.gz`

3. Run the following command to install the RPM package:

```
rpm -U <rpm package>
```

For example, `rpm -U HPOvXp1-12.01.xxx.rpm`

To install the RPM hotfix package using YUM:

1. Perform step 1 and 2.
2. Run the following command to install the RPM package:

```
yum install <rpm package>
```

**Note:** Once the RPM based hotfixes are installed, it cannot be removed. The command to remove the hotfix (for example, `oainstall.sh -r -a -pn <hotfixID>` command) does not work.

For RPM based hotfix installation, run the `ovdeploy -inv` command to verify the installation. In the output, the version of the individual components are updated but the version of the product bundle does not change as the RPM hotfixes are installed.

**For example:**

Run the following command:

```
ovdeploy -inv
```

The command generates the following output:

NAME	DESCRIPTION	VERSION	TYPE	OSTYPE
HPOvAgtLc	HPE Operations agent L10NPackage	12.01.010	pkg	Linux
HPOvBbc	HPE Software HTTP Communication	12.01.010	pkg	Linux
HPOvConf	HPE Software Configuration	12.01.010	pkg	Linux
HPOvCtrl	HPE Software Process Control	12.01.010	pkg	Linux
HPOvDepl	HPE Software Deployment	12.01.010	pkg	Linux
<b>HPOvEaAgt</b>	<b>HPE Software E/A Agent</b>	<b>12.01.011</b>	<b>pkg</b>	<b>Linux</b>
HPOvGlanc	HPE Software Performance Glance	12.01.010	pkg	Linux
HPOvPacc	HPE Software Performance Access	12.01.010	pkg	Linux
HPOvPerfAgt	HPE Software Performance Agent	12.01.010	pkg	Linux
HPOvPerfMI	HPE Software Measurement Interface	12.01.010	pkg	Linux
HPOvPerIA	HPE Software Perl	05.16.013	pkg	Linux
HPOvSecCC	HPE Software Certificate Management Client	12.01.010	pkg	Linux
HPOvSecCo	HPE Software Security Core	12.01.010	pkg	Linux
<b>HPOvXpl</b>	<b>HPE Software Cross Platform Component</b>	<b>12.01.011</b>	<b>pkg</b>	<b>Linux</b>
<b>Operations-agent</b>	<b>HPE Operations agent Product</b>	<b>12.01.010</b>	<b>bdl</b>	<b>linux</b>

The output shows that the version of the individual components - **HPOvEaAgt** and **HPOvXpl** are updated but the version of the **Operations-agent** product bundle does not change.



## Chapter 16: Installing the HPE Operations Agent on Platforms with Limitations

The installer may fail to install the HPE Operations Agent on platforms with limitations. For example, you may see the following error when you try to install the agent on such a platform:

```
The product bundle selected may not yet be supported on this node
```

To install the HPE Operations Agent on such a node, run the installer with the `-minprecheck` option along with the `-i` and `-a` options.

### Examples

To install the HPE Operations Agent 12.02 on a Windows system, run the following command:

```
cscript oainstall.vbs -i -a -minprecheck
```

To install the HPE Operations Agent 12.02 on a UNIX/Linux system, run the following command:

```
./oainstall.sh -i -a -minprecheck
```

See the [HPE Operation Agent Support Matrix](#) document for more details on platforms with limitations.

## Installing the HPE Operations Agent on Platforms with Limitation Remotely from the HPOM for Windows Console

To install the HPE Operations Agent 12.02 remotely from the HPOM for Windows console on platforms supported with limitation, you must perform the following pre-installation tasks on the management server:

1. Log on to the Management Server as an administrator.
2. Go to the `%ovdatadir%shared\conf\PMAD` directory .
3. Rename the `agent_install_defaults.cfg.sample` file as `agent_install_defaults.cfg`.

**Tip:** Take a backup of the `agent_install_defaults.cfg.sample` file.

4. Open the `agent_install_defaults.cfg` file with a text editor and add the following line:

```
[nonXPL.config]
MINPRECHECK=True
```

5. Save the file.

For more information on installing the HPE Operations Agent 12.02 remotely from the HPOM console, see *Configure the Agent Remotely from an HPOM for Windows Management Server Online Help*.

## Installing the HPE Operations Agent on Platforms with Limitation Remotely from the HPOM for UNIX Console

To install the HPE Operations Agent 12.02 remotely from the HPOM for UNIX console on platforms with limitation, you must perform the following pre-installation tasks on the management server:

1. Log on to the Management Server as an administrator.
2. Go to the directory `/etc/opt/OV/share/conf/OpC/mgmt_sv`.
3. Rename the file `bbc_inst_defaults.sample` as `bbc_inst_defaults`.
4. Open the file `bbc_inst_defaults` with a text editor and add the following line:

```
[nonXPL.config]
MINPRECHECK=true
```

5. Save the file.

For more information on installing the HPE Operations Agent 12.02 remotely from the HPOM console, see *HPOM for UNIX: New Agent Installation section in the HPOM on UNIX/Linux Online Help*.

**Note:** After installing the HPE Operations Agent 12.02 using `MINPRECHECK`, the changes done in the profile file must be reverted. When you install using `MINPRECHECK`, the version check for the Operating System and Architecture is skipped.

## Installing the HPE Operations Agent on Platforms with Limitation Remotely Using Command Line

To install the HPE Operations Agent 12.02 remotely on platforms supported with limitation:

1. Log on to the management server as an administrator.
2. Go to the following directory on the Management Server:

**On Windows:**

```
%ovinstalldir%bin
```

**On UNIX/Linux:**

```
/opt/OV/bin
```

3. Add the following line in a text file:

```
[nonXPL.config]
```

```
MINPRECHECK=true
```

4. Run the following command:

```
ovdeploy -install -bundle <path_to_OVO-Agent.xml> -node <node name> -af <path_of_profile_file>\<profile_file_name> -1 -configure <profile_file_name>
```

The command installs the HPE Operations Agent 12.02 on the node.

# Chapter 17: Installing the HPE Operations Agent Manually on the Node

## **Task 1: Prepare for Installation**

Before installing the HPE Operations Agent, you must extract or mount the *HPE Operations Agent and Infrastructure SPIs 12.02* media on the node.

Alternatively, you can manually transfer the agent deployment package from the HPOM management server.

### **To transfer the deployment package from a Windows management server:**

1. Make sure the node is added as a managed node on the HPOM console.
  - a. Create a directory on the management server and then go to the directory.
2. Run the following command:

```
ovpmutil dn1 pkg Operations-agent /pnn <node_FQDN>
```

In this instance, *<node\_FQDN>* is the fully-qualified domain name of the node.

The deployment package for the node is downloaded into the current directory.

3. Transfer the directory from the management server into a temporary directory on the node.

### **To transfer the deployment package from a UNIX/Linux management server:**

1. Log on to the management server and then go to the following directory:

```
/var/opt/OV/share/databases/OpC/mgd_  
node/vendor/<vendor>/<arch>/<ostype>/A.12.01.000
```

In this instance:

*<vendor>*: Name of the operating system vendor.

*<arch>*: Architecture of the node.

*<ostype>*: Operating system of the node.

The following table provides a list of *<vendor>/<arch>/<ostype>* combinations that you can use:

Operating System	Architecture	Select this combination..
Windows	x86_64	ms/x64/win2k3
Windows	x86	ms/x86/winnt
Linux	x86_64	linux/x64/linux26
Linux	x86	linux/x86/linux26
Linux	PowerPC (64-bit)	linux/powerpc/linux26
Linux (Debian)	x64	linux_deb/x64/linux26
HP-UX	Itanium	hp/ipf32/hpux1122
HP-UX	PA-RISC	hp/pa-risc/hpux1100
Solaris	SPARC	sun/sparc/solaris7
Solaris	x86	sun/x86/solaris10
AIX	PowerPC (64-bit)	ibm/rs6k64/aix5

- Transfer the contents of the RPC\_BBC directory (available inside the A.12.01.000 directory) to a temporary directory on the node.

### Optional. Installing HPE Operations Agent using Profile File

#### Task 2: Install the HPE Operations Agent and Infrastructure SPIs

In the following section:

<management\_server>: FQDN of the management server

<certificate\_server>: FQDN of the certificate server

<install\_directory>: Path to place all packages and binary files on the node.

<data\_directory>: Path to place all data and configuration files on the node.

<path> is the path to the profile file.

<profile\_file> is the name of the profile file.

- Log on to the node as root or administrator.
- If you want to install from the *HPE Operations Agent and Infrastructure SPIs 12.02* media, follow these steps:

- a. Go to the media root.
- b. Run the following command to install without a profile file:

**On Windows:**

```
cscript oainstall.vbs -i -a -s <management_server> [-cs <certificate_server>][-install_dir <install_directory> -data_dir <data_directory>]
```

**On UNIX/Linux:**

```
./oainstall.sh -i -a -s <management_server> [-cs <certificate_server>]
```

- c. Run the following command to install with a profile file:

**On Windows:**

```
cscript oainstall.vbs -i -a -agent_profile <path>\<profile_file> -s <management_server> [-cs <certificate_server>] [-install_dir <install_directory> -data_dir <data_directory>]
```

**On UNIX/Linux:**

```
./oainstall.sh -i -a -agent_profile <path>/<profile_file> -s <management_server> [-cs <certificate_server>]
```

**Tip:** On Windows, you can use the **oasetup** program instead of the **oainstall.vbs** script.

*To install the agent with the **oasetup** program:*

- i. Make sure that the Microsoft Visual C++ Redistributable Package is installed on the system.

If it is not installed on the system, follow these steps:

- Go to the packages\WIN directory from the media root.
- Go to the appropriate directory based on the architecture of the node (Windows\_X64 for x64 platforms and Windows\_X86 for x86 platforms).
- Run the following executable files:

**On Windows x86:** vc\_redist\_x86.exe and vc\_redist2k5\_x86.exe

**On Windows x64:** vc\_redist\_x64.exe and vc\_redist2k5\_x64.exe

- ii. Run the following command to install the agent:

```
oasetup -install -management_server <management_server> [-certificate_
server <certificate_server>] [-install_dir <install_directory> -data_dir
<data_directory>]
```

or

```
oasetup -install -management_server <management_server> [-certificate_
server <certificate_server>] -agent_profile <path>\<profile_file> [-
install_dir <install_directory> -data_dir <data_directory>]
```

3. If you manually transferred the agent deployment package from the HPOM management server, follow these steps:

- a. Go to the directory on the node where you stored the deployment package.

- b. Run the following command:

**On Windows:**

```
oasetup -install -management_server <management_server> [-certificate_server
<certificate_server>][-install_dir <install_directory> -data_dir <data_
directory>]
```

**On UNIX/Linux:**

- a. `chmod u+x oasetup.sh`

- b. `./oasetup.sh -install -management_server <management_server> [-certificate_
server <certificate_server>]`

To install with a profile file, add **-agent\_profile <path>\<profile\_file>** after **-install**.

**Tip:** The Operations agent provides you with an option to trace the agent processes. You can run the tracing option with the `oainstall` program, which generates trace files by using the following command:

```
-enabletrace <application name>
```

Run the following command to get the list of applications: `ovtrccfg -vc`

For example:

```
-enabletrace ovconfget
```

To trace all the agent processes, run the command with the following additional option:

```
-enabletrace ALL
```

For example:

```
./oainstall.sh -i -a -agent_profile /root/profile/profile_file -s test_
system1.domain.com -enabletrace ALL
```

The trace file (with the extension .trc) is available in the following location:

**On Windows**

%ovdatadir%Temp

**On UNIX/Linux**

/var/opt/OV/tmp

If you install the agent on an HPOM management server, you must restart all HPOM processes after installation.

*Placement of Packages*

When you install the HPE Operations Agent on the standalone server, the installer program places all necessary packages and files into the following locations:

- **On Windows:**

- %ovinstalldir%
- %ovdatadir%

The preceding files are placed at the location C:\Program Files\HP\HP BTO Software, by default. You can change the location as required.

- **On HP-UX, Linux, and Solaris:**

- /opt/OV
- /opt/perf
- /var/opt/OV
- /var/opt/perf

- **On AIX**

- /usr/lpp/OV
- /usr/lpp/perf
- /var/opt/OV
- /var/opt/perf

*Installation Log Files*

The installer places the installation log file (oainstall.log) into the following directory:



- **On Windows:** %ovdatadir%\log
- **On UNIX/Linux:** /var/opt/OV/log

### *Verifying the Installation*

After installing the HPE Operations Agent, review the contents of the installation log file (**oainstall.log**). If the installation is successful, the following message appears:

```
HP Operations Agent installation completed successfully
```

## Post-Installation Task in a NAT Environment

If you install the agent on nodes in the Network Address Translation (NAT) environment, you must configure the agent on the node to use the IP address that was used with HPOM while adding the node.

To configure the agent to use the IP address set with HPOM, follow these steps:

1. Log on to the node with the root or administrative privileges.
2. Go to the following directory:

#### **On Windows**

```
%ovinstalldir%bin
```

#### **On HP-UX, Linux, or Solaris**

```
/opt/OV/bin
```

#### **On AIX**

```
/usr/lpp/OV/bin
```

3. Run the following command:

```
ovconfchg -ns eaagt -set OPC_IP_ADDRESS <IP_Address>
```

In this instance, <IP\_Address> is the IP address of the node that was configured with HPOM while adding the node to the list of managed nodes.

4. Restart the agent by running the following commands:
  - a. `ovc -kill`
  - b. `ovc -start`

# Chapter 18: Installing the Infrastructure SPIs on the HPOM Management Server

## The Prerequisites for Installing the Infrastructure SPIs

### Hardware and Software Requirements

For a list of supported hardware, operating systems, HPOM version, and agent version, see the [Support Matrix](#).

### Disk Space Requirements

Operating System on the HPOM Management Server	Temporary Directory <sup>a</sup>	Total Disk Space
Windows	%tmp% - 15 MB	90 MB
Linux	/tmp - 35 MB	90 MB
HP-UX	/tmp - 17 MB	240 MB
Solaris	/tmp - 35 MB	80 MB

<sup>a</sup>The disk space for the temporary directory/drive is required only during installation. These are approximate values.

### Upgrade Requirements

The Installation of Infrastructure SPI version 12.03 is supported only on the following HPOM Management Servers:

- HPOM for Windows Management server version 8.x and 9.x
- HPOM for Linux Management server version 9.1 and 9.2
- HPOM for HP-UX Management server and
- HPOM for Solaris Management server

**Note:** Before upgrading from the Infrastructure SPI version 11.1x to 12.02, make sure that the Auto Deployment option is disabled on all the nodes.

Follow the steps to ensure that the Auto Deployment option is disabled:

1. On the HPOM console, select a node, right click and select **Properties**.
2. In the **Properties** window, select the **Network** tab.

3. Ensure that the **Enable Auto Deployment** option is unchecked.

You can upgrade from the Infrastructure SPIs version 11.1x to 12.03. After you upgrade from Infrastructure SPI version 11.1x to 12.03, Infrastructure SPI 11.1x policies are available in the v11.1x folder and Infrastructure SPI 12.03 policies are available in the v12.0 folder.

On the HPOM console, select **Policy management** → **Policy groups** → **Infrastructure Management** → **v11.1x and v12.0**

**Note:** After you upgrade from Infrastructure SPI version 11.1x to 12.03, the Infrastructure SPI 12.03 policies are available under the **Infrastructure Management** → **v12.0** policy group.

You can either deploy Infrastructure SPI 11.1x or 12.03 policies on a node.

**Note:** Deployment of both Infrastructure SPI 11.1x and 12.03 policies on the same node is not supported.

### Upgrading from Infrastructure SPIs 2.xx or earlier versions to Infrastructure SPI version 12.03

You must upgrade Infrastructure SPIs 2.xx or earlier versions to Infrastructure SPIs 11.1x and then upgrade to Infrastructure SPI 12.03.

#### ***Install the Infrastructure SPIs***

To install the Infrastructure SPIs, follow these steps:

1. Log on to the management server.
2. Perform one of the following tasks:
  - If you want to install the Infrastructure SPIs from the physical media, insert the *HPE Operations Agent and Infrastructure SPIs 12.02* DVD into the DVD-ROM drive.
  - Download the installation media (.iso file) from one of HPE's websites.

Use the physical DVD or the .iso file that includes deployment packages for all platforms. Platform-specific .iso files do not contain the Infrastructure SPIs.

3. The **oainstall** program installs the Infrastructure SPIs on the management server while registering the deployment package. This installation includes necessary report (to be used with HP Reporter) and graph (to be used with HP Performance Manager) packages for the Infrastructure SPIs. To skip the registration of the HPE Operations Agent packages, follow these steps:
  - a. Open the **default\_config** file. You will find the following default selection:

```
[agent.parameter]
```

```
REGISTER_AGENT=NO
[hpinfraspi.parameter]
InfraSPI= NO
InfraSPI_With_Graphs= YES
InfraSPI_With_Reports= YES
```

- b. Under the **[hpinfraspi.parameter]** section, you can set the following:
- Do not make any changes to the file that is, do not set any values for the properties under the [hpinfraspi.parameter] section if you want to install the Infrastructure SPIs with reports (for Windows only) and graphs.
  - Set **InfraSPI** to **YES** and the rest of the properties to **NO** if you want to install only the Infrastructure SPIs without reports (for Windows only) and graphs.
  - Set **InfraSPI\_With\_Graphs** to **YES** and the rest of the properties to **NO** if you want to install only the Infrastructure SPIs and graphs.

**Note:** Do not install the graph packages if HP Performance Manager is not installed on the management server. If HP Performance Manager is installed on a remote server, you must install graph packages separately on that server.

If you use HPOM on UNIX/Linux and want to see graphs with HP Performance Manager, you must integrate HP Performance Manager with HPOM on UNIX/Linux (see [Integrate HP Performance Manager with HPOM on UNIX/Linux](#)).

- Set **InfraSPI\_With\_Reports** to **YES** and the rest of the properties to **NO** if you want to install only the Infrastructure SPIs and reports (and no graphs).

**Note:** Since HP Reporter is not supported on UNIX/Linux, HP Reporter needs to be available on a remote server. To install report packages for the Infrastructure SPIs on the remote HP Reporter server, see [Install Report and Graph Packages on a Remote Server](#).

- c. Save the file.
4. Run the following command:

#### On Windows

```
cscript oainstall.vbs -i -m -spiconfig <config_file>
```

#### On UNIX/Linux

```
./oainstall.sh -i -m -spiconfig <config_file>
```

In this instance, `<config_file>` is the name of the configuration file (with the complete path to the file).

**Note:** If HPOM is in an HA cluster, follow the above steps on the active node in the cluster, and then perform [step 1](#) through [step 4](#) on all nodes in the HA cluster.

### Example

i. Create a configuration file with the following content:

```
[agent.parameter]
REGISTER_AGENT=NO

[hpinfraspi.parameter]
InfraSPI=YES
InfraSPI_With_Graphs=NO
InfraSPI_With_Reports=NO
```

ii. Save the file as **config\_file** in the following directory:

C:\temp

iii. Run the following command to install the Infrastructure SPIs.

```
cscript oainstall.vbs -i -m -spiconfig C:\temp\config_file
```

The command uses the **config\_file** to install the Infrastructure SPIs without installing the agent, report package, and graph package.

### Install Report and Graph Packages on a Remote Server

When the HP Reporter and the HP Performance Manager are installed on a server other than the HPOM management server, you must follow this procedure to install report and graph packages for the Infrastructure SPIs.

To install report packages:

1. Log on to the HP Reporter server as administrator.
2. Place or mount the *HPE Operations Agent and Infrastructure SPIs 12.02* media on the system.
3. Go to the following directory:

*For a Windows x64 system*

`<media_root>\integration\infraspi\WIN\Windows_X64`

*For a Windows x86 system*

`<media_root>\integration\infraspi\WIN\Windows_X86`

4. Double click to install HPSpiInfR.msi.

To install graph packages:

1. Log on to the HP Performance Manager server as administrator or root.
2. Place or mount the *HPE Operations Agent and Infrastructure SPIs 12.02* media on the system.
3. Go to the following directory:

*For a Linux system*

`<media_root>\integration\infraspi\LIN\Linux2.6_X64`

*For an HP-UX system*

`<media_root>\integration\infraspi\HP-UX\HP-UX_IA32`

*For a Solaris system*

`<media_root>\integration\infraspi\SOL\Solaris_SPARC32`

*For a Windows x64 system*

`<media_root>\integration\infraspi\WIN\Windows_X64`

*For a Windows x86 system*

`<media_root>\integration\infraspi\WIN\Windows_X86`

#### 4. **On Linux**

Extract the contents of the **HPSpiInfG.rpm.gz** file, and then install the **HPSpiInfG.rpm** file.

#### **On HP-UX**

Extract the contents of the **HPSpiInfG.depot.gz** file, and then install the **HPSpiInfG.depot** file.

#### **On Solaris**

Extract the contents of the **HPSpiInfG.sparc.gz** file, and then install the **HPSpiInfG.sparc** file.

#### **On Windows**

Double click to install the **HPSpiInfG.msi** file.

5. Integrate HP Performance Manager with HPOM on UNIX/Linux (see [Integrate HP Performance Manager with HPOM on UNIX/Linux](#)).

### **Log File**

The registration log file (**oainstall.log**) is available in the following directory:

#### **On Windows**

```
/var/opt/OV/shared/server/log
```

#### **On UNIX/Linux**

```
%OvDataDir%shared\server\log
```

#### ***Verifying the Installation***

After installing the Infrastructure SPIs, review the contents of the installation log file `oainstall.log`. If the installation is successful, the following message appears:

```
HPSpiSysI installation completed successfully
```

```
HPSpiVmI installation completed successfully
```

```
HPSpiClI installation completed successfully
```

In this instance:

- HPSpiSysI denotes HPE Operations Smart Plug-in for System Infrastructure
- HPSpiVmI denotes HPE Operations Smart Plug-in for Virtualization Infrastructure
- HPSpiClI denotes HPE Operations Smart Plug-in for Cluster Infrastructure.

#### **Integrate HP Performance Manager with HPOM on UNIX/Linux**

1. On the HPOM management server, go to the directory `/opt/OV/contrib/OpC/OVPM`.
2. Run the following command:

```
./install.sh <hostname>:<port>
```

In this instance, `<hostname>` is the FQDN of the HP Performance Manager server and `<port>` is the port used by the HP Performance Manager. Use the same command with the same options even if the HP Performance Manager is installed on the HPOM management server.

## Components of the Infrastructure SPI on HPOM for Windows

The following Infrastructure SPI components are available on the HPOM for Windows console.

#### **Services**

When you add a node to the HPOM for Windows node group, the SI SPI service discovery policy is automatically deployed.

This service discovery policy discovers the systems infrastructure and services on the node, and adds this information to the HPOM Services area.

To view the SI SPI service map, select **Services > Systems Infrastructure**. The SI SPI service map graphically represents the discovered systems and instances.

**Note:** The SI SPI discovery policy and QuickStart policies are autodeployed on the new nodes (if auto-deployment is enabled) added to the HPOM for Windows server. On the existing nodes, you must manually deploy the SI SPI discovery policy. For more information on automatic deployment of policies on the nodes, see the *HPE Operations Smart Plug-in for System Infrastructure User Guide*.

### Discovery of Virtual Infrastructure

After the SI SPI discovery policy identifies a node as a virtualization node, the VI SPI discovery is auto-deployed. The virtual machines running on those nodes are added under the respective Virtualization Infrastructure node group and the vendor specific QuickStart policies are auto-deployed on those nodes.

The VI SPI discovery policy adds the discovered elements to the HPOM service map. To view the VI SPI service map, select **Services > Virtualization Infrastructure**. The VI SPI service map graphically represents the discovered virtual systems.

### Discovery of Cluster Infrastructure

On HPOM for Windows, if the SI SPI discovery policy identifies the node as a cluster node, it initiates CISPI discovery policy on the node. The CI SPI discovery discovers the clusters, cluster nodes, and resource groups. To view the Cluster Infrastructure SPI service map, select **Services > Cluster Infrastructure**.

### Service Type Models

The service type models display the service type categories that the nodes from node bank are logically assigned to. You can view the service type model in HPOM for Windows.

### Node Groups

After installing Systems Infrastructure SPI 11.xx, the node groups are added under the console tree **Nodes** folder.

**Note:** The node group names appear in English even in the non-English locales.

### Policy Management



Under the Infrastructure Management group, the policies are grouped according to language. For example, English policies are grouped under **en**, Japanese policies are grouped under **ja**, and Simplified Chinese policies are grouped under **zh**. The language groups appear according to the language selected at the time of installation.

**Note:** The ConfigFile policies SI-ConfigureDiscovery and VI-VMwareEventTypes do not have a localized name. The policy names are same as the English name even in non-English locales.

There is also a vendor based policy group. Under this group, the policies are re-grouped based on different operating systems or vendors. The policies grouped by vendor include QuickStart policies and Advanced policies. The QuickStart policies are automatically deployed on the supported managed nodes once they are added to the respective node groups. You can choose to turn off automatic deployment of policies when services are discovered. In addition, you can modify and save preconfigured policies with new names to create custom policies for your own purposes.

To view and access the Systems Infrastructure SPI policies, select **Policy management** → **Policy groups** → **Infrastructure Management** → **v12.0 or v11.1x** → *<language>* → **Systems Infrastructure**.

To view and access the Virtualization Infrastructure SPI policies, select **Policy management** → **Policy groups** → **Infrastructure Management** → **v12.0 or v11.1x** → *<language>* → **Virtualization Infrastructure**.

To view and access the Cluster Infrastructure SPI policies, select **Policy management** → **Policy groups** → **Infrastructure Management** → **v12.0 or v11.1x** → *<language>* → **Cluster Infrastructure**.

## Tools

Tools are provided for the Systems Infrastructure SPI and Virtualization Infrastructure SPI. You can access the Systems Infrastructure SPI tool group by selecting **Tools** > **Systems Infrastructure**, and the VI SPI tools group by selecting **Tools** > **Virtualization Infrastructure**.

## Reports

If HP Reporter is installed on the HPOM for Windows management server, you can view the Reports group from the HPOM for Windows console.

## Graphs

A set of preconfigured graphs is provided with the SI SPI and the VI SPI. To access the graphs from the HPOM console, you must install HP Performance Manager on the HPOM management server prior to the installation of the Infrastructure SPI graphs package.

You can access the SI SPI graphs by selecting **Graphs** > **Infrastructure Performance**, and the VI SPI graphs by selecting **Graphs** > **Infrastructure Performance** > **Virtualization**.

Alternatively, if HP Performance Manager is installed on a separate (stand-alone) system connected to the HPOM management server, you can view the graphs on the HP Performance Manager stand-alone system.

## Components of the Infrastructure SPIs on HPOM for UNIX

The following Infrastructure SPIs components are available on the HPOM for UNIX (HP-UX, Linux, and Solaris) Admin UI.

### Services

The SI-service discovery policy discovers the systems infrastructure and services on the node and adds this information to the HPOM Services area. Use Java GUI to view the service map and the Operator's console. You must install Java GUI on a separate system.

### Discovery of Virtual Infrastructure

After the Systems discovery has identified a node as a virtualization node, the VI SPI discovery is auto-deployed. The virtual machines running on those nodes are added under the respective Virtualization Infrastructure node group and the vendor specific QuickStart policies are auto-assigned on those nodes.

The VI SPI discovery policy discovers the virtual machines (guest machines) hosted on the managed nodes (host machines), and adds this information to the HPOM Services area. Select **Services > Virtualization Infrastructure > Show Graph** to view the VI SPI service map. The service map graphically represents the discovered virtual systems.

### Discovery of Cluster Infrastructure

For the cluster nodes that are added to the HPOM for HP-UX, Linux, or Solaris node bank, manually deploy the CI SPI service discovery. The CI SPI discovery discovers the clusters, cluster nodes, and resource groups. Select **Services > Cluster Infrastructure > Show Graph**, to view the CI SPI service map.

### Policy Management

Under the Infrastructure Management group, the policies are grouped according to the language. For example, English policies are grouped under **en**, Japanese polices and grouped under **ja**, and Simplified Chinese policies are grouped under **zh**. The language groups appear according to the language selected at installation time.

There is also a vendor based policy group. Under this group, the policies are re-grouped based on different operating systems or vendors. The policies grouped by vendor include QuickStart policies and Advanced policies. The QuickStart policies are automatically assigned to the managed nodes after they are added to the respective node groups. You can manually deploy these policies on the nodes.

You can also modify and save preconfigured policies with new names to create custom policies for your own specialized purposes.

To view and access the SI SPI policies, select **Policy Bank** → **Infrastructure Management** → v12.0 or v11.1x → <language> → **Systems Infrastructure**.

To view and access the VI SPI policies, select **Policy Bank** → **Infrastructure Management** → v12.0 or v11.1x → <language> → **Virtualization Infrastructure**.

To view and access the CI SPI policies, select **Policy Bank** → **Infrastructure Management** → v12.0 or v11.1x → <language> → **Cluster Infrastructure**.

## Tools

The Infrastructure SPIs provides tools for the SI SPI and the VISPI. You can access the SI SPI tool group by selecting the **Tool Bank > Systems Infrastructure**, and the VI SPI tools group by selecting **Tool Bank > Virtualization Infrastructure**.

## Reports

If you use HPOM for HP-UX, Linux, and Solaris operating systems, HP Reporter is installed on a separate (stand-alone) system connected to the management server. You can view the reports on the HP Reporter stand-alone system.

For more information about the integration of HP Reporter with HPOM, see the *HP Reporter Installation and Special Configuration Guide*.

## Graphs

The Infrastructure SPIs provide graphs for the SI SPI and the VI SPI. To generate and view graphs from data collected, you must use HP Performance Manager in conjunction with HPOM.

To access the graphs, select the active message, open the Message Properties window, and click **Actions**. Under the Operator initiated action section, click **Perform**. Alternatively you can, right-click active message, select **Perform/Stop Action** and click **Perform Operator-Initiated Action**.

If HP Performance Manager is installed on the management server, you can launch and view graphs on the management server. If HP Performance Manager is installed on a separate (stand-alone) system connected to the HPOM management server, you can view the graphs on the HP Performance Manager stand-alone system.

# Chapter 19: Installing the HPE Operations Agent in the Inactive Mode

## About the Inactive Mode

While installing locally on the managed node, you can choose to program the agent installer to only place the necessary files and packages on the node without configuring any components. As a result, the agent does not start running automatically and remains *inactive*. At a later time, you must use the installer program again to configure and start the agent.

The advantage of using this mechanism is the ability to clone the image of a system where the HPE Operations Agent is installed in the inactive mode. Cloning a system with preinstalled HPE Operations Agent eliminates the requirement to install the agent on the system after adding the system to the list of managed nodes.

## Installing the HPE Operations Agent in the Inactive Mode

The inactive mode of installation ensures that the agent does not start its operation after installation.

To install the HPE Operations Agent:

1. Log on to the node as root or administrator.
2. If you want to install from the *HPE Operations Agent and Infrastructure SPIs 12.02* media, follow these steps:
  - a. Go to the media root.
  - b. Run the following command:

### On Windows:

```
cscript oainstall.vbs -i -a -defer_configure [-install_dir <install_directory> -data_dir <data_directory>]
```

### On UNIX/Linux:

```
./oainstall.sh -i -a -defer_configure
```

In this instance:

<install\_directory>: Path to place all packages and binary files on the node.

<data\_directory>: Path to place all data and configuration files on the node.

## Configure the Agent at a Later Time

You must configure the HPE Operations Agent with configuration details (including the information about the HPOM management server and certificate server) to set the agent in the active mode. The `-configuration` option of the `oainstall` program enables you to perform this task.

When you want to start the operation of the agent, follow these steps:

1. Go to the following directory:

**On Windows 64-bit nodes:**

```
%ovinstalldir%bin\win64\OpC\install
```

**On other Windows nodes:**

```
%ovinstalldir%bin\OpC\install
```

*On HP-UX, Linux, or Solaris nodes:*

```
/opt/OV/bin/OpC/install
```

**On AIX nodes:**

```
/usr/lpp/OV/bin/OpC/install
```

2. Run the following command:

**On Windows**

```
cscript oainstall.vbs -a -configure -s <management_server> [-cs <certificate_server>]
```

*Or*

```
oasetup -configure -management_server <management_server> [-certificate_server <certificate_server>]
```

**On UNIX/Linux**

```
./oainstall.sh -a -configure -s <management_server> [-cs <certificate_server>]
```

### Configure the Agent Remotely from an HPOM for Windows Management Server

If you install the HPE Operations Agent with the `-defer_configure` option, you must configure the agent to work with the HPOM management server - at a later time. You can either configure the agent locally on the node or remotely from the HPOM for Windows management server.

To configure the agent remotely:

Skip steps 1 and 2 if you are configuring agent for Windows.

## 1. Configure an SSH Client.

**Note:** HPOM for Windows provides you with the third-party SSH client software PuTTY. This procedure guides you to set up the PuTTY SSH client. PuTTY is not HPE software. It is provided as is for your convenience. You assume the entire risk relating to the use or performance of PuTTY.

2. On the %ovinstalldir%contrib\OVOW\PuTTY directory, copy the files **PLINK.EXE**, **PSCP.EXE**, and **runplink.cmd** to any directory that is included in your PATH environment variable. For example, if you installed the management server in C:\Program Files\HP\HP BTO Software, copy the files into the following directory: C:\Program Files\HP\HP BTO Software\bin.
3. Create a user. To remotely install agents, HPOM requires the credentials of a user who has administrative access to the node. The following list shows the specific permissions required, according to the node's operating system:

- **On Windows:**

- Write access to the admin\$ share. The user must be part of the local administrators group
- Read access to the registry
- Permission to log on as a service. This is only required if you select User/Password in the Set Credentials list.

- **On UNIX/Linux:**

- Permission to log in to SSH on the node for file transfers and to execute installation commands.

4. Configure the agent using the following commands:

**For Windows 64-bit nodes**

```
ovdeploy -cmd "%ovinstalldir%bin\win64\OpC\install\oasetup -configure -
management_server <management_server> -certificate_server <certificate_server>"
-node <node_name> -fem winservice -ostype Windows -user <node_user> -pw <node_
passwd>
```

Or

```
ovdeploy -cmd "%ovinstalldir%bin\win64\OpC\install\oasetup -configure -
management_server <management_server> -certificate_server <certificate_server>"
-node <node_name> -fem winservice -ostype Windows -user <node_user> -pw_prompt
```

**For other Windows nodes**

```
ovdeploy -cmd "%ovinstalldir%bin\OpC\install\oasetup -configure -management_
server <management_server> -certificate_server <certificate_server>" -node
<node_name> -fem winservice -ostype Windows -user <node_user> -pw <node_passwd>
```

Or

```
ovdeploy -cmd "%ovinstalldir%bin\OpC\install\oasetup -configure -management_
server <management_server> -certificate_server <certificate_server>" -node
<node_name> -fem winservice -ostype Windows -user <node_user> -pw_prompt
```

#### **For an HP-UX, Linux, or Solaris node**

```
ovdeploy -cmd "/opt/OV/bin/OpC/install/oainstall.sh -a -configure -srv
<management_server> -cs <certificate_server>" -node <node_name> -fem ssh -
ostype UNIX -user <node_user> -pw <node_passwd>
```

Or

```
ovdeploy -cmd "/opt/OV/bin/OpC/install/oainstall.sh -a -configure -srv
<management_server> -cs <certificate_server>" -node <node_name> -fem ssh -
ostype UNIX -user <node_user> -pw_prompt
```

#### **For an AIX node**

```
ovdeploy -cmd "/usr/lpp/OV/bin/OpC/install/oainstall.sh -a -configure -srv
<management_server> -cs <certificate_server>" -node <node_name> -fem ssh -
ostype UNIX -user <node_user> -pw <node_passwd>
```

Or

```
ovdeploy -cmd "/usr/lpp/OV/bin/OpC/install/oainstall.sh -a -configure -srv
<management_server> -cs <certificate_server>" -node <node_name> -fem ssh -
ostype UNIX -user <node_user> -pw_prompt
```

In this instance:

<management\_server>: Fully-qualified domain name of the management server.

<certificate\_server>: Fully-qualified domain name of the certificate server. This parameter is optional. If you do not specify the `-cs` option, the management server becomes the certificate server for the node.

<node\_name>: Fully-qualified domain name of the node.

<node\_user>: User with which you can configure the agent on the node; the user that was created.

<node\_passwd>: Password of the above user.

**Note:** Use the option `-pw_prompt` to prompt for a password. This password is not saved in history.



# Chapter 20: Monitoring the HPE Operations Agent in High Availability Clusters

You can use the HPE Operations Agent to monitor nodes in a High Availability (HA) cluster. To be able to monitor cluster-aware applications in an HA cluster, you must deploy the agent with the following guidelines:

- All the nodes in a cluster must be present in the list of managed nodes in the HPOM console.

The HPE Operations Agent must be installed on each of the nodes in the HA cluster.

- It is necessary that you set the `MAX_RETRIES_FOR_CLUSTERUP` variable (under the `conf.cluster` namespace) on the node to an integer value. The profile file-based installation ensures that the variable is set to an appropriate value on every node at the time of installation. An appropriate value depends on the system restart sequence and the time it takes for the cluster to be initialized during restart.

## Virtual Nodes

If you are using the node with the HPOM 9.x, you can take advantage of the concept of virtual nodes. A virtual node is a group of physical nodes linked by a common resource group. Based on the changes in the resource group, the agent can automatically enable or disable policies on the physical nodes.

To monitor nodes in a HA Cluster:

- Deploy the monitoring policies on virtual nodes if you want the policies to monitor a cluster aware application.

**Note:** If you deploy policies on virtual nodes, you will not receive alerts from these nodes if the resource group fails.

- Deploy the monitoring policies on physical nodes if you want the policies to monitor the cluster regardless of the state of the cluster.

Following are the guidelines for creating virtual nodes in the HPOM console:

- A virtual node must not itself be a physical node.
- Virtual nodes do not support DHCP, auto-deployment, and certificates.
- You must not install an agent on a virtual node.

## Monitoring Nodes in HA Clusters

If you want the messages to be coming from a virtual node, then you can configure the HPE Operations Agent to monitor cluster-aware applications that run on the nodes in an HA cluster. This procedure is mandatory if you have not created a virtual node.

If you are using HPOM for Windows 8.1x (lower than patch OMW\_00090), deploy the policies that you identified for monitoring the cluster-aware application (in ["Monitoring the HPE Operations Agent in High Availability Clusters" on the previous page](#)) on all physical nodes in the HA cluster.

For all other types of management servers, deploy the policies that you identified for monitoring the cluster-aware application (in ["Monitoring the HPE Operations Agent in High Availability Clusters" on the previous page](#)) on the virtual node created for the cluster.

To monitor cluster-aware applications on the nodes in an HA cluster, follow these steps:

1. *Microsoft Cluster Server clusters only.* Make sure that the resource group, which contains the resource being monitored, contains both a network name and an IP address resource.
2. Identify the policies that you will require to monitor the cluster-aware application.
3. Create an XML file that describes the cluster-aware application, and name it **apminfo.xml**.
4. This file is used to define the resource groups that will be monitored and to map the resource groups to application instances.
5. The **apminfo.xml** file has the following format:

**Note:** New lines are not allowed between package tags in the **apminfo.xml** file.

```
<?xml version="1.0" ?>

  <APMClusterConfiguration>

    <Application>

      <Name>Name of the cluster-aware application.</Name>

      <Instance>

        <Name>Application's name for the first instance. The instance name is
used for start and stop commands and corresponds to the name used to
designate this instance in messages.</Name>

        <Package>Resource group in which the application's first instance
runs.</Package>

      </Instance>

      <Instance>

        <Name>Application's name for the second instance.</Name>
```

```

    <Package>Resource group in which the application's second instance
    runs.</Package>

  </Instance>

</Application>

</APMClusterConfiguration>

```

### DTD for apminfo.xml

The following Document Type Definition (DTD) specifies the structure of apminfo.xml:

```

<!ELEMENT APMClusterConfiguration (Application+)>
<!ELEMENT Application (Name, Instance+)>
<!ELEMENT Name (#PCDATA)>
<!ELEMENT Instance (Name, Package)>
<!ELEMENT Package (#PCDATA)>

```

### EXAMPLE

In the example below, the name of the resource group is SQL-Server, and the network (or instance) name is CLUSTER04:

```

<?xml version="1.0" ?>
<APMClusterConfiguration>
  <Application>
    <Name>dbspi_mssqlserver</Name>
    <Instance>
      <Name>CLUSTER04</Name>
      <Package>SQL-Server</Package>
    </Instance>
  </Application>
</APMClusterConfiguration>

```

6. Save the completed **apminfo.xml** file on each node in the cluster in the following directory:

#### On Windows:

```
%OvDataDir%conf\conf\
```

**On UNIX/Linux:**

```
/var/opt/OV/conf/conf/
```

7. Create an XML file that describes the policies to be cluster-aware. The file name must have the format `<appl_name>.apm.xml`. `<appl_name>` must be identical to the content of the `<Application><Name>` tag in the `apminfo.xml` file. The `<appl_name>.apm.xml` file includes the names of the policies that you identified in ["Monitoring the HPE Operations Agent in High Availability Clusters" on page 153](#).
8. Use the following format while creating the `<appl_name>.apm.xml` file:

```
<?xml version="1.0" ?>

<APMApplicationConfiguration>

<Application>

<Name>Name of the cluster-aware application (must match the content of <Application><Name>
in the apminfo.xml file).</Name>

<Template>First policy that should be cluster-aware.</Template>

<Template>Second policy that should be cluster-aware.</Template>

<startCommand>An optional command that the agent runs whenever an instance of the
application starts.</startCommand>

<stopCommand>An optional command that the agent runs whenever an instance of the
application stops.</stopCommand>

</Application>

</APMApplicationConfiguration>
```

**Note:** Within the `startCommand` and `stopCommand` tags, if you want to invoke a program that was not provided by the operating system, you must specify the file extension of the program.

**For example:**

```
<startCommand>test_command.sh</startCommand>

<startCommand>dbspicol.exe ON $instanceName</startCommand>
```

The stop and start commands can use the following variables:

Variable	Description
\$instanceName	Name (as listed in <Instance><Name>) of the instance that is starting or stopping.
\$instancePackage	Name (as listed in <Instance><Package>) of the resource group that is starting or stopping.
\$remainingInstances	Number of the remaining instances of this application.
\$openViewDirectory	The commands directory on the agents.

### For example:

The following example file called **dbspi\_mssqlserver.apm.xml** shows how the Smart Plug-in for Databases configures the policies for the Microsoft SQL Server.

```
<?xml version="1.0"?>
<APMAApplicationConfiguration>
  <Application>
    <Name>dbspi_mssqlserver</Name>
    <Template>DBSPI-MSS-05min-Reporter</Template>
    <Template>DBSPI-MSS-1d-Reporter</Template>
    <Template>DBSPI-MSS-05min</Template>
    <Template>DBSPI-MSS-15min</Template>
    <Template>DBSPI-MSS-1h</Template>
    <Template>DBSPI-MSS6-05min</Template>
    <Template>DBSPI-MSS6-15min</Template>
    <Template>DBSPI-MSS6-1h</Template>
    <Template>DBSPI Microsoft SQL Server</Template>
    <StartCommand>dbspicol.exe ON $instanceName</StartCommand>
    <StopCommand>dbspicol.exe OFF $instanceName</StopCommand>
  </Application>
</APMAApplicationConfiguration>
```

9. Save the complete `<appl_name>.apm.xml` file on each node in the cluster in the following

directory:

**On Windows :**

```
%OvDataDir%\bin\instrumentation\conf
```

**On UNIX/Linux:**

```
/var/opt/OV/bin/instrumentation/conf
```

10. Ensure that the physical nodes where the resource groups reside are all managed nodes.
11. Check the syntax of the XML files on all physical nodes by running the following command:

**On Windows:**

```
%OvInstallDir%\bin\ovappinstance -vc
```

**On HP-UX, Linux, or Solaris:**

```
/opt/OV/bin/ovappinstance -vc
```

**On AIX:**

```
/usr/lpp/OV/bin/ovappinstance -vc
```

### Setting Cluster Local Node Name

For some physical nodes, for example for multihomed hosts, the standard hostname may be different from the name of the node in the cluster configuration. If this is the case, the agent cannot correctly determine the current state of the resource group. Follow the steps to configure the agent to use the hostname as it is known in the cluster configuration:

1. Run the `hostname` command to obtain the name of the physical node as it is known in the cluster configuration

**Note:** Run the following command to obtain the cluster details:

```
ovclusterinfo -a
```

2. Configure the agent to use the name of the node as it is known in the cluster configuration:

```
ovconfchg -ns conf.cluster -set CLUSTER_LOCAL_NODENAME <name>
```

In this instance, `<name>` is the name of the node as reported in the output of `hostname` command and is case-sensitive.

3. Restart the agent on every physical node by running the following commands:

```
ovc -kill
```

```
ovc -start
```

## Agent User

By default, the HPE Operations Agent regularly checks the status of the resource group. On UNIX and Linux nodes, the agents use cluster application-specific commands, which can typically only be run by root users. On Windows nodes, the agents use APIs instead of running commands.

If you change the user of an agent, the agent may no longer have the permissions required to successfully run cluster commands. In this case, you must configure the agent to use a security program (for example, sudo or .do) when running cluster commands.

To configure the agent running with a non-root account to run cluster commands, follow these steps:

1. Log on to the node with the root privileges.
2. Go to the following directory:

**On HP-UX/ Linux/Solaris:**

```
/opt/OV/bin
```

**On AIX:**

```
/usr/lpp/OV/bin
```

3. Run the following command to stop the agent:

```
ovc -kill
```

4. To configure the agent to use a security program, type the following command:

```
ovconfchg -ns ctrl.sudo -set OV_SUDO <security_program>
```

In this instance, <security\_program> is the name of the program you want the agent to use, for example /usr/local/bin/.do.

5. Run the following command to start the agent:

```
ovc -start
```

# Chapter 21: Configuring the HPE Operations Agent in a Secure Environment

The HPE Operations Agent and the HPOM or the HPE OMi management server communicate with each other over the network using the HTTPS protocol. The management server opens connections to the agent node to perform tasks, such as deploying policies and launching actions.

The HPE Operations Agent node opens connections to the management server to send messages and responses.

By default, the operating systems of the agent node and management server assign local communication ports. However, both the agent and management server use the **communication broker** component for inbound communication. The communication broker component, by default, uses the port 383 to receive data. Therefore, in effect, the node and management server use two sets of ports:

- Port assigned by the operating system for outbound communication
- Port used by the communication broker for inbound communication

In a highly-secure, firewall-based network, the communication between the management server and agent node may fail due to restrictions in the firewall settings. In these scenarios, you can perform additional configuration tasks to configure a two-way communication between the management server and managed node.

## Planning for Configuration

- If your network allows HTTPS connections through the firewall in both directions, but with certain restrictions, the configuration options are possible in HPOM or HPE OMi to accommodate these restrictions.
- If your network allows outbound connections from only certain local ports, you can configure HPOM or HPE OMi to use specific local ports.
- If your network allows inbound connections to only certain destination ports, but not to port 383, you can configure alternate communication broker ports.
- If your network allows only certain proxy systems to open connections through the firewall, you can redirect HPOM or HPE OMi communication through these proxies.
- If your network allows only outbound HTTPS connections from the management server across the firewall, and blocks inbound connections from nodes, you can configure a Reverse Channel Proxy (RCP).



**Note:** In an environment with multiple management servers, you can also configure the management servers to communicate with one another through firewalls. The configuration is the same as for communication between management servers and nodes.

### Before You Begin

*Skip this section if you are using the HPE Operations Agent only on Windows nodes.*

Most of the configuration tasks are performed through the `ovconfchg` utility, which resides in the following directory:

#### On HP-UX, Linux, and Solaris

```
/opt/OV/bin
```

#### On AIX

```
/usr/lpp/OV/bin
```

To run the **ovconfchg** command (and any other agent-specific command) from anywhere on the system, you must add the **bin** directory to the PATH variable of the system. On Windows systems, the **bin** directory is automatically added to the PATH variable. To add the **bin** directory to the PATH variable on UNIX/Linux systems, follow the below step:

Do one of the following:

On HP-UX, Solaris, or Linux nodes, run the following command:

```
export PATH=/opt/OV/bin:$PATH
```

On AIX nodes, run the following command:

```
export PATH=/usr/lpp/OV/bin:$PATH
```

The PATH variable of the system is now set to the specified location. You can now run agent-specific commands from any location on the system.

## Configuring Proxies

You can redirect connections from management servers and nodes that are on different networks through an HTTP proxy.

The management server opens connections to the proxy server, for example to deploy policies and instrumentation, for heartbeat polling, or to launch actions. The proxy server opens connections to the node on behalf of the management server, and forwards communication between them.

The node opens connections to the proxy server, for example to send messages, and action responses. The proxy server opens connections to the management server on behalf of the node.

You can also redirect communication through proxies in more complex environments as follows:

- Each management server and node can use a different proxy server to communicate with each other.
- You can configure management servers and nodes to select the correct proxy according to the host they need to connect to.

The figure below shows connections between a management server and nodes through multiple proxies as follows:

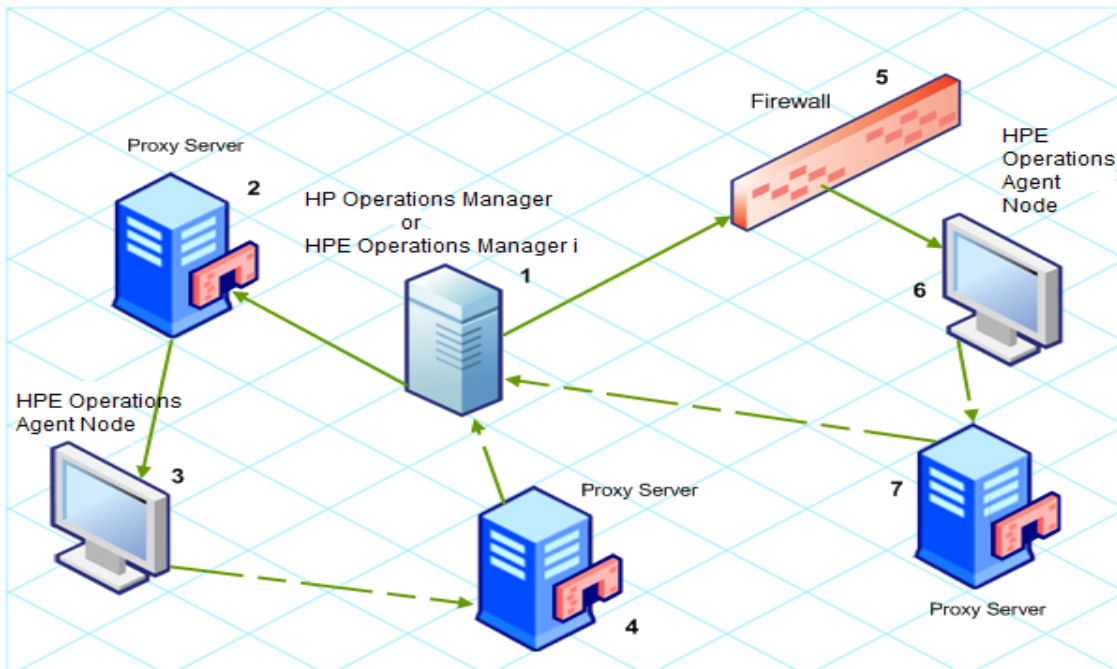
The management server (1) opens connections to a proxy (2). The proxy opens connections to the node (3) on behalf of the management server.

The node (3) opens connections to a different proxy (4). The proxy opens connections to the management server (1) on behalf of the node.

The network allows management server (1) to make outbound HTTP connections directly through the firewall (5) to another node (6). (The nodes (3, 6) are on different networks.)

The firewall (5) does not allow inbound HTTP connections. Therefore, node (6) opens connections to the management server through a proxy (7).

*Communication Using Proxies*



## PROXY Parameter Syntax

You can redirect outbound HTTPS communication through proxies by setting the PROXY parameter in the `bbc.http` name space on the management servers and nodes. You can configure this parameter in the following ways:

- Configure the values in the HPE Operations Agent installation defaults. For more information on the profile file, see [Installing HPE Operations Agent using Profile File](#). This is recommended if you need to configure proxies for large numbers of nodes. You must plan and configure the installation defaults before you create or migrate your nodes.
- Use `ovconfchg` at the command prompt.

The value of the PROXY parameter can contain one or more proxy definitions. Specify each proxy in the following format:

```
<proxy_hostname>:<proxy_port>+(<included_hosts>)-(<excluded_hosts>)
```

Replace `<included_hosts>` with a comma-separated list of hostnames or IP addresses to which the proxy enables communication. Replace `<excluded_hosts>` with a comma-separated list of hostnames or IP addresses to which the proxy cannot connect. Asterisks (\*) are wild cards in hostnames and IP addresses. Both `<included_hosts>` and `<excluded_hosts>` are optional.

To specify multiple proxies, separate each proxy with a semicolon (;). The first suitable proxy in the list takes precedence.

### Example PROXY Parameter Values

To configure a node to use `proxy1.example.com` port 8080 for all outbound connections, you would use the following value:

```
proxy1.example.com:8080
```

To configure a management server to use `proxy2.example.com:8080` to connect to any host with a hostname that matches `*.example.com` or `*example.org` except hosts with an IP address in the range 192.168.0.0 to 192.168.255.255, you would use the following value:

```
proxy2.example.com:8080+(*.example.com,*.example.org)-(192.168.*.*)
```

To extend the above example to use `proxy3.example.com` to connect to `backup.example.com` only, you would use the following value:

```
proxy3.example.com:8080+(backup.example.com); proxy2.example.com:8080+
(*.example.com,*.example.org)-(192.168.*.*)
```

In the above example, `proxy3.example.com:8080+(backup.example.com)` must be first, because the include list for `proxy2.example.com` contains `*.example.com`.

To redirect HTTPS communication through proxies:

1. Log on to the management server or node as an administrator or root and open a command prompt or shell.
2. Specify the proxies that the node should use. You can specify different proxies to use depending on the host that the agent wants to connect to. Run the following command:

```
ovconfchg -ns bbc.http -set PROXY <proxy>
```

**Note:** When you use the command **ovconfchg** on a management server that runs in a cluster, add the parameter **-ovrg <server>**.

### PROXY\_CFG\_FILE Parameter Syntax

Instead of specifying the details of the proxy server with the **PROXY** configuration variable, you can use an external configuration file to specify the list of proxy servers and configure the HPE Operations Agent to read the proxy server data from the configuration file.

Before configuring the **PROXY\_CFG\_FILE** variable, you must create the external configuration file. The proxy configuration file is an XML file that enables you to specify proxy server details within XML elements. Use a text editor to create the file; save the file under the following directory:

#### On Windows

```
%ovdatadir%conf\bbc
```

#### On UNIX/Linux

```
/var/opt/OV/conf/bbc
```

### Configuring backup proxies

The proxy configuration entry in the `bbc.http` namespace supports backup proxies. If the connection from the host to a proxy server fails, backup proxy servers can be configured for that host using the following format:

```
[bbc.http]
```

```
PROXY=<proxy1>:<port>|<proxy2>:<port>|<proxy3>:<port>+(hostname)
```

where `<proxy1>`, `<proxy2>` and `<proxy3>` are the IP addresses of the proxy server.

For example:

```
PROXY=<IP1>:<port>|<IP2>:<port>|<IP3>:<port>+(hostname.domain.com)
```

In this instance:

`<IP1>`, `<IP2>` and `<IP3>` are the proxy IP addresses.

`<IP2>` and `<IP3>` are the backup proxy servers for `<IP1>`.

If there is a failure to connect to <IP1> then <IP2> is used. If <IP2> also fails, <IP3> is used.

## Organizing the Proxy Configuration File

The proxy configuration XML file includes different XML elements for specifying proxy server, agent node, and management server details. You can provide the configuration data of multiple proxy servers in the configuration file.

### Structure of the Proxy Configuration XML File

```
<?xml version='1.0' encoding='UTF-8' standalone='yes'?>
<proxies>
  <proxy>
    <server>proxy_server.domain.example.com:8080</server>
    <for>
      <target>*.domain.example.com</target>
      <target>*.domain2.example.com</target>
      <target>*.domain3.example.com</target>
    </for>
  </proxy>
</proxies>
```

- **proxies:** The proxies element enables you to add details of proxy servers that you want to use in your HPOM or HPE OMi managed environment. All the contents of this XML file are enclosed within the proxies element.
- **proxy:** This element captures the details of the proxy server and systems that communicate with the local node through the proxy server. You can configure multiple proxy elements in this XML file.
- **server:** Use this element to specify the FQDN (or IP address) of the proxy server that you want to use in your monitoring environment.
- **for:** Within the for element, include the FQDNs or IP addresses of all other agent nodes or management servers that must communicate the local node only through the proxy server that you specified within the server element. You must add each FQDN or IP address within the target element.

### For example:

```
<for>
```

```
<target>system3.domain.example.com</target>
<target>system3.domain.example.com</target>
```

```
</for>
```

You can use the wildcard (\*) character to configure multiple system within a single target element. You can also specify an IP address range.

For example:

```
<for>
  <target>*.domain2.example.com</target>
  <target>172.16.5.*</target>
  <target>192.168.3.50-85</target>
```

```
</for>
```

- **except:** Use this element to create an exclusion list of systems that must *not* communicate with the local node through the configured proxy server (specified in the server element). Include the FQDNs or IP addresses of all such systems within the target element.

**For example:**

```
<except>
  <target>*.domain3.example.com</target>
  <target>172.16.10.*</target>
  <target>192.168.9.5-25</target>
```

```
</except>
```

### Examples of the Proxy Configuration File

Syntax	Description
<pre>&lt;proxies&gt;   &lt;proxy&gt;     &lt;server&gt;       server1.domain.example.com:8080     &lt;/server&gt;     &lt;for&gt;       &lt;target&gt;*.domain2.example.com&lt;/target&gt;     &lt;/for&gt;</pre>	<p>The server server1.domain.example.com is configured as the proxy server and all systems that belong to the domain domain2.example.com must communicate with the node or management server only through server1.domain.example.com.</p>

**Examples of the Proxy Configuration File, continued**

Syntax	Description
<pre> &lt;/proxy&gt; &lt;/proxies&gt; </pre>	
<pre> &lt;proxies&gt;   &lt;proxy&gt;     &lt;server&gt;       server2.domain.example.com:8080     &lt;/server&gt;     &lt;for&gt;       &lt;target&gt;*.domain2.example.com&lt;/target&gt;       &lt;target&gt;192.168.2.*&lt;/target&gt;     &lt;/for&gt;     &lt;/proxy&gt;     &lt;proxy&gt;       &lt;server&gt;         server3.domain.example.com:8080       &lt;/server&gt;       &lt;for&gt;         &lt;target&gt;192.168.3.*&lt;/target&gt;       &lt;/for&gt;       &lt;except&gt;         &lt;target&gt;192.168.3.10-20&lt;/target&gt;       &lt;/except&gt;     &lt;/proxy&gt;   &lt;/proxies&gt; </pre>	<p>The server server2.domain.example.com is configured as the proxy server and all systems that belong to the domain domain2.example.com or with the IP addresses that start with 192.168.2 must communicate with the node or management server only through server2.domain.example.com.</p> <p>The server server3.domain.example.com is configured as the second proxy server and all systems with the IP addresses that start with 192.168.3 must communicate with the node or management server only through server3.domain.example.com. In addition, systems within the IP address range 192.168.3.10-20 will not be able to use the proxy server server3.domain.example.</p>

**Configure the PROXY\_CFG\_FILE Variable**

1. Log on to the node as an administrator or root.
2. Create a new XML file with a text editor.

3. Add the following line at the beginning of the file:

```
<?xml version='1.0' encoding='UTF-8' standalone='yes'?>
```

4. Add content to the file.
5. Save the file under the following directory:

#### On Windows

```
%ovdatadir%conf\bbc
```

#### On UNIX/Linux

```
/var/opt/OV/conf/bbc
```

6. Run the following command:

#### On Windows

```
%ovinstalldir%bin\ovconfchg -ns bbc.http -set PROXY_CFG_FILE <filename>.xml
```

#### On HP-UX, Linux, or Solaris

```
/opt/OV/bin/ovconfchg -ns bbc.http -set PROXY_CFG_FILE <filename>.xml
```

#### On AIX

```
/usr/lpp/OV/bin/ovconfchg -ns bbc.http -set PROXY_CFG_FILE <filename>.xml
```

**Note:** You can verify the configuration using `bbcutil -gettarget <host name or IP address of the node>`.

## Configuring the Communication Broker Port

By default, the HPE Operations Agent nodes use the port 383 for inbound communication. The Communication Broker component facilitates the inbound communication on every HPE Operations Agent server or node through the port 383.

You can configure a communication broker to listen on a port other than 383. If you do this, you must also configure the other management servers and nodes in the environment, so that their outbound connections are destined for the correct port. For example, if you configure a node's communication broker to listen on port 5000, you must also configure the management server so that it connects to port 5000 when it communicates with this node.

### PORTS Parameter Syntax



You configure communication broker ports by setting the PORTS parameter in the `bbc.cb.ports` name space on all management servers and nodes that communicate with each other.

You can configure this parameter in the following ways:

- Configure the values in the HPE Operations Agent installation defaults in a profile file during installation. This is recommended if you need to configure communication broker ports for large numbers of nodes. You must plan and configure the installation defaults before you create or migrate your nodes.
- Use **ovconfchg** at the command prompt.

The values must contain one or more host names or IP addresses and have the following format:

```
<host>:<port>[,<host>:<port>] ...
```

The `<host>` can be either a domain name or IP address. For example, if the communication broker port is configured to run on port 5000 on a management server with the host name `manager1.domain.example.com`, use the following command on the management server itself, and also on any other management servers and nodes that open connections to it:

```
ovconfchg -ns bbc.cb.ports -set PORTS manager1.domain.example.com:5000
```

If you need to configure communication broker ports on multiple systems, you can use wildcards and ranges, as follows:

You use a wildcard at the start of a domain name by adding an asterisk (\*). For example:

```
*.test.example.com:5000
```

```
*.test.com:5001
```

```
*:5002
```

You can use wildcards at the end of an IP address by adding up to three asterisks (\*). For example:

```
192.168.1.*:5003
```

```
192.168.*.*:5004
```

```
10.*.*:5005
```

You can replace one octet in an IP address with a range. The range must be before any wildcards. For example:

```
192.168.1.0-127:5006
```

```
172.16-31.*.*:5007
```

If you specify multiple values for the PORTS parameter, separate each with a comma (,). For example:

```
ovconfchg -ns bbc.cb.ports -set PORTS *.test.example.com:5000,10.*.*.*:5005
```

When you specify multiple values using wildcards and ranges that overlap, the management server or node selects the port to use in the following order:

- Fully qualified domain names
- Domain names with wildcards
- Complete IP addresses
- IP addresses with ranges
- IP addresses with wildcards

**For example:**

You must configure the HPOM or the HPE OMi management environment for the following specification:

Configure all the systems within the domain \*.test2.example.com to use the port 6000 for the communication broker.

Configure all the systems with 10 as the first octet of the IP address (10.\*.\*.\*) to use the port 6001 for the communication broker with the following exception:

Configure all the systems where the second octet of the IP address is between 0 and 127 (10.0-127.\*.\*) to use the port 6003 for the communication broker.

Configure the system manager1.test2.example.com to use the port 6002 for the communication broker.

To configure the HPOM or the HPE OMi monitoring environment with the above specification, run the following command:

```
ovconfchg -ns bbc.cb.ports -set PORTS
*.test2.example.com:6000,10.*.*.*:6001,manager1.test2.example.com:6002,10
.0-127.*.*:6003
```

The changes will take effect only if you run this command on *all* the agent nodes and *all* the HPOM or the HPE OMi management servers in the monitoring environment.

To find out which port is currently configured, run the following command:

```
bbcutil -getcbport <host>
```

**To configure the Communication Broker to use a non-default port**

**Note:** Make sure to configure the Communication Broker on all HPOM or HPE OMi servers and HPE Operations Agent nodes in your environment to use the same port.

1. Log on to the HPE Operations Agent node.
2. Open a command prompt or shell.
3. Run the following command to set the Communication Broker port to a non-default value:

```
ovconfchg -ns bbc.cb.ports -set PORTS <host>:<port>[,<host>:<port>] ..
```

When you use the command **ovconfchg** on an HPE Operations Agent node that runs in a cluster, add the parameter **-ovrg**<server>, where <server> is the resource group.

4. Run the above command on all agent nodes and all management servers.

Follow these steps to configure the communication broker:

ovconfchg -ns bbc.cb.ports -set PORTS host1:483[,host2:583], where port 1 value is **483** and port 2 is **583**.

To update the port2 value from 583 to 683, run the following command:

```
ovconfchg -ns bbc.cb.ports -set PORTS host1:583[,host2:683]
```

To configure the communication broker to listen on a non-default port, change the SERVER\_PORT variable value in the bbc.cb namespace.

Run the following command to set different values to the SERVER\_PORT variable:

```
ovconfchg -ns bbc.cb -set SERVER_PORT <value>
```

In this instance, <value> is the value you want to assign to the SERVER\_PORT variable.

**Note:** When you change the value of the SERVER\_PORT variable, the communication broker restarts automatically and listens on the specified new port value.

## Configuring Local Communication Ports

By default, management servers and nodes use local port 0 for outbound connections, which means that the operating system allocates the local port for each connection. Typically, the operating system will allocate local ports sequentially. For example, if the operating system allocated local port 5055 to an Internet browser, and then the HTTPS agent opens a connection, the HTTPS agent receives local port 5056.

However, if a firewall restricts the ports that you can use, you can configure management servers and nodes to use a specific range of local ports instead.

### CLIENT\_PORT Parameter Syntax

You configure local communication ports by setting the CLIENT\_PORT parameter in the bbc.http name space on the management server or node. You can configure this parameter in the following ways:

- Configure the values in the HPE Operations Agent installation defaults. For more information on the profile file, see [Installing HPE Operations Agent using Profile File](#). This is recommended if you need to configure local communication ports for large numbers of nodes. You must plan and configure the installation defaults before you create or migrate your nodes.
- Use `ovconfchg` at the command prompt.

The value must be a range of ports in the following format:

*<lower port number>-<higher port number>*

There is no range defined for the port numbers. The range must support the number of outbound connections at a given point of time.

For example, if the firewall only allows outbound connections that originate from ports 5000 to 6000 you would use the following value:

5000-6000

To configure local communication ports:

1. Log on to the HPE Operations Agent node.
2. Open a command prompt or shell.
3. Specify the range of local ports that the management server or node can use for outbound connections by typing the following command:

```
ovconfchg -ns bbc.http -set CLIENT_PORT 5000 - 6000
```

When you use the command `ovconfchg` on a management server that runs in a cluster, add the parameter `-ovrg <server>`.

## Configuring Nodes with Multiple IP Addresses

If the node has multiple IP addresses, the agent uses the following addresses for communication:

- The communication broker accepts incoming connections on all IP addresses.
- The agent opens connections to the management server using the first network interface that it finds through the OS provided libraries.

- To communicate with HP Reporter or HP Performance Manager, the communication daemon (CODA) accepts incoming connections on all IP addresses.

Follow the steps below to configure the HPE Operations Agent to use a specific IP address:

1. Log on to the HPE Operations Agent node.
2. Open a command prompt or shell.
3. Run the following command to set the IP address for the Communication Broker:

```
ovconfchg -ns bbc.cb SERVER_BIND_ADDR <ip_address>
```

4. Run the following command to set the IP address that you want the agent to use while opening outbound connections to the management server:

```
ovconfchg -ns bbc.http CLIENT_BIND_ADDR <ip_address>
```

5. Run the following command to set the IP address that you want to use for incoming connections from HP Performance Manager or HP Reporter:

```
ovconfchg -ns coda.comm SERVER_BIND_ADDR <ip_address>
```

**Note:** See "Overview of Node Resolution" in the *HPE Operations Agent User Guide* for more information on node name resolution.

## Configuring HTTPS Communication through Proxies

If your network allows only certain proxy systems to open connections through the firewall, you can redirect HPOM or HPE OMi communication through these proxies. The following list presents the workflow of the management server and agent communication with this configuration:

1. The management server opens connections to the proxy.
2. The proxy opens connections to the node on behalf of the management server, and forwards communication between them.
3. The node opens connections to the proxy.
4. The proxy opens connections to the management server on behalf of the node.

To redirect the communication through proxies:

1. Log on to the management server or node with the root or administrative privileges.
2. Run the following command at the command prompt:

```
ovconfchg -ns bbc.http -set PROXY <proxy>: <port>
```

In this instance, <proxy> is the IP address or FQDN of the proxy server; <port> is the communication port of the proxy server.

**Note:** When you use the command `ovconfchg` on a management server that runs in a cluster, add the parameter `-ovrg <server>`.

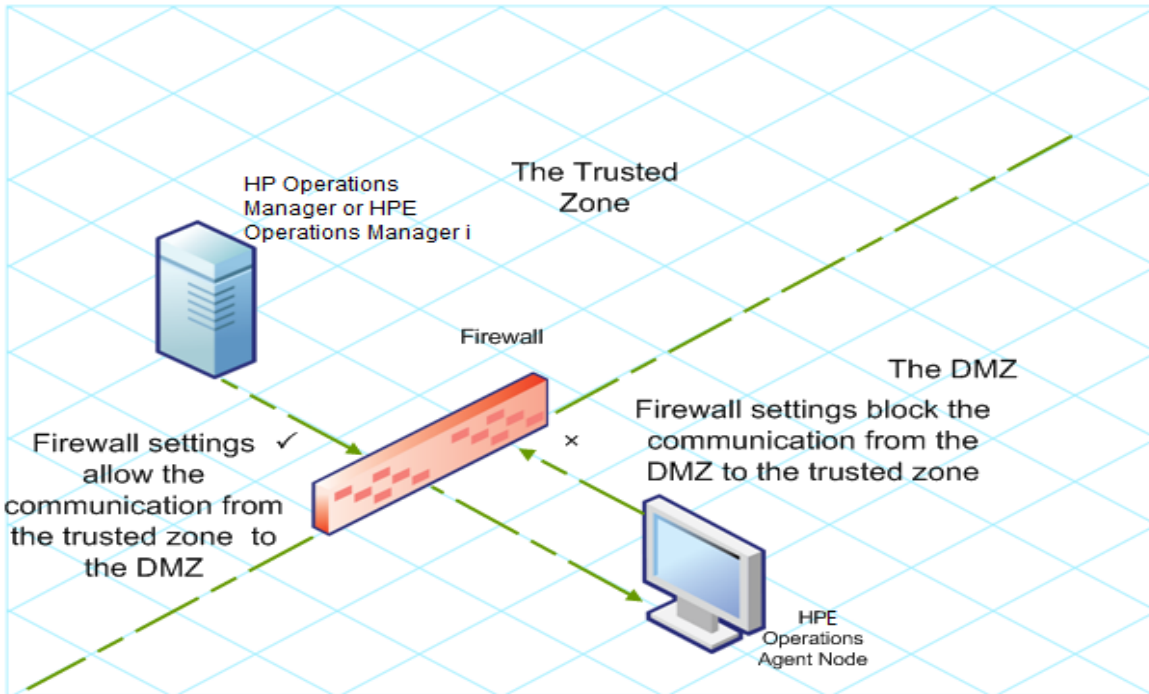
## Communication in a Highly Secure Environment

In a firewall-controlled, secure environment, systems that are present within the trusted zone can freely communicate and exchange information with one another. However, specific firewall settings can restrict communication with the systems that belong outside the trusted zone. The untrusted network, also known as the demilitarized zone (**DMZ**), may not send data to the trusted zone due to restrictions in firewall settings.

In many deployment scenarios, the HPOM or the HPE OMi management server may reside in the trusted zone and managed nodes may reside in the DMZ. If the firewall is configured to prevent the systems in the DMZ from communicating with the systems in the trusted zone, server-agent communication will become impossible.

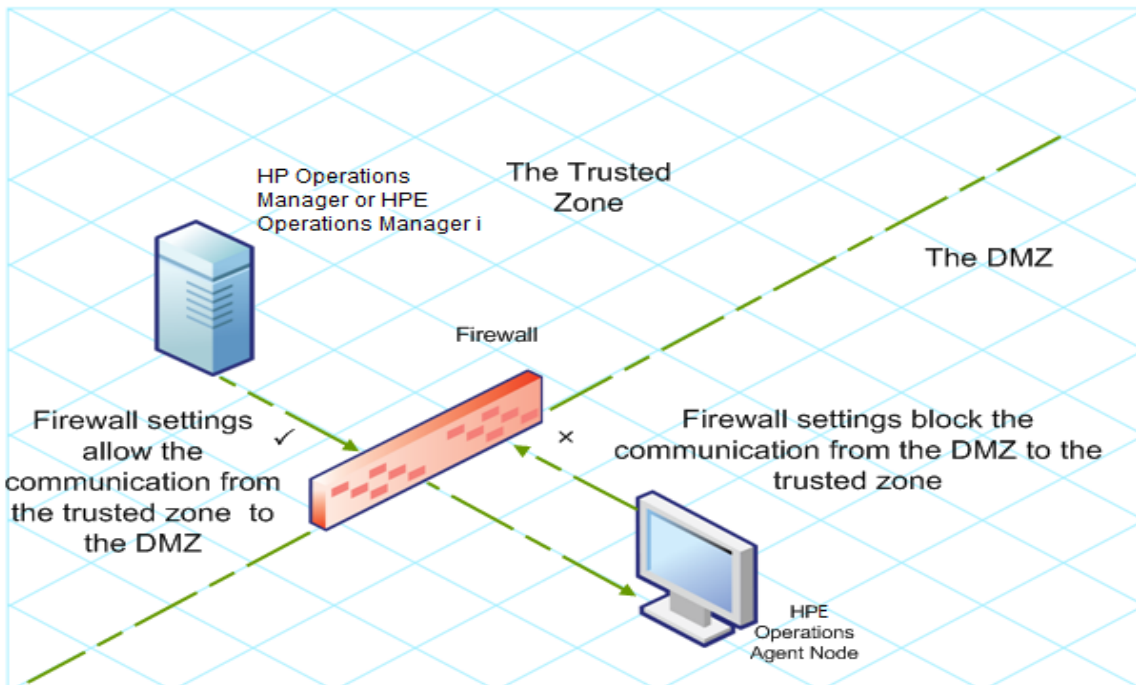
In the following scenario, managed nodes are located in the DMZ while the management server belongs to the trusted zone. The firewall settings in this example allow outbound-only communication. Therefore, inbound communication to the management server is blocked by the firewall.

*Managed Nodes in the DMZ*



In the following scenario, managed nodes are located in the trusted zone while the management server belongs to the DMZ. The firewall settings in this example allow outbound-only communication from the node to the HPOM or the HPE OMi management server, but block the inbound communication to node.

*HPOM or HPE OMi Management Server in the DMZ*



## Introduction to the Reverse Channel Proxy

One simple solution to enable bidirectional communication is to configure the firewall settings to allow inbound traffic to the port 383 (the Communication Broker port). However, this can make your system vulnerable to external attacks. To enable secure communication without allowing inbound traffic to the Communication Broker port, you must configure a Reverse Channel Proxy (**RCP**).

**Note:** On Windows, after agent installation, the firewall configuration changes when **HP Software HTTP Communication Broker** is added to the firewall inbound rules.

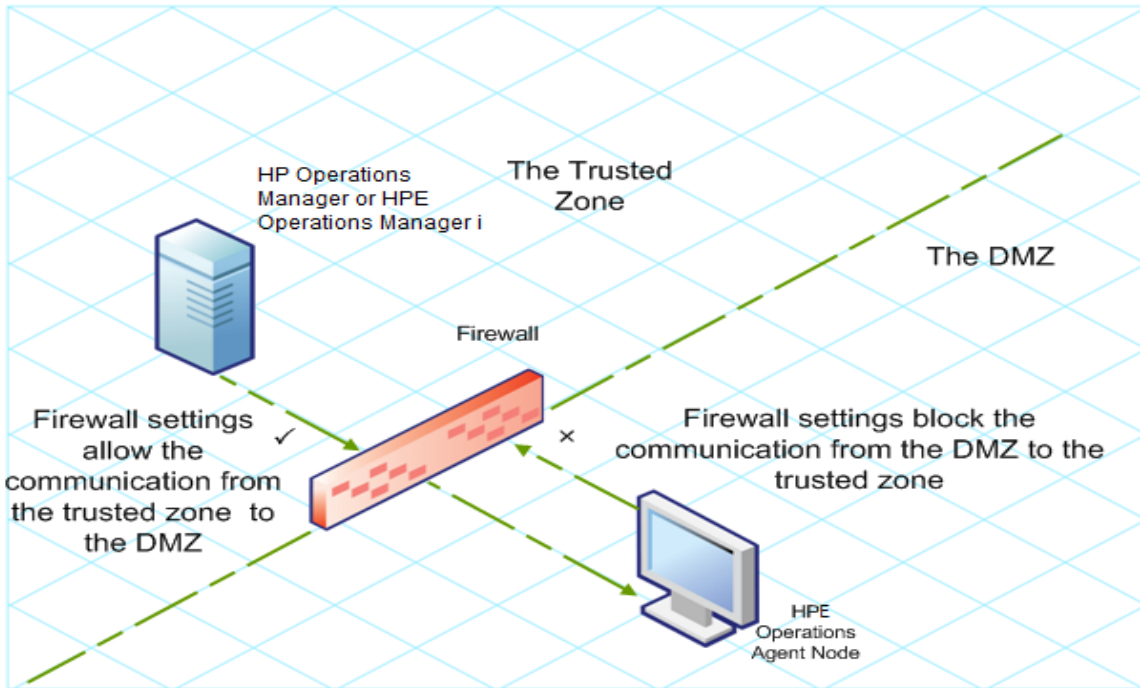
Systems belonging to the DMZ open connection to the RCP instead of the system inside the trusted zone. You can configure the system in the trusted zone to open an outbound communication channel—the reverse administration channel—to the RCP. The system in the trusted zone maintains the outbound channel; systems in the DMZ uses the reverse administration channel to send details to the trusted zone by using the RCP.

When the nodes are located in the DMZ and the management server in the trusted zone, the HPOM or the HPE OMi setup uses the following workflow:

1. The RCP is configured on a node in the DMZ.
2. All the nodes in the DMZ open connections to the RCP.
3. The management server opens an outbound connection to the RCP and establishes a reverse administration channel. The reverse administration channel allows the management server to accept inbound data originating from the RCP without any involvement of additional ports.
4. All nodes from the DMZ communicate to the HPOM or the HPE OMi management server through the reverse administration channel.

*Secure Communication through the RCP with Nodes in the DMZ*

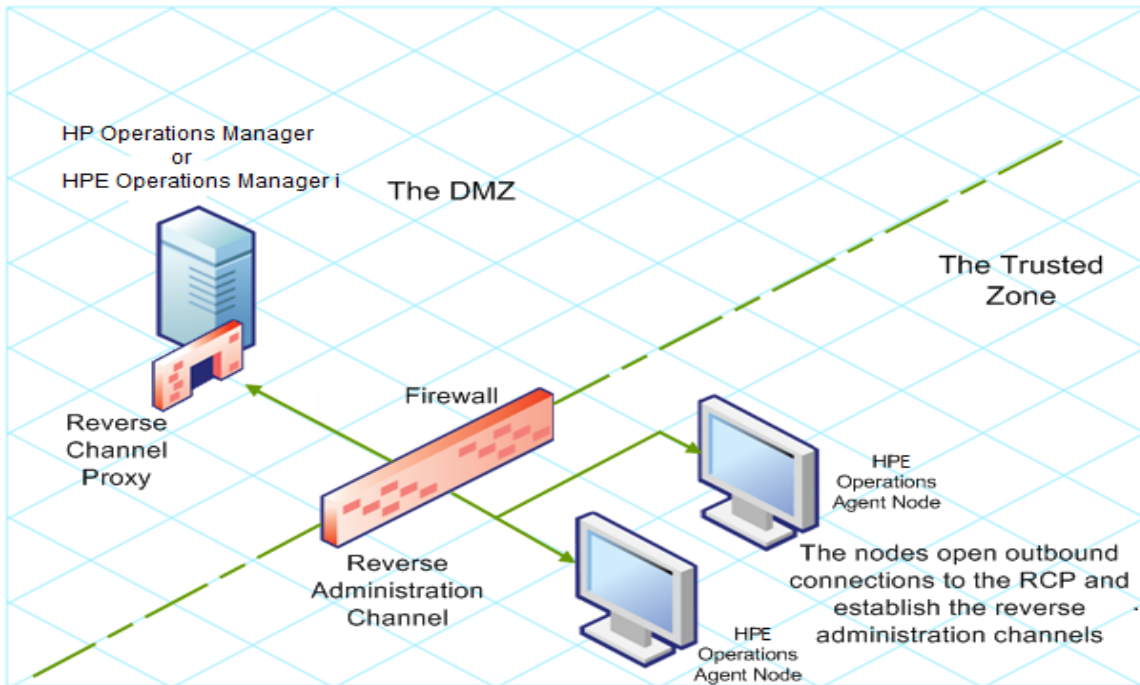




When the nodes are located in the trusted zone and the management server in the DMZ, the HPOM or the HPE OMi setup uses the following workflow:

1. The RCP is configured on the management server in the DMZ.
2. The nodes opens outbound connections to the RCP and establishes reverse administration channels. The reverse administration channels allow the nodes to accept inbound data originating from the RCP without any involvement of additional ports.
3. The management server in the DMZ communicates to the nodes through the reverse administration channel.

*Secure Communication through the RCP with the Management Server in the DMZ*



## Secure Communication in an Outbound-Only Environment

To configure secure communication with the help of the RCP and reverse administration channel in an outbound-only environment, perform the following tasks:

### Configure an RCP

Before you configure RCP, you must configure the node's certificate.

To configure an RCP:

1. Log on to the node or the management server (depending on their location on the network) as a user with the administrative or root privileges.
2. Open a command prompt or shell.
3. Run the following command:

```
ovconfchg -ns bbc.rcp -set SERVER_PORT <port_number>
```

In this instance, *<port\_number>* is the port that will be used by the RCP. Make sure the specified port is not used by another application.

4. *On UNIX/Linux only.* The Communication Broker (ovbbccb) runs with `/var/opt/OV` as the root directory. The configuration files that are necessary to open Transmission Control Protocol (TCP) connections are present in the `/etc` directory. This prevents **ovbbccb** from creating connections to the RCP. To resolve this problem, follow the steps:
  - a. Create the directory named `etc` under `/var/opt/OV`
  - b. Copy the relevant configuration files (for example, files such as **resolv.conf**, **hosts**, **nsswitch.conf**) from `/etc` to `/var/opt/OV/etc`.
  - c. Alternatively, you can also disable the **ovbbccb chroot** feature by running the following command. This method resolves the problem of preventing `ovbbccb` from creating connections to the RCP.

```
ovconfchg -ns bbc.cb -set CHROOT_PATH /
```

5. Register the RCP component so that `ovc` starts, stops and monitors it. Type the following commands:

```
ovcreg -add <install_dir>/newconfig/DataDir/conf/bbc/ovbbccrnp.xml
```

```
ovc -kill
```

```
ovc -start
```

#### *Configuring a Reverse Administration Channel*

With the help of the RCPs that you created, you must configure a reverse administration channel to facilitate the inbound communication in an outbound-only firewall environment. To configure a reverse administration channel when HPOM or HPE OMi is in HA cluster, follow these steps:

1. Log on to the node or the management server (depending on their location on the network) as a user with the administrative or root privileges.
2. Open a command prompt or shell.
3. Run the following command to create the reverse administration channel:

```
ovconfchg [-ovrg<server>] -ns bbc.cb -set ENABLE_REVERSE_ADMIN_CHANNELS true
```

4. Run the following commands to specify the RCP details:

```
ovconfchg [-ovrg<server>] -ns bbc.cb -set RC_CHANNELS <rcp>:<port>[,<OvCoreId>]
[;<rcp2>...]
```

```
ovconfchg [-ovrg<server>] -ns bbc.cb -set PROXY <rcp>:<port>[,<OvCoreId>]
[;<rcp2>...]
```

In this instance,

<*rcp*>: FQDN or IP address of the system where the RCP is configured.

<*port*>: The port number configured for the RCP (the port specified for the SERVER\_PORT variable)

<*OvCoreID*>: The core ID of the system where you configured the RCP.

Alternatively, you can provide the RCP details by using a configuration file.

5. *Optional*. Configure the server to automatically restore failed reverse administration channel connections. By default, the server does not restore failed connections. To change the default, run the following command:

```
ovconfchg [-ovrg<server>] -ns bbc.cb -set RETRY_RC_FAILED_CONNECTION TRUE
```

6. *Optional*. Set the maximum number of attempts that the server should make to connect to an RCP. By default, this is set to -1 (infinite). To change the default, run the following command:

```
ovconfchg [-ovrg<server>] -ns bbc.cb -set MAX_RECONNECT_TRIES<number of tries>
```

7. *Optional*. Configure the management server to generate a warning message when a reverse administration channel connection fails. By default, the management server does not generate the failure message. To change the default, run the following command:

```
ovconfchg [-ovrg <server>] -ns bbc.cb -set RC_ENABLE_FAILED_OVEVENT TRUE
```

If you set RETRY\_RC\_FAILED\_CONNECTION to TRUE, the management server does not generate the message.

8. *Optional*. To check that the reverse administration channel is open, run the following command:

```
ovbbccb -status
```

The output lists all open reverse administration channels.

9. *Optional*. To restore a failed reverse administration channel, run the following command:

```
ovbbccb -retryfailedrcp [-ovrg<server>]
```

### Performance Considerations for the Reverse Administration Channel

The performance of a reverse administration channel may depend on the number of nodes connected to the channel. The RC\_MAX\_WORKER\_THREADS variable helps you tune the performance of a reverse administration channel.

To use the RC\_MAX\_WORKER\_THREADS variable:

1. Log on to the node that establishes the reverse administration channel.
2. Note down the time taken by the agent to establish the channel. You can determine this by running the **ovbbccb -status** command. The **ovbbccb -status** command output shows the status of reverse administration channels originating from the system. By running the **ovbbccb -status** command repeatedly, you can determine the approximate time taken by the agent to establish the channel.
3. Calculate the ratio of the desired time to establish the channel and the approximate actual time taken by the agent to establish the channel.
4. Set the **RC\_MAX\_WORKER\_THREADS** variable to the next higher integer to the ratio. Use the following command to set this variable:

```
ovconfchg -ns bbc.cb -set RC_MAX_WORKER_THREADS <Maximum_Threads>
```

#### For example:

The management server or agent node establishes a reverse administration channel to 20 RCP nodes. When the **ovbbccb -status** command is run, the approximate time is derived as 10 seconds (without any **RC\_MAX\_WORKER\_THREADS** value set). If the required time is 5 seconds, then set **RC\_MAX\_WORKER\_THREADS** to **actual\_time/desired\_time**.

In this scenario:

Actual Time/Desired Time = 10/5 = 2

Set the value for the command:

```
ovconfchg -ns bbc.cb -set RC_MAX_WORKER_THREADS 2
```

If the **RC\_MAX\_WORKER\_THREADS** value exceeds the number of RCP nodes, then there may not be any performance improvement.

## Specifying the RCP Details with a Configuration File

With the help of a configuration file, you can specify the details of the RCPs. To use the configuration file, follow these steps:

1. Create a text file.
2. Specify the details of each RCP in a new line in the following format:

```
<rcp>:<port>[,<OvCoreId>]
```

In this instance,

*<rcp>*: FQDN or IP address of the system where the RCP is configured.

*<port>*: The port number configured for the RCP (the port specified for the SERVER\_PORT variable).

*<OvCoreID>*: The core ID of the system where you configured the RCP.

3. Save the file in the following location:

*<data\_dir>/conf/bbc*

If you are performing this step on a management server in a high-availability cluster or in a server pooling setup, save the file in the following location:

*<data\_dir>/shared/<server>/conf/bbc*

4. Run the following command:

```
ovconfchg [-ovrg<server>] -ns bbc.cb -set RC_CHANNELS_CFG_FILES <file_name>
```

In this instance,

*<file\_name>*: Name of the file created.

*<server>*: Name of the resource group of the cluster or server pooling setup.

## Configuring a RCP for Multiple Systems

You can configure only one RCP in the DMZ, and then configure other systems in the DMZ to use the RCP. To achieve this, you must set the PROXY variable of all the systems in the DMZ to the IP address (or FQDN) and port of the system that hosts the RCP. To configure multiple systems to use a single RCP, follow these steps:

1. Log on to the node with the root or administrative privileges.
2. Open a command prompt (shell).
3. Run the following command:

```
ovconfchg -ns bbc.http -set PROXY "<rcp>:<port>+<included_hosts>-<excluded_hosts>"
```

In this instance,

*<rcp>*: FQDN or IP address of the system where the RCP is configured.

**<port>**: The port number configured for the RCP (the port specified for the SERVER\_PORT variable)

**<included\_hosts>**: Specify the FQDN or IP address of the system that opens a reverse administration channel to the RCP. In this scenario, you must specify the FQDN or IP address of the management server that belongs to the trusted zone. If you want to use multiple management servers, you can specify multiple FQDNs separated by commas.

**<excluded\_hosts>**: Specify the FQDN or IP address of the systems that need not be contacted through the RCP. You can specify multiple FQDNs separated by commas. You must, however, specify the local system's FQDN and hostname (separated by commas). For example, `ovconfchg -ns bbc.http -set PROXY "<rcp>:<port>-<localhost>,<localhost>.domain.com"`

4. If the system is an HPE Operations Agent node, run the following command to restart the message agent:

```
ovc -restart opcmsga
```

Repeat step 3 and 4 on all the systems in the DMZ.

### Performance Considerations for the RCP

If you configure an RCP for only one system, meeting the minimum requirements for an agent system is sufficient.

If you configure an RCP that will be used by multiple agent nodes, you must make sure that the RCP system will be able to service all incoming requests without significant time delay.

## Verifying the Communication through the RCPs

After configuring the RCPs and establishing a reverse administration channel, you can perform the following tasks to verify if the server-node communications is established successfully:

### *Verifying the Communication to the RCP*

To verify that the system in the DMZ can communicate with the RCP, follow these steps:

1. Log on to the system in the DMZ with the root or administrative privileges.
2. Open a command prompt (shell).
3. Run the following command:

```
bbcutil -gettarget <FQDN>
```

In this instance, *<FQDN>* is the FQDN of the system that establishes the reverse administration channel to the RCP. If the management server is located in the trusted zone, specify the FQDN of the management server.

If the RCP was successfully created, the output should display the following message:

```
HTTP Proxy: <rcp>:<port>
```

In this instance,

*<rcp>*: FQDN or IP address of the system where the RCP is configured.

*<port>*: The port number configured for the RCP (the port specified for the SERVER\_PORT variable).

#### *Check the Reverse Administration Channel*

To verify that the reverse administration channel is correctly established, follow these steps:

1. Log on to the system in the trusted zone with the root or administrative privileges.
2. Open a command prompt (shell).
3. Run the following command:

```
ovbbccb -status
```

If the channels are established correctly, the output should display the following message:

```
HTTP Communication Reverse Channel Connections
```

```
Opened:
```

```
system1.mydomain.com:1025 BBC 11.00.000; ovbbcrpc 11.00.000
```

```
system2.mydomain.com:1025 BBC 11.00.000; ovbbcrpc 11.00.000
```

```
system3.mydomain.com:1025 BBC 11.00.000; ovbbcrpc 11.00.000
```

```
system4.mydomain.com:1025 BBC 11.00.000; ovbbcrpc 11.00.000
```

In this example, the system has established reverse administration channels to the following RCP systems: system1, system2, system3, and system4.

If the reverse administration channel to an RCP fails, the **ovbbccb -status** command displays the status in the following format:

```
Pending:
```

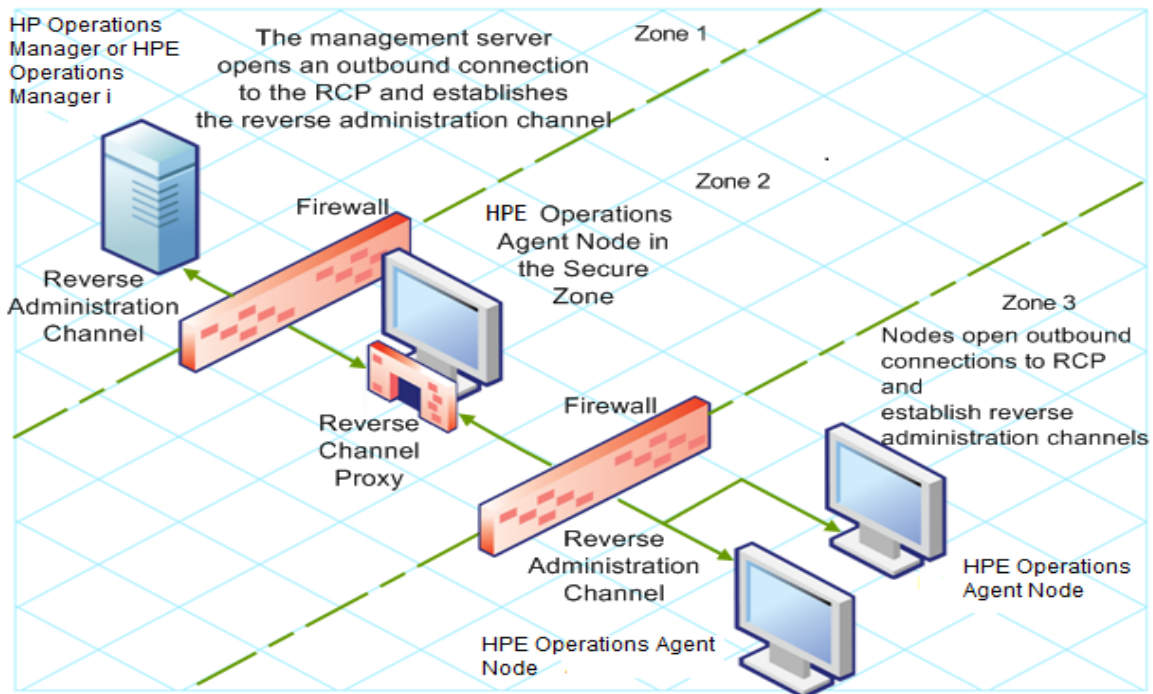
```
system5.mydomain.com:1025 Connection To Host Failed
```



## Communication through Two Firewalls

In certain cases, the management environment is set up with two different firewalls; the management server resides behind one firewall and the node group resides behind another firewall.

### *Secure Communication with Two Firewalls*



In this scenario, you must install the agent on a system in the intermediate zone (zone 2) and configure the RCP on the system. After you configure the nodes in the zone 3 and the management server in the zone 1 to establish reverse administration channels to the RCP, server-node bidirectional communication takes place through the RCP.

To configure secure bidirectional communication in this scenario, follow these steps:

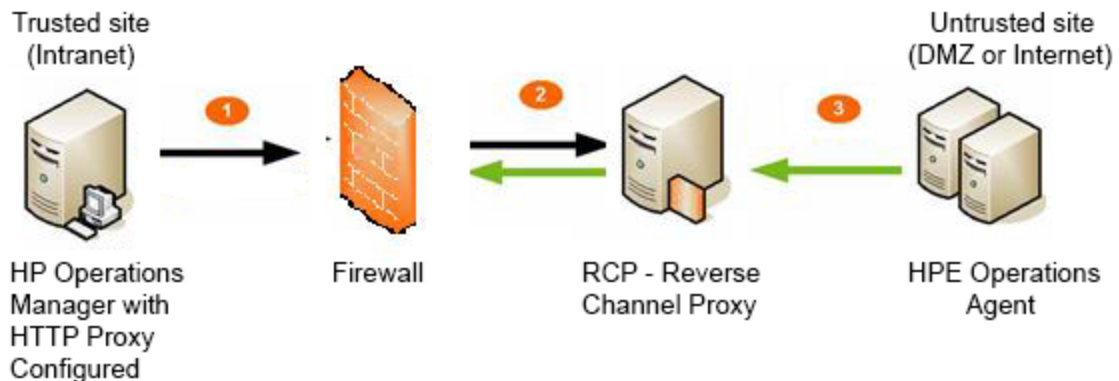
1. Install the agent on a node in the zone 2.
2. Configure an RCP on the node in the zone 2.
3. Configure the reverse administration channel from the management server to the RCP.
4. Configure reverse administration channels from the nodes in the zone 3 to the RCP.

## Configuring Amazon Linux VM Outbound Communication with HPOM

The Amazon Linux VM which is a DMZ untrusted zone and the HPOM management server in a trusted zone communicate through SSH using key authentication. The HPE firewall restricts all the other communication channels. The communication between the HPE network and the Amazon Linux VM can be established through HTTP proxy.

### Communication through a firewall

Secure unidirectional communication between the HPE network and the Amazon Linux VM can be established using the HTTP proxy and the RCP concept.



To establish secure communication between management server and HPE Operations Agent on Amazon Linux RCP is used.

### Reverse Channel Proxy (RCP)

An RCP is different from an HTTP proxy. A certificate is needed to set up an Admin Reverse Channel. A communication channel is established by management server to a Reverse Channel Proxy (RCP). The RCP uses the Admin Reverse Channel to establish data channels from client (HPE Operations Agent) to a server on request.

### How RCP works through firewall

1. Admin Reverse Channel.
  - a. Server sends a request to the RCP for an Admin Reverse Channel.
  - b. RCP confirms that an Admin Reverse Channel can be opened.
  - c. Persistent Admin Reverse Channel is established between the server and the RCP.
  - d. HPE Operations Agent sends a request to the RCP for a data channel with the server.
2. HPE Operations Agent sends data through the new data channel established by the RCP to the server.

In this secure server scenario, the RCP does the following:

- Runs on the agent system or on a dedicated system.
- Is configured using `ovconfchg`.
- Acts as a concentrator for multiple OVO HTTPS agents.

**Note:** Outbound-only communication includes an OVO management solution that is compliant with network security policies. All communication between multiple trust zones is initiated only from a trusted zone to an untrusted zone (outbound only). Communication from an OVO management server to an OVO HTTPS agent through a single firewall (outbound) goes through the firewall directly to the HPE Operations Agent. All communication from an HPE Operations Agent to a server (inbound) as well as all communication between a server and an HPE Operations Agent through multiple firewalls is conducted through an intermediary.

## Proxy Configuration and Setup Details

Configuration is required on the following setups:

- [Server](#)
- [Client](#)
- [RCP](#)

### Server:

1. Configure the **http** proxy:

```
[bbc.http]
```

```
PROXY=http-proxy:port1+(a)-(b)
```

TARGET\_FOR\_RC=<OV Core ID>

TARGET\_FOR\_RC\_CMD=<script | command>

**For example:**

[bbc.http]

PROXY=<http-proxy>:8080+(\*)-(localhost)

2. Establish the Admin Reverse Channels:

[bbc.cb]

ENABLE\_REVERSE\_ADMIN\_CHANNELS=true/false //Default = false

RC\_CHANNELS=<RCProxy1>:<RCP1\_port>[,<RCP1\_OvCoreID>][;<RCP2>...]

**For example:**

[bbc.cb]

CHROOT\_PATH=/  
/

ENABLE\_REVERSE\_ADMIN\_CHANNELS=true

RC\_CHANNELS=<RCProxy1>:9090

TARGET\_FOR\_RC=<OV Core ID>

**Client:**

1. Configure RCP proxy:

[bbc.http]

PROXY=rcp1:port1+(a)-(b)

TARGET\_FOR\_RC=<OV Core ID>

TARGET\_FOR\_RC\_CMD=<script | command>

**For example:**

[bbc.http]

CHROOT\_PATH=/  
/

PROXY=<RCProxy1>:9090+(\*)-(localhost)

TARGET\_FOR\_RC=<OV Core ID>

2. Set the following config variables:

[eaagt]

OPC\_IP\_ADDRESS=<Public IP>

```
OPC_NODENAME=<Public Hostname>
```

3. Configure the management server.

```
[sec.core.auth]
```

```
MANAGER=<HP Operations Manager IP or HOSTNAME>
```

```
MANAGER_ID=<HP Operations Manager CoreID>
```

```
[sec.cm.client]
```

```
CERTIFICATE_SERVER=<HP Operations Manager IP or HOSTNAME>
```

#### **RCP:**

1. Install HPE Operations Agent.
2. Set the oalicense.
3. Set the following config variables:

```
[eaagt]
```

```
OPC_IP_ADDRESS=<Public IP>
```

```
OPC_NODENAME=<Public Hostname>
```

4. Configure the management server.

```
[sec.core.auth]
```

```
MANAGER=<HP Operations Manager IP or HOSTNAME>
```

```
MANAGER_ID=<HP Operations Manager CoreID>
```

```
[sec.cm.client]
```

```
CERTIFICATE_SERVER=<HP Operations Manager IP or HOSTNAME>
```

5. Using the `ovcm` command issue the certificate from HPOM server in trusted zone. Transfer the file from the server and install the certificate manually using the `ovcert` command.

#### **For example:**

*On HPOM server:*

```
[root@server ~]# ovcm -issue -file aws_<http-proxy>.pem -name <http-proxy> -  
pass test -coreid <OV Core ID>
```

```
INFO: Issued certificate was written to file 'aws_<http-proxy>.pem'.
```

*On RCP node:*

```
[root@ip-rcp-node 12.02]# ovcert -importcert -file /tmp/aws_<http-proxy>.pem -
pass test
```

```
INFO: Import operation was successful.
```

6. Register ovbbcrpc (RCP process) with ovctrl.

```
$OvInstallDir/bin/ovcreg -add \
$OvInstallDir/newconfig/DataDir/conf/bbc/ovbbcrpc.xml
```

**For example:**

```
/opt/OV/bin/ovcreg -add \
/opt/OV/newconfig/DataDir/conf/bbc/ovbbcrpc.xml
```

7. Start ovbbcrpc along with the other registered processes using the following command:

```
ovc -start
```

8. Set RCP port :

```
"ovconfchg -ns bbc.rcp -set SERVER_PORT <RCP_port>"
```

By default port is set to 9090:

```
[bbc.rcp]
SERVER_PORT=0 //Default='9090'
```

**Note:** AIRVA (Agent Installation Repository Virtual Appliance) has to be setup in the Amazon network for remote deployment of the HPE Operations Agent. HPOM based remote deployment of the HPE Operations Agent is not supported in the Amazon network. For more information on AIRVA, see [Installing the HPE Operations Agent using Agent Installation Repository](#).

## Troubleshooting

### 1. Verifying RCP communication from an agent to the server

```
/opt/OV/bin/bbcutil -gettarget <management server>
```

### 2. Verifying RCP to server communication through a firewall

```
[root@server ~]# /opt/OV/bin/ovbbccb -status
```

```
Status: OK
```

```
(Namespace, Port, Bind Address, Open Sockets)
```

```
<default> 383 ANY 4
```

```
HP OpenView HTTP Communication Incoming Connections
```

To *<server>*:

localhost:29013 *<OV Core ID>* BBC 12.01.020; ovbbccb 12.01.020

localhost:46096 BBC 12.01.020; 18

localhost:46997 *<OV Core ID>* BBC 12.01.020; *<certificate\_server>* 00.00.000

HP OpenView HTTP Communication Reverse Channel Connections Opened from *<server>*:

*<http-proxy>*:9090 BBC 12.02.003; ovbbcrp 12.02.003 23 Sep 2016 15:13:09 GMT 572 ms

### 3. Verifying the connection to the RCP

```
[root@ip-rcp-node]# ovbbcrp -status
```

Status: OK

(Namespace, Port, Bind Address, Open Sockets)

bbc.rcp 9090 ANY 1

Admin Reverse Channel Connections Accepted

ip-rcp-node.ap-south-1.compute.internal:383 b8e025ca-dd79-758c-1eef-f96a5c11c719  
BBC 12.02.003; ovbbccb 12.02.003

*<server>*:383 *<OV Core ID>* BBC 12.01.020; ovbbccb 12.01.020

Admin Reverse Channel Connections Opened

Normal Connections

Incoming

localhost:34424 b8e025ca-dd79-758c-1eef-f96a5c11c719 BBC 12.02.003; ovbbcrp  
12.02.003

Outgoing

Queued CONNECT connections

```
+-----+-----+
```

```
| Source Address | Target Address
```

```
+-----+-----+
```

HTTP Tunnelled Connections

```
+-----+-----+-----+
```

```
| Source Address | Destination Address | Target Address |
```

```
+-----+-----+-----+
```

### 4. Verifying the OV Core IDs for agent

The problem that causes communication between OVO management server and agent to fail is a null OV Core ID for the agent system in the OVO management server database. This null OV Core ID occurs when agent is installed manually or a node is added to the OVO Node Bank although it is already configured. If the OV Core ID is all zeroes (000...), you must update the OV Core ID in the OVO management server database using the following command:

```
/opt/OV/bin/OpC/Utils/opcnode -chg_id node_name=myrcp.mydomain.com id="mycoreid"
```

## 5. Verifying the status of installed certificates on agent

### a. Check `bbcutil -ping` status

```
bbcutil -ping <management server>
```

```
<management server>: status=eServiceOK coreID=<OV Core ID>
```

```
bbcV=12.01.020 appN=ovbbccb appV=12.01.020 conn=8 time=3910 ms
```

```
bbcutil -ping https://<management server>
```

```
https://<management server>: status=eServiceOK coreID=<OV Core ID>
```

```
bbcV=12.01.020 appN=ovbbccb appV=12.01.020 conn=7 time=3265 ms
```

### b. Run `opcactivate` on node

```
/opt/OV/bin/OpC/install/opcactivate -srv <management server> -cert_srv <management server>
```

### c. Grant certificates from the server

```
ovcm -grant e7a130c6-2490-758d-0ea8-d1760965703b -host ec2-52-66-67-56.ap-south-1.compute.amazonaws.com.
```

## 6. Policy deployment and message verification

### a. Verify policy deployment

```
"/opt/OV/bin/OpC/Utils/opcnode" -assign_pol pol_name="opcmsg(1|3)" pol_type=Open_Message_Interface node_name=ec2-52-66-67-56.ap-south-1.compute.amazonaws.com net_type=NETWORK_IP
```

```
"/opt/OV/bin/OpC/opcragt" -distrib -force ec2-52-66-67-56.apsouth-1.compute.amazonaws.com
```

### b. Verify message to the server

```
opcmsg a=a o=o msg_text=Hello
```

## 7. Adding Amazon Linux node to HPE Operations Manager i (OMi)

To avoid duplication of Amazon Linux node entries with public IP and private IP in OMi, set the following XPL configuration:

```
set xpl.net:LOCAL_NODE_NAME=<public hostname of agent instance>
```



Or

You can also set the following configuration variable in the profile file during installation:

1. Create an agent profile `agent_profile.ini` with the following content:

```
set xpl.net:LOCAL_NODE_NAME=<public hostname of agent instance>
```

2. Run the installation script

**On Windows:** `cscript oainstall.vbs -i -a -agent_profile agent_profile.ini`

**On Linux:** `./oainstall.sh -i -a -agent_profile agent_profile.ini`

## 8. Verifying connection with HPE Operations Manager i (OMi)

- a. Set the proxy configuration variable and restart the process on OMi server using the following command:

**On Windows:** `c:/hpbsm/opr/support/opr-support-utils -restart mercuryAS`

**On Linux:** `/opt/HP/BSM/opr/support/opr-support-utils.sh -restart mercuryAS`

- b. Once the nodes are added to OMi, verify the communication from the server using the following command:

**On Windows:** `c:\hpbsm\opr\bin\opr-agt -user admin -pw admin -status -nl <public hostname of agent instance>`

**On Linux:** `/opt/HP/BSM/opr/bin/opr-agt -user admin -pw admin -status -nl <public hostname of agent instance>`

## Chapter 22: Configuring Certificates for the HPE Operations Agent and Infrastructure SPIs

Certificates must be installed on all managed nodes to facilitate network communication using the Secure Socket Layer (SSL) protocol with encryption. Certificates enable the nodes to communicate securely with the management server and other nodes.

The management server issues certificates to nodes and acts as the certificate authority. Each managed node needs the following certificates from the management server:

**A unique node certificate.** The node can identify itself to its management server and other nodes by sending them its node certificate.

**A copy of the management server's trusted certificate.** A node only allows communication from a management server if it has the trusted certificate for that management server.

In an environment with multiple management servers, a copy of the trusted certificates for all other management servers must be present on the node.

To enable the nodes to communicate securely in a managed environment by using certificates, you must install certificates after you install the agent on the nodes.

### Requesting Certificates Automatically

When you deploy the agent to a node from management server, the node requests certificates automatically from the management server. The node encrypts the certificate request with a key.

The management server then grants the certificate request. You can configure this to take place automatically. After granting the request, the management server sends the certificates to the node. If the management server denies the certificate request, you can send another request by running the following command on the managed node:

```
ovcert -certreq
```

After the management server grants the certificate request, run the following command on agent nodes that reside in high availability clusters:

```
ovc -restart ovconfd
```

In a highly secure environment, you can disable automatic certificate requests by setting the certificate deployment type to manual. You then must request the certificates with installation key or deploy the certificates manually.

## Requesting Certificates with an Installation Key

To encrypt certificate requests, you can use installation keys. You can generate an installation key on the management server, and then transfer it to the node.

Before you request certificates with an installation key, make sure that the HPE Operations Agent is running on the node. The agent sends a certificate request at the time of start. If you then request a certificate with an installation key, the new certificate request overwrites the original certificate request on the management server. You can suppress the first certificate request by setting the parameter `CERTIFICATE_DEPLOYMENT_TYPE` to `manual` in the `sec.cm.client` namespace by using the agent installation defaults in the profile file or by using the `ovconfchg` utility. For more information on the profile file, see [Installing HPE Operations Agent using Profile File](#).

To request certificates with an installation key:

1. Log on to the management server as an administrator.
2. Open a command prompt (shell).
3. Run the following command:

### From HPOM for Windows

```
ovowcsacm -genInstKey [-file <file_name>] [-pass <password>]
```

### From HPOM for UNIX/Linux

```
opccsacm -genInstKey [-file <file_name>] [-pass <password>]
```

### From HPE OMi

```
ovcm -genInstKey -file <file_name> [-pass <password>]
```

In this instance:

`<file_name>`: The name of the installation key file.

`<password>`: You need this password when you later request the certificates from the node. You can omit this option.

The command generates an installation key.

**Note:** Specify the complete path with `<file_name>`; otherwise, the certificate is stored in the current working directory. If you do not specify the `-file` option, the certificate is stored in `<data_dir>\shared\server\certificates`.

4. Securely transfer the generated file to the node. The installation key is valid for any node.
5. Log on to the node with the account used to install the node.
6. Open a command prompt (shell).
7. On UNIX/Linux nodes, make sure that the PATH variable contains the path to the `<install_dir>/bin` directory.
8. Run the following command:

```
ovcert -certreq -instkey <file_name>
```

The management server must grant the request. You can configure this to take place automatically or manually. After that, the management server sends the certificates to the node.

On agent nodes that reside in high availability clusters, run the following command:

```
ovc -restart ovconfd
```

## Deploying Certificates Manually

The node can automatically send certificate requests to the management server. If you want to install the certificates on the node manually, you can set the `CERTIFICATE_DEPLOYMENT_TYPE` variable (in the `sec.cm.client` namespace) on the node to `MANUAL`.

To deploy certificates manually:

1. Log on to the management server as an administrator.
2. Open a command prompt (shell).
3. Make sure the node is added to the list of managed nodes.
4. Run the following command:

### On HPOM for Windows

```
ovowcsacm -issue -name <node_name> [-file <file_name>] [-coreid <OvCoreId>] [-pass <password>]
```

### On HPOM for UNIX

```
opccsacm -issue -file <file_name> [-pass <password>] -name <node_name> [-coreid <OvCoreId>]
```

**Note:** Specify the complete path with <file\_name>; otherwise, the certificate is stored in the current working directory. If you do not specify the -file option, the certificate is stored in <data\_dir>\shared\server\certificates.

### On HPE OMi

```
ovcm -issue -file <file_name> [-pass <password>] -name <node_name> [-coreid <OvCoreId>]
```

In this instance,

<node\_name>: FQDN or IP address of the node.

<OvCoreId>: The core ID of the node. To retrieve the core ID of the node where the agent is already installed, perform the following step on the management server:

### On HPOM for UNIX/Linux

Run the following command:

```
opcnode -list_id node_list=<node_name>
```

### On HPOM for Windows

In the console tree, right-click the node, and then click **Properties**. The node properties dialog box opens. In the node properties dialog box, go to the General tab, click **Advanced Configuration**. The Advanced Configuration dialog box opens, which shows the core ID for the node.

### On HPE OMi

Open the **OMi Deployment with HPE Operations Agent** view, search the CI with label **HPE Operations Agent on <node>**, the name property of this CI contains the core ID for the node.

<file\_name>: The name of the certificate file generated by the command. If you do not specify this option, the command creates a file into the following directory with the default name <node\_name>-<OvCoreId>.p12:

### On HPOM for UNIX/Linux

```
/var/opt/OV/temp/OpC/certificates
```

### On HPOM for Windows

```
%OvShareDir%server\certificates
```

5. Securely transfer the generated file to the node. The installation key is valid for any node.

6. Install the agent on the node if not already installed. Use a profile file-based installation and set the `CERTIFICATE_DEPLOYMENT_TYPE` variable to `manual`. For more information on the profile file, see [Installing HPE Operations Agent using Profile File](#). Also, use the same `OvCoreID` that was generated on the management server (set the `CERTIFICATE_SERVER_ID` in the `sec.cm.client` namespace to the ID generated on the management server). For more information about preparing a profile file, see [Installing HPE Operations Agent using Profile File](#).
7. Open a command prompt (shell) on the node.
8. If the agent is running on the node, run the following command:

```
ovc -stop
```

9. To import the certificates from the generated file, run the following command:

```
ovcert -importcert -file <file_name>
```

10. Run the following command on the node:

```
ovc -start
```

After importing certificates, run the following command on agent nodes that reside in high availability clusters:

```
ovc -restart ovconfd
```

## Restoring the Certificates

If you lose the certificates on a node, you will have to create them again. If you back up the existing certificates into a file, you can restore them in the event of certificate failure. To back up certificates, follow these steps:

1. Log on to the node with the root or administrative privileges.
2. Open a command prompt (shell).
3. Run the following command:

```
ovcm -exportcacert -file <file_name> [-pass <password>]
```

The command backs up the management server certificate in the file specified with the `-file` option.

4. Run the following command:

```
ovcert -exporttrusted [-ovrg <server>] -file <file_name>
```

In this instance, <server> is the HA resource group name if the management server is installed in an HA cluster.

The command backs up the management server's trusted certificate in the file specified with the `-file` option.

5. Determine the alias of the node certificate by running the following command:

```
ovcert -list [-ovrg <server>]
```

The alias of the node certificate is the long sequence of characters, which appears under the Certificates section of the output. For example:

```
+-----+
| Keystore Content | +-----+
-----+
| Certificates: | cdc7b5a2-9dd6-751a-1450-eb556a844b55 (*) | +-----+
-----+
| Trusted Certificates: |
| CA_cdc7b5a2-9dd6-751a-1450-eb556a844b55 | +-----+
-----+
```

6. Run the following command:

```
ovcert -exportcert -file <file_name> -alias <alias> [-pass <password>]
```

The command backs up the node certificate in the file specified with the `-file` option.

To restore the certificates on the node, follow these steps:

1. Log on to the node with the root or administrative privileges.
2. Open a command prompt (shell).
3. To restore the management server certificate, run the following command:

```
ovcm -importcacert -file <file_name> [-pass<password>]
```

4. To restore the trusted certificate, run the following command:

```
ovcert -importtrusted -file<file_name>
```

5. To restore the node certificate, run the following command:

```
ovcert -importcert -file <file_name> [-pass <password>]
```

# Configuring SSL Certificates for the Agent Install Repository Virtual Appliance

To secure the Agent Install Repository Virtual Appliance with self-signed certificates or certificates signed by CA (Certificate Authority), you must configure the Secure Socket Layer (SSL) certificate.

Create a SSL certificate and copy it on to the Agent Install Repository Virtual Appliance. Configure the SSL certificate on the Lighttpd server.

**Note:** Lighttpd is a web server component present in Agent Install Repository.

After the Agent Install Repository is configured, install corresponding certificates on the nodes. You can then download the `oarepo.ps1` or `oarepo.sh` scripts for Windows and LINUX systems respectively to install HPE Operations Agent.

Follow the steps:

1. ["Creating a Certificate" below](#)
2. ["Configuring SSL Certificate on the Lighttpd Server " on page 202](#)
3. ["Importing the SSL Certificate on a Node" on page 203](#)

## Creating a Certificate

You can either create a self-signed certificate or send a certificate signing request to a Certificate Authority.

## Creating a Self-Signed Certificate

Follow the steps:

1. Create a certificate store on the Lighttpd server to save certificates and key files.
2. Log on to a node and then run the command:



```
openssl req -x509 -nodes -days <n> -newkey rsa: <nbits> -keyout <your_domain_name>.key -out <your_domain_name.>.crt
```

In this instance:

Command	Description
days	Specifies the number of days to certify the certificate.
newkey rsa :nbits	Newkey option creates a new certificate request and a new private key. The newkey rsa :nbits option generates an RSA key with the specified size.
keyout	Specifies the file name to write the newly created key.
out	Specifies the output file name.

**For example:**

```
# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout primary.key
-out cert.crt
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'primary.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

-----
Country Name (2 letter code) [XX]:in
State or Province Name (full name) []:ka
Locality Name (eg, city) [Default City]:bangalore
Organization Name (eg, company) [Default Company Ltd]:HP
Organizational Unit Name (eg, section) []:SM
Common Name (eg, your name or your server's hostname) []:16.184.47.108
```

3. A primary certificate (your\_domain\_name.crt) and private key (your\_domain\_name.key) is generated.
4. Use the primary certificate and private key to [configure the SSL certificate on the Lighttpd Server](#).

## Sending a Certificate Signing Request

1. Create a certificate store on the Lighttpd server to save certificates and key files.
2. Log on to a node and then run the following command:

```
openssl req -new -key <filename>.pem -out <filename>.csr
```

**For example:**

```
openssl req -new -key privkey.pem -out cert.csr
```

In this instance:

Command	Description
new	This command generates a new certificate request. It prompts users for the relevant field values and creates a certificate after accepting relevant information.
key	Specifies the file to read the private key.
out	Specifies the output file to output certificates.

3. Send the generated .csr file to the CA authority.
4. After you receive the signed certificate from the CA use the Intermediate (CA\_issuing.crt), primary certificate (your\_domain\_name.crt) and private key (your\_domain\_name.key) to configure SSL certificate on the Lighttpd Server.

## Configuring SSL Certificate on the Lighttpd Server

Follow the steps to configure SSL certificate on the Lighttpd server:

1. Copy the Intermediate certificate (CA\_issuing.crt), primary certificate (your\_domain\_name.crt) and private key (your\_domain\_name.key) to the certificate store.

**Note:**

A primary certificate (your\_domain\_name.crt) and private key (your\_domain\_name.key) is generated when you create self-signed certificate.

When you request for a CA certificate, the certificate authority provides you the intermediate (CA\_issuing.crt), primary certificate (your\_domain\_name.crt) and private key (your\_domain\_name.key).

2. Run the following command to combine the private key file and the primary certificate file into a single .pem file:

```
cat <your_domain_name.crt > <your_domain_name.key>> <your_domain_name>.pem
```

**For example:**

```
cat sitename.crt sitename.key > iwf0041067.pem
```

3. Open lighttpd.conf file located at /opt/vmware/etc/lighttpd/lighttpd.conf and change the following:

```
ssl.pemfile = "/cert_path/ <your_domain_name.pem>"
```

**Note:** Add the following to the lighttpd.conf file only if the certificate is issued by a certificate authority:

```
ssl.ca-file = ""/cert_path/CA_issuing.crt"
```

4. Run the following commands to restart Lighttpd server:

```
/etc/init.d/vami-sfcb restart
```

```
/etc/init.d/vami-lighttpd restart
```

## Importing the SSL Certificate on a Node

Follow the steps:

### On Linux

1. Copy the SSL certificate to a file in the directory /etc/pki/tls/certs.
2. Run the following command to compute a hash code for the certificate:

```
openssl x509 -noout -hash -in /etc/pki/tls/certs/<filename.pem>
```

3. Use the hash code to create a symbolic link in the certs directory. Run the following command to create a symbolic link:

```
ln -s /etc/pki/tls/certs/<filename.pem> /etc/pki/tls/certs/<hash code>
```

**For example:**

1. Copy the SSL certificate to a file - `myserver.pem` in the directory `/etc/pki/tls/certs`.
2. Run the following command to compute a hash code for the certificate:

```
openssl x509 -noout -hash -in /etc/pki/tls/certs/myserver.pem
```

Let us assume the hash code generated is `1a2b3c4d`.

3. Use the hash code to create a symbolic link in the `certs` directory. Run the following command to create a symbolic link:

```
ln -s /etc/pki/tls/certs/myserver.pem /etc/pki/tls/certs/1a2b3c4d.0
```

**Note:** If there are other certificates in the `certs` directory that hash to the same hash code (`1a2b3c4d.0`), then change the hash code to `1a2b3c4d.1` or `1a2b3c4d.2` and the like.

After the certificate is installed, the node is recognized as a trusted machine.

**On Windows:**

Copy the SSL certificate to the node and then import the certificate to the **Trusted Root Certification Authorities** folder. After the certificate is installed, the node is recognized as a trusted machine.

**Note:** To verify if the certificate is installed correctly, double-click to open the **Trusted Root Certification Authorities** folder > **Certificate** folder and then check if the certificate is installed.

**Note:** A signed certificate is valid only if you have the HP public key installed on your system.

Download the HP public key either from

Agent Install Repository Virtual Appliance - <https://<IP address of your system>/oarepo/hpPubKey2018.Pub>

or from the following link:

<https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning>

Copy the HP public key to the following location: `/etc/pki/rpm-gpg/hppubkey2048.pub`

## Installing HPE Operations Agent on a Trusted Machine

After you import and install SSL certificate, the node is recognized as a trusted machine. Ensure that you use the option `-sec | -secured` with `oarepo` to allow only secured connection with Agent Install

Repository Virtual Appliance (or standalone Agent Install Repository) to download and install HPE Operations Agent.

Run the following command to install HPE Operations Agent:

```
oarepo -i|-install -s|-server <server url> [-v|-version <version no.>] [-om|-om_
server <OM server name>] <[-unsec|-unsecure]||[-sec|-secure]>
```

### On Windows

```
./oarepo.ps1 -i -s <server url> -v <version no.> -sec
```

### On Linux

```
./oarepo.sh -i -s <server url> -v <version no.> -sec
```

In this instance:

<server url> URL of the Standalone Agent Install Repository or Agent Install Repository Virtual Appliance

<version no.> version number of the HPE Operations Agent

<OM server name> IP address or host name of the HP Operations Manager.

### For example:

```
oarepo -i -s https://myhostname:5480/ -v 12.01 -sec
```

## Chapter 23: Uninstalling the HPE Operations Agent and Infrastructure SPIs

**Note:** If the node hosts another HPE Software product, make sure to stop all the processes of the product prior to the agent uninstallation. After the agent is completely uninstalled, you can start the processes of the HPE Software product

1. Log on to the node as a root or an administrator.
2. Stop all agent processes by running the following commands:

```
opcagt -stop
```

```
ttd -k
```

3. Run the following command:

### On Windows 64-bit

```
cscript %OvInstallDir%bin\win64\OpC\install\oainstall.vbs -r -a
```

### On Windows x86

```
cscript %OvInstallDir%bin\OpC\install\oainstall.vbs -r -a
```

**Note:** On a Windows system, if the HPE Operations Agent is in NPU mode, you must provide the NPU password in the command line to remove patches or hotfixes.

```
cscript %OvInstallDir%bin\win64\OpC\install\oainstall.vbs -r -a -npu_  
password <password>
```

### On Linux/HP-UX/Solaris

```
/opt/OV/bin/OpC/install/oainstall.sh -r -a
```

### On AIX

```
/usr/lpp/OV/bin/OpC/install/oainstall.sh -r -a
```

4. Manually delete the following directories, if there are no other HPE Software products installed on the node:

### On Windows:

```
%OvInstallDir%
```

```
%OvDataDir%
```

**On Linux/HP-UX/Solaris**

```

/opt/OV
/var/opt/OV
/opt/perf
/var/opt/perf

```

**On AIX:**

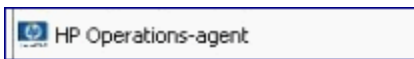
```

/usr/lpp/OV
/var/opt/OV
/usr/lpp/perf
/var/opt/perf

```

Alternatively, on a Windows node, you can remove the HPE Operations Agent 12.02 with the Programs and Features (Add/Remove Programs) window by selecting **HP Operations-agent**.

Installation of the HPE Operations Agent 12.02 adds the HPE Operations-agent program to the Programs and Features window.



Many new items such as HPE Software E/A Agent, HPE Software Measurement Interface, HPE Software Performance Core, and so on are also added to the Programs and Features window. While removing the HPE Operations Agent, choose only **HP Operations-agent** (and no other entries) in the Programs and Features window.

## Removing the Agent with the oacleanall Script

If the installation of the HPE Operations Agent is incomplete or unsuccessful, you must always try reinstallation only after uninstalling the agent. If the uninstallation command (`oainstall.sh -r -a` or `csccript oainstall.vbs -r -a`) fails to remove the agent, use the `oacleanall` script.

The `scripts` directory (directory where ISO is extracted or mounted) includes a set of `oacleanall` scripts—one script for each platform. You must choose the appropriate script to bring the system back to its original state. The `oacleanall` script **removes** the agent from the system completely and irreversibly. Use this script only to reverse the effect of an incomplete, unsuccessful, or incorrect installation of the HPE Operations Agent.

**Note:** The oacleanall script is *NOT* recommended to remove the HPE Operations Agent on a system running other HPE Software products.

The following table lists the commands for all supported platforms.

Operating System	Architecture	Command
Windows	x86	cscript oacleanall_Windows_X86.vbs
	x64	cscript oacleanall_Windows_X64.vbs
Linux	x86	./oacleanall_Linux2.6_X86.sh
	x64	./oacleanall_Linux2.6_X64.sh
	power (64-bit)	./oacleanall_Linux2.6_PPC64.sh
HP-UX	PA-RISC	./oacleanall_HP-UX_PA32.sh
	Itanium	./oacleanall_HP-UX_IA32.sh
Solaris	SPARC	./oacleanall_Solaris_SPARC32.sh
	x86	./oacleanall_Solaris_X86.sh
AIX	power (64-bit)	./oacleanall_AIX_powerpc64.sh



# Chapter 24: Uninstalling the Infrastructure SPIs

## Remove the Infrastructure SPI Policies from Managed Nodes

### From HPOM for Windows

1. In the HPOM console tree, expand the folders **Operations Manager > Policy Management > Policy groups > Infrastructure Management**.
2. Right-click **Infrastructure Management**, and then select **All Tasks > Uninstall from....**
3. In the Uninstall Policies dialog box, select **All Nodes**, and then click **OK**.

### From HPOM on UNIX/Linux

1. Log on to the HPOM console as an administrator.
2. Select **All Policy Assignments** from the Browse menu. The All Policy Assignments window opens.
3. Select the policy or policy groups you want to remove from a node or a node group by clicking the Assignment Mode check box against the policies.
4. Select **Delete Assignment...** from the **Choose an Action** box and click **Submit**. A message window appears specifying that the operation cannot be undone.
5. Click **OK**. The selected policy assignment is removed from the nodes.
6. From the HPOM Administration UI, click **Node Bank** under the **Object Banks** category. The **Node Bank** window opens.
7. Select the nodes or node groups from which you want to remove the policies.
8. Select **Deassign from this Group...** from the Choose an Action box and click **Submit**.

The policies are removed from the selected nodes.

You must wait until all policies are uninstalled from all nodes. The status of policy uninstallation can be viewed in the Deployment jobs window.

### Uninstall the Infrastructure SPIs

**Note:** To remove the Infrastructure SPIs, make sure you have approximately 240 MB of total disk space and 35 MB of space in the temporary folders available on the management server.

1. Log on to the management server.
2. Go to the following directory:

**On Windows**

```
%ovinstalldir%bin\OpC\agtinstall
```

**On UNIX/Linux**

```
/opt/OV/bin/OpC/agtinstall
```

3. Run the following command:

**On Windows**

```
cscript oainstall.vbs -r -m -spiconfig
```

**On UNIX/Linux**

```
./oainstall.sh -r -m -spiconfig
```

**Note:** In an HA cluster, perform the above steps on the active node first, and then on all nodes in the cluster.

# Chapter 25: Troubleshooting

This section helps you troubleshoot problems experienced during the installation and provides you with information to help you avoid problems.

## Installation

### Installation of the Infrastructure SPIs fails on the HPOM for Windows management server

The installation of the Infrastructure SPIs with the `cscript oainstall.vbs -i -m` command fails on the HPOM for Windows management server with the following error:

```
- VBS message
***** **** Error Number: 3000 - <date> - VBS message
***** **** Error Source: CheckRequirements - <date> - VBS message
***** **** Error Description: - general error checks.: ERRDESC -
Wrong number of arguments or invalid property assignment ; ERRNUM - 450
-<date> - VBS message
*****
- <date> - VBS message
***** !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!! - <date> - VBS message
Action ended <time>: VBSCheckRequirements. Return value 3.
Action ended <time>: INSTALL. Return value 3.
MSI (s) (CC:64) [<time>]: Product: HP Operations Smart Plug-in for
HA Cluster Infrastructure -- Installation operation failed.
MSI (s) (CC:64) [<time>]: Windows Installer installed the product.
Product Name: HP Operations Smart Plug-in for HA Cluster Infrastructure.
```

To resolve this issue, go to the `%ovdatadir%log` directory, remove the `oainstall.log` file (or save the file with a different name), and then start the installation process. It is recommended that you take a backup of the `oainstall.log` file before removing the file from the `%ovdatadir%log` directory.

### Installation of HPE Operations Agent remotely from HPOM for UNIX/Linux management server shows error message

When you are installing HPE Operations Agent for the first time, remotely from the HPOM for UNIX/Linux management server, and select the force option, the system displays the following error message:

```
ERROR: (depl-81) Unable to deploy 'OVO-Agent.xml' to node
'Management_server_name'.
(depl-153) Bundle is not installable on host.
ERROR: Error occurred during transfer or upgrade of packages.
```

To stop seeing this error message, update the HPE Operations Agent version on the management server to 12.02.

### **HP Performance Agent (PA) 5.0 packages on Windows nodes do not get replaced with HPE Operations Agent 12.02 deployment packages after upgrade**

When upgrading the Windows nodes, where PA 5.0 is installed, to HPE Operations Agent 12.02, the older PA packages are not replaced by the new packages. The PA packages still remain on the node. Even after applying the hotfix for the issue, the problem exists and you get the following error message:

**Failed to deploy package 'Performance-agent' to node 'xxxx'. Either the package itself or the requested package version was not found on the management server.**

**Because of this error, the following package(s) have not been deployed again.**

**All other packages which are also installed on the node have been successfully re-deployed.**

Check the deployment packages and synchronize the HPE Operations Agent packages to version 12.02 to resolve the issue. Perform the following tasks:

- ["Deploy the HPE Operations Agent 12.02 package" below](#)
- ["View the packages" on the next page](#)
- ["Synchronize the deployment packages with the HPE Operations Agent version 12.02 " on the next page](#)

### **Deploy the HPE Operations Agent 12.02 package**

1. Click **Deployment packages** in the console tree.
2. Select the packages to deploy.
3. Right-click the selected packages and select **All Tasks > Deploy on...**
4. Select the managed nodes to which you want to deploy the packages.

5. Click **OK**.

**Tip:** Alternatively, you can also drag-and-drop the packages to deploy.

### View the packages

1. In the console tree, right-click the node where you want to check the installed packages.
2. Click **View > Package Inventory**. A list of installed packages appear in the Details pane. The package inventory must have 12.02 Operations agent package.

If the older PA version and hotfix details are available in the package inventory, complete the task "[Synchronize the deployment packages with the HPE Operations Agent version 12.02](#)" below.

### Synchronize the deployment packages with the HPE Operations Agent version 12.02

1. From the console tree, right-click a node to open the context menu.
2. Select **All Tasks > Synchronize Inventory > packages**.

### Installation of deployable packages fail on the HPOM for Windows server with the Error 103 - PMAD corruption error

Installation of HPE Operations Agent fails if the undo log file is not present for a version (11.xx and 12.02) but the entry is present in the PMAD database. To resolve this issue, you have to clean the PMAD database. Use the **ovpmad\_dbcleanup** script to remove the corrupted entries from the PMAD database. **ovpmad\_dbcleanup** script is provided in the scripts folder in the media. The **ovpmad\_dbcleanup** script is designed only for the HPOM for Windows server.

#### Removing Corrupted Entries with ovpmad\_dbcleanup Script:

**Caution:** Backup the PMAD database before you use the **ovpmad\_dbcleanup** script.

Run the following command to remove corrupted entries:

```
cscript ovpmad_dbcleanup.vbs -p|-platform <OSname> -a|arch <arch> -v|-version <version>
```

In this instance;

- <OSname> specifies the platform-specific packages to be removed from the database and inventory on the management server.

You can use the following values:

- HP-UX
  - SOLARIS
  - AIX
  - LINUX
  - LINUX\_DEB
  - WINDOWS
- <version> specifies the active versions of the platform-specific packages to be removed from the database entries on the management server.
  - <arch> specifies the architecture for the platform-specific packages to be removed from the database entries on the management server.

**For example:**

```
cscript ovpmad_dbcleanup.vbs -p Linux -a X64 -v 11.00.044
```

**Note:** From the PMAD corruption error message you can get the parameters to run the **ovpmad\_dbcleanup** script .

**For example:**

```
server ERROR[103]: PMAD corruption C:\HPOM\data\shared\ Packages\undo\OA_
Linux2.6_X86_Ver_11.11.025.log not found

ERROR: PMAD corruption found for LINUX x86 11.11.025
```

In this instance; you get the following parameters from the error message:

- Operating System - LINUX
- Architecture - x86
- Version 11.11.025.

You can use the parameters to run the **ovpmad\_dbcleanup** script as follows:

```
cscript ovpmad_dbcleanup.vbs -p Linux -a X86 -v 11.11.025
```

**Registration of HPE Operations Agent fails on the HPOM for Windows Server**

Registration of HPE Operations Agent fails on the HPOM for Windows server with the following error:

```
Description: (PMD97) Exception has been caught in method
COvPmdPolicyManager::AddDeploymentPackage2
```

```

ERROR:      (NPREG1024) Cannot add deployment package (PD: 'E:\Agent
            Installer\OMWAgent_11_11\packages\WIN\Windows_X64\OVO-Agent.xml')
            to policy management server (PMAD)
Error during registration.

```

The error occurs if a directory or a file in the %OvDataDir%\shared\Packages\HTTPS directory has a long file name or path. To resolve this issue, delete the files or directories with long file names and then try to register HPE Operations Agent on the HPOM for Windows server.

To prevent this issue from occurring, ensure that you do not have many nested folders or files with long file names.

**Note:** On Windows, the maximum length for a path is defined as 260 characters.

### IPv4/IPv6 configuration check fails during the installation of the HPE Operations Agent

During the installation of the HPE Operations Agent, IPv4/IPv6 configuration check fails with the following error:

```

[ FAIL ] Check if IPV4/IPV6 configuration is fine
        IPV4/IPV6 configuration is not fine. Refer to oainstall.log at
/var/opt/OV/log location.

```

If the IPv4/IPv6 configuration check fails, HPE Operations Agent is successfully installed but the agent processes fail to function.

To resolve this issue:

- Ensure that at least one IP address is configured
- Ensure that IP address and the host name is mapped correctly.

To configure the HPE Operations Agent to use a specific IP address, see [Configuring Nodes with Multiple IP Addresses](#)

### Remote deployment of HPE Operations Agent 12.02 to a HP-UX IPF32 node fails

Remote deployment of HPE Operations Agent 12.02 from the HPOM management server to a HP-UX IPF32 node fails as the desired agent binary format for the HPE Operations Agent 12.02 is HP-UX IPF64.

#### For example:

You will get the following error message if you deploy HPE Operations Agent 12.02 from a HPOM for Windows management server to a HP-UX IPF32 node:

(PMD936) The package 'Operations-agent' does not support the platform of node 'hpvm38' (OS type 'HP-UX', OS version '11.31', agent binary format 'IPF32', and agent type 'HTTPS').

You can install the HPE Operations Agent 12.02 only on HP-UX IA64 systems with the patch level qpkbase package September 2013 or superseding patches.

To prevent the error during deployment, ensure that the HP-UX node where you want to install HPE Operations Agent 12.02 is a HP-UX IA64 systems with the patch level qpkbase package September 2013 or a superseding patch. Run the following command to check the patch level:

```
swlist | grep -i qpkbase
```

#### Note:

If you use the auto discovery option to add a HP-UX node, HP-UX IA64 node is added as HP-UX IPF32 node. This will cause the remote deployment of HPE Operations Agent 12.02 to fail on such nodes. To prevent this, use the expert mode to manually add a HP-UX IA64 node.

Follow the steps:

1. Log on to the HPOM management server, select **Nodes -> Configure -> Nodes**
2. In the **Configure Managed Nodes** Window, select **Nodes** -> right click to select **New Node**
3. In the **Base Setting** Window;
  - Enter the Fully Qualified Domain Name and Display Name
  - Select Use discovery service and then click **Next**
4. In the **OS Setup** Window, select the following:
  - o System Type - Itanium Compatible
  - o Operating System - HP-UX
  - o Bit Length - 64
  - o Version - B.11.31
 and then click the **Expert Mode**
5. In the **Node Properties** Window -> Go to the **System** tab -> select **IPF64** from the **Agent Binary Format** drop-down.

#### Installation of the third-party rpm fails on SLES 11 SP2 after installing the HPE Operations Agent

The installation of the third-party RPM package fails after installing the HP Operations Agent on SLES 11 SP2 with the following error:



```

insserv: warning: script '<Script_Name>' missing LSB tags and overrides
insserv: Default-Start undefined, assuming default start runlevel(s) for script
`<Script_Name>'
insserv: Stopping <Script_Name> depends on OVCtrl and therefore on system
facility
`$all' which cannot be true!
insserv: exiting now without changing boot order!
/sbin/insserv failed, exit code 1

```

HP Operations Agent 11.12 and above conform to the standard LSB tags. The LSB tags must be present in the init scripts on SLES 11 SP2 and above. During the installation of the third-party RPM package on SLES 11 SP2, the error occurs if the LSB tags are missing in the third-party application init scripts.

**Solution:**

The application vendors must add proper LSB tags in the third-party application scripts.

(or)

You must upgrade from SUSE Linux Enterprise Server 11 Service Pack 2 to SUSE Linux Enterprise Server 11 Service Pack 3. The HP Operations Agent 11.13 supports the SUSE Linux Enterprise Server 11 Service Pack 3.

**Installation of the Infrastructure SPIs Fails on HPOM for Solaris Management Server with the Error “XMLin() requires either XML::SAX or XML::Parser”**

Installation of the Infrastructure SPIs fails with the following message:

```

XMLin() requires either XML::SAX or XML::Parser at ./scripts/oaproductinstall.pl
line 402

```

**Solution:**

Ensure that the **libgcc\_s.so.1** library is present on Solaris system while registering the HPE Operations Agent on the Management Server.

**Remote deployment of HP Operations Agent 8.60.501 downgrades HP Operations Agent installed on Windows systems.**

HP Operations Agent 11.xx installed on Windows nodes are downgraded to HP Operations Agent 6.2 if you deploy HP Operations Agent 8.60.501 from HPOM for Windows Management Server.

Remote deployment of HP Operations Agent 8.60.501 triggers the installation of 8.60 bits with `-force` option. The `-force` option downgrades any available version of HP Operations Agent to 6.2.

The remote deployment of HP Operations Agent 8.60.501 from HPOM for Windows Management Server is not supported.

### Creating a zip of the product media without the digital signatures fail

Creating a zip of the product media without the digital signatures from msi packages and vbscripts fails with the following error:

```
E:\scripts\oainstall_Windows_X64.vbs(13623, 9) Microsoft VBScript runtime error:
Permission denied
```

This error occurs only when you use the **removesign** option with the zip media.

If you get this error, copy the ISO media to a read-write location, and then run the following command:

```
cscrip oainstall.vbs -createzip -p WIN -removesign
```

After the command is executed, a zip file containing the updated media (without signatures) is available at the location `-%TEMP%/OA_ZIP_MEDIA` folder.

### HPE OMi server does not get HPE Operations Agent install notification if the server is not active during HPE Operations Agent installation or upgrade.

HPE Operations Agent sends install notification to the HPE OMi server when the server is restored. HPE OMi server creates the node for this HPE Operations Agent automatically once the server is restored.

**Note:** If install notification is required to be sent voluntarily, then follow the steps:

- Create a empty `install_notif` file in the following location:

**On Windows:**

```
%OvDataDir%\tmp\OpC
```

**On HP-UX/Linux/Solaris:**

```
/var/opt/OV/tmp/OpC
```

- Run the following command to restart the message agent:

```
ovc -restart opcmsga
```

## Certificates

### Installation of the HPE Operations Agent on Linux machines shows warning messages in the log files associated with rpm signatures

The `oainstall.log` or `oapatch.log` files associated with rpm signatures may show the following warning message during the installation of the HPE Operations Agent on Linux machines:

**<Header V3 RSA/SHA1 signature>: NOKEY, <key ID>**

**For example:**

**Warning: /var/opt/OV/installation/standalone/HPOvXpl.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID 5ce2d476**

**Warning: /var/opt/OV/installation/standalone/HPOvBbc.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID 5ce2d476**

To resolve this issue, ensure that you import the HP public key before installing the HP Operations agent.

Follow the steps mentioned in the following link to import the HP public key:

<https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning>

The warning message does not affect installation of the HPE Operations Agent. If you do not want to import the HP public key, ignore the warning messages appearing in the log files.

### Signatures in vbs scripts are slow and causes delay when running some of the HPE Operations Agent commands

*Problem:* HPE Operations Agent contains digitally signed code. This is to protect the integrity of the software. Sometimes, when you run HPE Operations Agent commands on the managed node, the response is very slow. The signatures in vbs scripts causes delay when running the commands such as `opcagt -type`, `status` and so on. The delay may occur due to Certificate Revocation List (CRL) check.

*Solution 1:*

#### On Windows

1. Log on to the Windows system.
2. From the Start menu, open the **Run** prompt.
3. Type **SecPol.msc**, end then press **Enter**. The **Local Security Policy** editor window opens.
4. Click to open the **Public Key Policies** folder.
5. In the right pane, double-click **Certificate Path Validation Settings**. The **Certificate Path Validation Settings Properties** dialog box opens.
6. Click to select the **Define these policy settings** checkbox.

**Note:** Select the timeout values less than the recommended setting. For example, the Default retrieval settings can be reduced from 15-20 seconds to 1 second or to any lower suitable values.

7. Click **OK**.

#### *Solution 2:*

Run the following command in the command prompt to set a proxy, which allows CRL validation with external site:

```
netsh winhttp set proxy localhost "<local>"
```

(or)

1. In the Run prompt, type **control inetctl.cpl, 4** and then press **Enter**. The **Internet Properties** window opens with the **Connections** tab enabled.
2. Click **Lan settings**. The **Local Area Network (LAN) Settings** window opens.
3. Select the **Use a proxy server for your LAN** checkbox.
4. In the **Address** box, type the address of your proxy server.
5. In the **Port** box, type the port number of the port you want to access.
6. Click **OK**.

**Note:** You can set a proxy which allows CRL validation with external site only if you have environments with Internet access. A real proxy can be set if your environment allows, else set a dummy proxy.

# Coexistence of HP Computesensor Standalone Packages (shipped with vPV) and HPE Operations Agent 12.02

**Scenario 1:** On a VM, after you install HPE Operations Agent 12.02, installation of HPComputesensor 2.01.004 (or earlier versions) is not supported.

**Scenario 2:** Installation of HPE Operations Agent 12.02 is not supported on a machine where HP vPV (HP Virtualization Performance Viewer) 2.2 (or earlier versions) is installed.

### **Scenario 3: HP Computesensor process is in aborted state**

On a VM running with HPComputesensor 2.01.004 (or earlier versions) and HPE Operations Agent 12.02, if you uninstall HPComputesensor 2.01.004 (or earlier versions), the functionality of the hpsensor process is affected.

### **Workaround:**

1. Go to the following directory:

#### **On 64-bit versions of Windows**

```
%ovinstalldir%bin\win64\OpC\install
```

#### **On 32-bit versions of Windows**

```
%ovinstalldir%bin\OpC\install
```

#### **On Linux/HP-UX/Solaris**

```
/opt/OV/bin/OpC/install
```

#### **On AIX**

```
/usr/lpp/OV/bin/OpC/install
```

2. Run the following command:

#### **On Windows**

```
cscript oainstall.vbs -c -a
```

**On Linux/HP-UX/Solaris/AIX**

```
./oainstall.sh -c -a
```

After HPE Operations Agent 12.02 is reconfigured, the hpsensor process starts running.

**Note:** Run the following command to check the status of the hpsensor process:

```
ovc -status
```

**Scenario 4: The communication between a VM (where HP Computesensor is installed) and the HP vPV machine is disconnected, after HPE Operations Agent 12.02 is installed on the VM.**

The issue occurs only with HP vPV 2.20 and earlier versions. To resolve this issue follow the steps:

1. Install HPE Operations Agent certificate from a trusted CA onto the vPV machine.

**Note:** Run the `ovcert -list` command to ensure the certificate is installed.

2. vPV server reads the certificate from the `ovrg` namespace. Follow the steps to import the certificate into `ovrg` namespace:

- a. Log on to the vPV machine and export the certificate to the server resource group:

- Run the following command to export the certificate to a file:

```
ovcert -exportcert -file -pass
```

**For example:**

```
ovcert -exportcert -file C:\temp\cert -pass 123
```

- Run the following command to export the trusted certificate to a file:

```
ovcert -exporttrusted -file
```

**For example:**

```
ovcert -exporttrusted -file C:\temp\cert1
```

- b. Run the following command to import the certificate to the server resource group:

```
ovcert -importcert -file -ovrg server -pass
```

**For example:**

```
ovcert -importcert -file c:\temp\cert -ovrg server -pass 123
```

**Note:** To import these certificates, use the same password that you used while exporting

the certificate.

- c. Run the following command to import the trusted certificate to the server resource group:

```
ovcert -importtrusted -file -ovrg server
```

**For example:**

```
ovcert -importtrusted -file C:\temp\cert1 -ovrg server
```

## Other

**On Solaris 10, the `ovc -status` command reports the adminui process as stopped**

Although the adminui process with a longer path (which exceeds 80 characters) is running on Solaris 10, the `ovc -status` command reports the process as stopped. This is because on Solaris 10, the process details beyond 80 characters gets truncated, which is a limitation of Solaris 10.

# Send documentation feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

**Feedback on Installation Guide (Operations Agent and Infrastructure SPIs 12.03)**

Just add your feedback to the email and click send.

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

We appreciate your feedback!