

HP Operations Agent and HP Operations Smart Plug-ins for Infrastructure

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

Software Version: 11.11

Installation and Configuration Guide

Document Release Date: July 2013

Software Release Date: December 2012



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2010 - 2013 Hewlett-Packard Development Company, L.P.

Trademark Notices

Intel® and Itanium® are trademarks of Intel Corporation in the U.S. and other countries.

Microsoft®, Windows®, and Windows Vista® are U.S. registered trademarks of Microsoft Corporation.

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 software developed by the Apache Software Foundation (<http://www.apache.org/>).

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

Documentation Updates

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

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<http://h20230.www2.hp.com/selfsolve/manuals>

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

Or click the **New users - please register** link 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 HP sales representative for details.

Support

Visit the HP Software Support Online web site at:

<http://www.hp.com/go/hpsoftwaresupport>

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

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

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

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

<http://h20229.www2.hp.com/passport-registration.html>

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

Installation and Configuration Guide.....	1
Contents.....	5
Introduction.....	8
Planning for the Installation.....	8
Registering the HP Operations Agent on the HPOM Management Server (and Installing ... the Infrastructure SPIs).....	12
Registering on the HPOM for Windows Management Server.....	12
Registering on the HPOM on UNIX/Linux Management Server.....	20
Remove the HP Operations Agent Deployment Package.....	26
Prerequisites for Windows.....	28
Prerequisites for Linux.....	30
Prerequisites for HP-UX.....	32
Prerequisites for Solaris.....	33
Prerequisites for AIX.....	35
Upgrade Notes.....	36
Preinstallation Task: To Install the HP Operations Agent on HPOM in Cluster.....	39
Installing from the HPOM Console.....	41
Installing HP Operations Agent Using HP Server Automation.....	42
Import the HP Operations Agent Software.....	42
Create a Software Policy.....	43
Attach the Software Policy to a Device or Server.....	44
Verifying the Installation.....	45
Installing HP Operations Agent using Microsoft System Center 2012 Configuration	47
Manager.....	47
Create the HP Operations Agent Package.....	47
Deploy the HP Operations Agent Package.....	48
Verifying the Installation.....	49
Installing HP Operations Agent Using Red Hat Network Satellite Server.....	50

Collect and Store the Operations agent depot files (RPMs) in Software Delivery Repository.....	50
Create the Setup on the Target Node.....	50
Deploy the Packages on the Target Node.....	51
Installing the HP Operations Agent Manually on the Node.....	53
Post-Installation Task in a NAT Environment.....	58
Install Only the Infrastructure SPIs.....	59
Components of the Infrastructure SPIs on HPOM for Windows.....	63
Components of the Infrastructure SPIs on HPOM for UNIX.....	65
Installing the Agent in the Inactive Mode.....	67
HP Operations Agent in High Availability Clusters.....	70
Deploying the HP Operations Agent in a Secure Environment.....	76
Configuring Proxies.....	77
Organization of the Proxy Configuration File.....	79
Configuring the Communication Broker Port.....	83
Configuring Local Communication Ports.....	85
Configuring Nodes with Multiple IP Addresses.....	86
Configuring HTTPS Communication Through Proxies.....	86
Communication in a Highly Secure Environment.....	87
Introduction to the Reverse Channel Proxy.....	88
Configure Secure Communication in an Outbound-Only Environment.....	90
Specify the RCP Details with a Configuration File.....	93
Configure an RCP for Multiple Systems.....	93
Verify the Communication Through the RCPs.....	94
Communication Through Two Firewalls.....	95
Configuring the Performance Collection Component Remotely.....	97
Before You Begin.....	97
Deploy the OA-PerfCollComp-opcmmsg Policy.....	98
Configuring the Performance Collection Component.....	98
Configure the parm File.....	98
From HPOM for Windows.....	98
From HPOM on UNIX/Linux 9.10.....	99

Configure the alarmdef File.....	99
From HPOM for Windows.....	100
From HPOM on UNIX/Linux 9.10.....	100
Remotely Working with the HP Operations agent.....	101
Monitoring the HP Operations Agent.....	103
Before You Begin.....	103
Self Monitoring Policies.....	104
Deploying the Self Monitoring Policies.....	105
Viewing the Status of the Components.....	106
Configuring Certificates for the HP Operations Agent.....	107
Request Certificates Automatically.....	107
Request Certificates with an Installation Key.....	107
Deploy Certificates Manually.....	108
Restore Certificates.....	110
HP Operations Agent in High Availability Clusters.....	112
Deploying the HP Operations Agent in a Secure Environment.....	117
Configuring Proxies.....	118
Organization of the Proxy Configuration File.....	120
Configuring the Communication Broker Port.....	124
Configuring Local Communication Ports.....	126
Configuring Nodes with Multiple IP Addresses.....	127
Configuring HTTPS Communication Through Proxies.....	127
Communication in a Highly Secure Environment.....	128
Introduction to the Reverse Channel Proxy.....	129
Configure Secure Communication in an Outbound-Only Environment.....	131
Specify the RCP Details with a Configuration File.....	134
Configure an RCP for Multiple Systems.....	134
Verify the Communication Through the RCPs.....	135
Communication Through Two Firewalls.....	136
Uninstalling the HP Operations Agent.....	138
Uninstalling the Infrastructure SPIs.....	140
Troubleshooting.....	142

Chapter 6

Introduction

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

The *HP Operations Agent and Infrastructure SPIs 11.11* DVD media provides you with the HP 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.

Planning for the Installation

Installing the HP Operations Agent Remotely from the HPOM Management Server

In a centralized monitoring environment with HPOM, you can install the deployment packages for the HP Operations agent 11.11 on the management server, and then centrally deploy the agent packages on different nodes from the HPOM console.

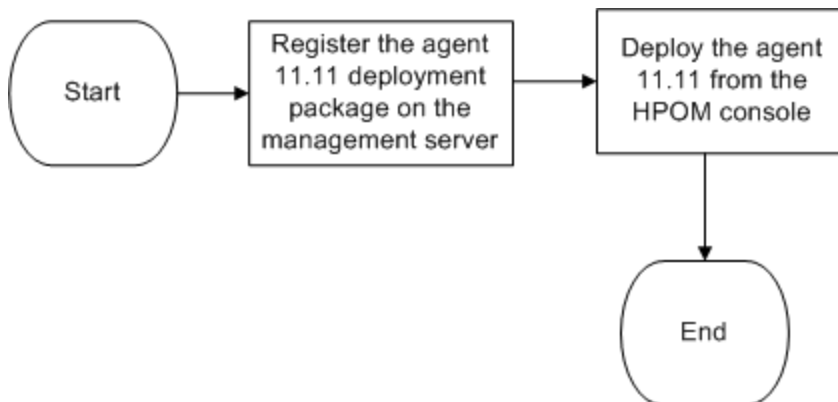
This process involves:

1. Registering the HP Operations agent 11.11 deployment packages on the HPOM management server.

Tip: A registration process ensures that the HP 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 HP Operations agent deployment packages automatically installs the Infrastructure SPIs on the HPOM management server. You can configure the installer to skip the installation of the Infrastructure SPIs.

2. Installing the HP Operations agent centrally from the HPOM console.



Installing the HP Operations Agent Manually on the Node

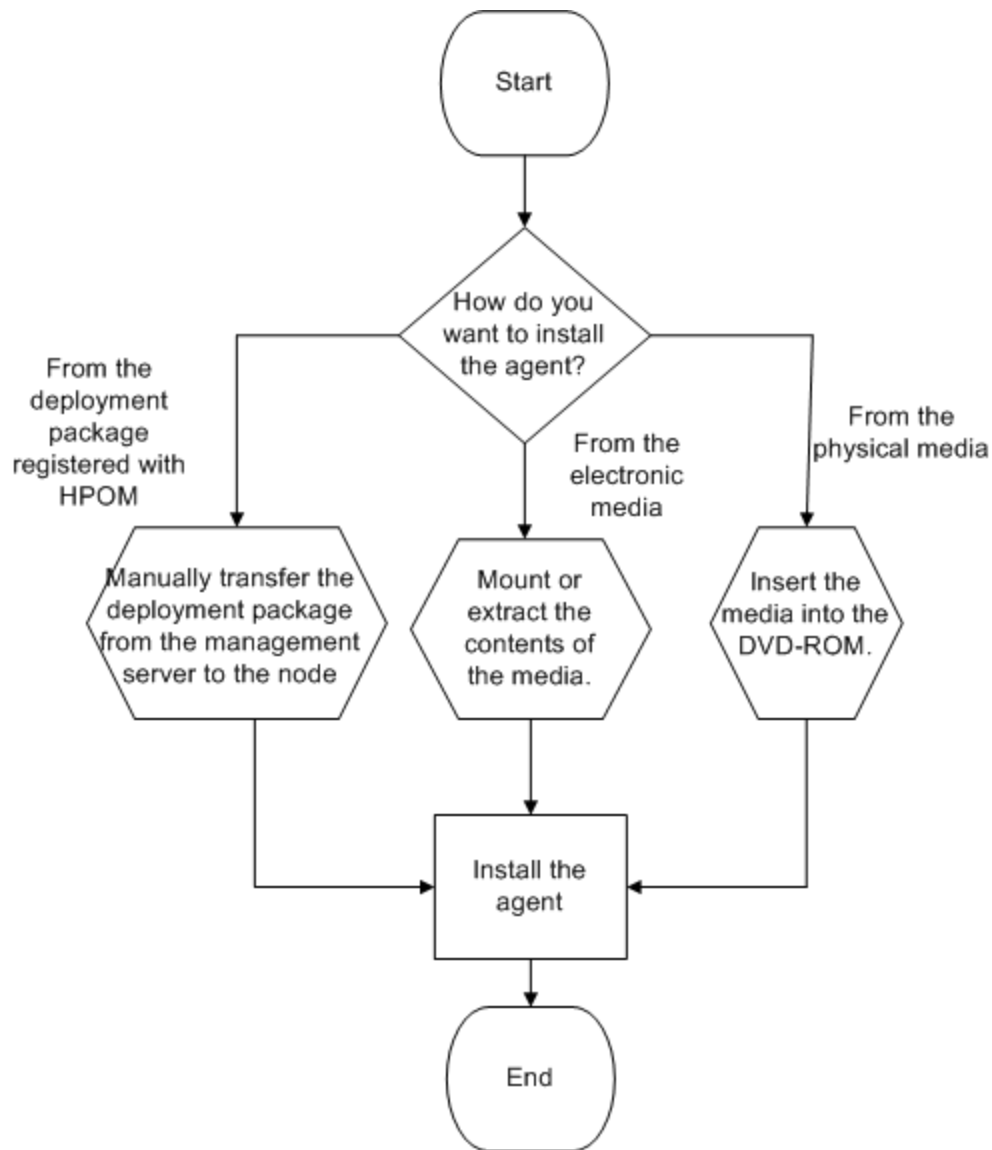
You can install the HP Operations agent from the *HP Operations Agent and Infrastructure SPIs 11.11* media by manually logging on to the managed node.

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 *HP Operations Agent and Infrastructure SPIs 11.11* physical media to the DVD drive.
 - Extract the contents of the *HP Operations Agent and Infrastructure SPIs 11.11* electronic media into a local directory.
 - Mount the *HP Operations Agent and Infrastructure SPIs 11.11* 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 *HP Operations Agent and Infrastructure SPIs 11.11* media or the deployment package.



Installing Only the Infrastructure SPIs

You can install only the Infrastructure SPIs on the HPOM management server by using the *HP Operations Agent and Infrastructure SPIs 11.11*.

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 *HP Operations Agent and Infrastructure SPIs 11.11* media.

Chapter 7

Registering the HP Operations Agent on the HPOM Management Server (and Installing the Infrastructure SPIs)

Registering on the HPOM for Windows Management Server

Prerequisites

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

To view the active deployment jobs:

1. In the console tree, expand 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 HP Operations agent 11.11. You can remove the deployable 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, HPOM version, and agent version, see the *Support Matrix*.

Disk Space Requirements

Temporary Directory ^a	Total Disk Space
%tmp% - 15 MB	90 MB

^aThe 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 1.60 or above to the version 11.11.

- You need *not* install the HP Operations agent 11.11 on the management server to be able to register the deployment packages. For more information upgrading the HP Operations agent, see "[Upgrade Notes](#)".

Register the Deployment Package

In addition to registering the deployment package for the HP 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 HP Operations agent deployment packages for select platforms and install the Infrastructure SPIs](#)

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

Task	Follow these steps
	<ol style="list-style-type: none"> 4. Add the following content: <pre>[agent.parameter] REGISTER_AGENT=YES [hpinfraspi.parameter] InfraSPI=YES InfraSPI_With_Graphs=NO InfraSPI_With_Reports=NO</pre> 5. Set the <code>InfraSPI_With_Graphs</code> and <code>InfraSPI_With_Reports</code> properties to YES or NO depending on whether you want to install the graph package or report package. 6. Save the file. 7. Go to the media root. 8. From the media root, run the following command: <pre>cscript oainstall.vbs -i -m -spiconfig <file_name></pre> <p>In this instance, <code><file_name></code> is the name of the file that you created in step 3 (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 HP Operations agent deployment packages for all platforms, but do not install the Infrastructure SPIs.</p>	<ol style="list-style-type: none"> 1. Make sure that you downloaded the .ISO file for all platforms or obtained the physical DVD. 2. Log on to the management server as administrator. 3. Create a new file with a text editor. 4. Add the following content: <pre>[agent.parameter] REGISTER_AGENT=YES [hpinfraspi.parameter] InfraSPI=NO</pre>

Task	Follow these steps
	<pre> InfraSPI_With_Graphs=NO InfraSPI_With_Reports=NO </pre> <ol style="list-style-type: none"> 5. Save the file. 6. Go to the media root. 7. From the media root, run the following command: <p>cscript oainstall.vbs -i -m -spiconfig <file_name with complete path></p> <p>In this instance, <file_name> is the name of the file that you created in step 3 (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>
Register the HP Operations agent deployment packages for select platforms and install the Infrastructure SPIs	<ol style="list-style-type: none"> 1. Make sure that you downloaded the .ISO file for all platforms or obtained the physical DVD. 2. Log on to the management server as administrator. 3. Create a new file with a text editor. 4. Add the following content: <pre> [agent.parameter] REGISTER_AGENT=YES [hpinfraspi.parameter] InfraSPI=YES InfraSPI_With_Graphs= InfraSPI_With_Reports= </pre> 5. Set the <code>InfraSPI_With_Graphs</code> and <code>InfraSPI_With_Reports</code> properties to YES or NO depending on whether you want to skip the installation of the graph or report packages. 6. Save the file. 7. Go to the media root. 8. From the media root, run the following command: <p>cscript oainstall.vbs -i -m -p <platform> -spiconfig <file_name></p>

Task	Follow these steps
	<p>In this instance, <i><file_name></i> is the name of the file that you created in step 3 (with complete path); <i><platform></i> is the node platform for which you want to register the deployment package.</p> <p>Use the following values for <i><platform></i>:</p> <p><i>For Windows:</i> WIN</p> <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 the specific 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> <p>cscript oainstall.vbs -i -m -p AIX -p SOL</p>

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:

%ovinstalldir%\bin\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 11.11, 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 HP 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


```
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

Active Versions
=====
AIX      :PowerPC(64)      :11.11.022
HP-UX    :IPF32           :11.11.022
HP-UX    :PA-RISC         :11.11.022
LIN      :PowerPC(2.6)    :11.11.022
LIN      :x64(2.6)        :11.11.022
LIN      :x86(2.6)        :11.11.022
LIN_DEB  :x64            :11.11.022
SOL      :SPARC           :11.11.022
SOL      :x86            :11.11.022
WIN      :x64            :11.11.022
WIN      :x86            :11.11.022

Backed-up Versions
=====
AIX      :PowerPC(32)     :08.60.005
AIX      :PowerPC(64)     :08.60.005
HP-UX    :IPF32           :08.60.005
HP-UX    :PA-RISC         :08.60.005
LIN      :IPF64(2.6)      :08.60.005
LIN      :x64(2.6)        :08.60.005
LIN      :x86(2.6)        :08.60.005
SOL      :SPARC           :08.60.005
SOL      :x86            :08.60.005
WIN      :IPF64           :08.60.010
WIN      :x64            :08.60.010
WIN      :x86            :08.60.010
```

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

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



```

Active Versions
=====
AIX      :PowerPC(64)      :11.11.025
HP-UX    :IPF32            :11.11.025
HP-UX    :PA-RISC          :11.11.025
LIN      :PowerPC(2.6)    :11.11.025
LIN      :x64(2.6)        :11.11.025
LIN      :x86(2.6)        :11.11.025
LIN_DEB  :x64              :11.11.025
SOL      :SPARC            :11.11.025
SOL      :x86              :11.11.025
WIN      :x64              :11.11.025
WIN      :x86              :11.11.025

```

```

SPI Active Version
=====

```

```

HPSpiUmI   : 11.11
HPSpiCLI   : 11.11
HPSpiSysI  : 11.11
HPSpiInfG  : 11.11
HPSpiInfR  : 11.11

```

```

Backed-up Versions
=====

```

```

AIX      :PowerPC(64)      :11.10.031
AIX      :PowerPC(64)      :11.10.035
AIX      :PowerPC(64)      :11.11.024
HP-UX    :IPF32            :11.10.031
HP-UX    :PA-RISC          :11.10.031
HP-UX    :IPF32            :11.10.035
HP-UX    :PA-RISC          :11.10.035
HP-UX    :IPF32            :11.11.024
HP-UX    :PA-RISC          :11.11.024
LIN      :PowerPC(2.6)    :11.10.031
LIN      :x64(2.6)        :11.10.031
LIN      :x86(2.6)        :11.10.031
LIN      :PowerPC(2.6)    :11.10.035
LIN      :x64(2.6)        :11.10.035
LIN      :x86(2.6)        :11.10.035
LIN      :PowerPC(2.6)    :11.11.024
LIN      :x64(2.6)        :11.11.024
LIN      :x86(2.6)        :11.11.024
LIN_DEB  :x64              :11.11.023
LIN_DEB  :x64              :11.11.024
SOL      :SPARC            :11.10.031
SOL      :x86              :11.10.031
SOL      :SPARC            :11.10.035
SOL      :x86              :11.10.035
SOL      :SPARC            :11.11.024
SOL      :x86              :11.11.024
WIN      :x64              :11.10.031
WIN      :x86              :11.10.031
WIN      :x64              :11.10.035
WIN      :x86              :11.10.035
WIN      :x64              :11.11.024
WIN      :x86              :11.11.024

```

```

SPI Backed up Version
=====

```

```

HPSpiUmI   : 2.01
HPSpiUmI   : 2.00
HPSpiCLI   : 2.01
HPSpiSysI  : 2.00
HPSpiSysI  : 2.01

```


Registering on 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 ^a	Total Disk Space
Linux	/tmp - 35 MB	90 MB
HP-UX	/tmp - 17 MB	240 MB
Solaris	/tmp - 35 MB	80 MB

^aThe 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 1.60 or above to the version 11.11.

- You need *not* install the HP Operations agent 11.11 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 HP 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 HP Operations agent deployment packages for select platforms and install the Infrastructure SPIs](#)

Task	Follow these steps
Register the HP Operations agent deployment packages for all platforms and install the Infrastructure SPIs.	<ol style="list-style-type: none"> 1. Make sure that you downloaded the .ISO file for all platforms or obtained the physical DVD. 2. Log on to the management server as root. 3. Go to the media root. 4. Run the following command: <code>./oainstall.sh -i -m</code> 5. Verify the registration process.
Register the HP Operations agent deployment package for a specific node platform by using a platform-specific ISO file.	<ol style="list-style-type: none"> 1. Make sure that you downloaded the .ISO file for the node platform of your choice. 2. Log on to the management server as root. 3. Go to the media root. 4. Run the following command: <code>./oainstall.sh -i -m</code> 5. Verify the registration process.
Register the HP 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"> 1. Make sure that you downloaded the .ISO file for all platforms or obtained the physical DVD. 2. Log on to the management server as root. 3. Create a new file with a text editor. 4. Add the following content: <pre>[agent.parameter] REGISTER_AGENT=YES [hpinfraspi.parameter] InfraSPI=NO InfraSPI_With_Graphs=NO</pre> 5. Save the file. 6. Go to the media root. 7. From the media root, run the following command: <code>./oainstall.sh -i -m -spiconfig <file_name></code>

Task	Follow these steps
	<p>In this instance, <i><file_name></i> is the name of the file that you created in step 3 (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 graph package for Infrastructure SPIs.</p>
<p>Register the HP Operations agent deployment packages for all platforms, but do not install the Infrastructure SPIs.</p>	<ol style="list-style-type: none"> 1. Make sure that you downloaded the .ISO file for all platforms or obtained the physical DVD. 2. Log on to the management server as root. 3. Create a new file with a text editor. 4. Add the following content: <pre>[agent.parameter] REGISTER_AGENT=YES [hpinfraspi.parameter] InfraSPI=NO InfraSPI_With_Reports=NO InfraSPI_With_Graphs=NO InfraSPI_With_Graphs_And_Reports=NO</pre> 5. Save the file. 6. Go to the media root. 7. From the media root, run the following command: <pre>./oainstall.sh -i -m -spiconfig <file_name with complete path></pre> <p>In this instance, <i><file_name></i> is the name of the file that you created in step 3 (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 HP Operations agent deployment packages for select platforms and install the Infrastructure SPIs</p>	<ol style="list-style-type: none"> 1. Make sure that you downloaded the .ISO file for all platforms or obtained the physical DVD. 2. Log on to the management server as root. 3. Create a new file with a text editor.

Task	Follow these steps
	<ol style="list-style-type: none"> 4. Add the following content: <pre>[agent.parameter] REGISTER_AGENT=YES [hpinfraspi.parameter] InfraSPI=YES InfraSPI_With_Graphs=</pre> 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. 6. Save the file. 7. Go to the media root. 8. From the media root, run the following command: <pre>./oainstall.sh -i -m -p <platform> -spiconfig <file_name></pre> <p>In this instance, <code><file_name></code> is the name of the file that you created in step 3 (with complete path); <code><platform></code> is the node platform for which you want to register the deployment package.</p> <p>Use the following values for <code><platform></code>:</p> <p><i>For Windows:</i> WIN</p> <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>

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.

Active Versions		
=====		
AIX	:PowerPC (64)	:11.11.022
HP-UX	:IPF32	:11.11.022
HP-UX	:PA-RISC	:11.11.022
LIN	:PowerPC (2.6)	:11.11.022
LIN	:x64 (2.6)	:11.11.022
LIN	:x86 (2.6)	:11.11.022
LIN_DEB	:x64	:11.11.022
SOL	:SPARC	:11.11.022
SOL	:x86	:11.11.022
WIN	:x64	:11.11.022
WIN	:x86	:11.11.022
Backed-up Versions		
=====		
AIX	:PowerPC (32)	:08.60.005
AIX	:PowerPC (64)	:08.60.005
HP-UX	:PA-RISC	:08.06.005
HP-UX	:IPF32	:08.60.005

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

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


```

Active Versions
=====
AIX      :PowerPC (64)      :11.11.025
HP-UX    :IPF32             :11.11.025
HP-UX    :PA-RISC           :11.11.025
LIN      :PowerPC (2.6)    :11.11.025
LIN      :x64 (2.6)        :11.11.025
LIN      :x86 (2.6)        :11.11.025
LIN_DEB  :x64              :11.11.025
SOL      :SPARC             :11.11.025
SOL      :x86               :11.11.025
WIN      :x64               :11.11.025
WIN      :x86               :11.11.025

SPI Active Version
=====
HPSpiVmI   : 11.11
HPSpiClI   : 11.11
HPSpiSysI  : 11.11
HPSpiInfG  : 11.11

Backed-up Versions
=====
AIX      :PowerPC (32)      :08.60.005
AIX      :PowerPC (64)      :08.60.005
HP-UX    :IPF32             :08.60.005
HP-UX    :PA-RISC           :08.60.005
LIN      :IPF64 (2.6)      :08.60.005
LIN      :x64 (2.6)        :08.60.005
LIN      :x86 (2.6)        :08.60.005
SOL      :SPARC             :08.60.005
SOL      :x86               :08.60.005
WIN      :IPF64             :08.60.007
WIN      :x64               :08.60.007
WIN      :x86               :08.60.007

SPI Backed up Version
=====
HPSpiClI   : 11.10
HPSpiVmI   : 11.10
HPSpiSysI  : 11.10

```

3. Locate the platform for which you installed the deployment package. If the active version is displayed as 11.11, 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 HP 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/HPOpsAgt/<OS>/<OA_  
Version>/<ARCH>
```

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

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

Remove the HP Operations Agent Deployment Package

1. On UNIX/Linux: Log on to the management server as administrator and go to the `%ovinstalldir%bin\OpC\agtinstall` directory.

On Windows: 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 HP 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 HP Operations agent package, use the command **`./oainstall.sh -r -m -v 11.11.025 -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 HP Operations agent 11.11 deployment packages, the installer program reinstates the highest backed-up version of deployment packages (if available) on the management server.

Chapter 8

Prerequisites for Windows

User

To install the HP Operations agent on a Windows node, 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
- Write access to the admin\$ share
- Read access to the registry
- Permission to log on as a service
- Permission to start and stop services

Necessary Software

Windows Installer 4.5 or higher: The Windows Installer software is packaged with the Microsoft Windows operating system. The installer program of the HP Operations agent requires the version 4.5 of this software component to be present on the system.

Windows Script Host: The Windows Script Host must be enabled on the system. The installer program of the HP 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, look 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 is the Value Data for the Enabled key is set to 0.
7. If the key Enabled is not present, you can safely 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
- Remote Registry
- Server
- Workstation

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

1. Log on to the system with the administrative privileges.
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. In the Services window, check if the status of each of the above services is Started. If the status of one of the services is found to be anything 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 or if you want to 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.

Additional Requirements for Hyper-V on Windows Server 2008

To be able to monitor virtual systems, apply the following hotfix:

<http://support.microsoft.com/kb/950050>

To be able to log the BYLS class of metrics, apply the following hotfix:

<http://support.microsoft.com/KB/960751>

Prerequisites for Linux

User

To install the HP Operations agent on a Linux node, you must use a user with the root privileges.

Note: Because the HP Operations agent cannot be installed without the root user on a Linux node, you cannot install the agent on a vSphere Management Assistant (vMA) node (where the root user is disabled by default) remotely from the HPOM console.

Necessary Software

To install the HP Operations agent, the following runtime libraries and packages are required:

- glibc-2.3.4-2.36.i686.rpm
- On x64 systems:
 - libgcc-3.4.6-8.i386.rpm
 - libstdc++-3.4.6-8.i386.

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 for.

- C++ runtime:
 - For systems with kernel version 2.6:
/usr/lib/libstdc++.so.5
 - For systems with kernel version 2.6 on Itanium :
/usr/lib/libstdc++.so.6
- Curses runtime library:
/usr/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 higher 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.

3. **For xglance:** To use the xglance utility, make sure the following components are available on the system:
4. 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.)

Additional Requirements for the vMA node

- Make sure that the portmap service is started.
- Disable the floppy drive on the vMA.
- Increase the RAM size for the vMA to 1 GB
- Enable the communication across firewalls on the vMA node

The agent uses the port 383 to facilitate the communication with other systems across firewalls. You must configure the vMA node to accept communication traffic on the port 383. To achieve this, run the following commands:

- **sudo iptables -I RH-Firewall-1-INPUT 3 -p tcp -m tcp --dport 383 --tcp-flags SYN,RST,ACK SYN -j ACCEPT**
- **sudo service iptables save**

To verify that the changes have taken effect, run the following command:

sudo vi /etc/sysconfig/iptables

The vi editor opens the iptables file from the `/etc/sysconfig` directory. In the iptables file, verify that the following line is present:

```
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 383 --tcp-flags  
SYN,RST,ACK SYN -j ACCEPT
```

Note: By default, the root user of a vMA (Linux) node is disabled. As a result, you cannot deploy the agent remotely from the HPOM console to a vMA node. The installer program for the HP Operations agent—the `oainstall` script—also requires the root privileges. Therefore, you must use the `sudo` command to switch to the root user before installing the agent manually on the vMA node.

Prerequisites for HP-UX

User

To install the HP Operations agent on an HP-UX node, you must use a user with the root privileges.

Necessary Software

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

- For HP-UX 11.23. PHKL_36853, PHCO_38149 (or superseding patches)
- 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 11.31. PHCO_36530 (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 HP 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)

Disk Space

For new installation

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

400 MB

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

550 MB

For upgrade

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

400 MB

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

550 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.

Prerequisites for Solaris

User

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

Necessary Software

- *For Solaris 10.* Before you install the HP Operations agent on a Solaris 10 node, make sure to install the following or superseding patches:

Operating System Version	Platform	Required Patches
10	32-bit (x86)	<ul style="list-style-type: none"> ■ 118345-03 SunOS 5.10_x86: ld & libc.so. ■ 119964-03 SunOS 5.10_x86 Shared library patch for C++_x86 ■ 120754-01 SunOS 5.10_x86 libmtsk
	64-bit (SPARC/x64)	<ul style="list-style-type: none"> ■ 117461-04 Linker ■ 120753-01 libmtsk ■ 119963-19 SunOS 5.10: Shared library patch for C++

- *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

Prerequisites for AIX

User

To install the HP 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:

```
lspp -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 **xlC.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/OV** and **/usr/lpp/perf**):

350 MB

For the data directory (**/var/opt/OV** and **/var/opt/perf**):

350 MB

For upgrade

For the installation directory (**/usr/lpp/OV** and **/usr/lpp/perf**):

350 MB

For the data directory (**/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 `/usr/lpp/OV` directory to the `/new` directory, run the following command:

`ln -s /new /usr/lpp/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 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 `perfagent.tools` file set and `xmservd` is bundled with the Performance Toolbox for AIX component (a licensed software program).

Upgrade Notes

Upgrade an agent older than 11.00

You can directly upgrade the HP Operations agent 11.00 to the version 11.11.

You can upgrade an older version (older than 11.00) of the HP Operations agent, HP Performance Agent, or HP GlancePlus to the HP Operations agent 11.11. The following versions can be directly upgraded to the HP Operations agent 11.11:

- HP Operations agent: 8.53, 8.60
- HP Performance Agent: 4.70, 5.00
- HP GlancePlus: 4.70, 5.00

The installation of the HP Operations agent 11.11 fails if any agent software older than the specified versions is installed. Before installing the HP Operations agent 11.11 on nodes with the HP Operations agent older than 8.53, the HP Performance Agent older than 4.70, and HP GlancePlus older than 4.70, do one of the following:

- Upgrade the agent software to the version that can be upgraded to the HP Operations agent 11.11.

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

- Remove the agent software completely.

This may result in removal of policies and instrumentation files from the node. After upgrading to the HP Operations agent 11.11, 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 with the administrative privileges.
2. Open a command prompt.
3. Run the following command:

```
opcagt -version
```

If the output of the command shows that the version is lower than A.8.53, you must upgrade to the version 8.53 or 8.60 first (or completely remove the installed version) before installing the HP Operations agent 11.11.

4. Check the version of the HP Performance Agent:
 - a. Open a command prompt.
 - b. Run the following command:

```
perfstat -v
```

The output of the command shows the versions of different components of the HP Performance Agent. If the version of the component **ovpa.exe** is listed as lower than C.04.70, you must upgrade to the version 4.70 or 5.00 first (or completely remove the installed version of the HP Performance Agent) before installing the HP Operations agent 11.11.

On UNIX/Linux

1. Log on to the node with the root privileges.
2. Open a command prompt.
3. Run the following command:

```
opcagt -version
```

If the output of the command shows that the version is lower than A.8.53, you must upgrade to the version 8.53 or 8.60 first (or completely remove the installed version) before installing the HP Operations agent 11.11.

4. Check the version of the HP Performance Agent:
 - a. Open a command prompt.
 - b. Run the following command:

```
perfstat -v
```

The output of the command shows the versions of different components of the HP Performance Agent. If the version of the component **ovpa** is listed as lower than C.04.70, you must upgrade to the version 4.70 or 5.00 first (or completely remove the installed version of the HP Performance Agent) before installing the HP Operations agent 11.11.

5. Check the version of HP GlancePlus:
 - a. Open a command prompt.
 - b. Run the following command:

```
perfstat -v
```

The output of the command shows the versions of different components of the HP Performance Agent and HP GlancePlus. If the version of the component **glance** is listed as lower than C.04.70, you must upgrade to the version 4.70 or 5.00 first (or completely remove the installed version of HP GlancePlus) before installing the HP Operations agent 11.11.

Data Collection and Storage with the HP Operations Agent 11.11

The older versions of the HP Operations agent (older than 11.00) stores the system performance data in the form of about 50 metrics in the embedded performance component (**EPC**), which is also known as **coda**. The HP Performance Agent collects more than 500 system performance metrics (with the help of the **scope** collector) and uses the log file-based storage mechanism to store the data. The version 11.11 of the HP Operations agent uses the data collection and storage mechanism of the HP Performance Agent, and therefore, collects a richer set of metrics and stores the metric data into the log file-based data store. However, any references to the EPC in external programs or HPOM policies are directed to the scope collector and the log file-based data store. This ensures that all previously deployed policies and integrations work without any interruptions after upgrading to the HP Operations agent 11.11 from an older version of the HP Operations agent (older than 11.00).

Check the Version of coda

If the available coda version on the system is between 10.50.215 and 10.50.245, it is recommended to take a backup of the coda data by using data analysis tools (like HP Reporter or HP Performance Insight). To check the version of coda, open the **coda.txt** file from the log directory (**%ovdatadir%log** on Windows; **/var/opt/OV/log** on UNIX/Linux), and then check the version of coda (next to the statement **Starting CODA**).

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

If you use a Solaris SPARC HPOM management server, and if the HP Operations agent 8.60—with the HP Software Security Core (HPOvSecCo) component, version 06.20.050—is installed on the management server, you must upgrade the agent on all the Solaris SPARC managed nodes in the environment to the version 11.11, and then upgrade the agent on the management server to the version 11.11. Otherwise, the communication between the agent on the Solaris SPARC node (with the agent 8.60) and the management server (with the agent 11.11) will fail until you upgrade the agent on the management server to the version 11.11.

In addition, you must apply the hotfix QCCR1A97520 on the management server before upgrading the agent on any of the SPARC managed nodes in the environment to the version 11.11.

If you use the SPARC HPOM management server with SPARC nodes, follow these steps:

1. Log on to the management server with the root privileges.
2. Run the following command to check the version of the HP Software Security Core (OvSecCo) component on the management server:

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


If the command output shows the version of HPOvSecCo as 06.20.050, apply the hotfix QCCR1A97520 on the management server (contact HP Support to obtain this hotfix). Otherwise, continue with upgrading.

This hotfix ensures that the SPARC nodes with the HP Operations agent 11.11 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 HP Operations agent 11.11 cannot communicate with the SPARC management server until you upgrade the agent on the management server to the version 11.11.

To verify if the version of the HPOvSecCo component on the management server is upgraded to 06.20.077, run the following command:

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

The command output shows the version of the HPOvSecCo component as 06.20.077 after installing the hotfix.

Preinstallation Task: To Install the HP Operations Agent on HPOM in Cluster

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

You must install the HP 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 with the administrative privileges.
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 HP Operations Agent Manually on the Node"](#).
5. Perform step 4 and 5 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 with the root privileges.
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 HP Operations Agent Manually on the Node](#)".

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

4. Perform step 2 and 3 on each node in the cluster.

Chapter 9

Installing from the HPOM Console

Note: Do not use this method of installation for vSphere Management Assistant (vMA) nodes (where the `root` user is disabled by default). Install the agent manually on vMA nodes.

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 HP Operations agent on managed nodes from the HPOM console, follow the *Remote agent installation* topic in the *HPOM 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"](#).

From HPOM on UNIX/Linux

To install the HP 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 HP 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 HP Operations agent twice.

Chapter 10

Installing HP Operations Agent Using HP Server Automation

HP Server Automation (SA) helps in automated application deployment. You can use HP Server Automation to deploy HP Operations agent. For more information on the prerequisites for installing HP Operations agent, see ["Prerequisites for Windows" \(on page 28\)](#). The target where you are installing HP Operations agent must always have SA agent installed on it.

To obtain platform specific packages from the HP Operations agent media, browse the media to the specific package location. For all platforms, you must obtain the `oainstall.vbs` or `oainstall.sh` package and the contents of the **scripts** folder. The following table lists the platform-specific packages to be obtained from the media

Operating System	Architecture	Packages
Windows	32-bit	packages/WIN/Windows_X86
	64-bit	packages/WIN/Windows_X64
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
HP-UX	HP-UX-IA32	packages/HP-UX/HP-UX_IA32
	HP-UX-PA32	packages/HP-UX/HP-UX_PA32
Solaris	Solaris_SPARC32	packages/SOL/Solaris_SPARC32
	Solaris_X86	packages/SOL/Solaris_X86
AIX	32-bit	packages/AIX/AIX_powerpc64

To install HP Operations agent using the SA console, perform the following tasks:

- ["Import the HP Operations Agent Software" \(on page 42\)](#)
- ["Create a Software Policy " \(on page 43\)](#)
- ["Attach the Software Policy to a Device or Server" \(on page 44\)](#)

Before starting the tasks to install HP 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*.

Import the HP Operations Agent Software

To import the HP Operations agent software, follow these steps:

1. Obtain the HP Operations agent media.

To extract the contents of the `.tar` file containing the HP Operations agent media, you can use the command `tar -xvf <filename>.tar` on the UNIX/Linux systems.

2. Browse to the **packages** folder and select the required Operating System.

For example, to obtain the AIX packages, browse to **packages > AIX**.

3. Extract the contents of the media.

4. Compress the extracted contents into a zip file.

You can use any available tool to create zip file.

5. Log on to the HP Server Automation Client console.

6. In the navigation pane, select **Library**.

7. Select the **By Folder** tab, and the required folder.

8. Click **Actions > Import Software**. The Import Software dialog box opens.

9. Browse and select the zip file that you created and select **ZIP Archive (.zip)** as the package type.

10. Browse and select the appropriate folder and platform.

11. Click **Import**.

12. Click **Close** when the import is successful. 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**. Click **Close** when the processes are successfully completed. To verify if the package is successfully installed, see ["Verifying the Installation" \(on page 45\)](#).

Create 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** and 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 and select it from the right pane.
9. Select the required package to attach the software policy.
10. Click **Select**. The package details appear in the Software Policy window.
11. Click  or double-click the package to edit the package details.
12. Provide the location on the system where the HP Operations agent package must unzip in the **Default Install Path** field.
13. Expand the **Install Scripts** section and provide the Pre-Install Script or Post-Install Script in the respective tabs, as required.

For Windows, the scripts must be in the BAT format and for UNIX/Linux, the scripts must be in the shell script format.

If you want to install agent but defer the configuration, in the Post-Install Script tab include the following command:

On Windows


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


On UNIX/Linux


```
./oainstall.sh -i -a -defer_configure
```
14. Expand the **Uninstall Scripts** section and provide the Pre-Uninstall Script or Post-Uninstall Script in the respective tabs, as required.

For example, if you want to uninstall HP Operations agent from the managed node, include the following command in the Post-Uninstall Script tab:


```
set BASE_PATH=C:\Windows_X64  
  
"%BASE_PATH%oasetup.exe -remove
```
15. In the left pane, click **Contents** to view the contents of the package.
16. Click **File > Save**. Close the window. The policy details appear on the contents pane.

Attach the Software Policy to a Device or Server

To attach a Software Policy, do one of the following:

- ["Attach from Software Policy list" \(on page 44\)](#)
- ["Attach from Devices list" \(on page 45\)](#)

Attach from 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.

Attach from 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.

Note: 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 HP 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 that the HP 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 HP Operations agent using SA console

To uninstall HP 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 HP Operations agent package to be uninstalled.
7. Click **Select** and then **Start Job**. The Job Status appears and uninstalls the HP Operations agent package.
8. Click **Close** after the job is completed.

Note: 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 HP Operations agent package after successful uninstallation.

Installing HP Operations Agent using Microsoft System Center 2012 Configuration Manager

Microsoft System Center 2012 Configuration Manager is a systems management software product. You can use Microsoft System Center 2012 Configuration Manager to install HP Operations agent on the required Windows nodes and servers. For more information on the prerequisites for installing HP Operations agent, see ["Prerequisites for Windows" \(on page 28\)](#).

You must add the node or server, where HP Operations agent must be installed, to the System Center 2012 Configuration Manager. 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 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 System Center 2012 Configuration Manager console, perform the following tasks:

- ["Create the HP Operations Agent Package" \(on page 47\)](#)
- ["Deploy the HP Operations Agent Package" \(on page 48\)](#)

Create the HP Operations Agent Package

To create an HP Operations agent deployment package, follow these steps:

1. Obtain the HP 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 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 HP 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 HP 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 initiate the installation on the node automatically with **oasetup.exe**, type `oasetup.exe -install` in the field.

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 as 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 specify any of the agent installation commands here and the appropriate action is performed during deployment.

17. Select and provide values in the following fields, as required.
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.

Deploy the HP Operations Agent Package

To deploy the HP Operations agent package on the required node or server, follow these steps:

1. Select the created HP Operations agent package.
2. Click **Deploy** (). The Deploy Software Wizard window opens.
3. Verify that the **Software** field contains the created 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 HP Operations agent.
6. Click **OK**.
7. Click **Next**.


8. Click **Add** and select **Distribution Point** or **Distribution Point Group**.

A window opens displaying the distribution points or the distribution point groups.

9. Select the required value and click **OK**.
10. Click **Next**.
11. Specify the required Deployment Settings in the following screens.
12. Click **Next** in the Summary screen. The window shows the progress of the deployment.
13. Click **Close** in the Completion screen after the wizard displays the message that the software is successfully deployed.

Verifying the Installation

To verify that HP Operations agent is successfully installed, follow these 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 created.
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 12

Installing HP Operations Agent Using Red Hat Network Satellite Server

You can use Red Hat Network Satellite server to deploy HP Operations agent on all the Linux nodes. For more information on the prerequisites for installing HP Operations agent, see ["Prerequisites for Windows" \(on page 28\)](#). The target node where you are installing HP Operations agent must always be added to communicate with Red Hat Network (RHN) Satellite server.

To obtain platform specific packages from the HP Operations agent media, browse the media to the specific package location. For all platforms, you must obtain the `oainstall.vbs` or `oainstall.sh` package and the contents of the **scripts** folder. 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 HP Operations agent using RHN Satellite server, perform the following tasks:

1. ["Collect and Store the Operations agent depot files \(RPMs\) in Software Delivery Repository " \(on page 50\)](#)
2. ["Create the Setup on the Target Node " \(on page 50\)](#)
3. ["Deploy the Packages on the Target Node" \(on page 51\)](#)

Collect and Store the Operations agent depot files (RPMs) in Software Delivery Repository

To download the HP Operations agent software, follow these steps:

1. Obtain the HP Operations agent media.

To extract the contents of the `.tar` file containing the HP Operations agent media, you can use the command `tar -xvf <filename>.tar` on the Linux systems.
2. Browse to the **packages** folder and select the required Operating System.

For example, to obtain the Linux packages, browse to **packages > Lin**.
3. Extract the contents of the media.
4. Collect and unzip all the depot files from media.
5. Upload the Operations agent RPMs to Software Delivery Repository location of the RHN Satellite server.

Create the Setup on the Target Node

To create the setup on the target node, follow these steps:

1. Add the node to RHN Satellite server. The node is known as target node.
2. On the target node, create a file and provide the location on the system where HP Operations agent package must create the **Default Agent File**.

For example, create a file `/etc/yum.repos.d/<Default Agent File>`.

Note: The agent depot files must be available in the **repos.d** location.

3. Update the contents of the file and specify the location where 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 agent package is available.

Deploy the Packages on the Target Node

1. Run the command to install the required RPMs: `# yum install <agent RPMs>`

For example, `# yum install HPOvOpsAgt`

Note: All the dependent agent RPMs will be 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
HPOvPerlA	x86_64
HPOvSecCC	x86_64
HPOvSecCo	x86_64
HPOvXpl	x86_64

After you complete installation, you can run the command to update the agent depot files (RPMs) from RHN Satellite server: `# yum update <agent RPMs>` The

For example, `# yum update HPOVopsAgt`

2. Run the command to verify that 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, the Operations agent RPMs are available on the node. Configure the management server by the following :

1. Go to the following directory on the linux node:
`/opt/OV/bin/OpC/install`
2. Run the command: `opcactivate -srv <management_server> -cert_srv <management_server> -f`

In this instance:

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

Chapter 13

Installing the HP Operations Agent Manually on the Node

Task 1: Prepare for Installation

Before installing the HP Operations agent, you must extract or mount the *HP Operations Agent and Infrastructure SPIs 11.11* 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 in the HPOM console.
2. Create a directory on the management server, and then go to the directory.
3. Run the following command:

```
ovpmutil dnl 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.

4. 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.11.11.000
```

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

Operating System	Architecture	Select this combination..
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

2. Transfer the contents of the `RPC_BBC` directory (available inside the `A.11.11.000` directory) into a temporary directory on the node.

Optional.Prepare the Profile File

About the 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). You must manually create the profile file with the instructions provided in this document.

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 an 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

- **Agent user:** At the time of installation, you can configure the user that the agent runs under. The `MODE` variable enables to choose a non-default user that can be used by the agent while running on the system.

To configure the agent to run under a non-root/non-privileged user, add the following content:

set `eaagt:MODE=NPU`

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):

set eaagt:MODE=MIXED

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 *Configure the Agent User During Installation* section in the *HP Operations Agent User Guide* for detailed information.

- **Licensing:** If you install the agent manually on a node (that is, without using the HPOM console), no evaluation licenses are enabled automatically after installation. 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.

For example, if you want to apply the HP Operations OS Inst Adv SW LTU permanently, add the following content:

set eaagt.license:HP_Operations_OS_Inst_Adv_SW_LTU=PERMANENT

For detailed information on applying licenses at the time of installation with a profile file, see the *HP Operations Agent License Guide*.

Task 2: Install the HP Operations Agent

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.

1. Log on to the node as root or administrator.
2. If you want to install from the *HP Operations Agent and Infrastructure SPIs 11.11* 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: `vcredist_x86.exe` and `vcredist2k5_x86.exe`

On Windows x64: `vcredist_x64.exe` and `vcredist2k5_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:

- i. **chmod u+x oasetup.sh**

ii. `./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 `oainstall` and `oasetup` programs provide you with an option to trace the installation process. If the installation of the agent fails and you are unable to detect the cause of failure, you can run the installer with the tracing option, which generates trace files. You can then send the generated trace files to HP Support for further analysis.

To trace the agent process during installation, run the above 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 HP 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 HP Operations agent, review the contents of the installation log file (`oainstall.log`). If the installation is successful, the file must be error-free and must display the following message near the end of the file:

```
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 14

Install Only the Infrastructure SPIs

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 ^a	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

^aThe 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 1.60 or above to the version 11.11.

Install the Infrastructure SPIs

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 *HP Operations Agent and Infrastructure SPIs 11.11* DVD into the DVD-ROM drive.
 - Download the installation media (.iso file) from one of HP's web sites.

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. Create a configuration file to specify installation details.
- The `oainstall` program installs the Infrastructure SPIs on the management server while registering the deployment package. This installation includes necessary report (for use with HP Reporter) and graph (for use with HP Performance Manager) packages for the Infrastructure SPIs. To skip the registration of the HP Operations agent packages, follow these steps:

- a. Create a new file with a text editor.
- b. Add the following content:

```
[agent.parameter]
REGISTER_AGENT=NO

[hpinfraspi.parameter]
InfraSPI=
InfraSPI_With_Graphs=
```

- c. *Only on Windows. Add the following line:*

```
InfraSPI_With_Reports=
```

Since HP Reporter is supported only on Windows, adding the above line in the configuration file on a UNIX/Linux system will have no effect.

- d. Under the `[hpinfraspi.parameter]` section:
 - 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.
 - 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: 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. 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, follow [this procedure](#).

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](#)).

- e. Save the file into a local directory.
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 HP Reporter and 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 *HP Operations Agent and Infrastructure SPIs 11.11* 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. Install the following file:

HPSpiInfR.msi

To install graph packages:

1. Log on to the HP Performance Manager server as administrator or root.
2. Place or mount the *HP Operations Agent and Infrastructure SPIs 11.11* 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

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 file must be error-free and must display the following message near the end of the file:

```
HPSpiSysI installation completed successfully
HPSpiVmI installation completed successfully
HPSpiClI installation completed successfully
```

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 HP Performance Manager. Use the same command with the same options even if HP Performance Manager is installed on the HPOM management server.

Components of the Infrastructure SPIs on HPOM for Windows

The following Infrastructure SPIs 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.

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 11.11, the node groups get added under the console tree **Nodes** folder.

Note: The node group names appear in English even in 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 installation time.

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 node 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 specialized purposes.

To view and access the Systems Infrastructure SPI policies, select **Policy management> Policy groups > Infrastructure Management > <language>> Systems Infrastructure**.

To view and access the VI SPI policies, select **Policy management→Policy groups → Infrastructure Management> <language>> Virtualization Infrastructure**.

To view and access the Cluster Infrastructure SPI policies, select **Policy management> Policy groups > Infrastructure Management> <language>> Cluster Infrastructure**.

Tools

Tools are provided for the SI SPI and VI 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 policies are 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 > <language> > Systems Infrastructure**.

To view and access the VI SPI policies, select **Policy Bank > Infrastructure Management > <language> > Virtualization Infrastructure**.

To view and access the CI SPI policies, select **Policy Bank > Infrastructure Management > <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 15

Installing the 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 HP Operations agent is installed in the inactive mode. Cloning a system with preinstalled HP Operations agent eliminates the requirement to install the agent on the system after adding the system to the list of managed nodes.

Install the HP 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 HP Operations agent:

1. Log on to the node as root or administrator.
2. If you want to install from the *HP Operations Agent and Infrastructure SPIs 11.11* 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 HP 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 HP 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 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 HP 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 management server, from the `%ovinstalldir%\contrib\OVOW\PuTTY` directory on the management server, 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 into `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:

- 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)
- 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\loasetup -configure -management_server <management_server> -certificate_server <certificate_server>" -node <node_name> -fem winservice -ostype Windows -user <node_user> -pw <node_passwd>
```

For other Windows nodes

```
ovdeploy -cmd "%ovinstalldir%\bin\OpC\install\loasetup -configure -management_server <management_server> -certificate_server <certificate_server>" -node <node_name> -fem winservice -ostype Windows -user <node_user> -pw <node_passwd>
```

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>
```

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>
```

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.

Chapter 16

HP Operations Agent in High Availability Clusters

You can use the HP 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.

You must install the HP Operations agent on every node 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 for UNIX 8.3x, HPOM on UNIX/Linux 9.1x, HPOM for Windows 8.1x (after patch OMW_00090), or HPOM for Windows 9.00, 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.

Note: The virtual node feature is not available with HPOM for Windows 8.1x (lower than patch OMW_00090).

To monitor nodes in an HA cluster, deploy monitoring policies only on the virtual node and not on every physical node. Therefore, it is important to create a virtual node for an HA cluster in the HPOM console before you start monitoring cluster-aware applications.

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, autodeployment, 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 HP 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.

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

```
<!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 ["HP Operations Agent in High Availability Clusters" \(on page 70\)](#).

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.

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`**

12. *Optional.* 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. Configure the agent to use the hostname as it is known in the cluster configuration:
13. Obtain the name of the physical node as it is known in the cluster configuration:

`ovclusterinfo -a`

14. 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 **`ovclusterinfo -a`** and is case-sensitive.

15. Restart the agent on every physical node by running the following commands:

`ovc -stop`

`ovc -start`

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 ["HP Operations Agent in High Availability Clusters" \(on page 70\)](#)) 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 ["HP Operations Agent in High Availability Clusters" \(on page 70\)](#)) on the virtual node created for the cluster.

Agent User

By default, the HP 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. Run the following command to stop the agent:

`ovc -kill`

2. 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*.

3. Run the following command to start the agent:

```
ovc -start
```


Chapter 17

Deploying the HP Operations Agent in a Secure Environment

The HP Operations agent and the HPOM 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 HP 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 following configuration options are possible in HPOM to accommodate these restrictions:
- If your network allows outbound connections from only certain local ports, you can configure HPOM 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 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).

Before You Begin

Skip this section if you are using the HP 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 these steps:

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 a 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:

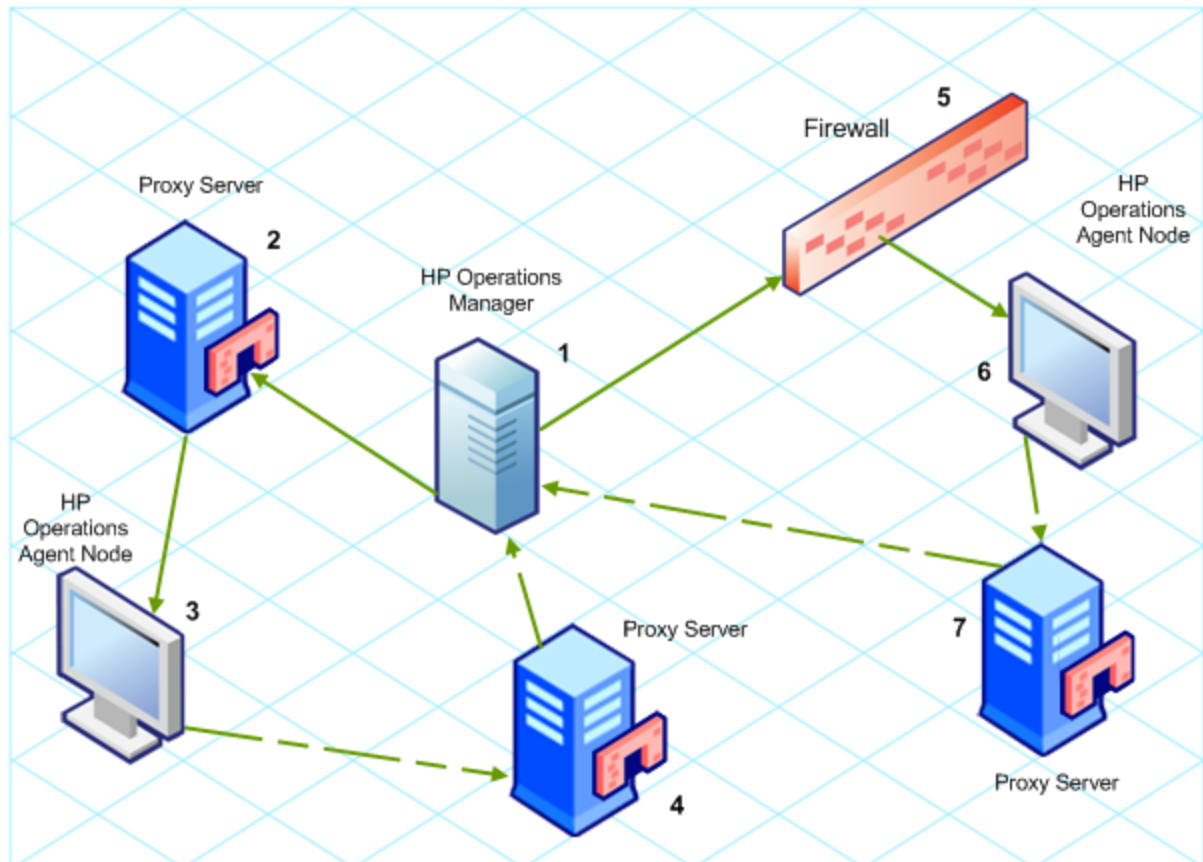
The management server (1) opens connections to a proxy (2). The proxy opens connections to the node (3) on behalf of the management server.

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 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 HP Operations agent installation defaults. For more information on the profile file, see ["Prepare the 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 HP 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
```

Organization of 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-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><proxies> <proxy> <server> server1.domain.example.com:8080 </server> <for> <target>*.domain2.example.com</target> </for> </proxy> </proxies></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>
<pre><proxies> <proxy> <server> server2.domain.example.com:8080 </server> <for> <target>*.domain2.example.com</target> <target>192.168.2.*</target> </for> </proxy> </proxies></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.com.</p>

Syntax	Description
<pre> <server> server3.domain.example.com:8080 </server> <for> <target>192.168.3.*</target> </for> <except> <target>192.168.3.10-20</target> </except> </proxy> </proxies> </pre>	

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 in 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\bbs

On UNIX/Linux

/var/opt/OV/conf/bbs

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

Configuring the Communication Broker Port

By default, the HP Operations agent nodes use the port 383 for inbound communication. The Communication Broker component facilitates the inbound communication on every HP 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 HP 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 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

Example

You must configure the HPOM 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 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 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 servers and HP

Operations agent nodes in your environment to use the same port.

1. Log on to the HP 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 HP 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.

The communication broker is configured as follows:

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 host1:483[,host2:683]
```

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 HP Operations agent installation defaults. For more information on the profile file, see ["Prepare the 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 HP 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 <lower port number>-<higher port number>
```

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.

To communicate with HP Reporter or HP Performance Manager, the communication daemon (CODA) accepts incoming connections on all IP addresses.

To configure the HP Operations agent to use a specific IP address:

1. Log on to the HP 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>
```

Configuring HTTPS Communication Through Proxies

If your network allows only certain proxy systems to open connections through the firewall, you can redirect HPOM 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.

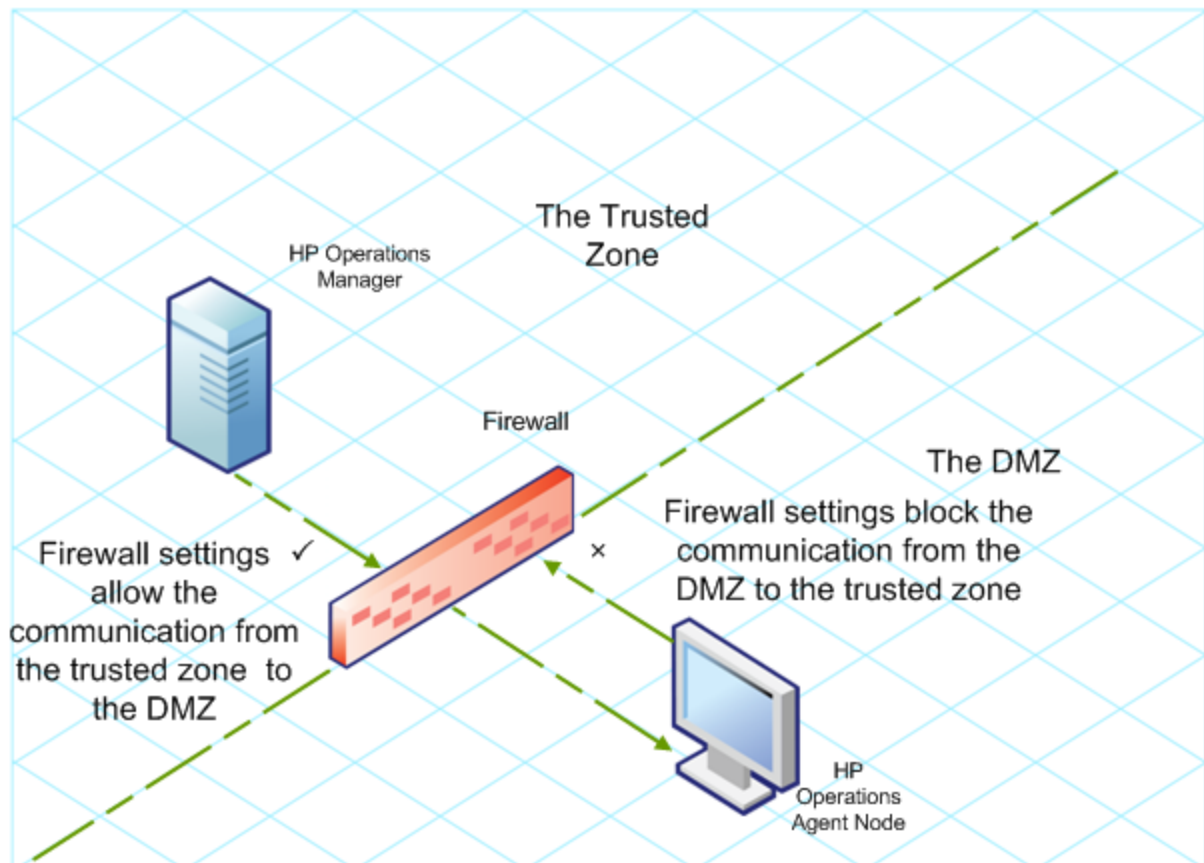
Communication in a Highly Secure Environment

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 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.

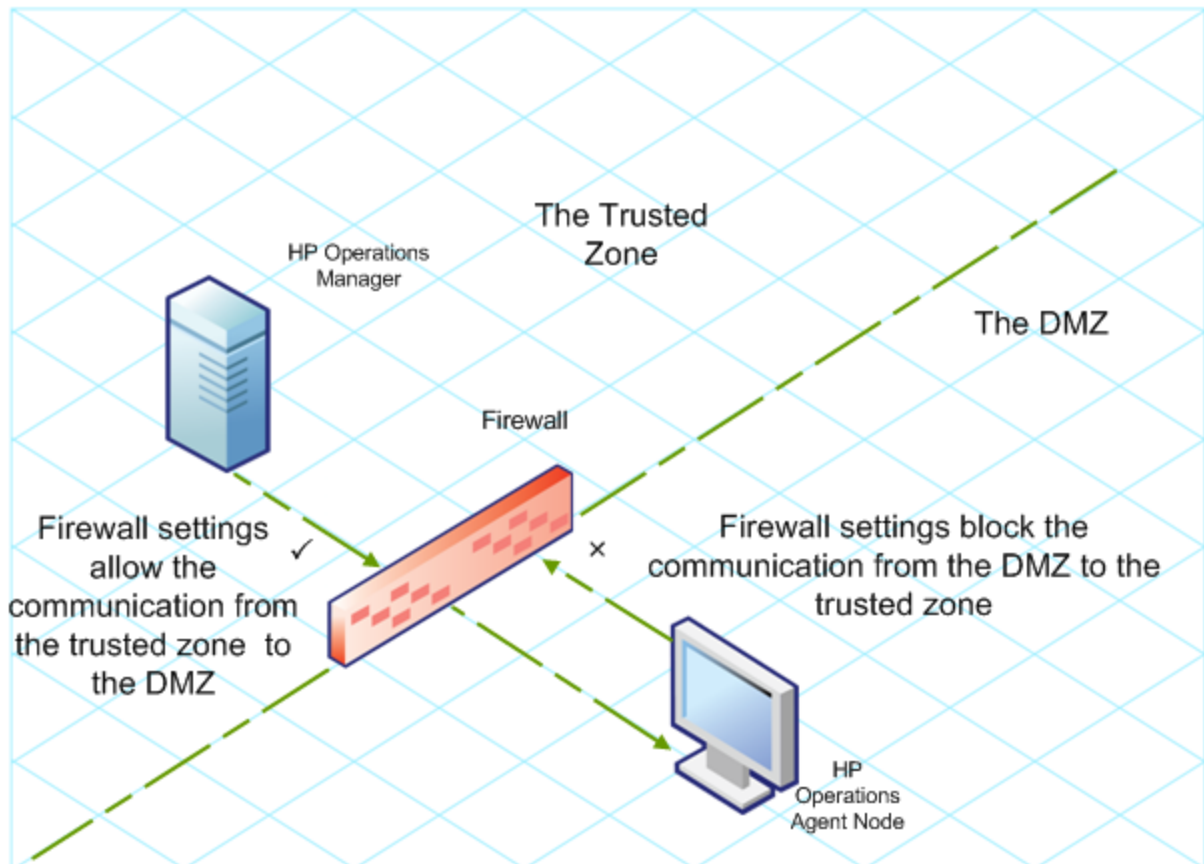
In the following scenario, managed nodes are located in the DMZ while the management server belongs to the trusted zone. The firewall settings in this example allow outbound-only communication. Therefore, inbound communication to the management server is blocked by the firewall.

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 management server, but block the inbound communication to node.

HPOM Management Server in the DMZ



Introduction to the Reverse Channel Proxy

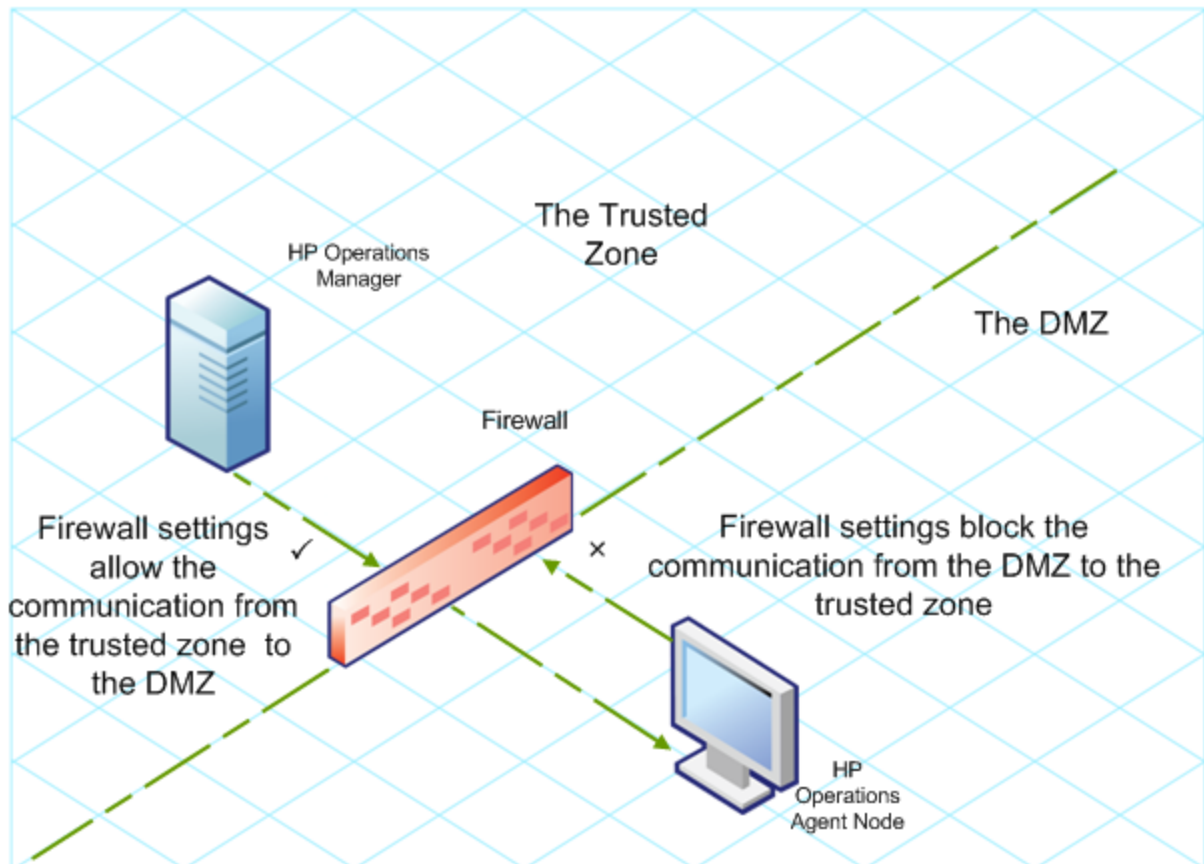
One simple solution to enable bidirectional communication is to configure the firewall settings to allow inbound traffic to the port 383 (the Communication Broker port). However, this can make your system vulnerable to external attacks. To enable secure communication without allowing inbound traffic to the Communication Broker port, you must configure a reverse channel proxy (**RCP**).

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 use 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 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 management server through the reverse administration channel.

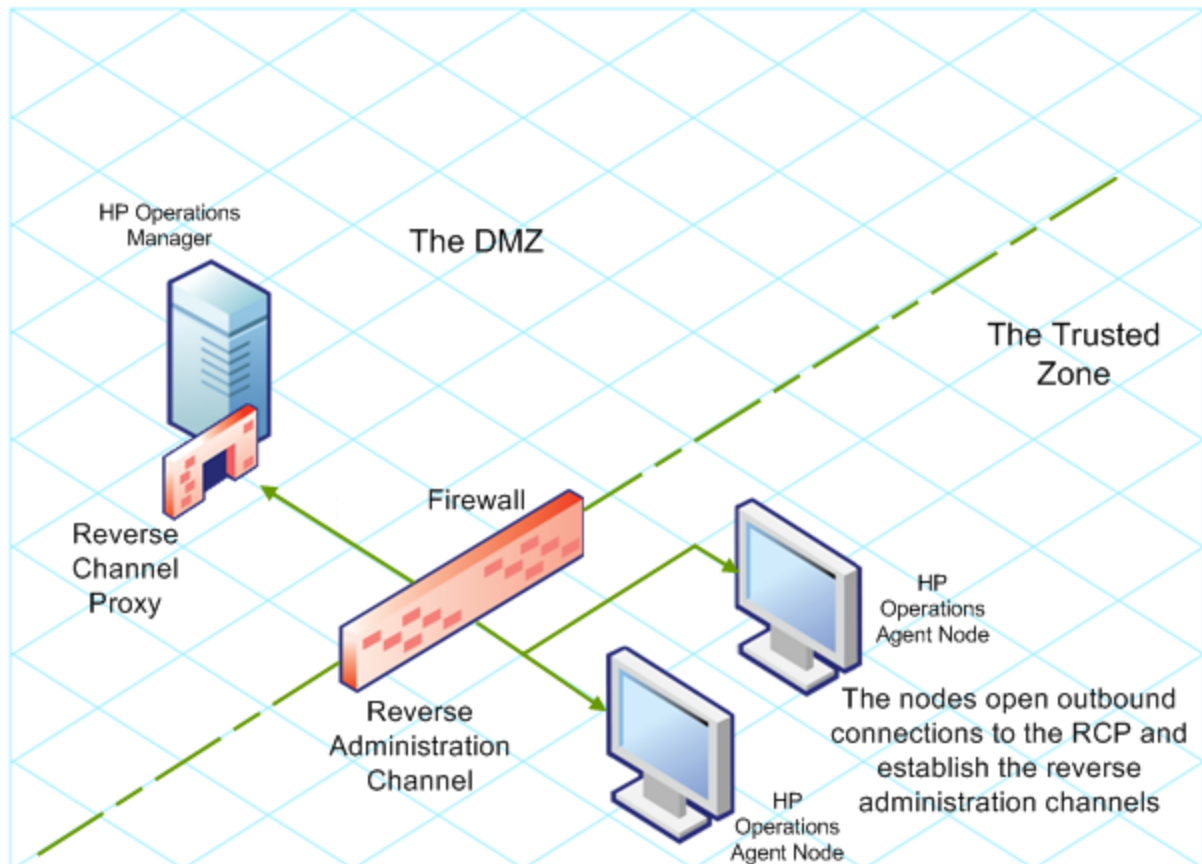
Secure Communication Through the RCP with Nodes in the DMZ



When the nodes are located in the trusted zone and the management server in the DMZ, the HPOM 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



Configure 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. You must do as follows to resolve this problem:

- 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

Configure 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 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 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>
```

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.

Specify 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.

Configure an 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 HP 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.

Verify 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:

Verify 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; ovbbcrp 11.00.000
```

```
system2.mydomain.com:1025 BBC 11.00.000; ovbbcrp 11.00.000
```

```
system3.mydomain.com:1025 BBC 11.00.000; ovbbcrp 11.00.000
```

```
system4.mydomain.com:1025 BBC 11.00.000; ovbbcrp 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:

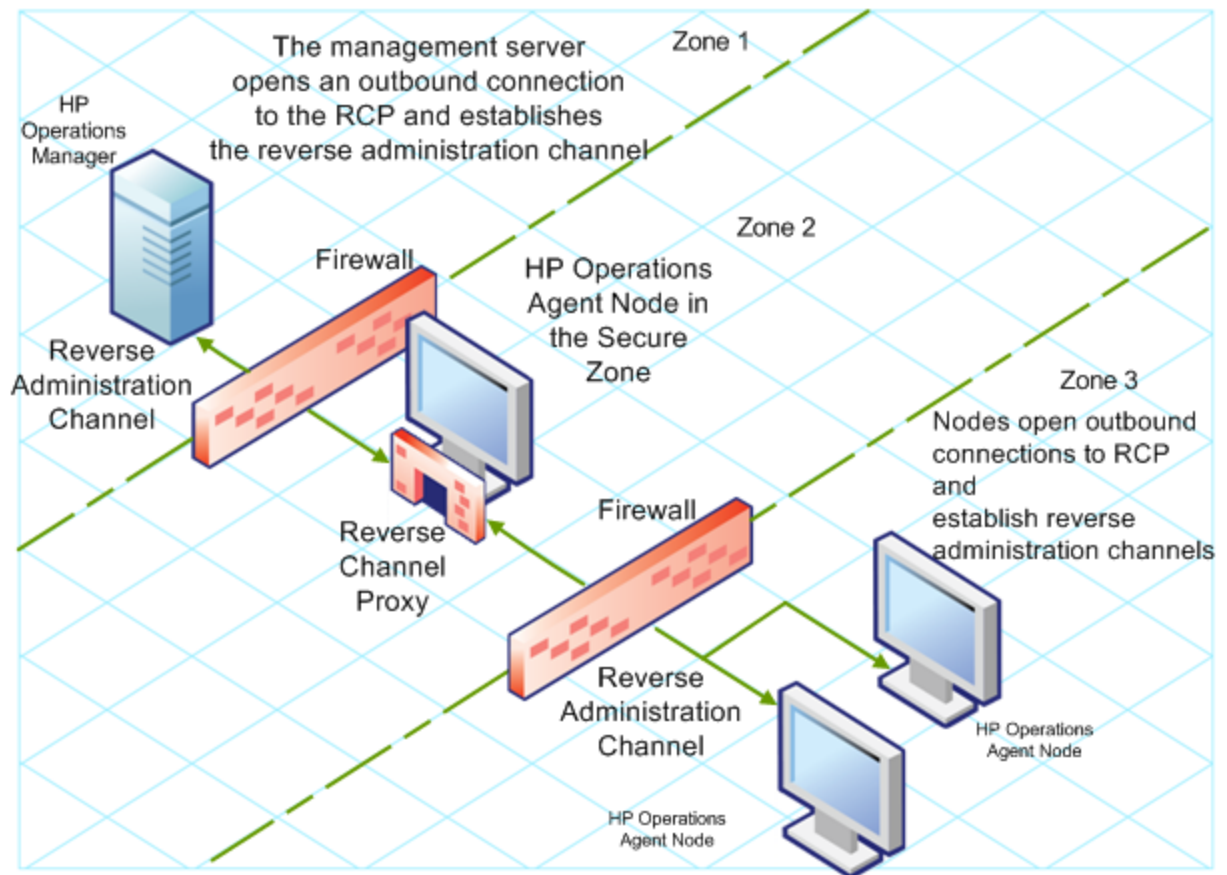
```
Pending:
```

```
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.

Chapter 18

Configuring the Performance Collection Component Remotely

You can perform certain configuration tasks on the managed node remotely from the management server. Instead of performing the configuration tasks for the Performance Collection Component locally on every node, you can use a special set of policies and tools from the HPOM console to configure and work with the Performance Collection Component multiple nodes.

This feature is available only if you install the HP Operations agent deployment package on the HPOM for Windows or HPOM on UNIX/Linux management servers. This feature is not available on the HPOM for UNIX 8.x management server.

Before You Begin

Before you begin configuring and controlling the Performance Collection Component remotely from the HPOM console, you must deploy the instrumentation files in the HP Operations Agent instrumentation group on the nodes where the agent is running.

To deploy the instrumentation from the HPOM for Windows console, follow these steps:

Note: If you monitor cluster nodes, make sure you deploy the instrumentation on all the nodes that constitute the cluster and not on the virtual node

1. In the console tree, right-click the node or the node group (where the agent is running), and then click **All Tasks > Deploy Instrumentation**. The Deploy Instrumentation dialog box opens.
2. In the Deploy Instrumentation dialog box, click **HP Operations Agent**, and then click **OK**. The deployment of the necessary instrumentation files begins on the nodes.

To deploy the instrumentation from HPOM on UNIX/Linux Console, follow these steps:

Note: If you monitor cluster nodes, make sure you deploy the instrumentation on all the nodes that constitute the cluster and not on the virtual node

1. Log on to the Administration UI.
2. Click **Deployment > Deploy Configuration**.
3. In the Distribution Parameters section, select Instrumentation, and then click **Please Select**. The Selector pop-up box opens.
4. In the Selector pop-up box, select the nodes where the agent program is running.
5. Select the Force Update option to overwrite the old instrumentation files.
Select this option on a node that was upgraded from an older version of the agent.
6. Click **Distribute**.

Deploy the OA-PerfCollComp-opcmsg Policy

The OA-PerfCollComp-opcmsg policy sends the alert messages to the HPOM message browser when the Performance Collection Component generates alarms. The policy is located in the **HP Operations Agent > Performance Collection Component > Message Interceptor** policy group. Before deploying other policies for the Performance Collection Component, deploy this policy on the nodes.

Note: If you monitor cluster nodes, make sure you deploy the policy on all the nodes that constitute the cluster and not on the virtual node.

Configuring the Performance Collection Component

The behavior of the Performance Collection Component of the HP Operations agent depends on the configuration settings specified in the following files:

- Collection parameter file (**parm**)
- Alarm definition file (**alarmdef**)

See the *Performance Collection Component* section in the *HP Operations Agent Concepts Guide* for more information on the collection parameter and alarm definition files.

Configure the parm File

The **parm** file defines the data collection mechanism of the scope collector. The HP Operations agent deploys a **parm** file on every node, which is available in the following path:

On HP-UX, Solaris, AIX, and Linux: **/var/opt/perf**

On Windows: **%ovdatadir%**

You can modify the settings specified in the **parm** file to customize the data collection mechanism. However, if you manage a large number of nodes with the HP Operations agent, it becomes difficult to modify every single copy of the **parm** file on every node.

With the help of the HPOM console, you can deploy the modified **parm** file on multiple node centrally from the management server.

From HPOM for Windows

The HPOM for Windows console provides you with ConfigFile policies which help you deploy any changes to the **parm** file across multiple nodes from the central management server. Different ConfigFile policies are available for different node operating systems.

To modify the collection mechanism by editing the **parm** file, follow these steps:

1. Identify the nodes where you want the modified collection mechanism to take effect.
2. In the console tree, click **Policy management > Policy groups > HP Operations Agent > Performance Collection Component > Collection configuration**. ConfigFile policies for configuring the **parm** file appear in the details pane.

3. Double-click the ConfigFile policy for the platform on which you want the modified collection mechanism to take effect (for example: **parm** file for HP-UX). The **parm** file for *<platform>* dialog box opens.
4. In the Data tab, modify the settings. See the *parm File Parameters* section in the *HP Operations Agent User Guide* for more details on configuration parameters in the **parm** file.
5. Click **Save and Close**. In the details pane, the version of the policy gets increased by .1.
6. Deploy the updated policy on the nodes of your choice.

Note: If you monitor cluster nodes, make sure you deploy the policy on all the nodes that constitute the cluster and not on the virtual node


From HPOM on UNIX/Linux 9.10

The HPOM on UNIX/Linux 9.10 console provides you with ConfigFile policies which help you deploy any changes to the **parm** file across multiple nodes from the central management server. Different ConfigFile policies are available for different node operating systems.

To modify the collection mechanism by editing the **parm** file from the HPOM for UNIX 9.10 console, follow these steps:

1. Identify the nodes where you want the modified collection mechanism to take effect.
2. In the console, click **Browse > All Policy Groups**. The list of all available policy groups appears on the page.
3. Click **H**. The HP Operations Agent policy group appears.
4. Click **HP Operations Agent**, click **Performance Collection Component**, and then click **Collection Configuration**. The list of available ConfigFile policies for the **parm** file appears.
5. Click the ConfigFile policy for the platform on which you want the modified collection mechanism to take effect. The Policy “OA_<platform>ParmPolicy” page appears.



6. Click  , and then click **Edit (Raw Mode)**. The Edit Config File policy... page appears.
7. In the Content tab, modify the settings

See the *parm File Parameters* section in the *HP Operations Agent User Guide* for more details on configuration parameters in the **parm** file.

8. Click **Save**.
9. Deploy the updated policy on the nodes of your choice.

Note: If you monitor cluster nodes, make sure you deploy the policy on all the nodes that constitute the cluster and not on the virtual node

Configure the alarmdef File

The alarm definition file (**alarmdef**) provides the performance subagent with the default specification for the alarm generation process. The HP Operations agent deploys an **alarmdef** file on every node, which is available in the following path:

On HP-UX, Solaris, AIX, and Linux: `/var/opt/perf/`

On Windows: `%ovdatadir%`

You can modify the default settings in the **alarmdef** file to customize the alarm generation mechanism. You can use the HPOM console to centrally distribute the modified **alarmdef** file on multiple nodes.

From HPOM for Windows

The HPOM for Windows console provides you with ConfigFile policies which help you deploy any changes to the **alarmdef** file across multiple nodes from the central management server. Different ConfigFile policies are available for different node operating systems.

To modify the collection mechanism by editing the **alarmdef** file, follow these steps:

Identify the nodes where you want the modified collection mechanism to take effect.

1. In the console tree, click **Policy management > Policy groups > HP Operations Agent > Performance Collection Component > Alarm definition**. ConfigFile policies for configuring the **alarmdef** file appear in the details pane.
2. Double-click the ConfigFile policy for the platform on which you want the modified collection mechanism to take effect (for example: Alarmdef file for HP-UX). The Alarmdef file for `<platform>` dialog box opens.
3. In the Data tab, modify the settings. See the *alarmdef File Parameters* section in the *HP Operations Agent User Guide* for more details on configuration parameters in the **alarmdef** file.
4. Click **Save and Close**. In the details pane, the version of the policy gets increased by .1.
5. Deploy the updated policy on the nodes of your choice.


Note: If you monitor cluster nodes, make sure you deploy the policy on all the nodes that constitute the cluster and not on the virtual node

From HPOM on UNIX/Linux 9.10

The HPOM on UNIX/Linux 9.10 console provides you with ConfigFile policies which help you deploy any changes to the **alarmdef** file across multiple nodes from the central management server. Different ConfigFile policies are available for different node operating systems.

To modify the collection mechanism by editing the **alarmdef** file from the HPOM for UNIX 9.10 console, follow these steps:

1. Identify the nodes where you want the modified alert mechanism to take effect.
2. In the console, click **Browse > All Policy Groups**. The list of all available policy groups appears on the page.
3. Click **H**. The HP Operations Agent policy group appears.
4. Click **HP Operations Agent**, click **Performance Collection Component**, and then click **Alarm Definition**. The list of available ConfigFile policies for the **alarmdef** file appears.
5. Click the ConfigFile policy for the platform on which you want the modified collection mechanism to take effect. The Policy "OA_<platform>AlarmdefPolicy" page appears.

6. Click  , and then click **Edit (Raw Mode)**. The Edit Config File policy... page appears.
7. In the Content tab, modify the settings. See the *alarmdef File Parameters* section in the *HP Operations Agent User Guide* for more details on configuration parameters in the **alarmdef** file.
8. Click **Save**.
9. Deploy the updated policy on the nodes of your choice.

Note: If you monitor cluster nodes, make sure you deploy the policy on all the nodes that constitute the cluster and not on the virtual node

Remotely Working with the HP Operations agent

You can use the HPOM console to start, stop, monitor, and view the details of the HP Operations agent. From the HPOM console, you can use different tools to manage the operation of the HP Operations agent. You must launch these tools on the nodes where the agent is deployed. The result of running a tool is displayed in the following section:

HPOM for Windows

Tool Output section in the Tool Status window

HPOM on UNIX/Linux

In the Application Output window in the Java GUI (HPOM for UNIX Operational UI)

You can use the following tools from the HPOM console:

Start Agent	Enables you to start the HP Operations agent on the managed node.
Stop Agent	Enables you to stop the HP Operations agent on the managed node.
Restart Agent	Enables you to restart the HP Operations agent on the managed node.
View Status	Enables you to view the status of the HP Operations agent process, services, and daemons on the managed node.
View Version Information	Enables you to view the version of the HP Operations agent on the managed node.
Refresh Alarm Service	Refreshes the Alarm service of the Performance Collection Component.
Scan Performance Component's Log Files	Scans the log files used by the scope collector on the node.
Check Performance Component's Parameter File Syntax	Helps you check the syntax of the parameter file in the managed node.
Check Performance	Helps you check the syntax of the alarmdef file in the managed node.

Component's Alarmdef File Syntax	
View status of post policy deploy action	<p>Helps you check the status of deployment of the parm or alarmdef policies on nodes. While launching this tool, make sure to specify either parm or alarmdef (as appropriate) as the tool parameter.</p> <p>You can set the tool parameter in the Parameter box in the Edit Parameters window when you use HPOM for Windows.</p> <p>When you use HPOM on UNIX/Linux, open the Edit Tool Status page for the tool, go to the OVO Tool tab, and then specify the tool parameter in the Parameters box</p>
Set Realtime Permanent License	Sets the permanent license for the HP Ops OS Inst to Realtime Inst LTU.
Set Glance Permanent License	Sets the permanent license for the Glance Software LTU.
Get License Status	Shows the status of LTUs on the node.

Chapter 19

Monitoring the HP Operations Agent

The HP Operations agent deployment package provides you with a set of policies to monitor the health of the HP Operations agent. With the help of these policies, you can make sure that necessary agent processes are not stopped.

When you install the HP Operations agent deployment package on the HPOM management server, the Self Monitoring policy group is created. The Self Monitoring policy group includes the policies that you need to ensure a smooth functioning of the HP Operations agent.

Note: The Self Monitoring policy group and the policies to monitor the health of HP Operations agent processes are available only if you install the HP Operations agent deployment package on the HPOM for Windows or HPOM on UNIX/Linux management servers. These policies are not available on the HPOM for UNIX 8.x management server.

Before You Begin

Before you begin monitoring the HP Operations agent with the Self Monitoring policies, you must deploy the instrumentation files in the HP Operations Agent instrumentation group on the nodes where the agent is running.

To deploy the instrumentation from the HPOM for Windows Console, follow these steps:

Note: If you monitor cluster nodes, make sure you deploy the instrumentation on all the nodes that constitute the cluster and not on the virtual node.

1. In the console tree, right-click the node or the node group (where the agent is running), and then click **All Tasks > Deploy Instrumentation**. The Deploy Instrumentation dialog box opens.
2. In the Deploy Instrumentation dialog box, click **HP Operations Agent**, and then click **OK**. The deployment of the necessary instrumentation files begins on the nodes.

To deploy the instrumentation on HPOM on UNIX/Linux:

Note: If you monitor cluster nodes, make sure you deploy the instrumentation on all the nodes that constitute the cluster and not on the virtual node.

1. Log on to the Administration UI.
2. Click **Deployment > Deploy Configuration**.
3. In the Distribution Parameters section, select Instrumentation, and then click **Please Select**. The Selector pop-up box opens.
4. In the Selector pop-up box, select the nodes where the agent program is running.

5. Select the Force Update option to overwrite the old instrumentation files (Select this option on a node that was upgraded from an older version of the agent.).
6. Click **Distribute**.

Self Monitoring Policies

You can monitor the health of the following components of the HP Operations agent by using the Self Monitoring policies:

- **opcmoma** (monitor agent)
- **opcmsga** (message agent)
- **opcmsgi** (message interceptor)
- **opcacta** (action agent)
- **scope** (data collector)
- **opcle** (logfile encapsulator)
- **opctrapi** (trap interceptor)
- **coda** (communication daemon)
- **perfd**

The Self Monitoring policy group includes the following policies:

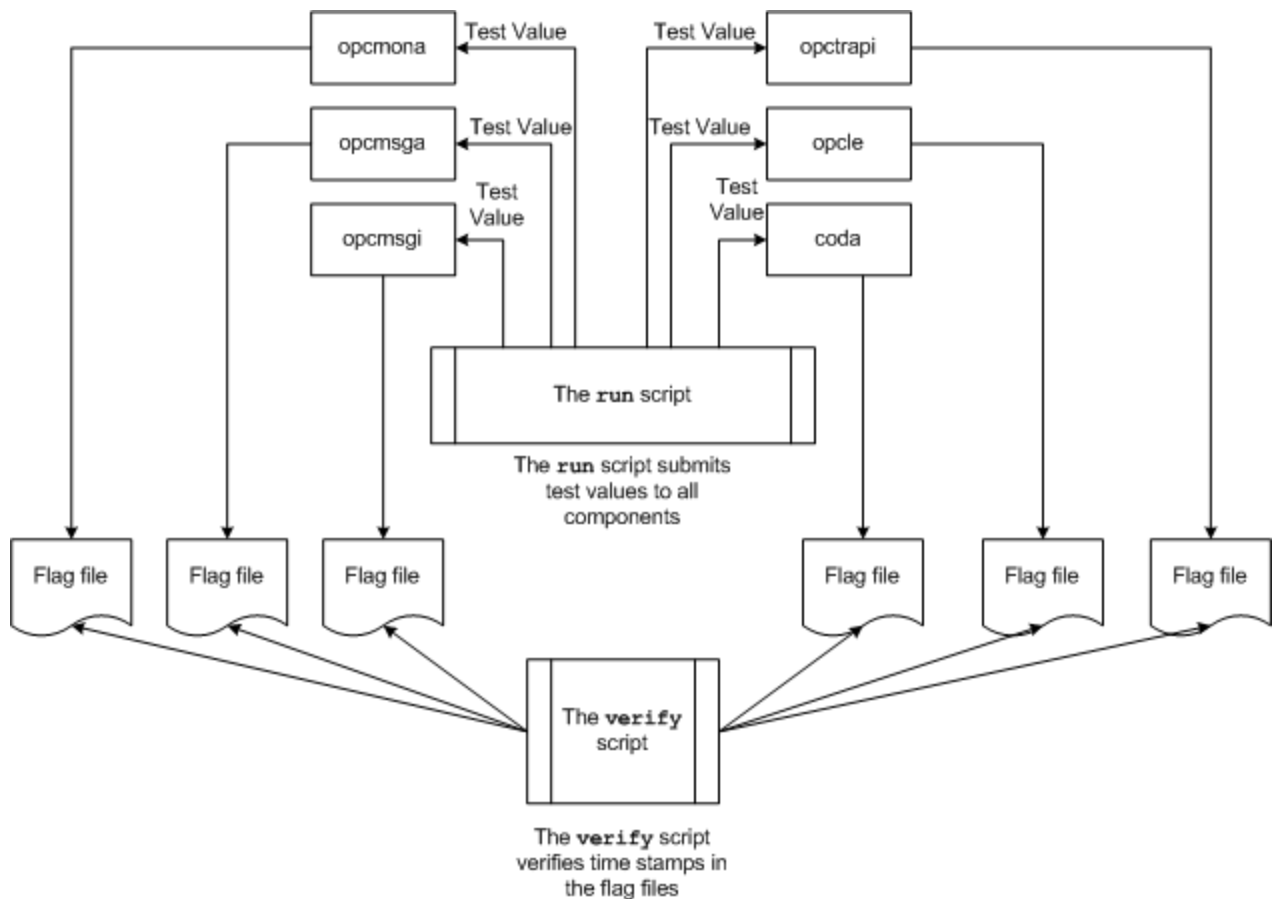
- **OA-SelfMonTstMonaExt**: Tests the monitor agent.
- **OA-SelfMonVerifyMon**: Verifies flag files by the monitor agent
- **OA-SelfMonTstLe**: Tests the logfile encapsulator
- **OA-SelfMonVerifyLe**: Verifies flag files by the logfile encapsulator
- **OA-SelfMonTstTrapi**: Tests the SNMP trap interceptor
- **OA-SelfMonTstMsgi**: Tests the message interceptor
- **OA-SelfMonTstActa**: Tests the action agent
- **OA-SelfMonTstAll**: Tests all the processes other than opcle, opcmoma, opcmsgi, and opctrapi.

To monitor the health and availability of the opctrapi component, the SNMP Trap daemon/service must be running on the node.

The scripts and programs deployed with the HP Operations Agent instrumentation group send test values (once every minute) to different components of the HP Operations agent. Also, the **flag files** are created for every monitored component. When a monitored component successfully receives the test value originating from the HP Operations Agent instrumentation scripts, the corresponding flag file is updated with the time stamp.

The verify script of the HP Operations Agent instrumentation constantly (once in **three minutes**) monitors the states of the flag files. When the script finds that the time stamp in the flag file is older than the current time, which means the monitored component failed to receive the test value, an alert message is sent to the HPOM message browser.

Workflow of the Self Monitoring Scripts



Deploying the Self Monitoring Policies

You cannot selectively deploy the policies available in the Self Monitoring policy group. These policies are dependent on one another, and therefore, all the policies must be deployed at the same time on the node.


To deploy the Self Monitoring policies from the HPOM for Windows console, follow these steps:

1. In the console tree of the HPOM console, expand **Policy management > Policy groups > HP Operations Agent**.
2. Right-click **Self Monitoring**, and then click **All Tasks > Deploy on**. The Deploy Policies on dialog box opens.
3. In the Deploy Policies on dialog box, select the nodes, and then click **OK**. HPOM starts deploying the Self Monitoring policies on the selected nodes.

Note: If you monitor cluster nodes, make sure you deploy the policies on all the nodes that constitute the cluster and not on the virtual node.

To deploy the Self Monitoring policies from the HPOM on UNIX/Linux console, follow these steps:

1. Log on to the Administration UI.
2. Click **OMU**, and then click **Browse > All Policy Groups**. The All Policy Groups page opens.

3. On the All Policy Groups page, select **HP Operations Agent** policy group, select **Assign to Node/ Group** from the Choose an Action drop-down list, and then click  . The Selector pop-up box opens.
4. In the Selector pop-up box, select the nodes where the agent program is running, and then click **OK**.

Note: If you monitor cluster nodes, make sure you deploy the policy on all the nodes that constitute the cluster and not on the virtual node

Viewing the Status of the Components

The Self Monitoring policies trigger the agent to send appropriate alert messages to the HPOM message browser when they detect failure in one of the components. The messages that originate from the Self Monitoring policies always have the prefix Self Monitor. You can open the messages with the Self Monitor prefix to view the details of failures.

Alternatively, you can check the flag files on the node to check if the agent components are operative. The flag files are available in the following locations:

On Windows: %ovdatadir%\tmp\OpC\selfmon

On UNIX/Linux: /var/opt/OV/tmp/selfmon

You can open the flag files with a text editor program and check the last time stamp. If the last time stamp is older than three minutes, you can conclude that the monitored component is not functioning.

Chapter 20

Configuring Certificates for the HP Operations Agent

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 the HPOM-managed environment by using certificates, you must install certificates after you install the agent on the nodes.

Request Certificates Automatically

When you deploy the agent to a node from the HPOM console, 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.

Request 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 HP 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 ["Prepare the Profile File"](#).

To request certificates with an installation key:

1. Log on to the management server with an account that belongs to the HPOM administrators group.
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 or HPOM on UNIX/Linux

```
opccsacm -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
```

Deploy 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 with an account that belongs to the HPOM administrators group.
2. Open a command prompt (shell).
3. Make sure the node is added to the list of managed nodes in the HPOM console.
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*.

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 or HPOM on 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.

<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 or HPOM on 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 "[Prepare the 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).

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
```

Restore 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>]
```

4. The command backs up the management server certificate in the file specified with the -file option.
5. 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.

6. 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 | +-----+
-----+
```

7. 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 management server certificate, run the following command:

ovcm -importcacert -file <file_name> [-pass <password>]

To restore the trusted certificate, run the following command:

ovcert -importtrusted -file <file_name>

To restore the node certificate, run the following command:

ovcert -importcert -file <file_name> [-pass <password>]

HP Operations Agent in High Availability Clusters

You can use the HP 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.

You must install the HP Operations agent on every node 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 for UNIX 8.3x, HPOM on UNIX/Linux 9.1x, HPOM for Windows 8.1x (after patch OMW_00090), or HPOM for Windows 9.00, 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.

Note: The virtual node feature is not available with HPOM for Windows 8.1x (lower than patch OMW_00090).

To monitor nodes in an HA cluster, deploy monitoring policies only on the virtual node and not on every physical node. Therefore, it is important to create a virtual node for an HA cluster in the HPOM console before you start monitoring cluster-aware applications.

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, autodeployment, 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 HP 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.

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

```
<!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 ["HP Operations Agent in High Availability Clusters" \(on page 112\)](#).
8. Use the following format while creating the **<appl_name>.apm.xml** file:

```
<?xml version="1.0" ?>

<APMAApplicationConfiguration>

  <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>

</APMAApplicationConfiguration>
```

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.

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"?>

<APMApplicationConfiguration>

  <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>

</APMApplicationConfiguration>
```

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`

12. *Optional.* 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. Configure the agent to use the hostname as it is known in the cluster configuration:
13. Obtain the name of the physical node as it is known in the cluster configuration:

ovclusterinfo -a

14. 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 **ovclusterinfo -a** and is case-sensitive.

15. Restart the agent on every physical node by running the following commands:

ovc -stop

ovc -start

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 ["HP Operations Agent in High Availability Clusters" \(on page 112\)](#)) 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 ["HP Operations Agent in High Availability Clusters" \(on page 112\)](#)) on the virtual node created for the cluster.

Agent User

By default, the HP 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. Run the following command to stop the agent:

ovc -kill

2. 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`.

3. Run the following command to start the agent:


```
ovc -start
```

Deploying the HP Operations Agent in a Secure Environment

The HP Operations agent and the HPOM 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 HP 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 following configuration options are possible in HPOM to accommodate these restrictions:
- If your network allows outbound connections from only certain local ports, you can configure HPOM 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 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).

Before You Begin

Skip this section if you are using the HP 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 these steps:

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 a 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:

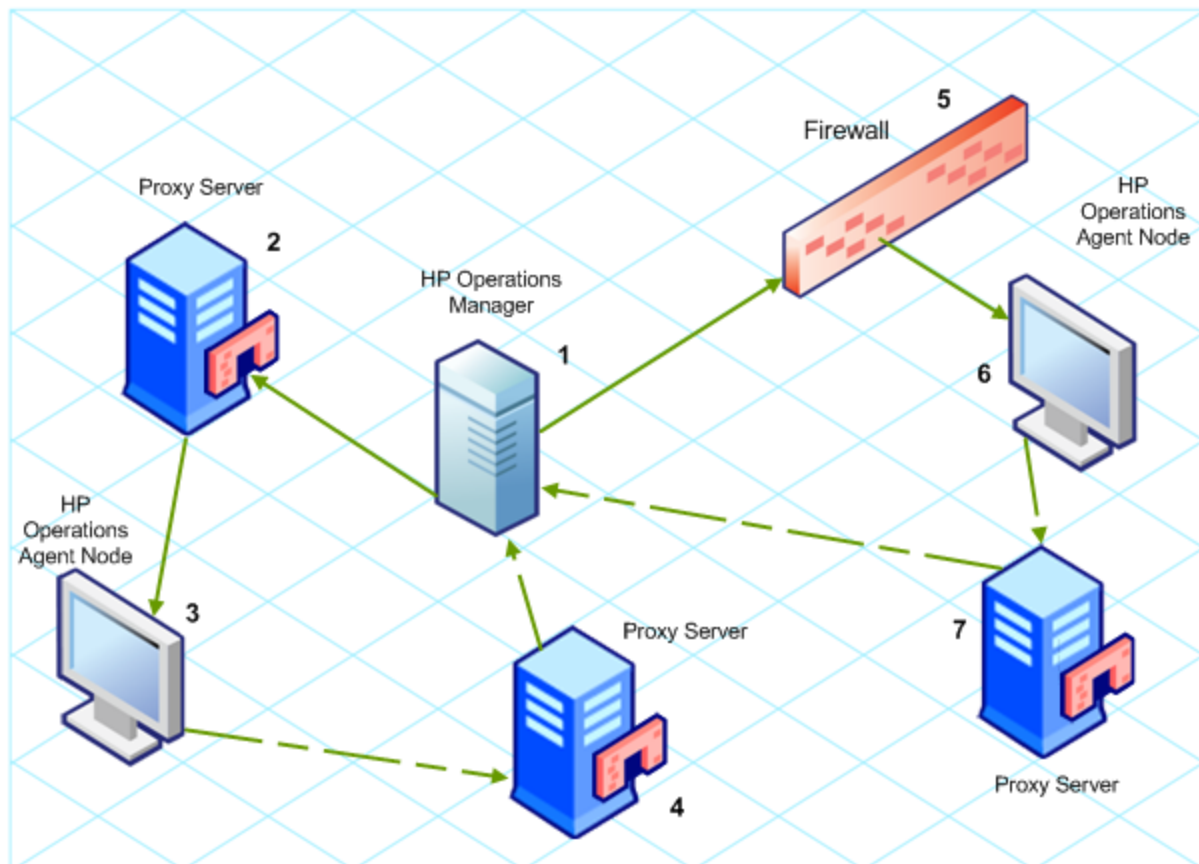
The management server (1) opens connections to a proxy (2). The proxy opens connections to the node (3) on behalf of the management server.

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 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 HP Operations agent installation defaults. For more information on the profile file, see ["Prepare the 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 HP 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
```

Organization of 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-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><proxies> <proxy> <server> server1.domain.example.com:8080 </server> <for> <target>*.domain2.example.com</target> </for> </proxy> </proxies></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>
<pre><proxies> <proxy> <server> server2.domain.example.com:8080 </server> <for> <target>*.domain2.example.com</target> <target>192.168.2.*</target> </for> </proxy> </proxies></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.com.</p>

Syntax	Description
<pre> <server> server3.domain.example.com:8080 </server> <for> <target>192.168.3.*</target> </for> <except> <target>192.168.3.10-20</target> </except> </proxy> </proxies> </pre>	

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 in 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\bbs

On UNIX/Linux

/var/opt/OV/conf/bbs

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

Configuring the Communication Broker Port

By default, the HP Operations agent nodes use the port 383 for inbound communication. The Communication Broker component facilitates the inbound communication on every HP 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 HP 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 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

Example

You must configure the HPOM 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 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 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 servers and HP

Operations agent nodes in your environment to use the same port.

1. Log on to the HP 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 HP 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.

The communication broker is configured as follows:

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 host1:483[,host2:683]
```

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 HP Operations agent installation defaults. For more information on the profile file, see ["Prepare the 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 HP 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 <lower port number>-<higher port number>
```

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.

To communicate with HP Reporter or HP Performance Manager, the communication daemon (CODA) accepts incoming connections on all IP addresses.

To configure the HP Operations agent to use a specific IP address:

1. Log on to the HP 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>
```

Configuring HTTPS Communication Through Proxies

If your network allows only certain proxy systems to open connections through the firewall, you can redirect HPOM 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.

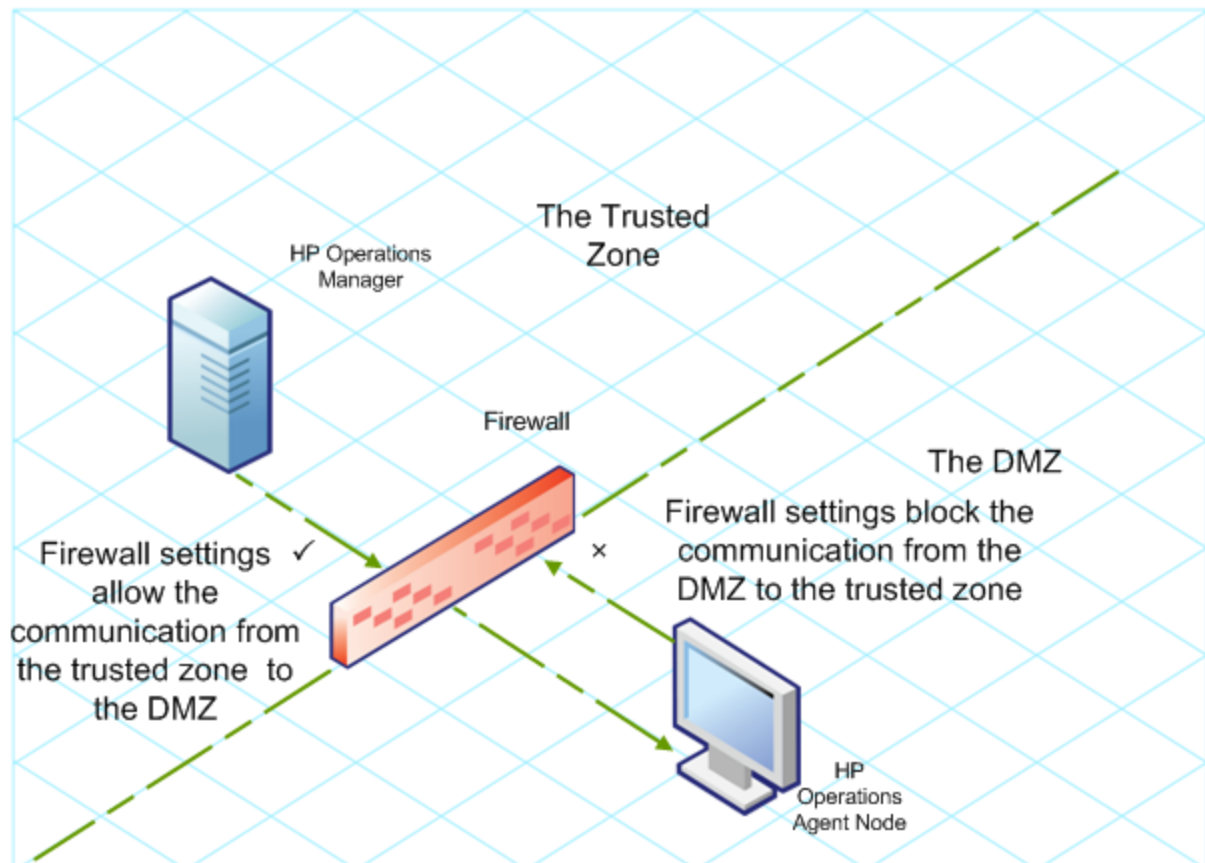
Communication in a Highly Secure Environment

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 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.

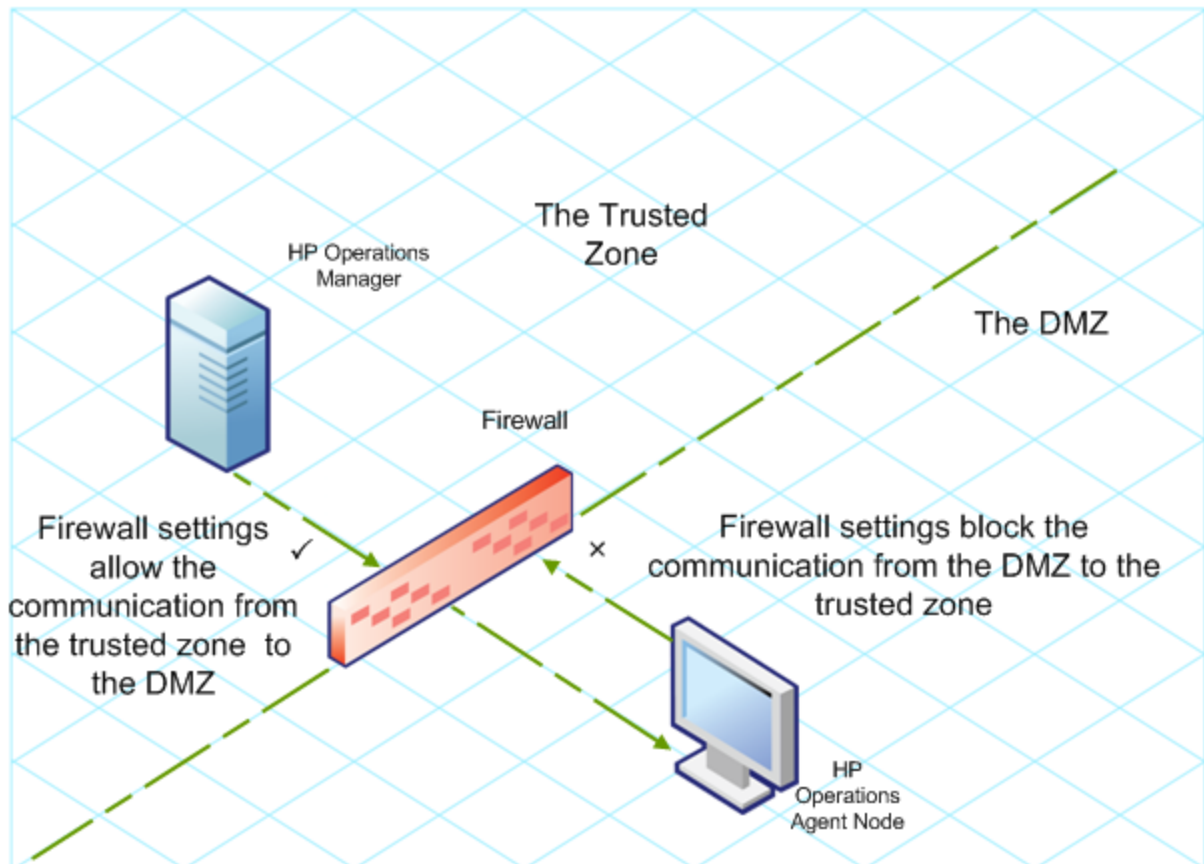
In the following scenario, managed nodes are located in the DMZ while the management server belongs to the trusted zone. The firewall settings in this example allow outbound-only communication. Therefore, inbound communication to the management server is blocked by the firewall.

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 management server, but block the inbound communication to node.

HPOM Management Server in the DMZ



Introduction to the Reverse Channel Proxy

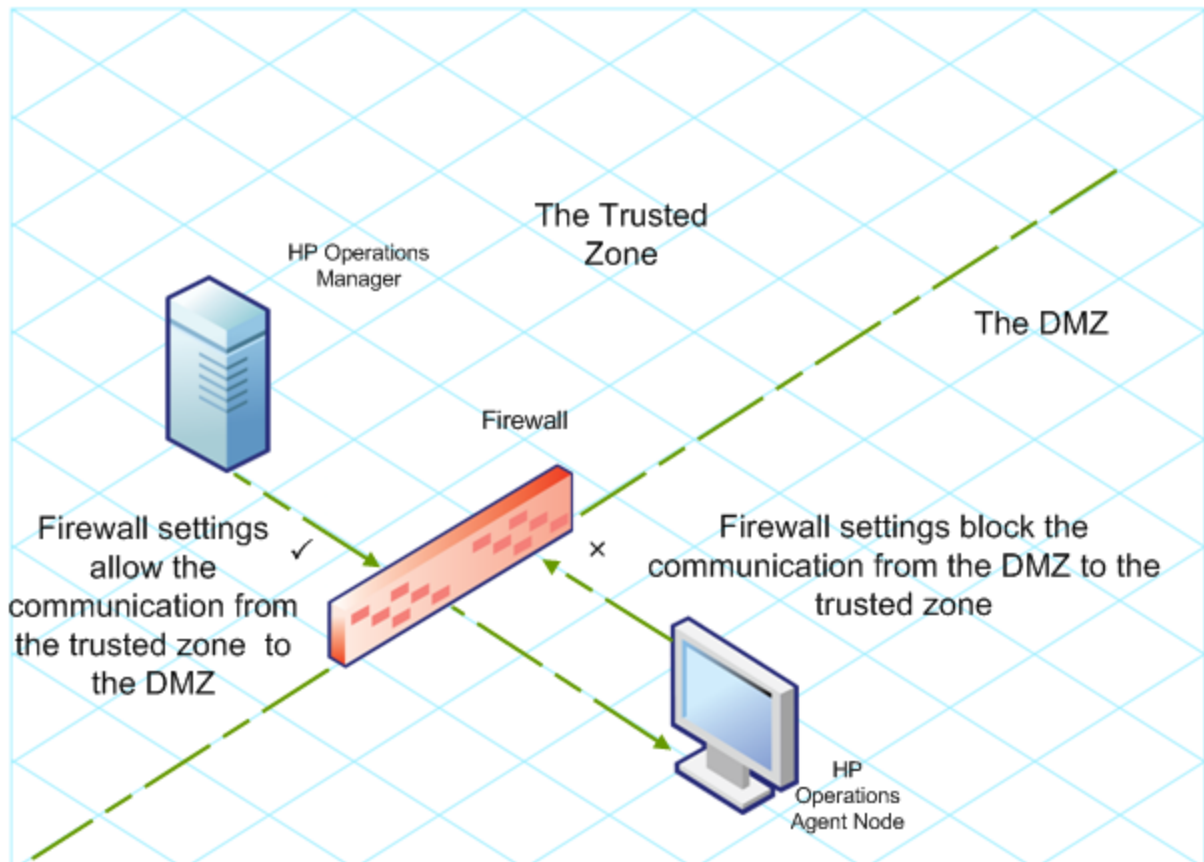
One simple solution to enable bidirectional communication is to configure the firewall settings to allow inbound traffic to the port 383 (the Communication Broker port). However, this can make your system vulnerable to external attacks. To enable secure communication without allowing inbound traffic to the Communication Broker port, you must configure a reverse channel proxy (**RCP**).

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 use 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 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 management server through the reverse administration channel.

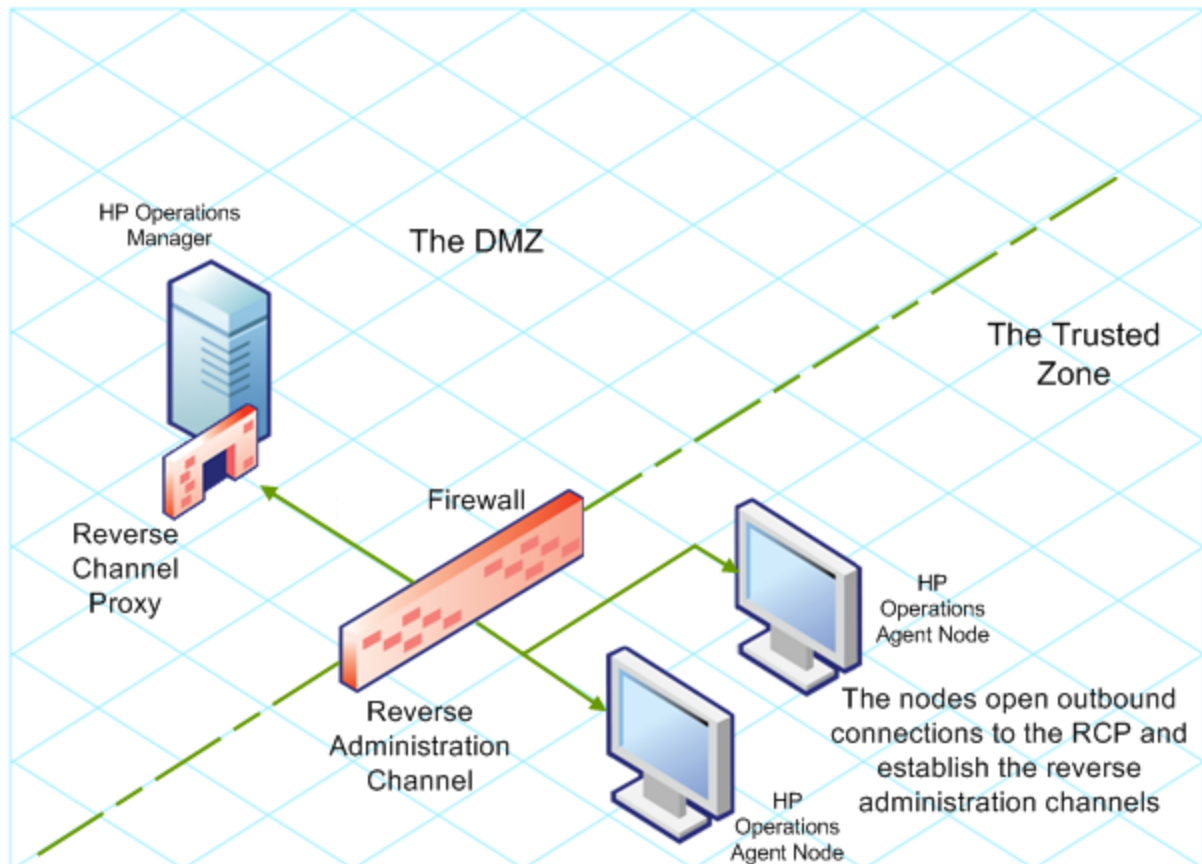
Secure Communication Through the RCP with Nodes in the DMZ



When the nodes are located in the trusted zone and the management server in the DMZ, the HPOM 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



Configure 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. You must do as follows to resolve this problem:

- 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

Configure 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 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 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>
```

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.

Specify 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.

Configure an 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 HP 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.

Verify 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:

Verify 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; ovbbcrp 11.00.000
```

```
system2.mydomain.com:1025 BBC 11.00.000; ovbbcrp 11.00.000
```

```
system3.mydomain.com:1025 BBC 11.00.000; ovbbcrp 11.00.000
```

```
system4.mydomain.com:1025 BBC 11.00.000; ovbbcrp 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:

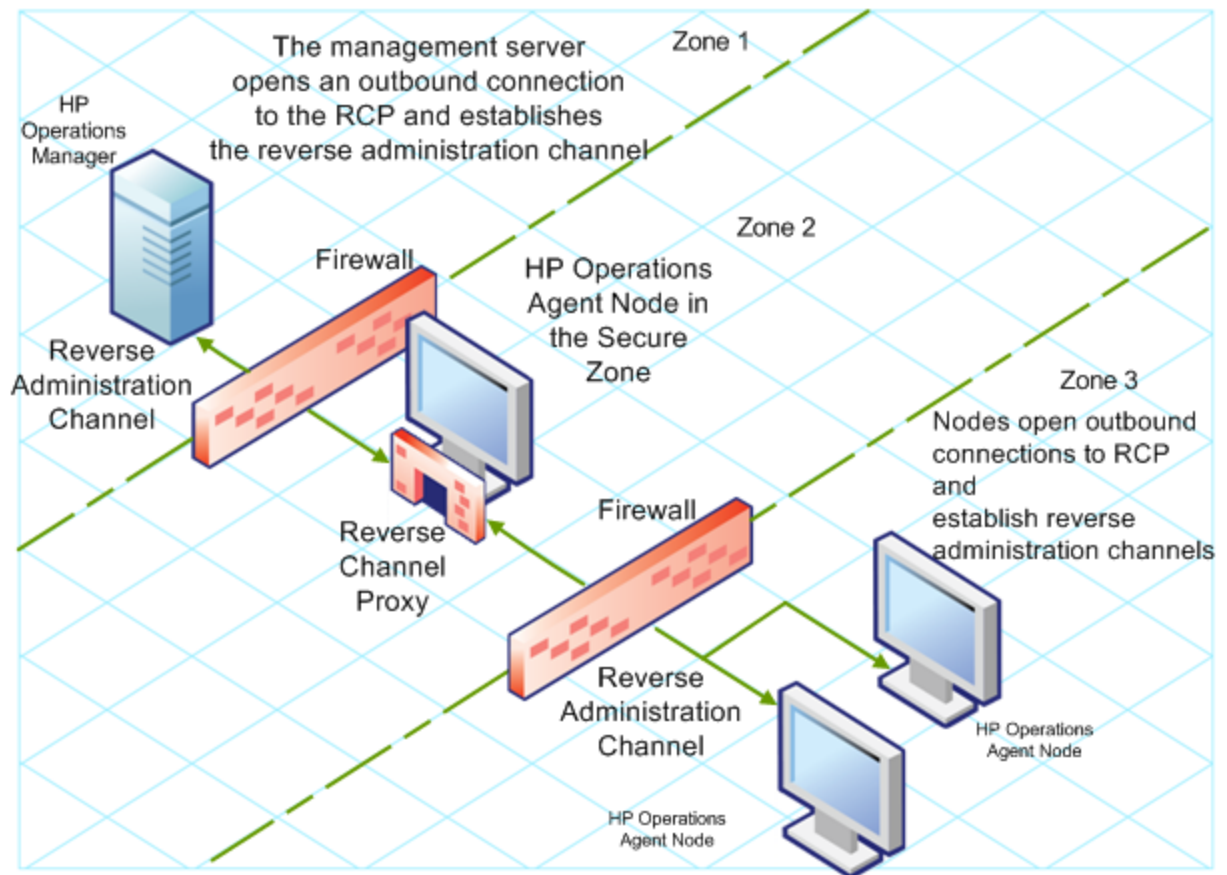
```
Pending:
```

```
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.

Chapter 21

Uninstalling the HP Operations Agent

Note: If the node hosts another HP 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 HP Software product

1. Log on to the node with root or administrator.
2. Stop all agent processes by running the following commands:

opcagt -stop

ttd -k

3. Go to the following directory:

Windows 64-bit

%OvInstallDir%bin\win64\OpC\install\%OvInstallDir%bin\win64\OpC\install

Other Windows

%OvInstallDir%bin\OpC\install\cscript oainstall.vbs -r -a

Linux, HP-UX, Solaris

/opt/OV/bin/OpC/install/oainstall.sh -r -a

AIX

/usr/lpp/OV/bin/OpC/install/oainstall.sh -r -a

4. Manually delete the following directories, if there are no other HP Software products installed on the node:

On Windows:

%OvInstallDir%

%OvDataDir%

On HP-UX, Solaris, and Linux:

/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 HP Operations agent 11.11 with the Programs and Features (Add/Remove Programs) window by selecting **HP Operations-agent**.

Installation of the HP Operations agent 11.11 adds the HP Operations-agent program to the Programs and Features window.



Many new items such as HP Software E/A Agent, HP Software Measurement Interface, HP Software Performance Core, and so on are also added to the Programs and Features window. While removing the HP Operations agent, choose only **HP Operations-agent** (and no other entries) in the Programs and Features window.

Chapter 22

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. In the All Policy Assignments window, 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. In the Node Bank window, 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 23

Troubleshooting

This section helps you troubleshoot such problems experienced during the installation and provides you with information to help you avoid problems from occurring.

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 HP Operations agent remotely from HPOM for UNIX/Linux management server shows error message

When you are installing HP 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 HP Operations agent version on the management server to 11.11.

HP Performance Agent (PA) 5.0 packages on Windows nodes do not get replaced with HP Operations agent 11.10/11.11 deployment packages after upgrade

When upgrading the Windows nodes, where PA 5.0 is installed, to HP Operations agent 11.10/11.11, 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 HP Operations agent packages to version 11.10/11.11 to resolve the issue. Perform the following tasks:

- ["Deploy the HP Operations agent 11.10/11.11 package" \(on page 143\)](#)
- ["View the packages" \(on page 143\)](#)
- ["Synchronize the deployment packages with the HP Operations agent version 11.10/11.11" \(on page 144\)](#)

Deploy the HP Operations agent 11.10/11.11 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 11.10/11.11 Operations agent packages.

If the older PA version and hotfix details are available in the package inventory, complete the task "[Synchronize the deployment packages with the HP Operations agent version 11.10/11.11](#)" (on page 144).

Synchronize the deployment packages with the HP Operations agent version 11.10/11.11

1. From the console tree, right-click a node to open the context menu.
2. Select **All Tasks > Synchronize Inventory > packages**.

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click on the bookmark “Comments”.

In case you do not have the email client configured, copy the information below to a web mail client, and send this email to **docfeedback@hp.com**

Product name:

Document title:

Version number:

Feedback:

