HP Operations Agent and Infrastructure SPIs

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

Installation Guide

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

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

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

Microsoft®, Windows®, Windows® XP, 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: **https://softwaresupport.hp.com**

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

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

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

Support

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

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

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

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

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

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

To find more information about access levels, go to:

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

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

Contents

Chapter 1: Introduction

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

HP Operations Agent 11.16 is a security patch release, you can obtain the HP Operations Agent 11.16 from the Software Support Online website. The HP Operations Agent 11.16 is available in the ISO format—five different ISO files for five operating systems supported by the HP Operations Agent and one ISO file for Infrastructure SPI.

The following table lists the patch names for all five platforms of HP Operations agent and one patch of Infrastructure SPI:

Operations agent

Platform	File Name
Windows	OAWIN_00044
Linux	OALIN_00044
HP-UX	OAHPUX_00044
Solaris	OASOL_00044
AIX	OAAIX_00044
Infra SPI	INFSPI_00007

Downloading the HP Operations Agent and Infrastructure SPIs 11.16

To download HP Operations Agent 11.16 ISO files, follow these steps:

1. Go to the following website:
   http://h20230.www2.hp.com/selfsolve/patches
2. Log on to the web site with your HP Passport credentials.
3. Search with the keyword HP Operations Agent 11.16. The search result includes links to download the ISO files for the HP Operations Agent 11.16.
4. Click one of the links and download the ISO file on your system.

Tip: You are required to install the HP Operations Agent 11.02 or higher on the management server before installing the deployment packages. For OALIN_00044 patch registration, make sure to

upgrade the management server to HP Operations Agent 11.13 or higher. Therefore, if the managed nodes and the management server are running on different operating systems, you must download the ISO file for the management server's operating system too.

Planning for the Installation of HP Operations Agent 11.16

Installing the Operations Agent on the HPOM Management Server

Download the platform specific patch ISO file for the management server's operating system.

Installing the HP Operations Agent Manually on the Node

You can install the HP Operations Agent 11.16 manually on an HPOM-managed or standalone node, or you can use the HPOM management server to deploy the Operations Agent and Infrastructure SPIs 11.16 centrally on all managed nodes.

Installing only Infrastructure SPIs

The process is as follows:

1. Make sure that HP Operations Agent 11.11 deployment packages are installed on the management server.
2. Download the Infrastructure SPIs patch ISO file.

Chapter 2: Registering the Operations Agent on the HPOM Management Server

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.

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.

Choose one of the following tasks based on your requirement:

- "Register the HP Operations Agent deployment package (version 11.16) for a specific node platform by using a platform-specific ISO file" on the next page
- "Register the HP Operations Agent deployment packages for all platforms, but do not install the Infrastructure SPIs

Install the HP Operations Agent on the Management Server

Follow the steps below to install HP Operations Agent on management server. For OALIN_00044 patch registration, make sure to upgrade the management server to HP Operations Agent 11.13 or higher.

Note: Skip step 3 to step 8 if HP Operations Agent 11.02 or higher is running on the management server. In case of OALIN_00044 patch registration, skip step 3 to step 8 if HP Operations Agent 11.13 or higher is running on the management server.

1. Make sure that HP Operations Agent 11.11 deployment packages are installed on the management server.
2. Make sure that the HP Operations Agent 11.1x or HP Operations Agent 11.0x (patch) is running on the management server.

3. Download the platform specific patch ISO file for the management server's operating system.
4. Transfer the downloaded ISO file onto the management server.
5. Log on to the management server with the root or administrator privileges.
6. Extract the contents of the ISO file into a local directory on the management server, or mount the ISO file.
7. Go to the directory where you extracted or mounted the ISO file, and then install the agent by running the following command:

   On Windows:

   ```
   cscript oainstall.vbs -i -a
   ```
8. Restart HPOM processes:

   On HPOM for Windows:

   ```
   vpstat -3 -r stop
   vpstat -3 -r start
   ```

Register the HP Operations Agent deployment package (version 11.16) for a specific node platform by using a platform-specific ISO file

Follow the steps:

1. Make sure that you downloaded the patch .ISO file for the respective platforms.
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.

For more information about installation procedures, see *HP Operations Agent* and Infrastructure SPIs *Installation guide 11.11.*

Register the Operations Agent deployment packages for all platforms, but do not install the Infrastructure SPIs

Follow the steps:

1. Make sure that you downloaded the patch .ISO file for all platforms.
2. Log on to the management server as administrator.
3. Create a new file with a text editor.
4. Add the following content:

```
[agent.parameter]

REGISTER_AGENT=YES

[hpinfraspi.parameter]

InfraSPI=NO

InfraSPI_With_Reports=NO

InfraSPI_With_Graphs=NO
```

5. Save the file.
6. Go to the media root.
7. From the media root, run the following command:

   ```
   cscript oainstall.vbs -i -m -spiconfig <file_name>
   ```

   In this instance, `<file_name>` is the name of the file (with the complete path to the file) that you created in step 3.

   The command registers the agent deployment packages for all platforms on the management server, but skips the installation of the Infrastructure SPIs.

Log File

The registration log file (`oainstall.log`) for 11.11 and 11.16 is available in the following directory:

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

You can now apply the patches for 11.16 on managed nodes remotely and centrally from the management server.

You can view the patch log file (`oapatch.log`) for version 11.16 in the following location:

```
%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
```

To check that the Infrastructure SPIs are installed, run the command with the includespi option:

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

Registering on the HPOM for UNIX 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.

Register the Deployment

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

Choose one of the following tasks based on your requirement:

- "Register the HP Operations Agent deployment packages (version 11.16) for a specific node platform by using a platform-specific ISO file" on the next page
- Register the HP Operations Agent deployment packages for all platforms, but do not install the Infrastructure SPIs
- After you complete the registration process on HPOM for UNIX management server, before you add the nodes and select the platforms from the list available on the console (user interface), follow the steps:

  On HPOM on UNIX/Linux:

  a. Go to the following directory: `/opt/OV/OMU/adminUI`

  b. Run the command: `./adminui machtypes`

  The updated platform list appears on the console only after you run the command.

Install the HP Operations Agent on the Management Server

Note: Skip step 3 to step 8 if HP Operations agent 11.02 or higher is running on the management server.

1. Make sure that HP Operations Agent 11.11 deployment packages are installed on the management server.
2. Make sure that the HP Operations Agent 11.1x or HP Operations Agent 11.0x (patch) is running on the management server.
3. Download the platform specific patch ISO file for the management server's operating system.
4. Transfer the downloaded ISO file onto the management server.
5. Log on to the management server with the root or administrator privileges.

6. Extract the contents of the ISO file into a local directory on the management server, or mount the ISO file.
7. Go to the directory where you extracted or mounted the ISO file, and then install the agent by running the following command:

   On UNIX/Linux:

   ```
   ./oainstall.sh -i -a
   ```
8. Restart HPOM processes:

   On HPOM on UNIX/Linux:

   ```
   /opt/OV/bin/OpC/opcsv -stop
   /opt/OV/bin/OpC/opcsv -start
   ```

Back Up the OpenVMS Deployment Package (Only on HPOM for UNIX)

If you are installing the HP Operations agent 11.16 deployment packages on the HPOM for UNIX management server, and if the HP Operations agent deployment package for the OpenVMS platform is already available on the server, you must take a backup of the deployment package for OpenVMS before the installation procedure starts.

1. Log on to the management server as root.
2. Transfer the contents of the directory `/var/opt/OV/share/databases/OpC/mgd_node/vendor/hp/alpha/ovms` into the `/tmp/alpha` directory (or any directory of your choice).
3. Transfer the contents of the directory `/var/opt/OV/share/databases/OpC/mgd_node/vendor/hp/ipf64/ovms` into the `/tmp/ipf64` directory (or any directory of your choice)

After installation, you must copy the backed-up contents of the `alpha` and `ipf64`directory into the original location (`/var/opt/OV/share/databases/OpC/mgd_node/vendor/hp/alpha/ovms`) and (`/var/opt/OV/share/databases/OpC/mgd_node/vendor/hp/ipf64/ovms`

Register the HP Operations Agent deployment packages (version 11.16) for a specific node platform by using a platform-specific ISO file

Follow the steps:

1. Make sure that you downloaded the patch .ISO file for the respective platforms.
2. Log on to the management server as administrator.
3. Go to the media root.
4. Run the following command:

   ```
   ./oainstall.sh -i -m
   ```
5. Verify the registration process.

Register the HP Operations Agent deployment packages for all platforms, but do not install the Infrastructure SPIs

Follow the steps:

1. Make sure that you downloaded the .ISO file for all platforms.
2. Log on to the management server as root.
3. Create a new file with a text editor.
4. Add the following content:

   ```
   [agent.parameter]

   REGISTER_AGENT=YES

   [hpinfraspi.parameter]

   InfraSPI=NO

   InfraSPI_With_Reports=NO

   InfraSPI_With_Graphs=NO
   ```

5. Save the file.
6. Go to the media root.
7. From the media root, run the following command:

   ```
   ./oainstall.sh -i -m -spiconfig <file_name>
   ```

   In this instance, `<file_name>` is the name of the file (with the complete path to the file) that you created in step 3.

   The command registers the agent deployment packages for all platforms on the management server, but skips the installation of the Infrastructure SPIs

Log File

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

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

You can now apply 11.16 patch on managed nodes remotely and centrally from the management server. You can view the installation log file (`oapatch.log`) in the following location:

```
/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
```

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

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

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

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

Chapter 3: Removing the Deployment Package

To remove the updates applied on the deployment packages, follow these steps:

1. Log on to the management server with the root or administrator privileges.
2. Go to the following directory:

   On Windows (32-bit systems):

   `%ovinstalldir%bin\OpC\agtinstall`

   On Windows (64-bit systems):

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

   On UNIX/Linux:

   `/opt/OV/bin/OpC/agtinstall`
3. Run the following command:

   On Windows:

   `cscript oainstall.vbs -r -m -pn <Patch_name>`

   On UNIX/Linux:

   `./oainstall.sh -r -m -pn <Patch_name>`

   In this instance, *<Patch_name>* is the file name of the patch file that you downloaded (without the extension .ISO). The following table lists the patch names for all five node platforms:

   Patch Names

Platform	File Name
Windows	OAWIN_00044
Linux	OALIN_00044
HP-UX	OAHPUX_00044
Solaris	OASOL_00044
AIX	OAAIX_00044

This procedure reinstates the version of the HP Operations Agent 11.11 deployment package that was in effect prior to applying this patch.

Chapter 4: Upgrading to the HP Operations Agent 11.16 from the Previous Versions

You can upgrade an older version of the HP Operations Agent, HP Performance Agent, or HP GlancePlus to the HP Operations Agent 11.16.

Upgrade Scenario	Procedure
From version 11.11 to version 11.16	You can use the patch download procedure to upgrade from version 11.11.
From version 11.12, 11.13 or 11.14 to version 11.16	You can use the patch download procedure to upgrade from version 11.12, 11.13 or 11.14.

Chapter 5: Update Deployment Packages on Management Servers in Clusters

For HPOM management servers that exist in high-availability (HA) clusters, you must install the deployment packages for the HP Operations Agent 11.16 only on active nodes.

To install HP Operations Agent 11.16 deployment packages, follow these steps:

1. "Install the HP Operations Agent 11.16 on the Active Management Server" below.
2. "Install HP Operations Agent 11.16 Deployment Packages on the Active Management Server" on page 21.
3. "Install the HP Operations agent on Other Management Servers in the Cluster" on page 22
4. "Synchronize Installer Scripts After Failover" on page 22. Perform this step only after HPOM fails over to another node in the HA cluster.

Install the HP Operations Agent 11.16 on the Active Management Server

You are required to install HP Operations Agent 11.02 or higher on the active management server before installing HP Operations Agent 11.16. For OALIN_00044 patch registration, make sure to upgrade the active management server to HP Operations Agent 11.13 or higher.

To install the agent in an HA cluster on the active management server, follow these steps:

1. Make sure that the management server meets the disk space requirement:

   Disk Space Requirements

OS	Free Disk Space
Windows	150 MB
Linux	• 50 MB on `/opt` • 100 MB on `/var`
HP-UX	• 50 MB on `/opt` • 100 MB on `/var`
Solaris	• 50 MB on `/opt` • 100 MB on `/var`

   Note: On UNIX/Linux., at least 20% of the original volume of the `/tmp` directory must be free while you install the agent.

2. Disable the mechanism to monitor HPOM's resource group.

   If you use HPOM for Windows, follow these steps on *all* nodes in the HA cluster:

   a. Log on to the management server as an administrator.

   b. Set the management server to the unplanned outage mode by running the following command:

      `ovownodeutil -outage_node -unplanned -node_name <FQDN_of_node>-on`

      In this instance, `<FQDN_of_node>` is the fully qualified domain name of the management server.

   If you use HPOM on UNIX/Linux, follow these steps *only* on active nodes in the HA cluster:

   a. Log on to the management server as root.

   b. Disable monitoring of the resource group:

      `/opt/OV/lbin/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 HP Operations Agent 11.16 on the management server.

   a. Log on to the management server as root or administrator.

   b. Stop all agent and HPOM processes:

      On Windows:

      `vpstat -3 -r stop`

      On UNIX/Linux:

      `/opt/OV/bin/OpC/opcsv -stop`

      `/opt/OV/bin/opcagt -stop`

   c. Extract the contents of the HP Operations Agent 11.16ISO file into a local directory. Alternatively, you can mount the ISO file.

d. Go to the directory where you extracted (or mounted) the ISO file, and then run the following command:

On Windows:

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

On UNIX/Linux:

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

e. Restart all HPOM processes:

On Windows:

```
vpstat -3 -r stop
vpstat -3 -r start
```

On UNIX/Linux:

```
/opt/OV/bin/OpC/opcsv -stop
/opt/OV/bin/OpC/opcsv -start
```

4. Enable the mechanism after installing HP Operations Agent 11.16 on the management server.

If you use HPOM for Windows, follow these steps on *all* nodes in the HA cluster:

a. Log on to the management server as an administrator.

b. Turn off the unplanned outage mode on the management server by running the following command:

```
ovownodeutil -outage_node -unplanned -node_name <FQDN_of_node>-off
```

In this instance, `<FQDN_of_node>` is the fully qualified domain name of the management server.

If you use HPOM on UNIX/Linux, follow these steps *only* on active nodes in the HA cluster:

a. Log on to the management server as root.

b. Enable monitoring of the resource group:

```
/opt/OV/lbin/ovharg -monitor <HA_resource_group_name> enable
```

In this instance, `<HA_resource_group_name>` is the HA resource group for HPOM on the management server.

Install HP Operations Agent 11.16 Deployment Packages on the Active Management Server

Install the deployment packages for the HP Operations Agent 11.16 on the active management server:

1. Log on to the management server as root or administrator.
2. Go to the directory where you extracted (or mounted) the HP Operations Agent 11.16 ISO file.
3. From the command prompt, run the following command:
On Windows:

```
cscript oainstall.vbs -i -m
```

On UNIX/Linux:

```
./oainstall.sh -i -m
```

Tip: If you use different operating systems for different node groups in your environment, you must perform step 1 through step 3 for each operating system that is in use in your environment. If you are installing with one ISO with all platforms, then use the following command:

- **On Windows:**
  `cscript oainstall.vbs -i -m -p <platform>`
- **On UNIX/Linux:**
  `./oainstall.sh -i -m -p <platform>`

Install the HP Operations agent on Other Management Servers in the Cluster

Verify that the HP Operations Agent 11.16 works correctly on the active node, and then install the HP Operations Agent 11.16 on other management servers in the cluster that are not active.

Follow the instructions in "Installing the HP Operations Agent 11.16" on page 26.

Synchronize Installer Scripts After Failover

After failover, perform this task to make sure that the correct version of the installer program for the HP Operations Agent is transferred to the currently active node in the cluster (you need the updated installer program to remove the agent deployment packages or to view the package inventory). To copy the scripts to the other management servers in cluster, you must switch (failover) the HPOM server to the next cluster node.

After HPOM fails over to a node in the HA cluster, follow these steps:

1. Log on as root or administrator to the node where HPOM is currently active.
2. Run the following command:

   On Windows:

   `cscript %OvShareDir%server\installation\oainstall_sync.vbs`

   On UNIX/Linux:

   `/var/opt/OV/shared/server/installation/oainstall_sync.sh`

   The command transfers the latest version of the `oainstall.vbs` or `oainstall.sh` script to the currently active node from the failed node.
3. View the package inventory for the agent on the currently active node to make sure that deployment packages for the HP Operations Agent are available.

   To view the package inventory, run the following command:

   On Windows:

   `cscript oainstall.vbs -inv`

   On UNIX/Linux

   `./oainstall.sh -inv`

The command displays the list of HP Operations Agent 11.16 deployment packages that are installed on the system under the `Active Agent Patches Installed` section.

Chapter 6: Different Modes of the HP Operations Agent Installation

The HP Operations agent installer enables you to install the Operations Agent and Infrastructure SPIs either on an HPOM-managed node or on a standalone server. If you install the agent on an **HPOM-managed** node, you must provide the details of the management server at the time of installation and make sure that the node belongs to the list of managed nodes in the HPOM console. This mode of the installation enables you to use the operations monitoring component of the agent to monitor the system and send alerts to the HPOM console.

If you want to use the HP Operations agent only to monitor system performance metrics locally, you can perform the installation without providing any details of the HPOM management server. This **standalone** mode of the installation enables you to use the performance collection component (and HP GlancePlus, if installed on UNIX/Linux) to monitor system performance metrics that indicate the health and performance of the system.

With the **-defer_configure** option, you can install the agent in the **inactive** mode—a mode where all the processes of the agent remain inactive after installation and the agent does not perform any tasks. At a later time, you can use the **-configure** option of the agent installer to set the agent running. The **-configure** option helps you set the operation of the agent in the HPOM-managed or standalone mode.

With the **-defer_activate** option, you can install the HP Operations Agent by deferring the agent activation.

Note: On Windows, the following command can be used to install the HP Operations Agent by deferring the agent activation:

```
cscript oainstall.vbs -i -a -minprecheck -includeupdates -defer_activate
```

The advantage of using this mechanism is the ability to create images of the OS platforms with Operations agent pre-installed that can later be cloned or instantiated. You may also create virtual machine templates that can later be used for deployments. This option helps in distributing a standard version of Operations agent to all the managed systems that would get deployed in your environment.

Different Modes of the HP Operations Agent Installation

Agent Installation Mode	Description
HPOM-managed/active	The agent is installed on a managed node and details of the management server (and the certificate server) are specified at the time of installation; the installation started all necessary agent processes. Remote installation from a management server always ensures this mode of the agent is set.
Standalone/ active	The agent is installed on a standalone system. Management server details are not provided at the time of installation. However, the installation started all necessary agent processes.

Different Modes of the HP Operations Agent Installation, continued

Agent Installation Mode	Description
Inactive	The agent is installed with the **-defer_configure** option. The installation procedure places all the necessary files on the system, but the agent remains inactive after installation. You cannot use this mode of installation if you want to install the agent remotely from the management server. For information about installing the agent in the inactive mode, see "Installing the HP Operations Agent in the Inactive Mode".

Chapter 7: Installing the HP Operations Agent 11.16

You can install the HP Operations Agent 11.16 manually on an HPOM-managed or standalone node, or you can use the HPOM management server to deploy the 11.16 centrally on all managed nodes..

Note: No additional steps are required for installing the HP Operations Agent on nodes in a high-availability cluster. The agent installation process does not stop cluster services or daemons running on the node. Installing the agent deployment packages, however, requires additional steps ("Update Deployment Packages on Management Servers in Clusters" on page 19).

To install only the HP Operations Agent 11.16, do one of the following:

- Install from the management server:
  - To install from the HPOM console, see "Install from the HPOM Console" on page 41.
  - To install with the command line, see "Installing the HP Operations Agent Remotely" on page 38.
- "Install the HP Operations Agent 11.16 on a Node Manually" on page 36.

To install the HP Operations Agent 11.16 with the HP Operations Agent 11.11, do one of the following:

- To install from the HPOM console, see "Install from the HPOM Console" on page 41.

Prerequisites for Installing the HP Operations Agent 11.11

Before you begin the installation, make sure that all the prerequisites are met. After evaluating your requirements, identify the most suitable option to install the product in your environment.

General Considerations

- If you want to deploy the agent remotely from the HPOM console, make sure firewall settings are disabled between the management server and nodes.
- If you want to install the agent manually on the node in a firewall-controlled environment, make sure that the firewall setting allows the agent to contact the management server through the port 383 on the management server.
- Before installing the product in an HPOM-managed environment, always make sure the node is added as a managed node before you begin the installation process.
- If you want to work with the agent immediately after installation, make sure the automatic certificate requests are enabled on the management server.

- In a highly-secure environment, if you disable the automatic certificate request property on HPOM, you must exchange certificate manually with the management server after the agent installation completes.
- The HP Operations Agent is a cluster-aware application. However, the HP Operations Agent software cannot failover automatically to the standby node in the event of failover.

Prerequisites for Windows

User

To install the HP Operations Agent on a Windows node, you must log on 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

<Following privileges are only for remote deployment>

- 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. To check if the Windows Installer 4.5 or higher is present, follow these steps:
  a. Log on to the Windows system.
  b. From the Start menu, open the Run prompt.
  c. At the Run prompt, type **regedit**, end then press **Enter**. The Registry Editor window opens.
  d. In the Registry Editor window, expand **HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft**, and then click **DataAccess**.
  e. In the right pane, double-click **FullInstallVer**. The Edit String dialog box opens.
  f. In the Edit String dialog box, check if the version string is set to 2.00 or higher.
- **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:
  a. Log on to the Windows system.
  b. From the Start menu, open the Run prompt.
  c. At the Run prompt, type **regedit**, end then press **Enter**. The Registry Editor window opens.
  d. In the Registry Editor window, expand **HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft**, and then click **Windows Script Host**.
  e. In the right pane, look for the key Enabled:
  f. If the key Enabled is present, double-click the key and make sure the Value Data is set to 1. The Windows Script Host i s disabled is the Value Data for the Enabled key is set to 0.

g. 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
- <*only for remote deployment*> Remote Registry
- <*only for remote deployment*>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

This is the disk space requirement for HP Operations Agent 11.11 and 11.16.

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 (WMI) Service is required if you want to deploy the WMI Interceptor policies or Measurement Threshold policies. WMI is also used to monitor the WMI events and classes or 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 log on 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. You can run the below command to list the RPM packages:

```
rpm –qa | grep –i <package_name>
```

- 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`
- **Only required for Glance**- Curses runtime library:
  libncurses.so.5

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

On Linux (64-bit systems):

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

On Linux (32-bit systems):

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

- Make sure that the m4 utility is installed at the path `/usr/bin/m4`.
- **On x64 systems**:
  - libgcc-3.4.6-8.i386.rpm and above
  - glibc-2.3.4-2.36.i686.rpm and above
  - libstdc++-3.4.6-8.i386.rpm and above
  - compat-libstdc++-33.i386.rpm and above
  - libstdc++33-32bit-3.3.3-7.8.1.x86_64.rpm and above

Note: Make sure that libstdc++33-32bit-3.3.3-7.8.1.x86_64.rpm is installed before you install HP Operations agent 11.11 on SLES10 SP4 x64 system. This rpm is applicable only for SUSE Linux Enterprise Server 10 and above.

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

Disk Space

For new installation for HP Operations Agent 11.11 and 11.16

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

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

For upgrade

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

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

Note: If you do not have sufficient space in the installation or data directory, you can symbolically link the install or data directory to another location on the same system by using the `ln -s` command.
For example, to symbolically link the `/opt/OV` directory to the `/new` directory, run the following command:

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

Recommended Software and Services

- **For SNMP MIB monitoring:** If you want to monitor objects in an SNMP Management Information Base (MIB) on the agent system, make sure the SNMP agent (compliant with MIB-I and MIB-II) is installed on the system.
- **For xglance:** To use the xglance utility, make sure the following components are available on the system:
- Open motif toolkit 2.2.3 (On Linux platforms other than Red Hat Enterprise Linux 5.x and SUSE Linux Enterprise Server 10.x on x86_64 and Itanium, the 32-bit version of the Open motif toolkit and associated libraries must be present.)

Prerequisites for HP-UX

User

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

Necessary Software

On HP-UX, make sure that the following patches are installed. You can run the below command to list the RPM packages:

```
swlist –l | grep –i <package_name>
```

- *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

This is the disk space requirement for HP Operations Agent 11.11 and 11.16.

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 log on with the root privileges.

Necessary Software

Before you install the HP Operations Agent on a Solaris node, make sure to install the following or superseding patches. You can run the below command to list the RPM packages:

`pkginfo –l | grep –i <package_name>`

In addition, make sure the following packages are available:

SUNWlibC

SUNWlibms

SUNWmfrun

SUNWxwplt

Kernel Settings

Set the following minimum kernel parameter values for Solaris 9:

semsys:seminfo_semmni=30

semsys:seminfo_semmns=200

semsys:seminfo_semmsl=100

For Solaris 10, no specific kernel settings are required.

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

Disk Space

This is the disk space requirement for HP Operations Agent 11.11 and 11.16

For new installation of HP Operations Agent 11.11 and 11.16

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.

Note: Prerequisites for Solaris 11 are same as that of Solaris 10.

Prerequisites for AIX

User

To install the HP Operations Agent on an AIX node, you must log on with the root privileges.

Necessary Software

You can run the below command to list the RPM packages:

`lslpp –l | grep –I <package_name>`

- 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.
- To remotely install the HP Operations Agent from the HPOM for Windows console, make sure that the 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

This is the disk space requirement for HP Operations Agent 11.11 and 11.16.

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 the directory (*/*): 10 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

For the directory (*/*): 10 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).

Prerequisites for Debian and Ubuntu

User

To install the HP Operations Agent on a Linux node, you must log on 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. You can run the below command to list the RPM packages:

`dpkg –l | grep -i <package_name>`

- C++ runtime:
  - For systems with kernel version 2.6:
    `/lib/libstdc++.so.5`
  - For systems with kernel version 2.6 on Itanium :
    `/lib/libstdc++.so.6`
- **Only required for Glance**- Curses runtime library:
  `/lib/libncurses.so.5`
- Make sure that the m4 utility is installed at the path `/usr/bin/m4`.

- **On x64 systems:**
  - libgcc-3.4.6-8.i386.rpm and above
  - glibc-2.3.4-2.36.i686.rpm and above
  - libstdc++-3.4.6-8.i386.rpm and above
  - compat-libstdc++-33.i386.rpm and above
  - libstdc++33-32bit-3.3.3-7.8.1.x86_64.rpm and above

    Note: Make sure that libstdc++33-32bit-3.3.3-7.8.1.x86_64.rpm is installed before you install HP Operations Agent 11.11 on SLES10 SP4 x64 system.

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

For more information about disk space requirements, see "Disk Space" on page 30

Prerequisites for Installing the HP Operations Agent 11.16

Hardware Requirements

For information about supported architecture types, see the Support Matrix at:

https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM323488

The following table describes the disk space requirements for the HP Operations Agent 11.16:

Disk Space Requirements

OS	Free Disk Space
Windows	150 MB
Linux	• 50 MB on `/opt` • 100 MB on `/var`
HP-UX	• 50 MB on `/opt` • 100 MB on `/var`
Solaris	• 50 MB on `/opt` • 100 MB on `/var`
AIX	• 50 MB on `/usr` • 100 MB on `/var`

Disk Space Requirements, continued

OS	Free Disk Space
	• 10 MB on /

Note: On UNIX/Linux, at least 20% of the original volume of the `/tmp` directory must be free while you install the agent.

Software Requirements

- **Operating system:** For a list of supported operating systems, see the Support Matrix at:
  https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM323488
- Windows Installer 4.5 or higher must be installed on Windows nodes.

Additional Requirements for vSphere Management Assistant Nodes

- **Login requirement**

  By default, the root login is disabled on vSphere Management Assistant (vMA). As a result, you cannot deploy the agent remotely from the HPOM console to a vMA node. 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.
- **viserver.properties**

  Note: If you want to roll back to previous version of HP Operations Agent, you must always back up the existing **viserver.properties** file (which is available in the `/var/opt/perf` directory) before installing the HP Operations Agent 11.16

  After installing HP Operations Agent 11.16, the new **viserver.properties** file will replace the existing file. The recommended values are set in the properties file.

Install the HP Operations Agent 11.16 on a Node Manually

The HP Operations Agent 11.16 media enables you to install the agent manually using command-line utilities. The installer programs, available with the media, enable you to install the product on a node in the HPOM-managed environment or on a standalone system.

Note: The HP Operations Agent 11.11 media provided you with the `oasetup` program, which could be used in installing the agent (instead of the `oainstall` scripts). Although the agent 11.16 ISO file includes the `oasetup` program (within the `patches` directory), use only the `oainstall` script for

installing the HP Operations Agent 11.16.

On Windows Nodes

1. Log on to the node with the administrator privileges.
2. Download the patch ISO and extract contents of the ISO file into a local directory.
3. Go to the directory where you extracted the contents of the ISO file.

   Note: Before installing the HP Operations Agent 11.16 patch, if you have already installed the Performance Manager 9.0 (component patch HPPM8X9XCPW_00002) and LCore hotfixes in your system, remove the hotfix inventory **xml** files, example **HPOvXpl-HFWIN_00045.xml** from the location `%OvDataDir%\installation\inventory`.

4. Run the following command to install the agent (on an HPOM-managed node or on a standalone system):
   ```
   cscript oainstall.vbs -i -a
   ```

After you run the command, the installation procedure begins. At the end of the installation, the agent starts its operation on the node and all the necessary components start running.

On UNIX/Linux Nodes

1. Log on to the node with the root privileges.
2. Download the patch ISO and extract contents of the ISO file into a local directory.
3. Go to the directory where you extracted the contents of the ISO file.
4. Run the following command to install the agent (on an HPOM-managed node or a standalone system):
   ```
   ./oainstall.sh -i -a
   ```

After you run the command, the installation procedure begins. At the end of the installation, the agent starts its operation on the node and all the necessary components start running.

If you install the HP Operations agent on the HPOM on UNIX/Linux management server (that is, if you select the management server as a managed node), you must manually restart all HPOM processes by running the following commands on the management server:

- `/opt/OV/bin/OpC/opcsv -stop`
- `/opt/OV/bin/OpC/opcsv -start`

Post-Installation Task for Nodes Under HPOM for Windows

If the agent node is managed by HPOM for Windows and if you remotely installed the HP Operations Agent 11.11 on the node from the HPOM console, you must perform the following steps after manually installing the agent 11.16 on the node:

1. Go to the console tree of the HPOM console.
2. Right-click the node, and then click **All Tasks > Synchronize > Packages**.

Verify the installation

To verify that the HP Operations Agent 11.16 is installed on the system successfully, follow these steps:

1. Go to the following directory on the node:

   On Windows:

   `%ovinstalldir%bin`

   On HP-UX, Linux, and Solaris:

   `/opt/OV/bin`

   On AIX:

   `/usr/lpp/OV/bin`
2. Run the following command:

   On Windows:

   `ovdeploy -inv -includeupdates`

   On UNIX/Linux:

   `./ovdeploy -inv -includeupdates`

The command lists the version of the agent installed on the system.

Note: On AIX nodes, preinstallation details appear twice in the log file.

Installing the HP Operations Agent Remotely

From the management server, you can install the HP Operations Agent 11.16 remotely on managed nodes.

Before You Begin

Determine the location of the `OVO-Agent.xml` file on the management server for the node where you want to install the HP Operations Agent 11.16.

Location of the OVO-Agent.xml File on the HPOM for Windows Management Server

Node Platform	Location of the OVO-Agent.xml File
Windows (x64)	`%ovdatadir%shared\Packages\HTTPS\windows\ms\5.1 5.2 6.0 6.1 6.2\x64\Operations-agent\11.11.025\64\https\oawin_00044`

Location of the OVO-Agent.xml File on the HPOM for Windows Management Server, continued

Node Platform	Location of the OVO-Agent.xml File
Windows (x86)	%ovdatadir%shared\Packages\HTTPS\windows\ ms\5.0 5.1 5.2 6.0 6.1 6.2\x86\Operations-agent\11.11.025\32 64\https\oawin_00044
HP-UX (Itanium)	%ovdatadir%shared\Packages\HTTPS\hp-ux\ hp\11.23 11.31\ipf32\Operations-agent\11.11.025\64\https\oahpux_00044
HP-UX (PA-RISC)	%ovdatadir%shared\Packages\HTTPS\hp-ux\ hp\11.11 11.23 11.31\pa-risc\Operations-agent\11.11.025\32 64\https\oahpux_00044
Linux (POWER)	%ovdatadir%shared\Packages\HTTPS\linux\ linux\2.6 3.0\powerpc\Operations-agent\11.11.025\64\https\oalin_00044
Linux (x86)	%ovdatadir%shared\Packages\HTTPS\linux\linux\2.6\x86\Operations-agent\11.11.025\32 64\https\oalin_00044
Linux (x64)	%ovdatadir%shared\Packages\HTTPS\linux\ linux\2.6 3.0\x64\Operations-agent\11.11.025\64\https\oalin_00044
Linux (Debian)	%ovdatadir%shared\Packages\HTTPS\linux_deb\ linux_deb\2.6 3.0 3.2\x64\Operations-agent\11.11.025\64\https\oalin_ 00044
Solaris (SPARC)	%ovdatadir%shared\Packages\HTTPS\solaris\ sun\5.9 5.10 5.11\sparc\Operations-agent\11.11.025\32 64\https\oasol_ 00044
Solaris (x86)	%ovdatadir%shared\Packages\HTTPS\solaris\ sun\5.10 5.11\x86\Operations-agent\11.11.025\32 64\https\oasol_00044
AIX (6.1)	%ovdatadir%shared\Packages\HTTPS\aix\ ibm\6.1 7.1\powerpc\Operations-agent\11.11.025\64\https\oaaix_00044

Location of the OVO-Agent.xml file on the HPOM on UNIX/Linux Management Server

Node Platform	Location of the OVO-Agent.xml File
Windows (x64)	/var/opt/OV/share/databases/OpC/mgd_node/vendor/ms/ x64/win2k3/A.11.00.000/RPC_BBC/OAWIN_00044
Windows (x86)	/var/opt/OV/share/databases/OpC/mgd_node/vendor/ms/ x86/winnt/A.11.00.000/RPC_BBC/OAWIN_00044
HP-UX (Itanium)	/var/opt/OV/share/databases/OpC/mgd_node/vendor/hp/ ipf32/hpux1122/A.11.00.000/RPC_BBC/OAHPUX_00044

Location of the OVO-Agent.xml file on the HPOM on UNIX/Linux Management Server, continued

Node Platform	Location of the OVO-Agent.xml File
HP-UX (PA-RISC)	/var/opt/OV/share/databases/OpC/mgd_node/vendor/hp/pa-risc/hpux1100/A.11.00.000/RPC_BBC/OAHPUX_00044
Linux (POWER)	/var/opt/OV/share/databases/OpC/mgd_node/vendor/linux/ppc/linux26/A.11.00.000/RPC_BBC/OALIN_00044
Linux (x86)	/var/opt/OV/share/databases/OpC/mgd_node/vendor/linux/x86/linux26/A.11.00.000/RPC_BBC/OALIN_00044
Linux (x64)	/var/opt/OV/share/databases/OpC/mgd_node/vendor/linux/x64/linux26/A.11.00.000/RPC_BBC/OALIN_00044
Linux (Debian)	/var/opt/OV/share/databases/OpC/mgd_node/vendor/linux_deb/x64/linux26/A.11.00.000/RPC_BBC/ OALIN_00044
Solaris (SPARC)	/var/opt/OV/share/databases/OpC/mgd_node/vendor/sun/sparc/solaris7/A.11.00.000/RPC_BBC/OASOL_00044
Solaris (x86)	/var/opt/OV/share/databases/OpC/mgd_node/vendor/sun/x86/solaris10/A.11.00.000/RPC_BBC/OASOL_00044
AIX (6.1)	/var/opt/OV/share/databases/OpC/mgd_node/vendor/ibm/rs6k64/aix5/A.11.00.000/RPC_BBC/OAAIX_00044

Install the Operations Agent

To install the Operations Agent remotely from the command line, follow these steps:

1. Log on to the management server as root or administrator.
2. Go to the following directory on the management server:

   On Windows:

   *%ovinstalldir%*bin

   On UNIX/Linux:

   /opt/OV/bin
3. Run the following command:

   ovdeploy -install -bundle <path-to-OVO-Agent.xml>-host <node name> -ovrg server

   In this instance:

   <path-to-OVO-Agent.xml> is the path to the **OVO-Agent.xml** file for the node type.

   <node name> is the FQDN of the node

   The command installs the Operations Agent on the node.

   If you updated the deployment packages of the agent with hotfixes, the command installs the hotfixes as well after installing the Operations Agent 11.16.
4. Run the following command on the management server to check that the installation is

successful:

For Windows nodes:

```
ovdeploy -cmd "%ovinstalldir%bin\opcagt -version" -host <node_name>
```

For HP-UX, Linux, and Solaris nodes:

```
ovdeploy -cmd "/opt/OV/bin/opcagt -version" -host <node_name>
```

For AIX nodes:

```
ovdeploy -cmd "/usr/lpp/OV/bin/opcagt -version" -host <node_name>
```

The command output shows 11.16 if the installation is successful.

Note: On AIX nodes, the preinstall log messages will appear twice on a successful installation of the Operations Agent 11.16.

Verify Installation on the Node

To verify that the installation is successful, follow these steps on the node:

1. Log on to the node as administrator or root.
2. Go to the following directory:

   On Windows:

   ```
   %ovinstalldir%bin
   ```

   On HP-UX, Linux, and Solaris:

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

   On AIX:

   ```
   /usr/lpp/OV/bin
   ```
3. Run the following command:

   On Windows:

   ```
   ovdeploy -inv -includeupdates
   ```

   On UNIX/Linux:

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

   The command output shows the list of components upgraded by the installer in the `PATCH` section. If you updated the deployment packages with hotfixes, the command lists the details of each hotfix under the `HOTFIX:` *<hotfix_name>* section.

Install from the HPOM Console

Installation of the deployment packages for the HP Operations Agent 11.16 on the management server makes necessary changes in the configuration to enable you to install the HP Operations Agent 11.16 and 11.11 (together) remotely on nodes from the HPOM console. You cannot install the HP Operations Agent 11.16 (or the hotfix) alone on the node from the HPOM console. In addition, if HP Operations Agent 11.11 is already present on the node, then only 11.16 is installed.

Prerequisites for Installing the HP Operations Agent from the HPOM Console

- Auto granting of the certificates must be enabled on the management server. This is optional.
- The `INCLUDEUPDATES` variable can be set to `true` on the management server. Installing deployment packages for the HP Operations Agent 11.16 ensures that this variable is set to `true`.

  For verification, run the following command on the management server:

  ```
  ovconfget -ovrg server depl INCLUDEUPDATES
  ```

  If the command returns `true`, you can go ahead with installation. Otherwise, you must change the setting to `true`.
- If you want to install the agent on one of the newly supported platforms, you must do the following:

  Install HPOM for UNIX/Linux patch (OM 9.10.220) or above.

  You do not need any additional hotfixes if you are using HPOM for Windows.
- The node must also meet the requirements listed in "Prerequisites for Installing the HP Operations Agent 11.16" on page 35

From the HPOM for Windows Console

To install the HP Operations Agent 11.16 and 11.11 together from the HPOM for Windows console:

Follow the instructions in the *Remote Agent Installation* section in *HPOM for Windows Online Help*.

Note: You need not select the **Run prerequisites check automatically before deployment** check box while installing the agent. The installation process on the node always performs prerequisite checks and the error or failure messages are annotated with the deployment job in the HPOM console. You can reduce the installation time by clearing this check box.

Depending on the original state of the node, you will see one of the following results:

- If the node did not have any agent software installed, the HP Operations Agent 11.11 and 11.16 are installed.
- If the node had old agent software that *can* be upgraded to the version 11.11, the existing agent is upgraded to the version 11.11 first, and then the agent 11.16 is installed.

  Note: In the above two scenarios, the remote installation mechanism first installs the HP Operations Agent 11.11 on the node, and then installs the HP Operations Agent 11.16. Therefore, the installation process might take longer than usual.
- If the node has old agent software that *cannot* be upgraded to the version 11.11, the installation fails.
- If the HP Operations Agent 11.11 was already installed on the node, follow these additional steps after the remote installation is complete:
  a. In the console tree, right-click the node, and then click **All Tasks > Reinstall/Update**. The Reinstall/Update Node dialog box opens.

b. Select **Update**, select **Packages** in the Scope section, clear the **Deploy Only if Version is Lower** check box, and then click **OK**.

c. After the installation is complete, go to the console tree of the HPOM console, right-click the node, and then click **All Tasks > Synchronize > Packages**.

The HP Operations Agent 11.16 is now installed on the node.

Note: Installation from the HPOM console might take longer than usual as HPOM first installs the HP Operations Agent 11.11 on the node, and then installs the HP Operations Agent 11.16.

From the HPOM for UNIX Console

To install the HP Operations Agent 11.16 and 11.11 together from the HPOM for UNIX console:

Follow the instructions in the *HPOM for UNIX: New Agent Installation* section in *HPOM for UNIX Online Help* to install the agent remotely from the HPOM console.

Depending on the original state of the node, you will see one of the following results:

- If the node did not have any agent software installed, HPOM installs both the agent versions 11.11 and 11.16. Make sure to select the **Force** check box in the Install Agent window.
- If the agent 11.11 was already installed on the node, you must select the **Force** check box in the Install Agent window while installing the agent. At the end of the installation, the agent 11.16 is installed.
- If the node has older agent software that *cannot* be upgraded to the version 11.11, installation fails.
- If the node had old agent software that *can* be upgraded to the version 11.11, the existing agent is upgraded to the version 11.11 first, and then the agent 11.16 is installed (this two-step upgrade takes place automatically; no additional steps are involved).

Note: Installation from the HPOM console might take longer than usual as HPOM first installs the HP Operations Agent 11.11 on the node, and then installs the HP Operations Agent 11.16.

Modify the Default Deployment Behavior

If you do not want to install the HP Operations Agent 11.16 patch and HP Operations Agent 11.11 together anymore, follow these steps:

1. Log on to the management server with the administrator or root privileges.
2. Go to the directory `%ovinstalldir%bin` or `/opt/OV/bin`.
3. Run the following command:

```
ovconfchg -ovrg server -ns depl -set INCLUDEUPDATES false
```

Reverting to the HP Operations Agent 11.11

After installing the HP Operations Agent 11.16, if you want to revert to HP Operations Agent 11.11, you can do so by removing the agent from the node. See "Removing the HP Operations Agent 11.16 Patch"

on page 64 for more details.

Stopping Unnecessary Processes

If you do not want to use all the components of the HP Operations Agent, you can run specific commands to stop unnecessary processes. Stopping unnecessary processes is useful when you are upgrading only from the HP Operations Agent, HP Performance Agent, or HP GlancePlus and you do not want to use the other components of the HP Operations Agent

When you are upgrading from the HP Operations Agent 8.xx only

In this scenario, you can stop the `rtmd` process if you do not want to use the Performance Collection Component and RTM.

The simplest way to stop the `rtmd` process is running the `ovc -stop rtmd` command. However, the `rtmd` process starts running again when you restart the system. Therefore, it is important to unregister the process from the `control` component instead of just stopping its operation.

Perform the following steps to unregister the **rtmd** process:

1. Log on to the node as root or administrator.
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:

   ovcreg -del rtmd

The command stops the **rtmd** process and unregisters the **rtmd** process from the `control` component.

When you are upgrading from the HP Performance Agent 4.7 and above

In this scenario, you can stop the **rtmd** process if you do not want to use RTM.

The simplest way to stop the **rtmd** process is running the `ovc -stop rtmd` command. However, the **rtmd** process starts running again when you restart the system. Therefore, it is important to unregister the process from the `control` component instead of just stopping its operation.

Perform the following steps to unregister the `rtmd` process:

Log on to the node as root or administrator.

1. Go to the following directory:

   On Windows:

   %ovinstalldir%bin

   On HP-UX, Linux, or Solaris:

   /opt/OV/bin

On AIX:

/usr/lpp/OV/bin

2. Run the following command:

   ovcreg -del rtmd

The command stops the **rtmd** process and unregisters the **rtmd** process from the `control` component.

When you are upgrading from HP GlancePlus 5.0 only

HP GlancePlus does not require the **ovc** process. When you want to run only HP GlancePlus (and no other components of the HP Operations Agent 11.00), follow these steps:

1. Log on to the node as root.
2. Go to the following directory:

   On HP-UX, Linux, and Solaris:

   `/opt/OV/bin`

   On AIX:

   `/usr/lpp/OV/bin`
3. Run the following command stop all agent processes (including processes for the Performance Collection Component):

   `opcagt -kill`

   This command stops all HP Operations Agent processes.
4. Run the following command to restart the `midaemon` process:

   On HP-UX, Linux, and Solaris:

   /opt/perf/bin/midaemon

   On AIX:

   /usr/lpp/perf/bin/midaemon
5. Run the following command to restart the `perfd` process:

   On HP-UX, Linux, and Solaris:

   /opt/perf/bin/perfd

   On AIX:

   /usr/lpp/perf/bin/perfd

   The **ovc** process is already stopped by the command that was run in step 3. However, the `ovc` process will start running again when you restart the system.

   Run the following command to prevent the **ovc** process from starting its operation when the system is restarted:

   On HP-UX, Linux, and Solaris:

   /opt/OV/bin/ovconfchg -ns ctrl -set START_ON_BOOT false

   On AIX:

   /usr/lpp/OV/bin/ovconfchg -ns ctrl -set START_ON_BOOT false

   The **ovc** process does not start anymore after you restart the system.

Perform step 6 through step 8 to prevent the Performance Collection Component from starting its operation when the system is restarted

6. Go to the following location:

   On Linux:

   /etc/sysconfig

   On HP-UX:

   /etc/rc.config.d

   On Solaris and AIX:

   /etc/default

7. Open the **ovpa** file with a text editor.
8. Set the variable `OVPA_START` to 0, and then save the **ovpa** file

If the **ttd** process does not start after you restart the system, run the following command:

On HP-UX, Linux, and Solaris:

```
/opt/perf/bin/ttd
```

On AIX:

```
/usr/lpp/perf/bin/ttd
```

Stopping Operations agent Processes

With the current version, if you want to stop all the processes of the HP Operations Agent and HP Performance Agent, you can run a single command (`opcagt -kill`) to stop all the processes.

Note: The DSI and ARM applications may have dependency on **midaemon** or **ttd** processes. There might be an impact on these applications if you use (`opcagt -kill`) command.

Follow the steps to stop all the processes:

1. Log on to the node as root.
2. Go to the following directory:

   On Windows:

   `%ovinstalldir%bin`

   On HP-UX, Linux, and Solaris:

   `/opt/OV/bin`

   On AIX:

   `/usr/lpp/OV/bin`

3. Run the following command to stop all agent processes (including processes for the HP Performance Agent):

   On Windows:

   `opcagt -kill`

   On UNIX:

```
./opcagt –kill
```

This command stops all HP Operations Agent processes including **midaemon** and **ttd** processes.

Note: As **ttd** process is stopped, any ARM-instrumented applications that are running must also be stopped before you restart **ttd** process.

Chapter 8: Installing Infrastructure SPIs

Prerequisites for Installing the Infrastructure SPIs

Hardware and Software Requirement:

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

Install Infrastructure SPIs 11.16 Patch Only

Follow the steps:

1. Make sure that you have downloaded the HP Infrastructure SPIs 11.16 patch .ISO file.
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.

Log File

You can view the patch log file (`oapatch.log`) in the following location:

On Windows:

```
%OvDataDir%shared\server\log\oapatch.log
```

On UNIX/Linux:

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

Verifying the Installation

After installing, review the contents of the installation log file `oapatch.log`. If the installation is successful, the file must be error-free and must display the messages near the end of the file.

Chapter 9: 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 Installing the HP Operations Agent 11.16" on page 35. 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	64-bit	packages/AIX/AIX_powerpc64

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

- "Import the HP Operations Agent Software" below
- "Create a Software Policy " on the next page
- "Attach the Software Policy to a Device or Server" on page 51

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 52.

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" below
- "Attach from Devices list" on the next page

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.

Chapter 10: 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 Installing the HP Operations Agent 11.16" on page 35.

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

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 11: 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 Installing the HP Operations Agent 11.16" on page 35. The target node where you are installing HP Operations agent must always be added to communicate with Red Hat Network (RHN) Satellite server.

Note: When you upgrade from the HP Operations agent 8.60 to 11.1x, ensure that you uninstall HP Operations Agent 8.60 using the `opc_inst.sh -r` command and then install the HP Operations Agent 11.1x using the Red Hat Network Satellite server.

To obtain platform specific packages from the HP Operations Agent media, browse the media to the specific package location. The following table lists the platform-specific packages to be obtained from the media.

Operating System	Architecture	Packages
Linux	Linux2.6 x64	packages/LIN/Linux2.6_X64 patches/<OALIN_00044>/Linux2.6_X64
	Linux2.6 x86	packages/LIN/Linux2.6_X86 patches/<OALIN_00044>/Linux2.6_X86
	Linux2.6 PPC64	packages/LIN/Linux2.6_PPC64 patches/<OALIN_00044>/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 the next page
2. "Create the Setup on the Target Node " on the next page
3. "Deploy the Packages on the Target Node" on page 59

To remove the packages from the target node, see "Remove the Packages from the Target Node " on page 60

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 and mount it to your desired location.
2. To obtain the Linux packages, browse to the **packages** folder and select **Lin**.
3. Collect and unzip all the gzip files from media using the **– N** option.

   Note: Make sure to repeat the step 2 to step 4 for patches/ OALIN_00044 folder.

4. 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 the 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 (oa.repo)**.

   For example, create a file `/etc/yum.repos.d/`<oa.repo>.

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

3. Update the contents of the file and specify the location (`baseurl`) where 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.

   gpgcheck is the additional check to verify the RPMs. To disable this additional check, set the value as 0.

   OR

   Use the content if you want to verify the RPMs with the public key.

[oa]

Name=**Operations Agent**

baseurl=System_name/SDR/downloads/Extras/RedHat/6Server/x86_64/current/operation-agent/<*Agent RPMs location*>

gpgcheck=1

gpgkey=file://<path of hpPublicKey.pub>

In this instance:

<*Name*> is the product name.

<*baseurl*> is the location where agent package is available.

gpgcheck is the additional check to verify the RPMs. To enable this additional check, set the value as **1**.

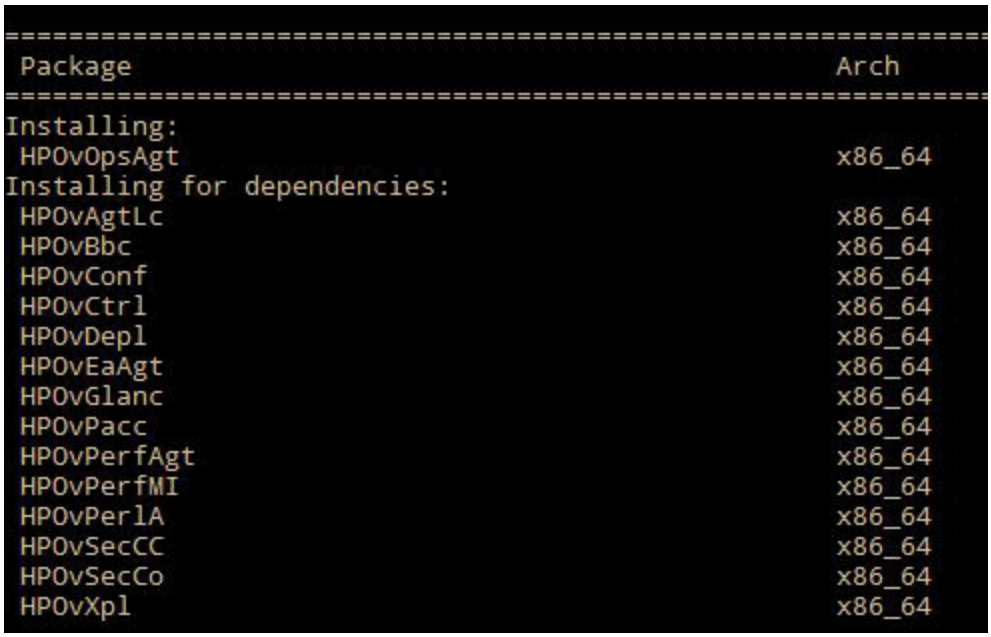
gpgkey is the path to get the HP public key. This is key is only required if you need additional security.

Deploy the Packages on the Target Node

Follow these steps:

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

   Note: All the dependent agent RPMs will be installed.



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.

Remove the Packages from the Target Node

You can remove the packages by using either the `YUM` command or *oainstall.sh* program.

Using YUM Commands to remove the packages

Run the command to remove the package or the specific RPMs only

```
yum remove <package name>
```

Note: Make sure that you install *yum-plugin-remove-with-leaves* to remove all the Operations agent packages by using a single command.

Run the command to remove Operations agent completely:

```
yum remove --remove-leaves HPOvOpsAgt HPOvSecCo
```

Using oainstall.sh program to remove the packages

Run the command: `/opt/OV/bin/OpC/install/oainstall.sh -r -a`

Chapter 12: Installing the HP Operations agent on Platforms Supported with Limitation

See the HP Operations Agent *Support Matrix* document for more details on platforms supported with limitation.

The installer may fail to install the HP Operations Agent on platforms supported with limitation. You may see the following error when you try to install the agent on such platforms:

```
The product bundle selected may not yet be supported on this node
```

To install the HP Operations Agent on such nodes, you must run the installer with the **-minprecheck** option along with the **-i** and **-a** options.

Examples

To install the HP Operations Agent 11.16 on a Windows system, run the following command:

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

To install the HP Operations Agent 11.16 on a UNIX/Linux system, run the following command:

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

Install the HP Operations agent on Platforms Supported with Limitation Remotely from the HPOM for Windows Console

To install the HP Operations agent 11.16 remotely from the HPOM for Windows console on platforms supported with limitation, you must perform the following preinstallation tasks on the management server:

1. Log on to the management server as administrator.
2. Go to the directory:
   `%ovdatadir%share\conf\PMAD`
3. Rename the **agent_install_defaults.cfg.sample** file to **agent_install_defaults.cfg**.

   Tip: Take a backup of the **agent_install_defaults.cfg.sample** file.
4. Open the **agent_install_defaults.cfg** file with a text editor and add the following line:

   ```
   [eaagt]
   ```

```
MINPRECHECK=TRUE
```

5. Save the file.

You can now follow the steps in "From the HPOM for Windows Console" on page 42 to install the HP Operations Agent 11.16 remotely from the HPOM console.

Install the HP Operations Agent on Platforms Supported with Limitation Remotely from the HPOM for UNIX Console

To install the HP Operations Agent 11.16 remotely from the HPOM for UNIX console on platforms supported with limitation, you must perform the following preinstallation tasks on the management server:

1. Log on to the management server with the root privileges.
2. Go to the directory:
   `/etc/opt/OV/share/conf/OpC/mgmt_sv`
3. Rename the file **bbc_inst_defaults.sample** to **bbc_inst_defaults**.
4. Open the file ***bbc_inst_defaults*** with a text editor and add the following line:

   ```
   [eaagt]
   MINPRECHECK=TRUE
   ```

5. Save the file.

Follow the steps in "From the HPOM for UNIX Console" (on page 43) to install the HP Operations Agent 11.16 remotely from the HPOM console.

Note: After installing the HP Operations Agent 11.16 using MINPRECHECK, the changes done in the profile file must be reverted. When you install using MINPRECHECK, the version check for the Operating System and Architecture will be skipped.

Install the HP Operations Agent on Platforms Supported with Limitation Remotely Using Command Line

To install the HP Operations Agent 11.16 remotely on platforms supported with limitation:

1. Log on to the management server with root or administrator privileges.
2. Go to the following directory on the management server:

   On Windows:

```
%ovinstalldir%bin
```

On UNIX/Linux:

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

3. Add the following line in a text file:

   ```
   [eaagt]
   MINPRECHECK=TRUE
   ```

4. Run the following command:

   ```
   ovdeploy –install –bundle <path_to_OVO-Agent.xml> –node <node name> –af <path_
   of_profile _file>\<profile_file_name> –1 –configure <profile_file_name>
   ```

The command installs the HP Operations Agent 11.16 on the node.

Chapter 13: Removing the HP Operations Agent

To remove the complete product from For the Windows ®, HP-UX, Solaris, Linux, and AIX operating systems see Removing the HP Operations Agent 11.11 and 11.16 Together.

To remove HP Operations agent and Infrastructure SPIs 11.16 see Removing the HP Operations Agent 11.16.

To remove HP Operations Agent from Linux, see Remove the HP Operations Agent from Linux Nodes.

Removing the HP Operations Agent 11.16 Patch

To remove the HP Operations Agent 11.16 patch only, follow these steps after you log on to the node as root or administrator:

Note: You cannot remove HP Operations Agent 11.16 alone from Linux nodes; you can only remove the complete product (versions 11.11 and 11.16 together) from Linux nodes. Do not follow these steps on Linux nodes. To remove the complete product from Linux nodes, see "Remove the HP Operations Agent from Linux Nodes" on page 66.

1. Go to the following directory:

   On Windows (32-bit systems):

   `%ovinstalldir%bin\OpC\install`

   On Windows (64-bit systems):

   `%ovinstalldir%bin\win64\OpC\install`

   On HP-UX or Solaris

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

   On AIX

   `/usr/lpp/OV/bin/OpC/install`

2. Run the following command to remove the HP Operations Agent 11.16:
   On Windows:
   `cscript oainstall.vbs -r -a -pn OAWIN_00044`

   On HP-UX:

   `./oainstall.sh -r -a -pn OAHPUX_00044`

   On Solaris:

   `./oainstall.sh -r -a -pn OASOL_00044`

On AIX:

```
./oainstall.sh -r -a -pn OAAIX_00044
```

On all platforms other than Linux, uninstallation of the HP Operations Agent 11.16 reinstates the version of the HP Operations Agent 11.11.

On all platforms other than Linux, removing the HP Operations Agent 11.16 reinstates the agent 11.11 on the node.

For information on removing the agent on Linux, see "Remove the HP Operations Agent from Linux Nodes" on the next page.

Remove the HP Operations agent Remotely Using the Command Line

To remove the HP Operations Agent 11.16 from a managed node remotely by using the `ovdeploy` command from the management server, follow these steps:

Note: You cannot remove the HP Operations Agent 11.16 alone from Linux nodes; you can only remove the complete product (versions 11.11 and 11.16 together) from Linux nodes. Do not follow these steps on Linux nodes. To remove the complete product from Linux nodes, see "Remove the HP Operations Agent from Linux Nodes" on the next page.

1. Log on to the management server as root or administrator.
2. Go to the following directory on the management server:

   On Windows:

   `%ovinstalldir%bin`

   On HP-UX, Solaris, and Linux:

   `/opt/OV/bin`
3. Run the following command:

   ```
   ovdeploy -remove -patch <patch-ID>-host <node name>
   ```

   In this instance:

   `<patch-ID>` is the name of the patch ISO file that was downloaded while installing the patch (see ISO file names).

   `<node name>` is the FQDN of the node.

   Note: Do not specify the FQDN of a Linux node. You cannot remove just the HP Operations Agent 11.16 from a Linux node.

On all platforms other than Linux:

On all platforms other than Linux, removing the HP Operations Agent 11.16 reinstates the agent 11.11 on the node.

For information on removing the HP Operations Agent on Linux, see "Remove the HP Operations Agent from Linux Nodes" on the next page.

Remove the HP Operations Agent from Linux Nodes

You cannot remove the HP Operations Agent 11.16 alone from Linux nodes. However, you can remove both the versions of the HP Operations Agent (11.11 and 11.16) together with a single command.

To remove the HP Operations Agent 11.11 and 11.16 from Linux nodes, follow these steps:

1. Log on to the node as root.
2. Go to `/opt/OV/bin/OpC/install`.
3. Run the following command:

   ```
   ./oainstallsh -r -a
   ```

   The command removes both the versions of the HP Operations Agent (11.11 and 11.16).

Reinstall the HP Operations Agent 11.16 on Linux

On Linux systems, you cannot remove just the HP Operations Agent 11.16 with the HP Operations Agent 11.11 still in effect. Uninstallation procedure removes both the versions of the agent (11.11 and 11.16) completely from the Linux system. If you want to install the HP Operations Agent 11.16 again on the same system, do one of the following:

- Install the HP Operations Agent 11.11 and 11.16 together ("Install the HP Operations Agent 11.11 and 11.16 Together").
- Install the HP Operations Agent 11.11 first (follow the instructions in the *HP Operations Agent 11.11 Installation Guide*), and then install the HP Operations Agent 11.16 (see "Install the HP Operations Agent 11.16 on a Node Manually" on page 36).

Removing the Agent with the oacleanall Script

If the installation of the HP Operations Agent is incomplete or unsuccessful, you must always try reinstallation only after uninstalling the agent. If the uninstallation command (`oainstall.sh -r -a` or `cscript oainstall.vbs -r -a`) fails to remove the agent, use the `oacleanall` script.

The `scripts` directory (directory where ISO is extracted or mounted) includes a set of `oacleanall` scripts—one script for each platform. You must choose the appropriate script to bring the system back to its original state. The `oacleanall` script **removes** the agent (11.16 and 11.11) from the system completely and irrecoverably. Use this script only to reverse the effect of an incomplete, unsuccessful, or incorrect installation of the HP Operations Agent.

Note: The oacleanall script is *NOT* recommended to remove the HP Operations Agent on a system running other HP Software products.

The following table lists the commands for all supported platforms.

Operating System	Architecture	Command
Windows	x86	`cscript oacleanall_ Windows_X86.vbs`

Operating System	Architecture	Command
	x64	`cscript oacleanall_ Windows_X64.vbs`
Linux	x86	`./oacleanall_Linux2.6_ X86.sh`
	x64	`./oacleanall_Linux2.6_ X64.sh`
	power (64-bit)	`./oacleanall_Linux2.6_ PPC64.sh`
HP-UX	PA-RISC	`./oacleanall_HP-UX_PA32.sh`
	Itanium	`./oacleanall_HP-UX_IA32.sh`
Solaris	SPARC	`./oacleanall_Solaris_ SPARC32.sh`
	x86	`./oacleanall_Solaris_ X86.sh`
AIX	power (64-bit)	`./oacleanall_AIX_ powerpc64.sh`

Removing the HP Operations Agent 11.11 and 11.16 Together

To remove the HP Operations Agent complete product (versions 11.11 and 11.16) using a single command, follow these steps after you log on to the node as root or administrator:

1. Go to the following directory:

   On Windows (32-bit systems):

   `%ovinstalldir%bin\OpC\install`

   On Windows (64-bit systems):

   `%ovinstalldir%bin\win64\OpC\install`

   On HP-UX or Solaris:

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

   On AIX:

   `/usr/lpp/OV/bin/OpC/install`
2. Run the following command to remove the agent:

   On Windows:

   `cscript oainstall.vbs -r -a`

   On UNIX/Linux:

```
./oainstall.sh -r -a
```

The command removes the HP Operations Agent (11.11 and 11.16 together) from the node. After uninstallation, the complete data directory remains on the system (on Windows: `%ovdatadir%`; on UNIX/Linux: `/var/opt/OV`).

Alternatively, if you do not want to retain the data files on the system, run the following command:

On Windows:

```
cscript oainstall.vbs -r -a -clean
```

On UNIX/Linux:

```
./oainstall.sh -r -a -clean
```

The command removes the HP Operations Agent (11.11 and 11.16 together) from the node. After uninstallation, only the following files remain on the system:

On Windows:

```
%ovinstalldir%inventory\Operations-Agent.xml
%ovdatadir%log\oainstall.log
%ovdatadir%log\oainstall.bin
```

On HP-UX, Linux, and Solaris:

```
/opt/OV/inventory/Operations-Agent.xml
/var/opt/OV/log/oainstall.log
/var/opt/OV/log/oainstall.bin
```

On AIX:

```
/usr/lpp/OV/inventory/Operations-Agent.xml
/var/opt/OV/log/oainstall.log
/var/opt/OV/log/oainstall.bin
```

Chapter 14: Removing 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`

   The command removes Infrastructure SPIs version 11.11 and 11.16 patch installed on the management server.

   `cscript oainstall.vbs -r -m -spiconfig - removepatch`

   The command removes the highest Infrastructure SPIs patch version installed on the management server.

   `cscript oainstall.vbs -r -m -spiconfig - removeallpatch`

   The command removes all Infrastructure SPIs patches installed on the management server.

   On UNIX/Linux:

   `./oainstall.sh -r -m -spiconfig`

   The command removes Infrastructure SPIs version 11.11 and 11.16 patch installed on the management server.

   `./oainstall.sh -r -m -spiconfig -removepatch`

   The command removes the highest Infrastructure SPIs patch version installed on the management server.

   `./oainstall.sh -r -m -spiconfig - removeallpatch`

   The command removes all Infrastructure SPIs patches installed on the management server.

Note: In an HA cluster, perform the above steps on the active node first, and then on all nodes in the cluster.

Chapter 15: 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 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 HP Operations 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, auto deployment, and certificates.
- You must not install HP Operations 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.

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" above) 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" above) on the virtual node created for the cluster.

To monitor cluster-aware applications on the nodes in an HA cluster, follow these steps:

1. *Microsoft Cluster Server clusters only.* Make sure that the resource group, which contains the resource being monitored, contains both a network name and an IP address resource.
2. Identify the policies that you will require to monitor the cluster-aware application.
3. Create an XML file that describes the cluster-aware application, and name it **apminfo.xml**.
4. This file is used to define the resource groups that will be monitored and to map the resource groups to application instances.
5. The **apminfo.xml** file has the following format:

   Note: New lines are not allowed between package tags in the **apminfo.xml** file.

```
<?xml version="1.0"?>
 <APMClusterConfiguration>
 <Application>
 <Name>Name of the cluster-aware application.</Name>
 <Instance>
 <Name>Application's name for the first instance. The instance name is
used for start and stop commands and corresponds to the name used to
designate this instance in messages.</Name>
 <Package>Resource group in which the application's first instance
runs.</Package>
 </Instance>
 <Instance>
 <Name>Application's name for the second instance.</Name>
 <Package>Resource group in which the application's second instance
runs.</Package>
 </Instance>
 </Application>
 </APMClusterConfiguration>
```

   DTD for apminfo.xml

```
<!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"?>
<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, and Solaris: `/opt/OV/bin/ovappinstance -vc`

On AIX: `/usr/lpp/OV/bin/ovappinstance -vc`

Note: *Optional.*

For some physical nodes, for example for multi-homed 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:

1. Obtain the name of the physical node as it is known in the cluster configuration:

   `ovclusterinfo -a`
2. Configure the agent to use the name of the node as it is known in the cluster configuration:

   `ovconfchg -ns conf.cluster -set CLUSTER_LOCAL_NODENAME <name>`

   In this instance, `<name>` is the name of the node as reported in the output of `ovclusterinfo -a` and is case-sensitive.
3. Restart the agent on every physical node by running the following commands:

   `ovc -stop`

   `ovc -start`

Agent User

By default, the HP Operations Agent regularly checks the status of the resource group. On UNIX and Linux nodes, the HP Operations Agent use cluster application-specific commands, which can typically only be run by root users. On Windows nodes, the HP Operations Agent 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 HP Operations Agent to use a security program (for example, sudo or .do) when running cluster commands.

To configure the HP Operations Agent running with a non-root account to run cluster commands, follow these steps:

1. Run the following command to stop the HP Operations 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 16: Configuring 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).

Note: In an environment with multiple management servers, you can also configure the management servers to communicate with one another through firewalls. The configuration is the same as for communication between management servers and nodes.

Before You Begin

Skip this section if you are using the 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 an HTTP proxy.

The management server opens connections to the proxy server, for example to deploy policies and instrumentation, for heartbeat polling, or to launch actions. The proxy server opens connections to the node on behalf of the management server, and forwards communication between them.

The node opens connections to the proxy server, for example to send messages, and action responses. The proxy server opens connections to the management server on behalf of the node.

You can also redirect communication through proxies in more complex environments as follows:

- Each management server and node can use a different proxy server to communicate with each other.
- You can configure management servers and nodes to select the correct proxy according to the host they need to connect to.

The figure below shows connections between a management server and nodes through multiple proxies as follows:

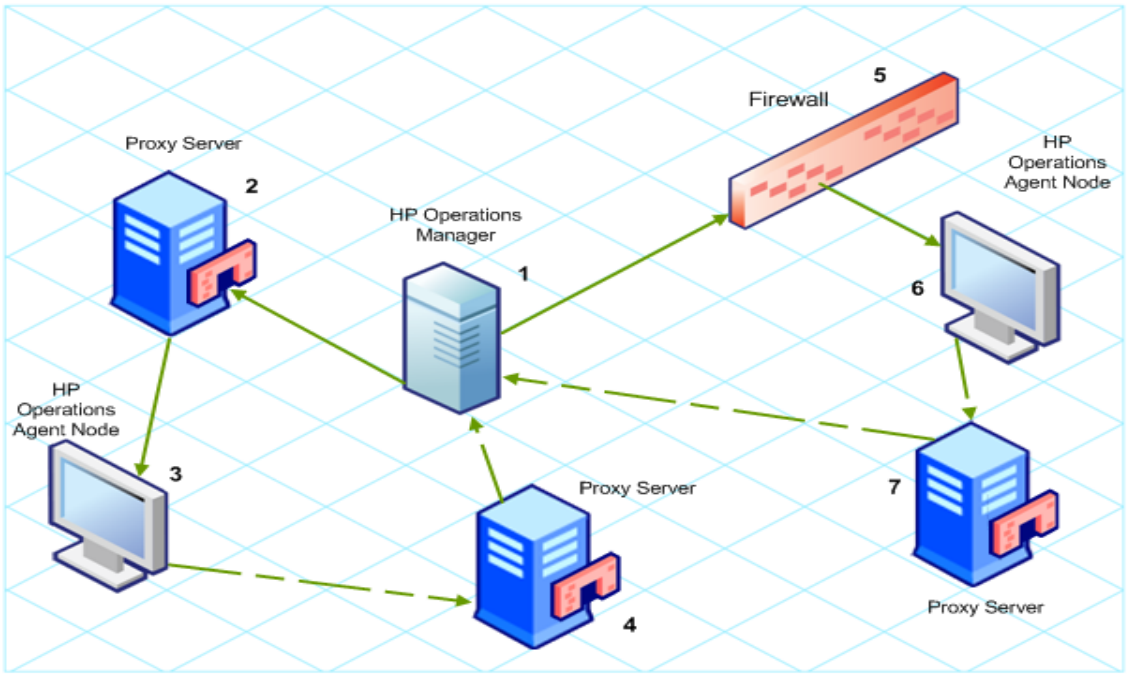
The management server (1) opens connections to a proxy (2). The proxy opens connections to the node (3) on behalf of the management server.

The node (3) opens connections to a different proxy (4). The proxy opens connections to the management server (1) on behalf of the node.

The network allows management server (1) to make outbound HTTP connections directly through the firewall (5) to another node (6). (The nodes (3, 6) are on different networks.)

The firewall (5) does not allow inbound HTTP connections. Therefore, node (6) opens connections to the management server through a proxy (7).

Communication Using Proxies



PROXY Parameter Syntax

You redirect outbound HTTPS communication through proxies by setting the PROXY parameter in the `bbc.http` namespace 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 *HP Operations Agent and Infrastructure SPIs Installation guide 11.11*. 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
```

Configuring backup proxies

The proxy configuration entry in the `bbc.http` namespace supports backup proxies. If the connection from the host to a proxy server fails, backup proxy servers can be configured for that host using the following format:

```
[bbc.http]
```

```
PROXY=<proxy1>:<port>|<proxy2>:<port>|<proxy3>:<port>+(hostname)
```

where <proxy1>, <proxy2> and <proxy3> are the IP addresses of the proxy server.

For example:

```
PROXY=<IP1>:<port>|<IP2>:<port>|<IP3>:<port>+(hostname.domain.com)
```

In this instance:

<IP1>, <IP2> and <IP3> are the proxy IP addresses.

<IP2> and <IP3> are the backup proxy servers for <IP1>.

If there is a failure to connect to <IP1> then <IP2> is used. If <IP2> also fails, <IP3> is used.

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
<proxies> <proxy> <server> server1.domain.example.com:8080 </server> <for> <target>*.domain2.example.com</target> </for> </proxy> </proxies>	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.
<proxies>	The server server2.domain.example.com

Examples of the Proxy Configuration File, continued

Syntax	Description
<proxy> <server> server2.domain.example.com:8080 </server> <for> <target>*.domain2.example.com</target> <target>192.168.2.*/target> </for> </proxy> <proxy> <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>	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. 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.

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\bbc

   On UNIX/Linux:

```
/var/opt/OV/conf/bbc
```

6. Run the following command:

   On Windows:

   ```
   %ovinstalldir%bin\ovconfchg -ns bbc.http -set PROXY_CFG_FILE <filename>.xml
   ```

   On HP-UX, Linux, or Solaris:

   ```
   /opt/OV/bin/ovconfchg -ns bbc.http -set PROXY_CFG_FILE <filename>.xml
   ```

   On AIX:

   ```
   /usr/lpp/OV/bin/ovconfchg -ns bbc.http -set PROXY_CFG_FILE <filename>.xml
   ```

Note: You can verify the configuration using `bbcutil -gettarget <host name or IP address of the node>`.

Configuring the Communication Broker Port

By default, the 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` namespace 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 host1:583[,host2:683]
```

To configure the communication broker to listen on a non-default port using the SERVER_ PORT variable

To configure the communication broker to listen on a non-default port, change the SERVER_PORT variable value in the `bbc.cb` namespace.

Run the following command to set different values to the SERVER_PORT variable:

```
ovconfchg -ns bbc.cb -set SERVER_PORT <value>
```

In this instance, `<value>` is the value you want to assign to the SERVER_PORT variable.

Note: When you change the value of the SERVER_PORT variable, the communication broker restarts automatically and listens on the specified new port value.

Configuring Local Communication Ports

By default, management servers and nodes use local port 0 for outbound connections, which means that the operating system allocates the local port for each connection. Typically, the operating system will allocate local ports sequentially. For example if the operating system allocated local port 5055 to an

Internet browser, and then the HTTPS agent opens a connection, the HTTPS agent receives local port 5056.

However, if a firewall restricts the ports that you can use, you can configure management servers and nodes to use a specific range of local ports instead.

CLIENT_PORT Parameter Syntax

You configure local communication ports by setting the CLIENT_PORT parameter in the `bbc.http` namespace 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 *HP Operations Agent and Infrastructure SPIs Installation guide 11.11*. 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 5000 - 6000
   ```

   When you use the command `ovconfchg` on a management server that runs in a cluster, add the parameter -ovrg <*server*>.

Configuring Nodes with Multiple IP Addresses

If the node has multiple IP addresses, the agent uses the following addresses for communication:

The communication broker accepts incoming connections on all IP addresses.

The agent opens connections to the management server using the first network interface that it finds through the OS provided libraries.

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

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>
   ```

Note: See *"Overview of Node Resolution"* in the *HP Operations Agent User Guide* for more information on node name resolution.

Configuring HTTPS Communication through Proxies

If your network allows only certain proxy systems to open connections through the firewall, you can redirect HPOM communication through these proxies. The following list presents the workflow of the management server and agent communication with this configuration:

1. The management server opens connections to the proxy.
2. The proxy opens connections to the node on behalf of the management server, and forwards communication between them.
3. The node opens connections to the proxy.
4. The proxy opens connections to the management server on behalf of the node.

To redirect the communication through proxies:

1. Log on to the management server or node with the root or administrative privileges.
2. Run the following command at the command prompt:

   ```
   ovconfchg -ns bbc.http -set PROXY <proxy>:<port>
   ```

In this instance, `<proxy>` is the IP address or FQDN of the proxy server; `<port>` is the communication port of the proxy server.

Note: When you use the command `ovconfchg` on a management server that runs in a cluster, add the parameter `-ovrg <server>`.

Communication in a Highly Secure Environment

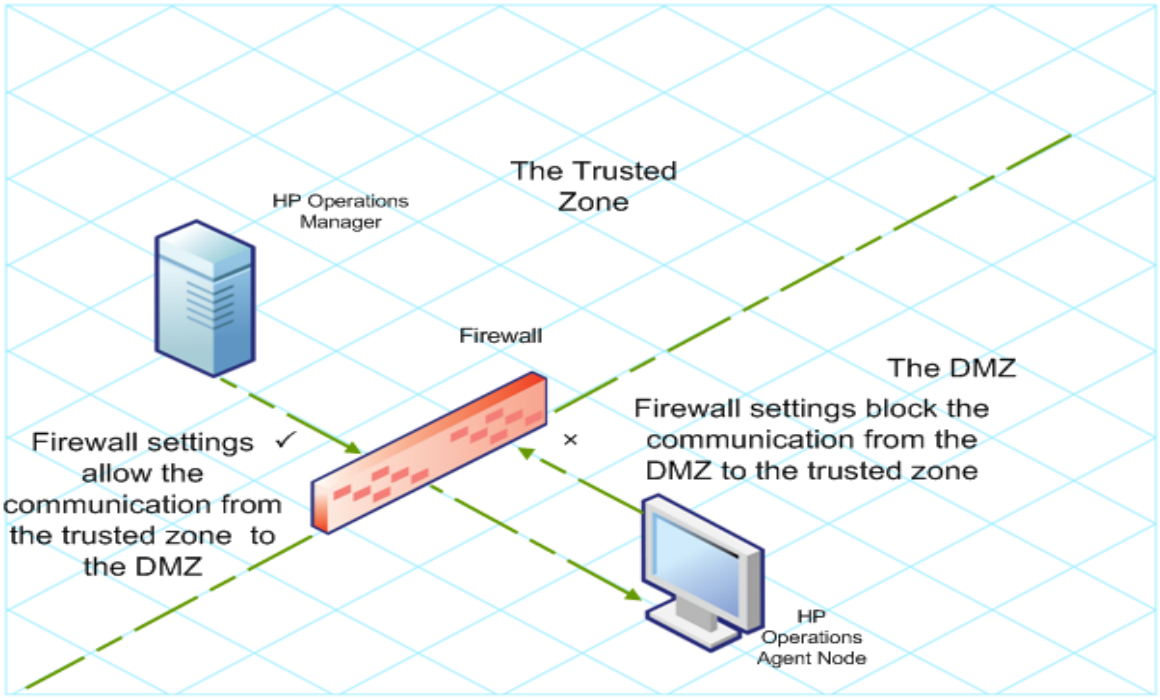
In a firewall-controlled, secure environment, systems that are present within the trusted zone can freely communicate and exchange information with one another. However, specific firewall settings can

restrict communication with the systems that belong outside the trusted zone. The untrusted network, also known as the demilitarized zone (**DMZ**), may not send data to the trusted zone due to restrictions in firewall settings.

In many deployment scenarios, the HPOM 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.

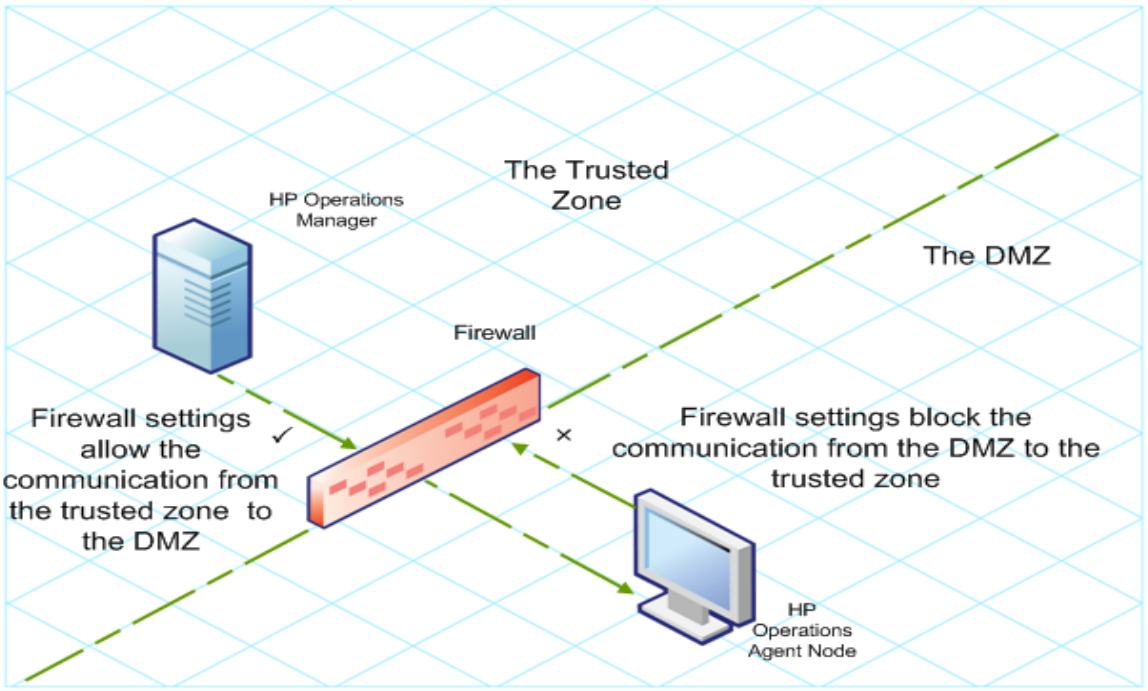
In the following scenario, managed nodes are located in the DMZ while the management server belongs to the trusted zone. The firewall settings in this example allow outbound-only communication. Therefore, inbound communication to the management server is blocked by the firewall.

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**).

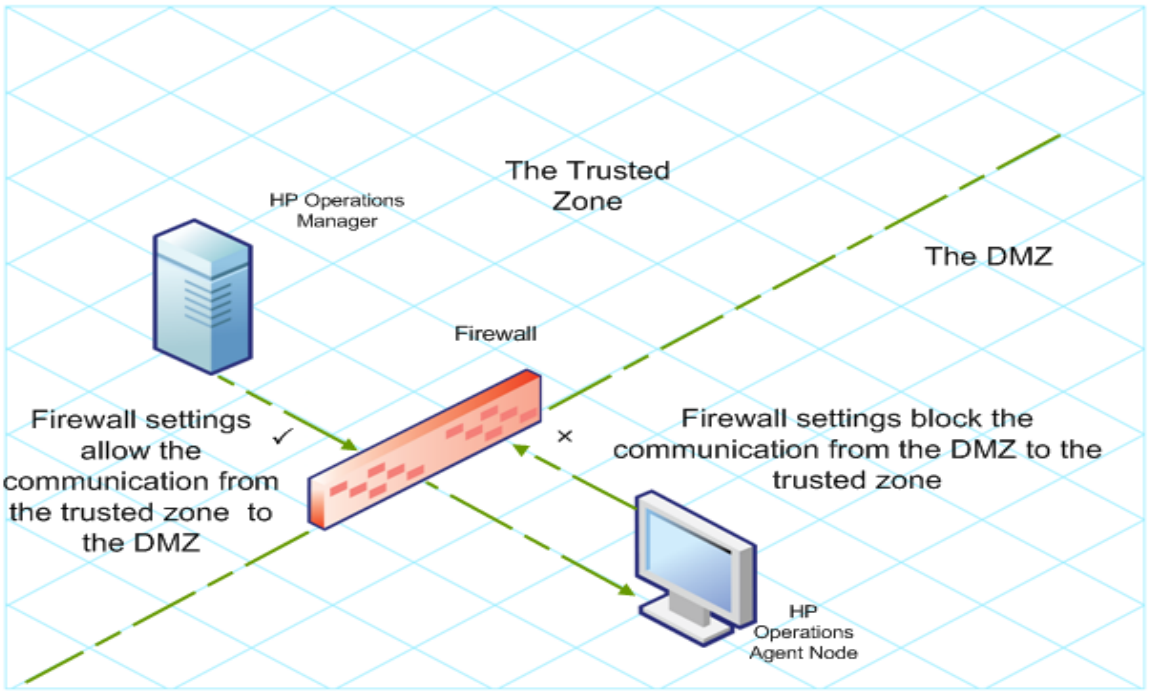
Note: On Windows, after agent installation, the firewall configuration changes when **HP Software HTTP Communication Broker** is added to the firewall inbound rules.

Systems belonging to the DMZ open connection to the RCP instead of the system inside the trusted zone. You can configure the system in the trusted zone to open an outbound communication channel—the reverse administration channel—to the RCP. The system in the trusted zone maintains the outbound channel; systems in the DMZ uses the reverse administration channel to send details to the trusted zone by using the RCP.

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

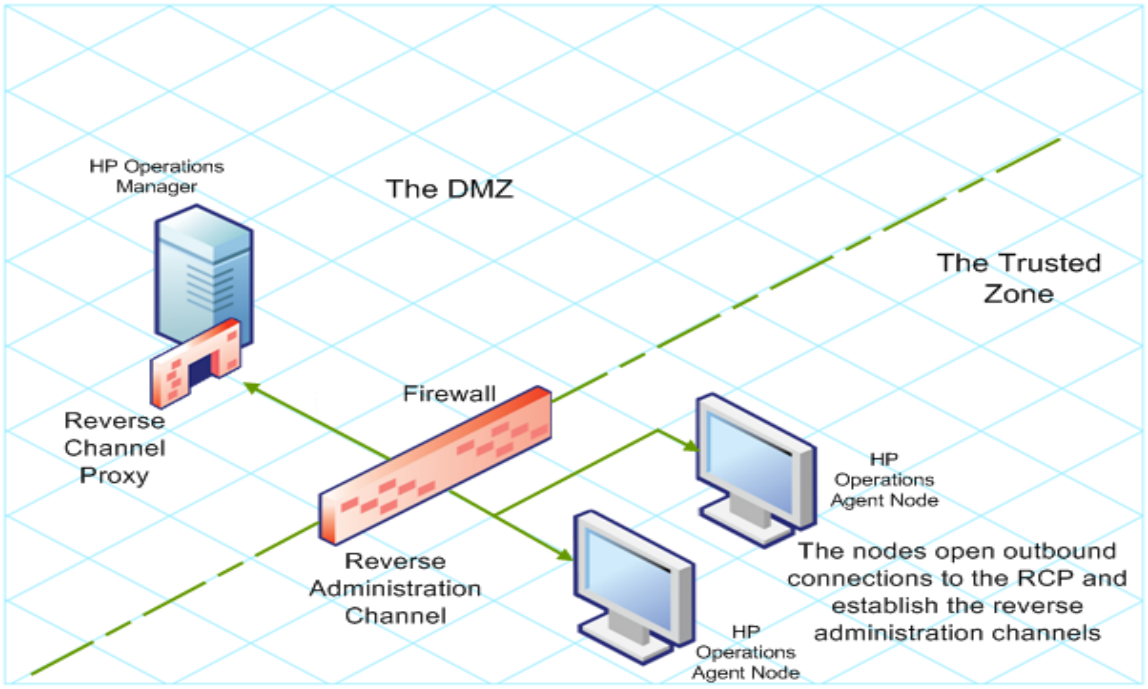
Secure Communication through the RCP with Nodes in the DMZ



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. To resolve this problem, follow the steps:

a. Create the directory named `etc` under `/var/opt/OV`

b. Copy the relevant configuration files (for example, files such as **resolv.conf**, **hosts**, **nsswitch.conf**) from `/etc` to `/var/opt/OV/etc`.

c. Alternatively, you can also disable the **ovbbccb chroot** feature by running the following command. This method resolves the problem of preventing ovbbccb from creating connections to the RCP.

```
ovconfchg -ns bbc.cb -set CHROOT_PATH /
```

5. Register the RCP component so that ovc starts, stops and monitors it. Type the following commands:

```
ovcreg -add <install_dir>/newconfig/DataDir/conf/bbc/ovbbcrcp.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 `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; ovbbcrcp 11.00.000
system2.mydomain.com:1025 BBC 11.00.000; ovbbcrcp 11.00.000
system3.mydomain.com:1025 BBC 11.00.000; ovbbcrcp 11.00.000
system4.mydomain.com:1025 BBC 11.00.000; ovbbcrcp 11.00.000
```

In this example, the system has established reverse administration channels to the following RCP systems: system1, system2, system3, and system4.

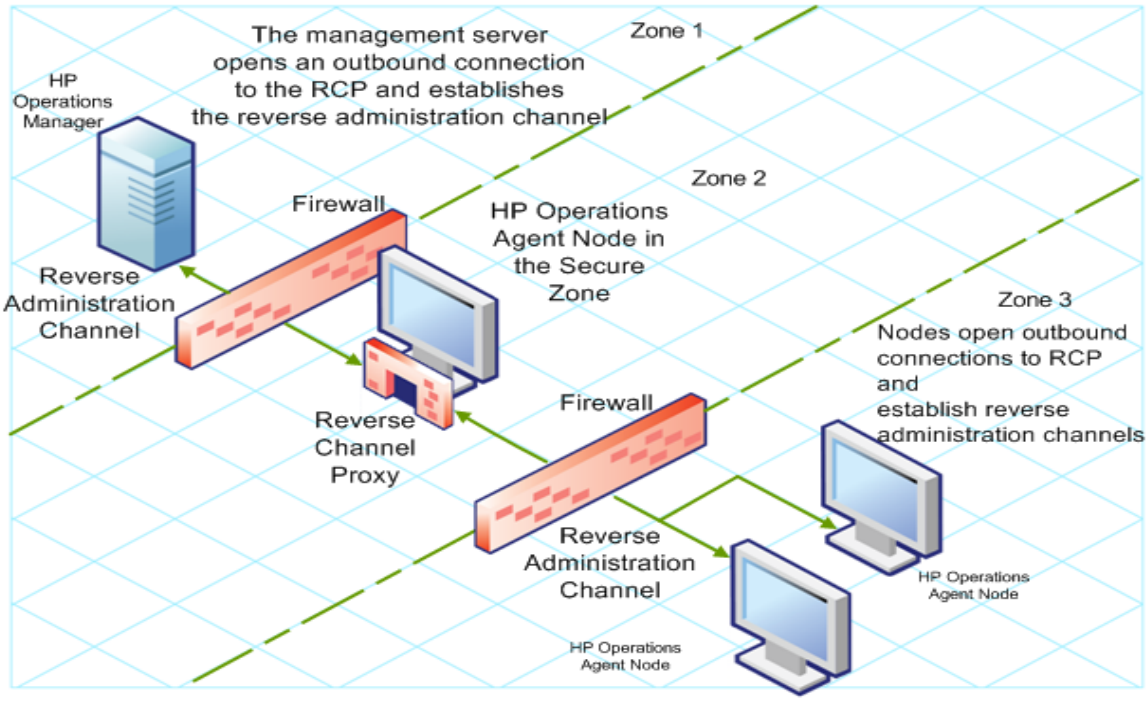
If the reverse administration channel to an RCP fails, the `ovbbccb -status` command displays the status in the following format:

```
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 17: Configuring Certificates for the HP Operations Agent and Infrastructure SPIs

Certificates must be installed on all managed nodes to facilitate network communication using the Secure Socket Layer (SSL) protocol with encryption. Certificates enable the nodes to communicate securely with the management server and other nodes.

The management server issues certificates to nodes and acts as the certificate authority. Each managed node needs the following certificates from the management server:

A unique node certificate: The node can identify itself to its management server and other nodes by sending them its node certificate.

A copy of the management server's trusted certificate: A node only allows communication from a management server if it has the trusted certificate for that management server.

In an environment with multiple management servers, a copy of the trusted certificates for all other management servers must be present on the node.

To enable the nodes to communicate securely in the HPOM-managed environment by using certificates, you must install certificates after you install the HP Operations 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 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 preparing the profile file, see the *HP Operations Agent and HP Operations Smart Plug-ins for Infrastructure Installation Guide, version 11.11*.

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 preparing the profile file, see the *HP Operations Agent and HP Operations Smart Plug-ins for Infrastructure Installation Guide, version 11.11*. 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>]
```

Chapter 18: Troubleshooting

While installing the HP Operations Agent 11.16, you may experience certain problems. This section helps you troubleshoot such problems and provides you with information to help you avoid problems from occurring.

Installation

Installation Fails on a Windows Node with the Error "MSI version is less than 4.5"

Installation of the HP Operations Agent 11.16 on a Windows node fails with the following message in the command line console (as well as in the `oapatch.log` file):

```
[FAIL ] Check if MSI engine version is 4.5 or higher. MSI version is less than 4.5, installation not supported,update to Service Pack 2
```

Solution:

1. Go to the `patches\OAWIN_00044` directory on the HP Operations Agent 11.16 media.
2. Go to one of the following directories depending on the architecture of the Windows node:
   - For Itanium nodes: `Windows_IA64`
   - For x64 nodes: `Windows_X64`
   - For x86 nodes: `Windows_X86`
3. Run one of the following commands depending on the architecture of the Windows node:
   - For Itanium nodes: `wusa Windows6.0-ia64.msu /quiet /norestart`
   - For x64 nodes: `wusa Windows6.0-x64.msu /quiet /norestart`
   - For x86 nodes: `wusa Windows6.0-x86.msu /quiet /norestart`

   Tip: Alternatively, you can double-click the ***.msu** file.
4. Restart the system.
5. Install the HP Operations Agent again.

Deployment Package for a Platform is Downgraded to the Version 8.x

This scenario is seen on a management server where you installed the HP Operations Agent 11.16 deployment package only for select platforms (and not for all the five platforms).

You might see that the 11.16 deployment package is automatically downgraded to the version 8.x after performing the following operations:

1. Removing the agent 11.11 deployment package for a platform that was not updated with the agent 11.16
2. Installing the agent 11.11 deployment package again for the same platform

Solution:

After installing the agent deployment package 11.16 for a platform, if you want to remove and reinstall the agent 11.11 deployment package for another platform, make sure you do the following at the time of reinstallation:

1. Copy the `oainstall.vbs` or `oainstall.sh` script from the directory where you extracted or mounted the agent 11.16 ISO file.
2. Place the copied `oainstall.vbs` or `oainstall.sh` script into the directory where you extracted or mounted the agent 11.11 ISO file.
3. Copy the `scripts` sub-directory from the directory where you extracted or mounted the agent 11.16 ISO file.
4. Place the copied `scripts` sub-directory into the directory where you extracted or mounted the agent 11.11 ISO file.
5. Now start reinstalling the agent 11.11 deployment packages. After installation, an already-installed instance of the agent 11.16 deployment package does not get automatically downgraded to the version 8.x anymore.

Remote Installation of the Agent from the HPOM for Windows Console Fails

Installation of the agent (11.11 and 11.16 together) from the HPOM for Windows console fails; the `oapatch.log` file is not created. The following error message appears in the HPOM console:

```
(PMD1240) Cannot deploy package 'Operations-agent' to node <node_name>. The agent
API returned the following errors:

(depl81) Unable to deploy OVO-Agent.xml to node <node_name>

(depl81) Unable to deploy oasetup to node <node_name>
```

The installation mechanism first transfers and installs the packages for the agent 11.11 on the node, and then triggers the installation of the agent 11.16 packages. This failure occurs if the agent tries to start its processes on the node even before the installation of the agent 11.16 is complete.

Solution:

1. On the HPOM management server, set the `SELFPATCHUPLOADRETRYLIMIT` variable to a higher value. For example, if you set `SELFPATCHUPLOADRETRYLIMIT` to 90 it will increase the timeout period by 90 seconds till the agent tries to start its processes on the node. Run the following command on the management server to set this variable to a value of your choice:

   ```
   ovconfchg ovrg -server -ns depl -set SELFPATCHUPLOADRETRYLIMIT<value>
   ```
2. Try to install the agent 11.11 and 11.16 together again from the HPOM console.

Disk Space Check Fails on HP-UX

On HP-UX nodes, prerequisite check fails although adequate disk space is available for the installation and data directories.

One of the following error messages appears in the command-line console:

- `Not enough disk space on /opt`
- `Not enough disk space on /var`

If the name of the file system for the `/opt` or `/var` directory is too long, the installer cannot perform the disk space check correctly.

Solution:

Apply the hotfix QCCR1A126636. Contact HP Support to obtain this hotfix.

Note: A similar problem exists with the installer for the HP Operations Agent 11.11. If you are installing the agent 11.11 and 11.16 together, obtain the hotfix QCCR1A123980 as well from HP Support.

Error Messages Appear in the "status.perfalarm" File After Installing the Agent with the "syncwpar" Command

On AIX systems, after you install the HP Operations Agent by using the syncwpar command, the following error messages appear in the status.perfalarm file (in the /var/opt/perf/log directory):

```
ERROR: Connection to localhost failed ((bbc-42) Unable to connect to the OV
Communication Broker.Update to Service Pack
```

Solution:

Start the ovc process by running the following command:

```
/usr/lpp/OV/bin/ovc -start
```

Reinstallation of the Agent Fails on Windows

Reinstallation of the agent (11.11 or 11.16) on Windows fails with the following error:

```
The service 'lanmanserver' is not running on the system. This service is required
to run this tool.
```

Solution:

Restart the Server service (service name: lanmanserver) from the Services window:

1. At the Run prompt, type **services.msc**, and then press **Enter**.
2. In the Services window, right-click **Server**, and then click **Restart**.

Remote Installation from the HPOM Console Fails on Windows 7 x64 Nodes

Remote installation of the HP Operations Agent from the HPOM console fails on Windows 7 x64 nodes with the following error:

```
REQCHK8016 The platform/OS version on node <node_name> is not yet supported -
please consult the latest support matrix; if platform is supported ignore
prerequisite check and check prerequisites manually
```

Solution:

Clear the **Run prerequisites check automatically before deployment** option while installing the agent from the HPOM console.

Installation of the Infrastructure SPIsFails on HPOM for Solaris Management Server with the Error "XMLin() requires eitherXML::SAX or XML::Parser"

Installation of the Infrastructure SPIs fails with the following message:

```
XMLin() requires either XML::SAX or XML::Parser at ./scripts/oaproductinstall.pl
line 402
```

Solution:

Ensure that the **libgcc_s.so.1** library is present on Solaris system while registering the HP Operations Agent on the Management Server.

Upgrading from 8.60 to 11.1x fails using Red Hat Network Satellite Server

The HP Operations Agent 8.60 was not supported with the `yum` installation, hence upgrading HP Operations Agent from 8.60 to 11.1x fails using the Red Hat Network Satellite Server.

Solution:

1. Uninstall the HP Operations Agent 8.60 using the `opc_inst.sh -r` command.
2. Install the HP Operations Agent 11.1x using the Red Hat Network Satellite Server.

Installation of the third-party rpm fails on SLES 11 SP2 after installing the HP Operations Agent

The installation of the third-party RPM package fails after installing the HP Operations Agent on SLES 11 SP2 with the following error:

```
insserv: warning: script '<Script_Name>' missing LSB tags and overrides

insserv: Default-Start undefined, assuming default start runlevel(s) for script
`<Script_Name>'

insserv: Stopping <Script_Name> depends on OVCtrl and therefore on system
facility `$all' which cannot be true!

insserv: exiting now without changing boot order!

/sbin/insserv failed, exit code 1
```

HP Operations Agent 11.12 and above conform to the standard LSB tags. The LSB tags must be present in the init scripts on SLES 11 SP2 and above. During the installation of the third-party RPM package on SLES 11 SP2, the error occurs if the LSB tags are missing in the third-party application init scripts.

Solution:

The application vendors must add proper LSB tags in the third-party application scripts.

(or)

You must upgrade from SUSE Linux Enterprise Server 11 Service Pack 2 to SUSE Linux Enterprise Server 11 Service Pack 3. The HP Operations Agent 11.13 supports the SUSE Linux Enterprise Server 11 Service Pack 3.

Installation of the HP Operations Agent 11.16 fails on HP-UX 11.31 with the Error "Internal Error 7 in function "IC_TargetSoftwareGet"

While installing Operations Agent on HP-UX 11.31 system, the Operations Agent fails to install the OVSecCore installation package and the following error message appears in oainstall.log:

```
ERROR: Internal Error 7 in function "IC_TargetSoftwareGet"
```

Solution:

1. Log on to the HP-UX node with the root privileges.
2. From the `/etc` directory, open the `profile` file with a text editor.
3. Add the following lines at the end of the `profile` file:

   ```
   SDU_DEBUG_DISABLE_CLIENT_LOCALAUTH=1
   ```

```
export SDU_DEBUG_DISABLE_CLIENT_LOCALAUTH
SDU_DEBUG_DISABLE_SERVER_LOCALAUTH=1
export SDU_DEBUG_DISABLE_SERVER_LOCALAUTH
```

4. Save the file.

Certificates

Signatures in vbs scripts are slow and causes delay when running some of the HP Operations Agent commands

HP Operations Agent contains digitally signed code. This is to protect the integrity of the software. Sometimes, when you run Operations Agent commands on the managed node, the response is very slow. The signatures in vbs scripts causes delay when running the commands such as `opcagt -type, status` and so on. The delay may occur due to Certificate Revocation List (CRL) check.

Solution 1:

On Windows:

1. Log on to the Windows system.
2. From the Start menu, open the Run prompt.
3. In the Run prompt, type **SecPol.msc**, and then press **Enter**. The **Local Security Policy** editor window opens.
4. In the **Local Security Policy** editor window, click to open the **Public Key Policies** folder.
5. In the right pane, double-click **Certificate Path Validation Settings**. The **Certificate Path Validation Settings Properties** dialog box opens.
6. In the **Certificate Path Validation Settings Properties** dialog box, click to select the **Define these policy settings** checkbox.

   Note: Select the timeout values less than the recommended setting. For example, the Default retrieval settings can be reduced from 15-20 seconds to 1 second or to any lower suitable values.

7. Click **OK**.

Solution 2:

Run the following command in the command prompt to set a proxy, which allows CRL validation with external site:

```
netsh winhttp set proxy localhost "<local>"
```

(or)

1. In the Run prompt, type **control inetcpl.cpl,,4** and then press **Enter**. The **Internet Properties** window opens with the **Connections** tab enabled.
2. Click **Lan settings**. The **Local Area Network (LAN) Settings** window opens.
3. Select the **Use a proxy server for your LAN** checkbox.
4. In the **Address** box, type the address of your proxy server.

5. In the **Port** box, type the port number of the port you want to access.
6. Click **OK**.

Note: You can set a proxy which allows CRL validation with external site only if you have environments with internet access. A real proxy can be set if your environment allows, else set a dummy proxy.

Other

On Solaris 10, the Ovc -status command reports the adminui process as stopped

Although the adminui process with a longer path (which exceeds 80 characters) is running on Solaris 10, the `ovc –status` command reports the process as stopped. This is because on Solaris 10, the process details beyond 80 characters gets truncated, which is a limitation of Solaris 10.

Additional text and tty related warnings appear on the HP-UX node

Scenario 1: On HP-UX node when you execute the tools such as OMW, OMU and run the automatic, operator-initiated and scheduled actions the 'logout root' text appends in the output.

Cause:

On HP-UX node, the profile file setting includes the line of code that appends the text 'logout root' after shell exits. Because of this, the text "logout root" gets appended during command execution.

Solution:

Before running the test script, comment the lines in the profile file located in `/` and `/etc` directories on the HP-UX node:

- Comment the `trap "echo 'logout root'" 0` line in the `/.profile` file:

```
# Set up shell environment

 set -u                          # trap "echo 'logout root'" 0 # what to do on
                                 exit

 # trap "echo 'logout root'"     # what to do on exit
 0
```

- Comment the `trap "echo logout" 0` line in the `/etc/profile` file:

```
# Set up shell environment:
# trap "echo logout" 0
```

Scenario 2: The tty related warnings appear on the HP-UX node when you execute the tools such as OMW, OMU and run the automatic, operator-initiated and scheduled actions.

Solution:

The tty related warnings can be fixed by setting a condition in the profile file for the commands that tries to use the terminal such as `ttytype`, `tset` and `stty`:

```
if [ -o interactive ]
then
```

```
<ttytype, tset and stty commands to be executed>
fi
```

The `ttytype`, `tset` and `stty` commands will be executed only in an interactive mode.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Installation Guide (Operations Agent and Infrastructure SPIs 11.16)

Just add your feedback to the email and click send.

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

We appreciate your feedback!