HP Operations Agent

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

Software Version: 11.00

Deployment Guide

Document Release Date: June 2011
Software Release Date: October 2010

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 Notices

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:

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

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

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

Or click the **New users - please register** link on the HP Passport login page.

Support

Visit the HP Software Support Online web site at:

www.hp.com/go/hpsoftwaresupport

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

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

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

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

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

To find more information about access levels, go to:

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

Contents

1 Overview

With the combination of HP Operations Manager (HPOM) and the HP Operations agent, you can create a distributed monitoring solution to monitor multiple systems in your environment. The agent on every node monitors the performance of the system and sends alert messages to the central HPOM console. In addition to providing a central console to monitor the responses of the agent, the HPOM console helps you perform certain configuration tasks on the agent.

Large networks of systems managed by HPOM often create additional challenges in deploying and maintaining the agent. This guide contains information, guidelines, and best practices for deploying the HP Operations agent product in an HPOM-managed environment.

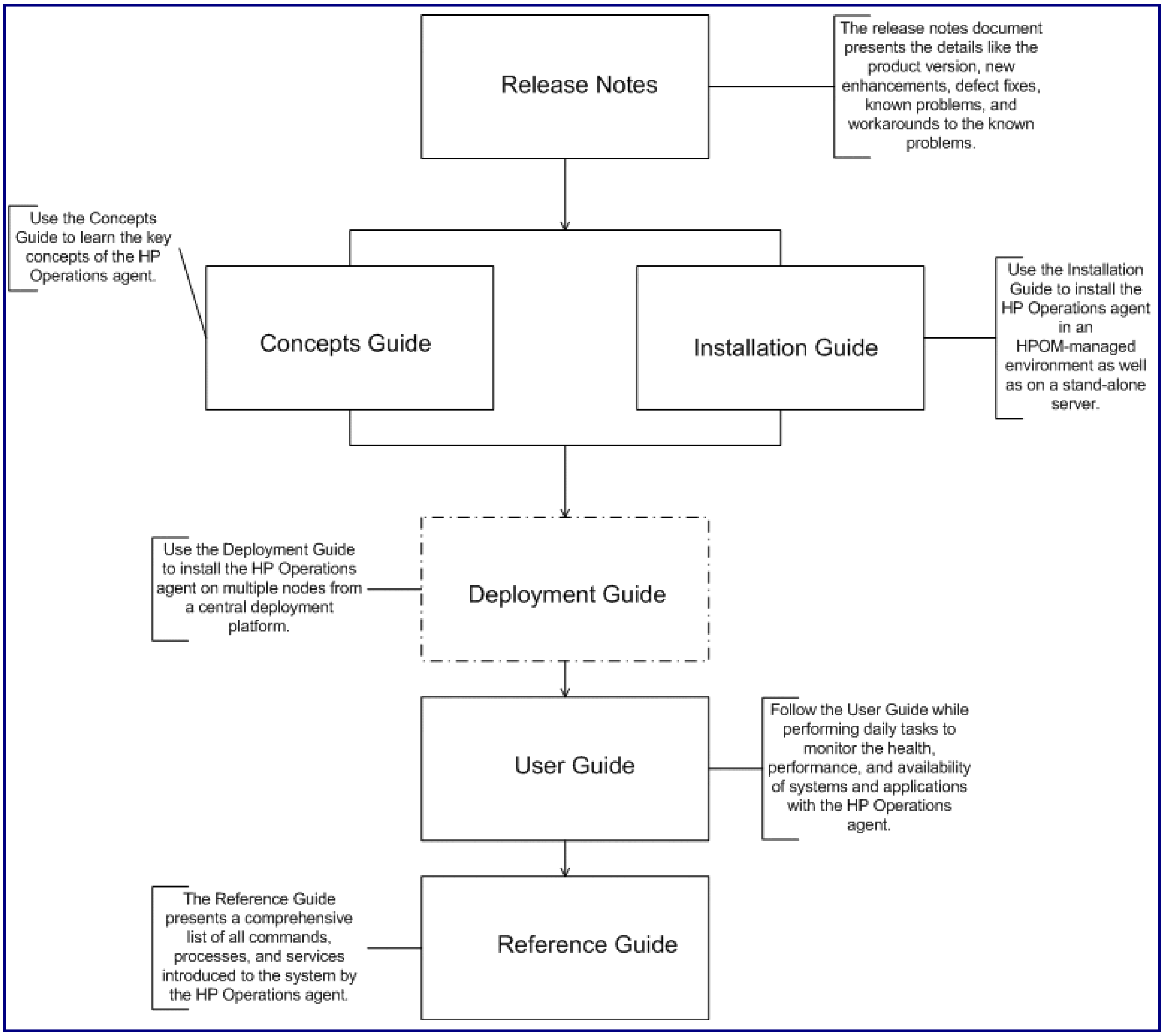
After installing the HP Operations agent on nodes, use this guide for information on the following tasks:

- Deploying certificates on nodes
- Configuring the agent to communicate with the HPOM management server in a firewall-controlled secure environment
- Configuring the agent with multiple management servers
- Configuring the data collection mechanism of the agent remotely from the HPOM console
- Deploying the agent in a high availability (HA) cluster

Documentation Map

The documentation map presents a list of all the major documents for the HP Operations agent. You can use the map to identify the necessary document when you need assistance.

Figure 1 Documentation Map for the HP Operations Agent


Release Notes
The release notes document presents the details like the product version, new enhancements, defect fixes, known problems, and workarounds to the known problems.
Use the Concepts Guide to learn the key concepts of the HP Operations agent.
Concepts Guide
Installation Guide
Use the Installation Guide to install the HP Operations agent in an HPOM-managed environment as well as on a stand-alone server.
Use the Deployment Guide to install the HP Operations agent on multiple nodes from a central deployment platform.
Deployment Guide
User Guide
Follow the User Guide while performing daily tasks to monitor the health, performance, and availability of systems and applications with the HP Operations agent.
The Reference Guide presents a comprehensive list of all commands, processes, and services introduced to the system by the HP Operations agent.
Reference Guide

Related Documentation

You can find all the user documentation for the HP Operations agent inside the `paperdocs` directory on the product media. To check for recent updates or to verify that you are using the most recent edition of a document, go to:

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

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

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

Or click the **New users - please register** link on the HP Passport login page.

Table 1 User Documentation for the HP Operations Agent

Document	Use	Key Topics
Release Notes	Refer to this document for information on the product version, new features, and known problems.	• New features • Enhancements • Fixes • Known issues and limitations
Concepts Guide	The Concepts Guide helps you understand the working mechanism of the HP Operations agent in different environments.	• Introduction to the HP Operations agent • Major components of the HP Operations agent
Installation Guide	With the help of the Installation Guide, you can install the HP Operations agent in the following environments: • On an HPOM management server (for use in the HPOM-managed distributed management environment) • On a standalone server (to collect system performance metric of the local server for use with external data analysis tools like HP Performance Manager)	• Installing the HP Operations agent from the HPOM console • Manually installing the HP Operations agent • Licensing
User Guide	While performing daily tasks on the HP Operations agent, refer to this guide if you need assistance.	• Managing data collection • Generating alarms
Reference Guide	The Reference Guide presents a comprehensive list of all commands, processes, and services available on the HP Operations agent node.	• Command-line utilities • Configuration variables

2 Configuring Certificates

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

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

- **A unique node certificate.** The node can identify itself to its management server and other nodes by sending them its node certificate.
- **A copy of the management server's trusted certificate.** A node only allows communication from a management server if it has the trusted certificate for that management server.

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

To enable the nodes to communicate securely in the HPOM-managed environment by using certificates, you must install certificates after you install the agent on the nodes.

Installing Certificates

You can install the certificate in one of the following ways:

- Request certificates automatically
- Request certificates with an installation key
- Deploy certificates manually

Request Certificates Automatically

When you deploy the agent to a node from the HPOM console, the node requests certificates automatically from the management server. The node encrypts the certificate request with a key.

The management server then grants the certificate request. You can configure this to take place automatically. After granting the request, the management server sends the certificates to the node. If the management server denies the certificate request, you can send another request by running the following command on the managed node:

```
ovcert -certreq
```

After the management server grants the certificate request, run the following command on agent nodes that reside in high availability clusters:

```
ovc -restart ovconfd
```

In a highly secure environment, you can disable automatic certificate requests by setting the certificate deployment type to manual. You then must request the certificates with installation key or deploy the certificates manually.

Request Certificates with an Installation Key

To encrypt certificate requests, you can use installation keys. You can generate an installation key on the management server, and then transfer it to the node.

Before you request certificates with an installation key, make sure that the HP Operations agent is running on the node. The agent sends a certificate request at the time of start. If you then request a certificate with an installation key, the new certificate request overwrites the original certificate request on the management server. You can suppress the first certificate request by setting the parameter `CERTIFICATE_DEPLOYMENT_TYPE` to `manual` in the `sec.cm.client` namespace by using the agent installation defaults or by using the `ovconfchg` utility.

To request certificates with an installation key, follow these steps:

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.

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`.

<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.

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>
```

9 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.

10 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, follow these steps:

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:

   From HPOM for Windows

   ovowcsacm -issue -name *<node_name>* **[-file** *<file_name>*] **[-coreid** *<OvCoreId>*] **[-pass** *<password>*]

   From HPOM for UNIX or HPOM on UNIX/Linux

   opccsacm -issue -file *<file_name>* **[-pass** *<password>*] **-name** *<node_name>* **[-coreid** *<OvCoreId>*]

   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 Configuratio**n. 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`. 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>
   ```

   The command may prompt you to specify the password provided in step 4 on page 13.

10. Run the following command on the node:

    ```
    ovc -start
    ```

11. 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>]
   ```

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

4. Run the following command:

   ```
   ovcert -exporttrusted [-ovrg <server>] -file <file_name>
   ```

   In this instance, *<server>* is the HA resource group name if the management server is installed in an HA cluster.

   The command backs up the management server’s trusted certificate in the file specified with the `-file` option.

5. Determine the alias of the node certificate by running the following command:

   ```
   ovcert -list [-ovrg <server>]
   ```

   The alias of the node certificate is the long sequence of characters, which appears under the `Certificates` section of the output. For example:

```
+---------------------------------------------------------+
| Keystore Content                             |
+---------------------------------------------------------+
| Certificates:                                           |
cdc7b5a2-9dd6-751a-1450-eb556a844b55 (*)                  |
+---------------------------------------------------------+
| Trusted Certificates:                                   |
|     CA_cdc7b5a2-9dd6-751a-1450-eb556a844b55             |
+---------------------------------------------------------+
```

6 Run the following command:

ovcert -exportcert -file <*file_name*> **-alias** <*alias*> **[-pass** <*password*>**]**

The command backs up the node certificate in the file specified with the `-file` option.

To restore the certificates on the node, follow these steps:

1 Log on to the node with the root or administrative privileges.

2 Open a command prompt (shell).

3 To restore the management server certificate, run the following command:

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

In this instance, <*file_name*> is the file name specified in step 3 on page 14.

4 To restore the trusted certificate, run the following command:

ovcert -importtrusted -file <*file_name*>

In this instance, <*file_name*> is the file name specified in step 4 on page 14.

5 To restore the node certificate, run the following command:

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

In this instance, <*file_name*> is the file name specified in step 6 on page 15.

Troubleshooting Certificate Problems

To verify if all the necessary certificates are correctly installed on the node, run the following command on the node:

ovcert -list

The command shows the output in the following format:

```
+---------------------------------------------------------+
| Keystore Content                             |
+---------------------------------------------------------+
| Certificates:                                           |     | |
cdc7b5a2-9dd6-751a-1450-eb556a844b55 (*)                  |
+---------------------------------------------------------+
| Trusted Certificates:                                   |
|      CA_cdc7b5a2-9dd6-751a-1450-eb556a844b55             |
+----------------------------------------------------------+
```

The `Certificates` section of the output shows the name of the node certificate. The `Trusted Certificates` section of the output shows the name of the management server's trusted certificate.

The node certificate name is identical with the `OvCoreID` parameter of the node.

The trusted certificate name is created with the `CA_` prefix and the `OvCoreID` parameter of the trusted certificate authority (the management server).

Missing Node Certificate

To check if the node certificate is missing, run the following command on the node:

`ovcert -list`

If the node certificate is missing, the command shows the output in the following format:

```
+----------------------------------------------------------+

| Keystore Content                         |
+----------------------------------------------------------+

| Certificates:                                            |
+----------------------------------------------------------+

| Trusted Certificates:                                    |

|      CA_cdc7b5a2-9dd6-751a-1450-eb556a844b55             |
+----------------------------------------------------------+
```

The empty `Certificates` section indicates the node certificate is not present.

To resolve this, follow these steps:

1 Remove the management server's trusted certificate from the node by running the following command:

   `ovcert -remove` *<certificate_name>*

   In this instance, *<certificate_name>* is the name of the trusted certificate (`CA_cdc7b5a2-9dd6-751a-1450-eb556a844b55` in the example).

2 Stop all the processes for the Operations Monitoring Component by running the following command:

   `ovc -kill`

3 Start the core processes by running the following command:

   `ovc -start CORE`

4 If the management server and node are configured to deploy the certificate automatically, the node send a request to the management server, and then the management server grants the request.

   To check if the certificate request arrived on the management server, run the following command (on the management server):

   `ovcm -listpending -l`

   The command output should show the node's core ID in the `CN` field.

If you cannot see the node's core ID in the `CN` field, run the following command on the node to trigger a certificate request manually:

ovcert -certreq

If the management server and node are configured for the manual deployment of the certificate, follow the instructions in Deploy Certificates Manually on page 13.

To check if the certificates are correctly installed on the node, run the following command (on the node):

ovcert -list

The output should display a valid certificate name in the `Certificates` section (which identical with the core ID of the node).

Missing Trusted Certificate

To check if the trusted certificate is missing, run the following command on the node:

ovcert -list

If the trusted certificate is missing, the command shows the output in the following format:

```
+---------------------------------------------------------+

| Keystore Content                           |
+---------------------------------------------------------+

| Certificates:                                                           |

| cdc7b5a2-9dd6-751a-1450-eb556a844b55 (*)
+---------------------------------------------------------+

| Trusted Certificates:                                    |

+---------------------------------------------------------+
```

The empty `Trusted Certificates` section indicates the trusted certificate is not present.

You can resolve this problem by importing the trusted certificate from the management server or another node managed by the same management server.

To import the trusted certificate from another source, follow these steps:

1 Log on to the management server or another node (managed by the same management server) with the root or administrative privileges.

2 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 exports the management server's trusted certificate in the file specified with the `-file` option.

3 Transfer the file on the node (where the trusted certificate is missing).

4 To import the trusted certificate, run the following command:

   ovcert -importtrusted -file <*file_name*>

5 To check if the certificates are correctly installed on the node, run the following command (on the node):

`ovcert -list`

The output should display a valid certificate name in the `Trusted Certificates` section.

Missing Node Private Key

To check if the private key of the node certificate is missing, run the following command on the node:

`ovcert -list`

If the node private key is missing, the command shows the output in the following format:

```
+---------------------------------------------------------+
| Keystore Content                           |
+---------------------------------------------------------+
| Certificates:                                                          |
| cdc7b5a2-9dd6-751a-1450-eb556a844b55
+---------------------------------------------------------+
| Trusted Certificates:                                   |
|     CA_cdc7b5a2-9dd6-751a-1450-eb556a844b55             |
+---------------------------------------------------------+
```

The absence of the `*` sign next to the node certificate name indicates that the node private key is missing. To resolve this, you must remove the node certificate, and then install a new certificate on the node. Follow these steps:

1 Remove the node certificate from the node by running the following command:

`ovcert -remove` *<certificate_name>*

In this instance, *<certificate_name>* is the name of the node certificate (`cdc7b5a2-9dd6-751a-1450-eb556a844b55` in the example).

2 Follow step 2 on page 16 through step 4 on page 16.

3 To check if the node private key is correctly installed on the node, run the following command (on the node):

`ovcert -list`

The output should display the `*` sign next to the node certificate name in the `Certificates` section.

3 Deploying the HP Operations Agent in a Secure Environment

The HP Operations agent and the HPOM management server communicate with each other over the network using the HTTPS protocol. The management server opens connections to the agent node to perform tasks like deploying policies, launching actions, and so on.
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 (Configuring the Communication Broker Port on page 22).
- If your network allows only certain proxy systems to open connections through the firewall, you can redirect HPOM communication through these proxies (see Configuring HTTPS Communication Through Proxies on page 26).
- 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) (Communication in a Highly Secure Environment on page 26).

➤ 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:

1. On the node, open a command prompt (shell).
2. 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.

Configure Proxies

You can redirect connections from management servers and nodes that are on different networks through a proxy.

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

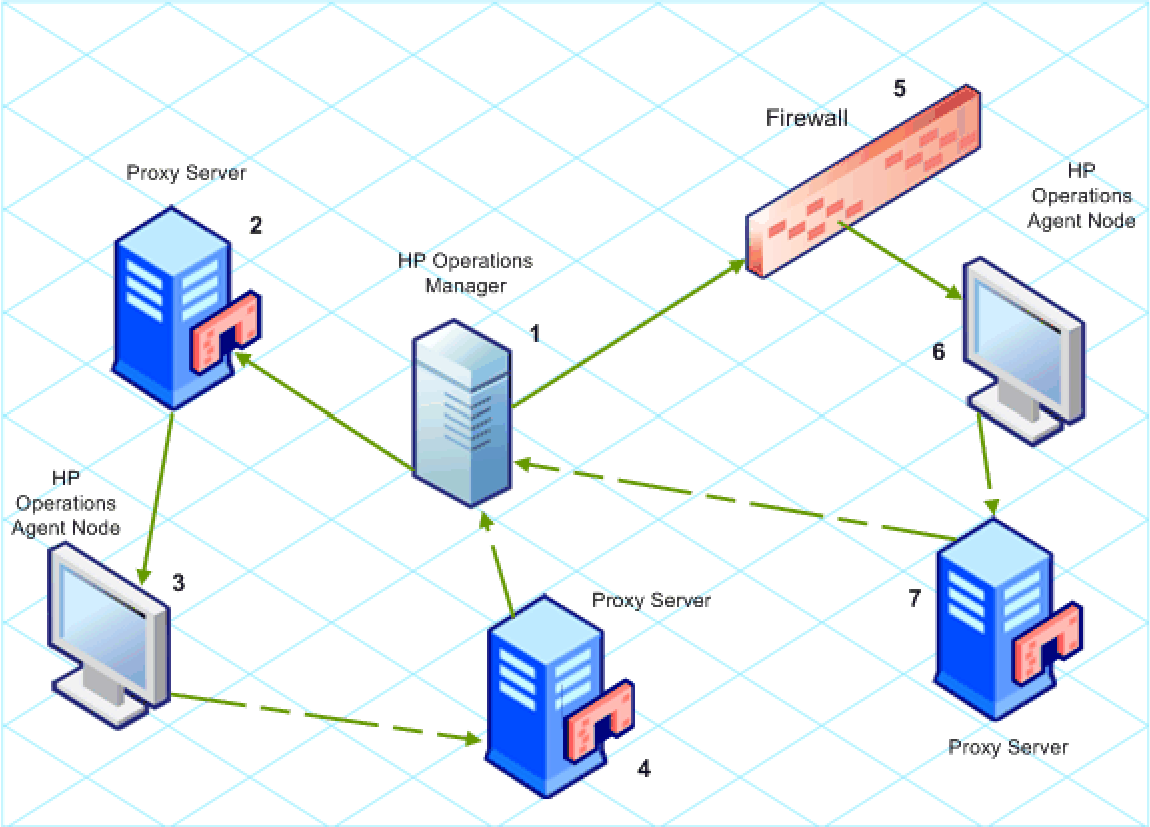
You can also redirect communication through proxies in more complex environments as follows:

- Each management server and node can use different a 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).

Figure 2 Communication Using Proxies



PROXY Parameter Syntax

You redirect outbound HTTPS communication through proxies by setting the PROXY parameter in the bbc.http name space on the management servers and nodes. You can configure this parameter in the following ways:

- Configure the values in the HP Operations agent installation defaults. 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, follow these steps:

1 Log in to the management server or node as a user with the administrative or root rights 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*>

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

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 any communication broker to listen on a port other than 383. If you do this, you must also configure the other management servers and nodes in the environment, so that their outbound connections are destined for the correct port. For example, if you configure a node's communication broker to listen on port 5000, you must also configure the management server so that it connects to port 5000 when it communicates with this node.

PORTS Parameter Syntax

You configure communication broker ports by setting the `PORTS` parameter in the `bbc.cb.ports` name space on all management servers and nodes that communicate with each other.

You can configure this parameter in the following ways:

- Configure the values in the HP Operations agent installation defaults in a profile file during installation. This is recommended if you need to configure communication broker ports for large numbers of nodes. You must plan and configure the installation defaults before you create or migrate your nodes.
- Use **ovconfchg** at the command prompt.

The values must contain one or more host names or IP addresses and have the following format:

<host>:*<port>*[,*<host>*:*<port>*] ...

The *<host>* can be either a domain name or IP address. For example, to configure the communication broker port to 5000 on a management server with the host name manager1.emea.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, follow these steps:

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.

Configuring Local Communication Ports

By default, management servers and nodes use local port 0 for outbound connections, which means that the operating system allocates the local port for each connection. Typically, the operating system will allocate local ports sequentially. For example if the operating system allocated local port 5055 to an Internet browser, and then the HTTPS agent opens a connection, the HTTPS agent receives local port 5056.

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

CLIENT_PORT Parameter Syntax

You configure local communication ports by setting the `CLIENT_PORT` parameter in the bbc.http name space on the management server or node. You can configure this parameter in the following ways:

- Configure the values in the HP Operations agent installation defaults. 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>*

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, follow these steps:

1. Log on to the HP Operations agent node.
2. Open a command prompt or shell.
3. Specify the range of local ports that the management server or node can use for outbound connections by typing the following command:

   ovconfchg -ns bbc.http -set CLIENT_PORT *<lower port number>*-*<higher port number>*

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

Configuring Nodes with Multiple IP Addresses

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

- The communication broker accepts incoming connections on all IP addresses.
- The agent opens connections to the management server using the first network interface that it finds.
- To communicate with HP Reporter or HP Performance Manager, the communication daemon (CODA) accepts incoming connections on all IP addresses.

To configure the HP Operations agent to use a specific IP address, follow these steps:

1. Log on to the HP Operations agent node.
2. Open a command prompt or shell.
3. Run the following command to set the IP address for the Communication Broker:

   ovconfchg -ns bbc.cb SERVER_BIND_ADDR *<ip_address>*

4 Run the following command to set the IP address that you want the agent to use while opening outbound connections to the management server:

ovconfchg -ns bbc.http CLIENT_BIND_ADDR <*ip_address*>

5 Run the following command to set the IP address that you want to use for incoming connections from HP Performance Manager or HP Reporter:

ovconfchg -ns coda.comm SERVER_BIND_ADDR <*ip_address*>

Configuring HTTPS Communication Through Proxies

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

1 The management server opens connections to the proxy.

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

3 The node opens connections to the proxy.

4 The proxy opens connections to the management server on behalf of the node.

To redirect the communication through proxies, follow these steps:

1 Log on to the management server or node with the root/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.

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

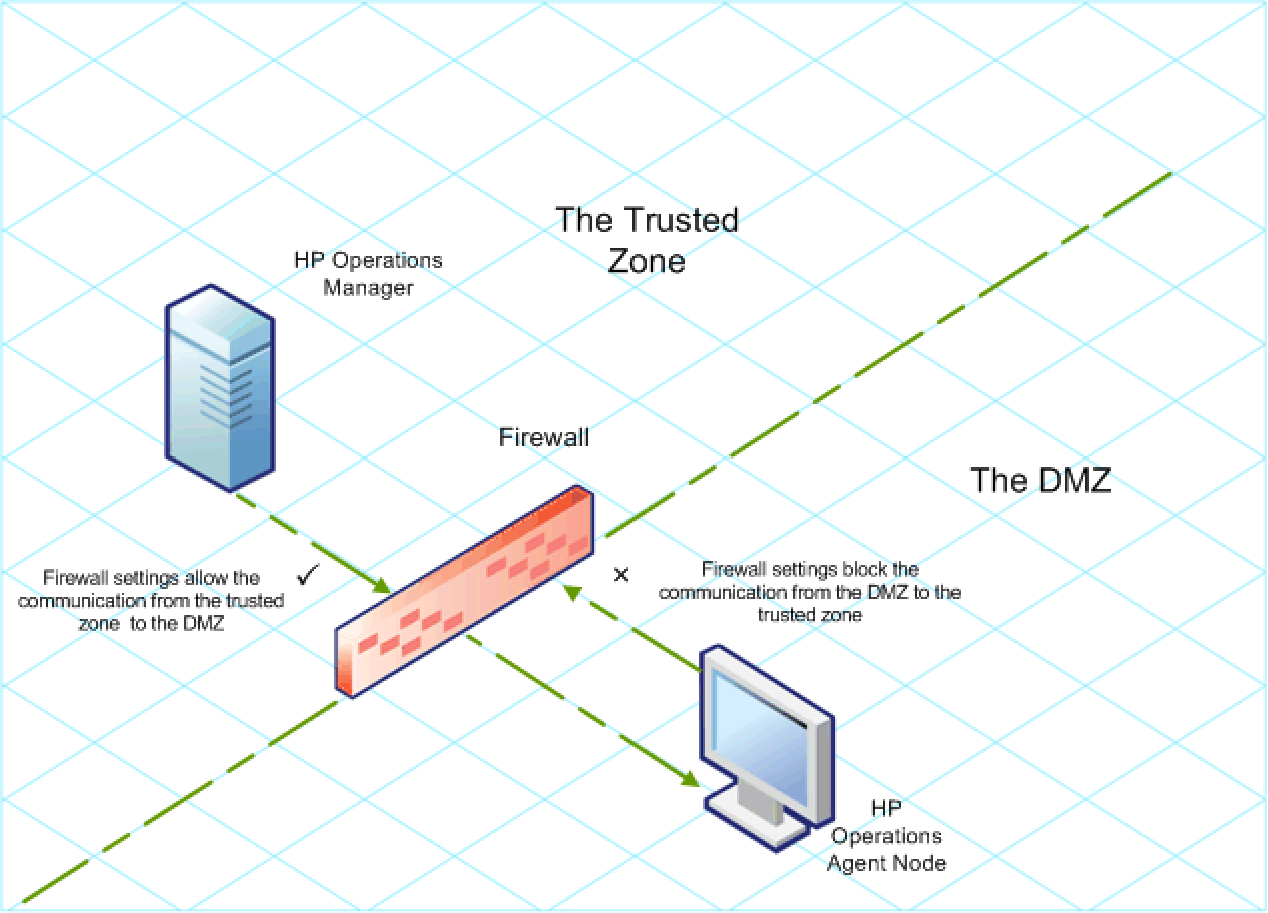
Communication in a Highly Secure Environment

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.

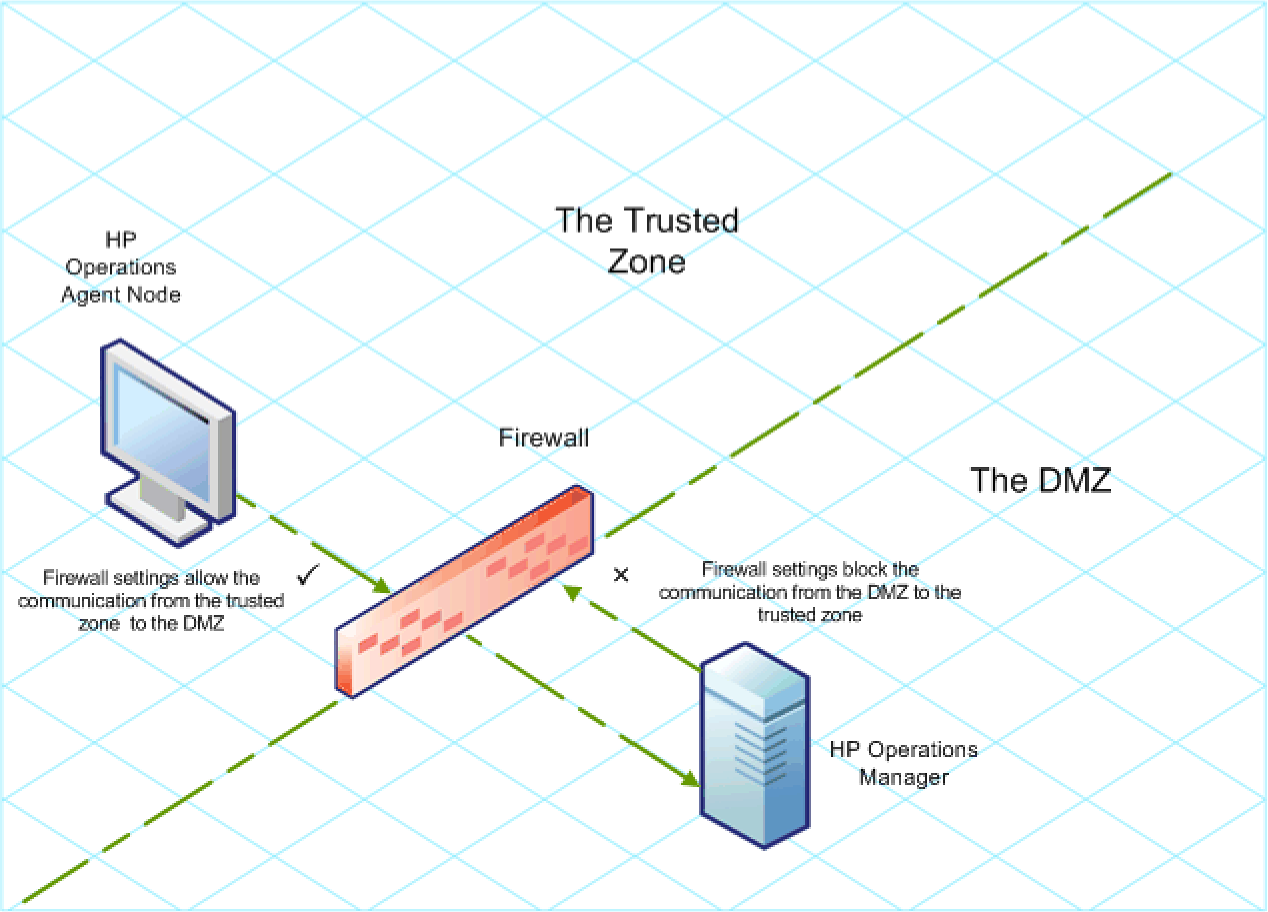
In the following scenario, managed nodes are located in the DMZ while the management server belongs to the trusted zone. The firewall settings in this example allow outbound-only communication. Therefore, inbound communication to the management server is blocked by the firewall.

Figure 3 Managed Nodes in the DMZ


The Trusted Zone
HP Operations Manager
Firewall
The DMZ
Firewall settings allow the communication from the trusted zone to the DMZ
✓
×
Firewall settings block the communication from the DMZ to the trusted zone
HP Operations Agent Node

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.

Figure 4 HPOM Management Server in the DMZ


The Trusted Zone
HP Operations Agent Node
Firewall
The DMZ
Firewall settings allow the communication from the trusted zone to the DMZ ✓
× Firewall settings block the communication from the DMZ to the trusted zone
HP Operations Manager

Introduction to the Reverse Channel Proxy

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

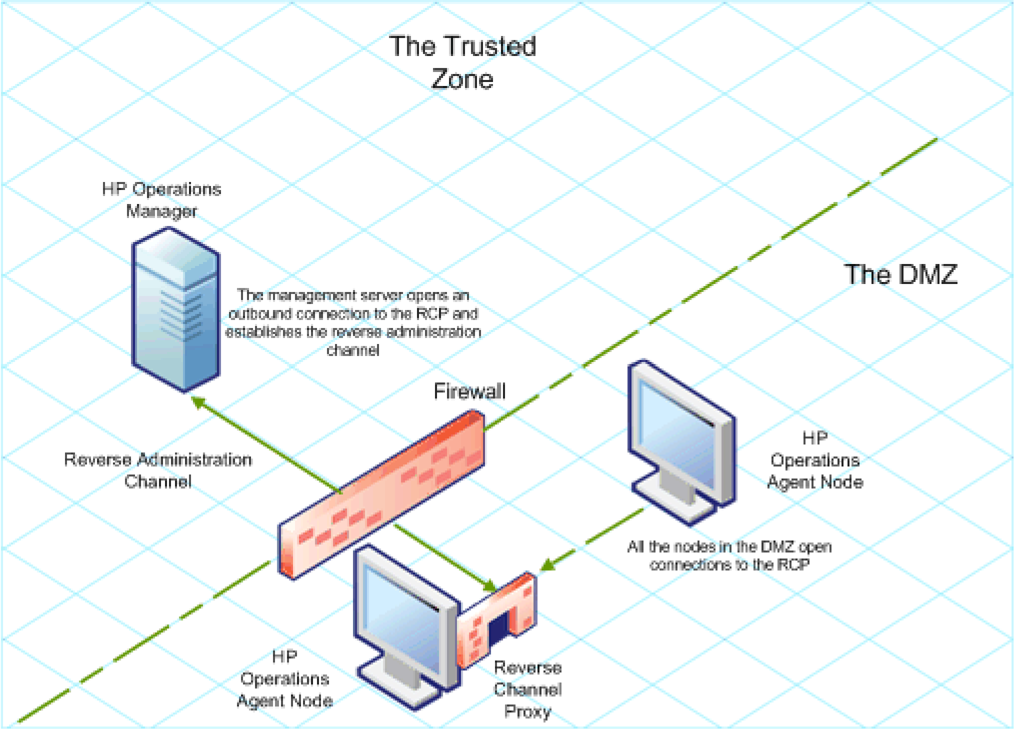
Systems belonging to the DMZ open connection to the RCP instead of the system inside the trusted zone. You can configure the system in the trusted zone to open an outbound communication channel—the reverse administration channel—to the RCP. The system in the trusted zone maintains the outbound channel;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

- The RCP is configured on a node in the DMZ.
- All the nodes in the DMZ open connections to the RCP.

- 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.
- All nodes from the DMZ communicate to the HPOM management server through the reverse administration channel.

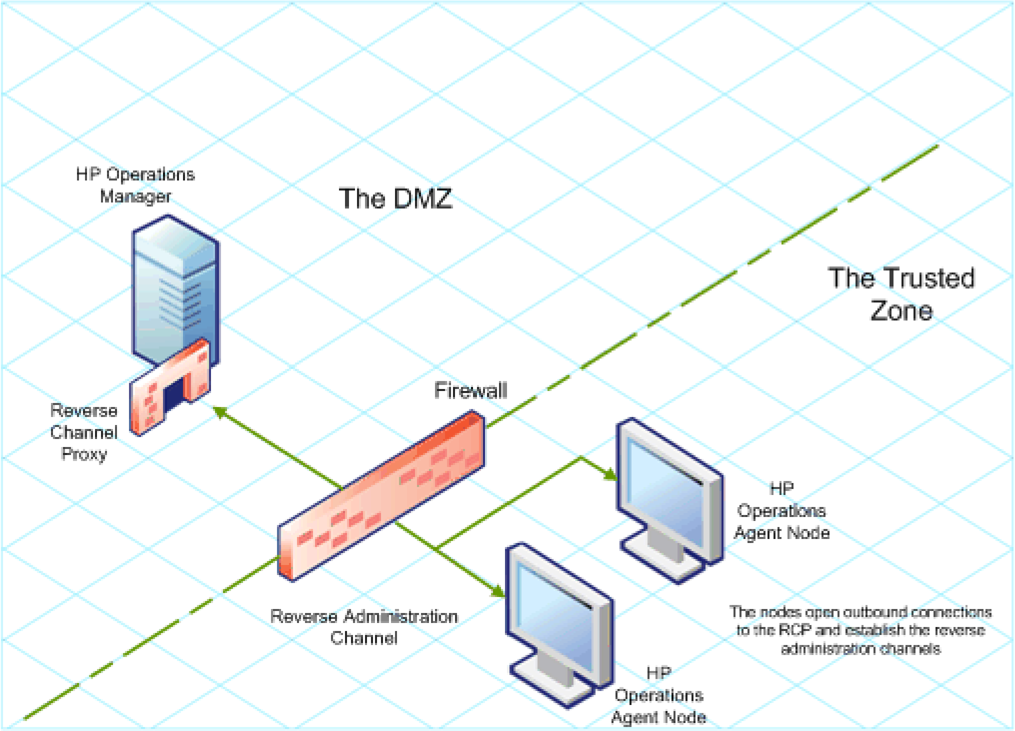
Figure 5 Secure Communication Through the RCP with Nodes in the DMZ


The Trusted Zone
HP Operations Manager
The management server opens an outbound connection to the RCP and establishes the reverse administration channel
The DMZ
Firewall
Reverse Administration Channel
HP Operations Agent Node
All the nodes in the DMZ open connections to the RCP
HP Operations Agent Node
Reverse Channel Proxy

When the nodes are located in the trusted zone and the management server in the DMZ, the HPOM setup uses the following workflow:

- The RCP is configured on the management server in the DMZ.
- 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.
- The management server in the DMZ communicates to the nodes through the reverse administration channel.

Figure 6 Secure Communication Through the RCP with the Management Server in the DMZ


HP Operations Manager
The DMZ
The Trusted Zone
Reverse Channel Proxy
Firewall
HP Operations Agent Node
Reverse Administration Channel
The nodes open outbound connections to the RCP and establish the reverse administration channels
HP Operations Agent Node

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:

Task 1: Configure an RCP

Before you configure RCP, you must configure the node's certificate.

To configure an RCP, 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:

ovconfchg -ns bbc.rcp -set SERVER_PORT *<port_number>*.

➤ When you use the command **ovconfchg** on the HPOM management server that runs in a cluster, add the parameter **-ovrg** *<server>*, where *<server>* is the resource group.

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

a **ovcreg -add** *<install_dir>***/newconfig/DataDir/conf/bbc/ovbbcrcp.xml** b `ovc -kill`

c `ovc -start`

Task 2: 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, 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
```

When you use the command **ovconfchg** on the HPOM management server that runs in a cluster, add the parameter **-ovrg** <*server*>, where <*server*> is the resource group.

4 Run the following commands to specify the RCP details:

a
```
ovconfchg [-ovrg <server>] -ns bbc.cb -set RC_CHANNELS
<rcp>:<port>[,<OvCoreId>][;<rcp2>...]
```

b
```
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 in step 3 on page 30)

<*OvCoreID*>: The core ID of the system where you configured the RCP.

Alternatively, you can provide the RCP details by using a configuration file. See Specify the RCP Details with a Configuration File on page 32 for more information.

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, follow these steps:

1 Log on to the node that establishes the reverse administration channel.

2 Note down the time taken by the agent to establish the channel. You can determine this by running the **ovbbccb -status** command. The the **ovbbccb -status** command output shows the status of reverse administration channels originating from the system. By running the **ovbbccb -status** command repeatedly, you can determine the approximate time taken by the agent to establish the channel.

3 Calculate the ratio of the desired time to establish the channel and the approximate actual time taken by the agent to establish the channel.

4 Set the RC_MAX_WORKER_THREADS variable to the next higher integer to the ratio. Use the following command to set this variable:

```
ovconfchg -ns bbc.cb -set RC_MAX_WORKER_THREADS <Maximum_Threads>
```

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 in step 3 on page 30

<OvCoreID>: The core ID of the system where you configured the RCP.

3 Save the file in the following location:

<data_dir>\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 in step 1 on page 32.

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 in step 3 on page 30

<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
```

5 Repeat step 3 and step 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:

Task 1: 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 in step 3 on page 30

Task 2: 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:

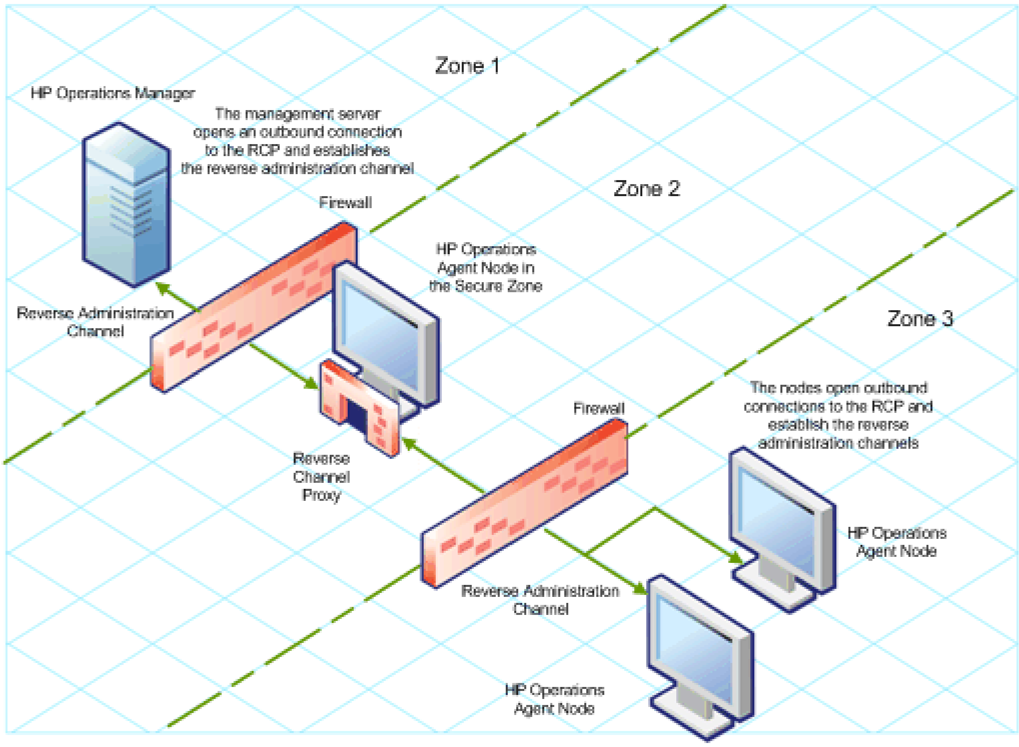
```
Pending:

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.

Figure 7 Secure Communication with Two Firewalls


Zone 1
HP Operations Manager
The management server opens an outbound connection to the RCP and establishes the reverse administration channel
Firewall
Zone 2
HP Operations Agent Node in the Secure Zone
Reverse Administration Channel
Zone 3
Reverse Channel Proxy
Firewall
The nodes open outbound connections to the RCP and establish the reverse administration channels
HP Operations Agent Node
Reverse Administration Channel
HP Operations Agent Node

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.

4 HP Operations Agent in High Availability Clusters

You can use the HP Operations agent to monitor nodes in a High Availability (HA) cluster. To be able to monitor cluster-aware applications in an HA cluster, you must deploy the agent with the following guidelines:

- All the nodes in a cluster must be present in the list of managed nodes in the HPOM console.
- You must install the HP Operations agent on every node in the HA cluster.
- **Virtual Nodes.** If you are using the node with the HPOM for UNIX 8.35, HPOM on UNIX/Linux 9.1x, or HPOM for Windows 9.00, you can take advantage of the concept of virtual nodes. A virtual node is a group of physical nodes linked by a common resource group. Based on the changes in the resource group, the agent can automatically enable or disable policies on the physical nodes.

  The virtual node feature is not available with HPOM for Windows 8.1x.

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

  Following are the guidelines for creating virtual nodes in the HPOM console:

  — A virtual node must not itself be a physical node.

  — Virtual nodes do not support DHCP, autodeployment, and certificates.

  — You must not install an agent on a virtual node.

Monitoring Nodes in HA Clusters

You can configure the HP Operations agent to monitor cluster-aware applications that run on the nodes in an HA 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`.

   This file is used to define the resource groups that will be monitored and to map the resource groups to application instances.

The `apminfo.xml` file has the following format:

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>
```

4. 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/`

5. 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 step 2.

   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>
```

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.

Variable	Description
$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>
```

6. 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`

7. Ensure that the physical nodes where the resource groups reside are all managed nodes.

8. Check the syntax of the XML files on all physical nodes by running the following command:

   - On Windows: *%OvInstallDir%***`\bin\ovappinstance -vc`**
   - On HP-UX, Linux, or Solaris: **`/opt/OV/bin/ovappinstance -vc`**
   - On AIX: **`/usr/lpp/OV/bin/ovappinstance -vc`**

9 *Optional.* For some physical nodes, for example for multihomed hosts, the standard hostname may be different from the name of the node in the cluster configuration. If this is the case, the agent cannot correctly determine the current state of the resource group. Configure the agent to use the hostname as it is known in the cluster configuration:

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

  ```
  ovclusterinfo -a
  ```

  b 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**.

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

  a **ovc -stop**

  b **ovc -start**

11 If you are using HPOM for Windows 8.1x, deploy the policies that you identified for monitoring the cluster-aware application (in step 2) 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 step 2) on the virtual node created for the cluster.

Agent User

By default, the HP Operations agent regularly checks the status of the resource group. On UNIX and Linux nodes, the agents use cluster application-specific commands, which can typically only be run by root users. On Windows nodes, the agents use APIs instead of running commands.

If you change the user of an agent, the agent may no longer have the permissions required to successfully run cluster commands. In this case, you must configure the agent to use a security program (for example, `sudo` or `.do`) when running cluster commands.

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

1 Log on to the node with the root privileges.

2 Go to the following directory:

  On HP-UX, Linux, or Solaris:

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

  On AIX:

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

3 Run the following command to stop the agent:

  ```
  ovc -kill
  ```

4 To configure the agent to use a security program, type the following command:

  ```
  ovconfchg -ns ctrl.sudo -set OV_SUDO <security_program>
  ```

In this instance, <*security_program*> is the name of the program you want the agent to use, for example /usr/local/bin/.do.

5 Run the following command to start the agent:

```
ovc -start
```

5 Configuring the Performance Collection Component Remotely

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

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

Before You Begin

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

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

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

1 In the console tree, right-click the node or the node group (where the agent is running), and then click **All Tasks > Deploy Instrumentation**. The Deploy Instrumentation dialog box opens.

2 In the Deploy Instrumentation dialog box, click **HP Operations Agent**, and then click **OK**. The deployment of the necessary instrumentation files begins on the nodes.

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

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

1 Log on to the Administration UI.

2 Click **Deployment > Deploy Configuration**.

3 In the Distribution Parameters section, select Instrumentation, and then click **Please Select**. The Selector pop-up box opens.

4 In the Selector pop-up box, select the nodes where the agent program is running.

5 Select the Force Update option to overwrite the old instrumentation files.

Select this option on a node that was upgraded from an older version of the agent.

6 Click **Distribute**.

Deploy the OA-PerfCollComp-opcmsg Policy

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

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

Configuring the Performance Collection Component

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

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

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

Configure the parm File

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

- On HP-UX, Solaris, AIX, and Linux: `/var/opt/perf/`
- On Windows: *%ovdatadir%*

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

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

From HPOM for Windows

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

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

1. Identify the nodes where you want the modified collection mechanism to take effect.
2. In the console tree, click **Policy management** → **Policy groups** → **HP Operations Agent** → **Performance Collection Component** → **Collection configuration**. ConfigFile policies for configuring the `parm` file appear in the details pane.
3. Double-click the ConfigFile policy for the platform on which you want the modified collection mechanism to take effect (for example: `parm` file for HP-UX). The `parm` file for <*platform*> dialog box opens.

4 In the Data tab, modify the settings. See the *parm File Parameters* section in the *HP Operations Agent User Guide* for more details on configuration parameters in the `parm` file.

5 Click **Save and Close**. In the details pane, the version of the policy gets increased by `.1`.

6 Deploy the updated policy on the nodes of your choice.

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

From HPOM on UNIX/Linux 9.10

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

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

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

2 In the console, click **Browse** → **All Policy Groups**. The list of all available policy groups appears on the page.

3 Click **H**. The HP Operations Agent policy group appears.

4 Click **HP Operations Agent**, click **Performance Collection Component**, and then click **Collection Configuration**. The list of available ConfigFile policies for the `parm` file appears.

5 Click the ConfigFile policy for the platform on which you want the modified collection mechanism to take effect. The Policy "OA_<*platform*>ParmPolicy" page appears.

6 Click ⚙▾ , and then click **Edit (Raw Mode)**. The Edit Config File policy... page appears.

7 In the Content tab, modify the settings. See the *parm File Parameters* section in the *HP Operations Agent User Guide* for more details on configuration parameters in the `parm` file.

8 Click **Save**.

9 Deploy the updated policy on the nodes of your choice.

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

Configure the alarmdef File

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

- On HP-UX, Solaris, AIX, and Linux: `/var/opt/perf/`
- On Windows: *%ovdatadir%*

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

From HPOM for Windows

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

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

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

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

From HPOM on UNIX/Linux 9.10

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

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

1. Identify the nodes where you want the modified alert mechanism to take effect.
2. In the console, click **Browse** → **All Policy Groups**. The list of all available policy groups appears on the page.
3. Click **H**. The HP Operations Agent policy group appears.
4. Click **HP Operations Agent**, click **Performance Collection Component**, and then click **Alarm Definition**. The list of available ConfigFile policies for the `alarmdef` file appears.
5. Click the ConfigFile policy for the platform on which you want the modified collection mechanism to take effect. The Policy “OA_<*platform*>AlarmdefPolicy” page appears.
6. Click ⚙▾ , and then click **Edit (Raw Mode)**. The Edit Config File policy... page appears.
7. In the Content tab, modify the settings. See the *alarmdef File Parameters* section in the *HP Operations Agent User Guide* for more details on configuration parameters in the `alarmdef` file.
8. Click **Save**.
9. Deploy the updated policy on the nodes of your choice.

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

Remotely Working with the HP Operations agent

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

- *HPOM for Windows*

  Tool Output section in the Tool Status window

- *HPOM on UNIX/Linux*

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

You can use the following tools from the HPOM console:

Start Agent
Enables you to start the HP Operations agent on the managed node.

Stop Agent
Enables you to stop the HP Operations agent on the managed node.

Restart Agent
Enables you to restart the HP Operations agent on the managed node.

View Status
Enables you to view the status of the HP Operations agent process, services, and daemons on the managed node.

View Version Information
Enables you to view the version of the HP Operations agent on the managed node.

Refresh Alarm Service
Refreshes the Alarm service of the Performance Collection Component.

Scan Performance Component's Log Files
Scans the log files used by the scope collector on the node.

Check Performance Component's Parameter File Syntax
Helps you check the syntax of the parameter file in the managed node.

Check Performance Component's Alarmdef File Syntax
Helps you check the syntax of the alarmdef file in the managed node.

View status of post policy deploy action Helps you check the status of deployment of the parm or alarmdef policies on nodes. While launching this tool, make sure to specify either `parm` or `alarmdef` (as appropriate) as the tool parameter.

You can set the tool parameter in the Parameter box in the Edit Parameters window when you use HPOM for Windows.

When you use HPOM on UNIX/Linux, open the Edit Tool Status page for the tool, go to the OVO Tool tab, and then specify the tool parameter in the Parameters box

Set Realtime Permanent License Sets the permanent license for the HP Ops OS Inst to Realtime Inst LTU.

Set Glance Permanent License Sets the permanent license for the Glance Software LTU.

Get License Status Shows the status of LTUs on the node.

6 Monitoring the HP Operations Agent

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

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

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

Before You Begin

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

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

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

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

To deploy the instrumentation, follow these steps:

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

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

5 Select the Force Update option to overwrite the old instrumentation files.

Select this option on a node that was upgraded from an older version of the agent.

6 Click **Distribute**.

Self Monitoring Policies

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

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

The `Self Monitoring` policy group includes the following policies:

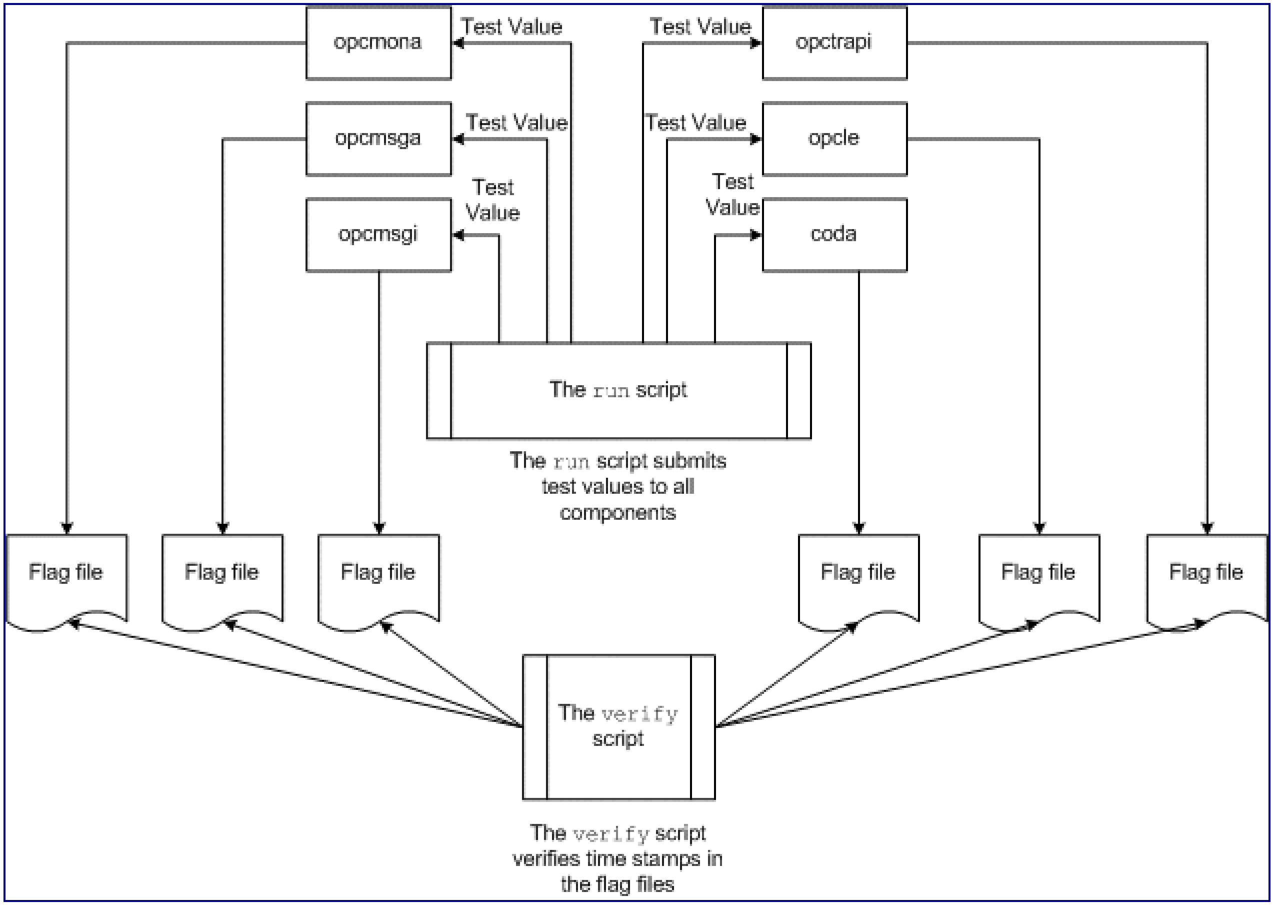
- **OA-SelfMonTstMonaExt:** Tests the monitor agent.
- **OA-SelfMonVerifyMon:** Verifies flag files by the monitor agent
- **OA-SelfMonTstLe:** Tests the logfile encapsulator
- **OA-SelfMonVerifyLe:** Verifies flag files by the logfile encapsulator
- **OA-SelfMonTstTrapi:** Tests the SNMP trap interceptor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

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

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

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

Figure 8 Workflow of the Self Monitoring Scripts



Deploying the Self Monitoring Policies

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

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

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

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

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

1 Log on to the Administration UI.

2 Click **OMU**, and then click **Browse > All Policy Groups**. The All Policy Groups page opens.

3 On the All Policy Groups page, select **HP Operations Agent** policy group, select **Assign to Node/Node Group** from the Choose an Action drop-down list, and then click » . The Selector pop-up box opens.

4 In the Selector pop-up box, select the nodes where the agent program is running, and then click **OK**.

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

Viewing the Status of the Components

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

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

- *On Windows: %ovdatadir%*`tmp\OpC\selfmon`
- *On UNIX/Linux:* `/var/opt/OV/tmp/selfmon`

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

Index

We appreciate your feedback!

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

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

Product name:

Document title:

Version number:

Feedback: