Configuring outbound-only communication with HP Operations Manager 8 (December 2008)

White paper

Abstract

HP Operations Manager for UNIX (HPOM for UNIX) and HP Operations Manager for Windows (HPOM for Windows) have been enhanced to provide uni-directional secure communication between HP Operations management servers and HPOM HTTPS agents through multiple firewalls and trust zones. This white paper describes the steps needed to configure HPOM to work in this even more secure environment.

Before reading this white paper, make sure you have read and understood the appropriate sections of the following Windows or UNIX documents:

- HPOM for UNIX
  - *Firewall Concepts and Configuration Guide*
  - *HTTPS Agent Concepts and Configuration Guide*
- HPOM for Windows
  - *Firewall Concepts and Configuration Guide*
  - *Online Help*

Outbound-only communication in HPOM

Customers use firewalls to protect their networked environments from intruders who try to penetrate their corporate intranets. Many customers need to manage systems located in sites that are less trusted than the HP Operations management server site. These systems must be managed through one or more firewalls. In the standard setup, HPOM supports communication through firewalls if limited communication from the outside is restricted to certain ports. For details about using HPOM in such an environment, refer to the *HP Operations Manager for UNIX Firewall Concepts and Configuration Guide* or the *HP Operations Manager for Windows Firewall Concepts and Configuration Guide*.

For firewalls to offer maximum security, they must completely block traffic from the outside unless it is initiated from the secure (trusted) side of the firewall, as shown in Figure 1.

Figure 1. Initiating agent-server communication today

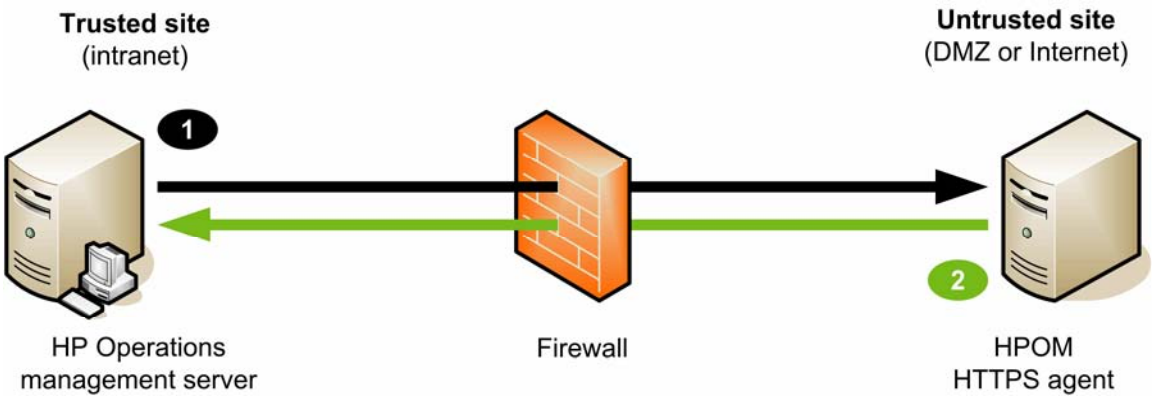


Figure 1 shows two different types of communication through a firewall:

1. **Outbound communication**
   - Policy and instrumentation deployment
   - Heartbeat monitoring
   - Application launch
   - Remote action launch from the server
   - Operator-initiated action launch
2. **Inbound communication**
   - HPOM message
   - Action response

Enhanced secure communication

HPOM for UNIX and HPOM for Windows have been enhanced to provide uni-directional secure communication between HP Operations management servers and HPOM HTTPS agents through one or two firewalls and trust zones.

Secure communication through a firewall

HPOM has been enhanced to provide secure uni-directional communication between the HP Operations management server and HPOM HTTPS agents through a firewall, as shown in Figure 2. A new special-purpose Reverse Channel Proxy (RCP) process (`ovbbcrcp`) provides the secure link between the server and the agents. The RCP enables secure data flow from an agent (untrusted side) through the firewall to the server (trusted side). All inbound communication from the agent to the server is conducted through an intermediary. The RCP is that intermediary.

Figure 2. Outbound-only communication: Summary

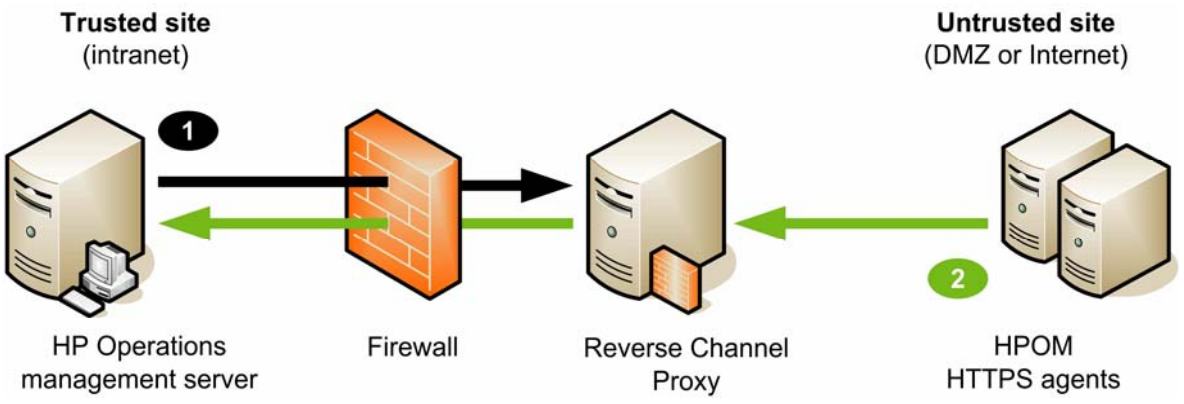


Figure 2 shows two different types of communication through a firewall:

1. Communication initiation
2. Data flow

Network security

Outbound-only communication includes an HPOM management solution that is compliant with company-wide network security policies. All communication between multiple trust zones is initiated only from a trusted zone to an untrusted zone (outbound only). Communication from an HP Operations management server to an HPOM HTTPS agent through a single firewall (outbound) goes through the firewall directly to the agent. All communication from an agent to a server (inbound), as well as all communication between a server and an agent through multiple firewalls, is conducted through an intermediary. Most agent systems can be used to host an RCP. The RCP is included in the agent software. To find out which platforms support RCP, see "Limitations of outbound-only communication" on page 8.

Use cases

Outbound-only communication enables you to do the following:

- Run an HP Operations management server in a secure environment (as shown in Figure 3 in "RCP communication through one firewall" on page 5).
- Run an HPOM HTTPS agent in a secure environment, with one RCP between the server and the agent, one firewall between the server and the RCP, and one firewall between the agent and the RCP (as shown in Figure 5 in "RCP communication through two firewalls" on page 7).
- Run an HPOM HTTPS agent under a non-root user account (with RCP server port >1024).
- Run RCP on a different system or on the same system as the agent.
- Re-establish outbound-only connections after any of the involved parties has been restarted.
- Run all types of communication required by HPOM over the RCP.
- Lock the firewall completely from one side. Outbound-only communication still works.
- Set up an HTTP proxy between a server and an RCP, and between an RCP and an agent.
- Set up HTTPS-based communication between management servers through one or two firewalls.

Firewall configuration

You can configure the firewall to allow communication from any source port on the HP Operations management server (trusted zone). If necessary, you can further restrict outbound-only communication from the server to specific client port ranges. The default heartbeat polling setting for managed nodes does not work through a firewall. For every node that is separated from the management server by a firewall, you need to change the heartbeat polling setting on the management server to the "RPC Only (for firewalls)" setting. For details, refer to the *HP Operations Manager for UNIX Firewall Concepts and Configuration Guide* or the *HP Operations Manager for Windows Firewall Concepts and Configuration Guide*.

HP Operations traffic only

RCP is not a generic proxy. A certificate is needed to set up an Admin Reverse Channel, a communication channel established by an HP Operations management server to a Reverse Channel Proxy (RCP). The RCP uses the Admin Reverse Channel to establish data channels from clients (HPOM HTTPS agents) to a server on request.

Outbound-only communication is designed to cover all HP Operations traffic using the HTTP Communication Component (BBC). Applications other than HPOM for UNIX (for example, OVPM, OVR, and OVIS) are not supported by outbound-only communication. Applications like OVPM do not require outbound-only communication because they communicate from the more secure side to the less secure side (for example, from the same system as the HP Operations management server to an agent system where OVPA is running).

RCP communication through one firewall

Figure 3 shows how communication between HP Operations management servers and HPOM HTTPS agents using a Reverse Channel Proxy (RCP) works. An RCP can be used for one or more agents. A server establishes a persistent Admin Reverse Channel to an RCP. As long as this Admin Reverse Channel is open, the RCP is able to establish a data channel from an agent to the server.

Figure 3. Outbound-only communication: Details

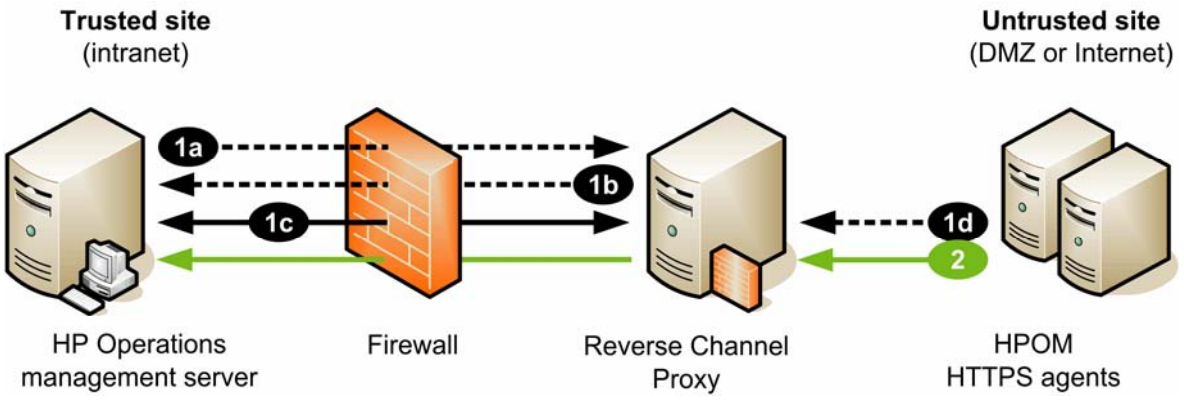


Figure 3 shows how RCP communication works:

1. Admin Reverse Channel
   a. Server sends a request to the RCP for an Admin Reverse Channel.
   b. RCP confirms that an Admin Reverse Channel can be opened.
   c. Persistent Admin Reverse Channel is established between the server and the RCP.
   d. Agent sends a request to the RCP for a data channel with the server.
2. Agent sends data through the new data channel established by the RCP to the server.

In this secure-server scenario, the RCP does the following:

- Runs on the agent system or on a dedicated system.
- Is configured using `ovconfchg`.
- Acts as a concentrator for multiple HPOM HTTPS agents.

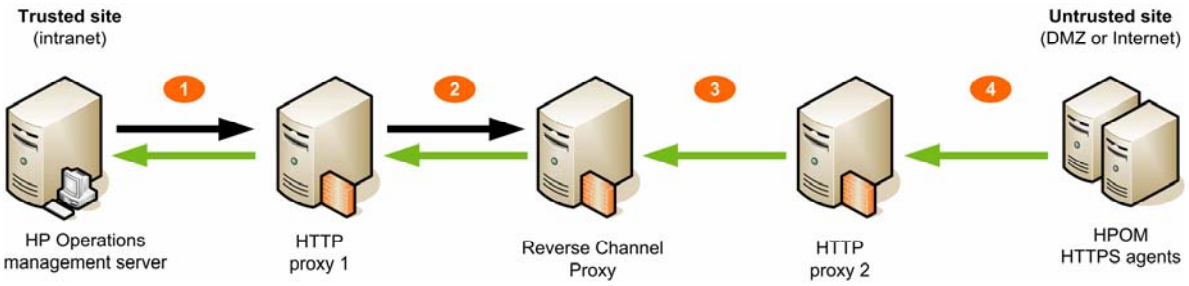
An RCP is different from an HTTP proxy:

- **Advantage of RCP**
  Unlike an HTTP proxy, RCP can route inbound traffic through a firewall that is completely blocked for inbound traffic.
- **Disadvantage of RCP**
  An RCP is able to route traffic for HP Operations applications (for example, HPOM) only. In contrast, an HTTP proxy can route all traffic, but not inbound through the blocked firewall.

NOTE:
You can use one RCP (concentrator) to enable outbound-only communication for multiple HPOM HTTPS agents, including agents on HTTPS platforms that do not currently support RCP.

Secure uni-directional communication is also possible with optional HTTP proxies between the server and the RCP, as well as between the HPOM HTTPS agents and the RCP, as shown in Figure 4.

Figure 4. Outbound-only communication: Optional HTTP proxies



Firewalls can be located between any of the following:

1. HP Operations management server and HTTP proxy 1
2. HTTP proxy 1 and the Reverse Channel Proxy
3. Reverse Channel Proxy and HTTP proxy 2
4. HTTP proxy 2 and the HPOM HTTPS agents

RCP communication through two firewalls

A Reverse Channel Proxy (RCP) can also provide secure communication between HP Operations management servers and HPOM HTTPS agents through two firewalls, as shown in Figure 5. Each connection through a firewall requires its own Admin Reverse Channel, which is the basis for a secure connection through a firewall. For this scenario to work, one Admin Reverse Channel must be established between the server and the RCP, and another Admin Reverse Channel must be established between the agent and the RCP.

Figure 5.Outbound-only communication: High-secure scenario

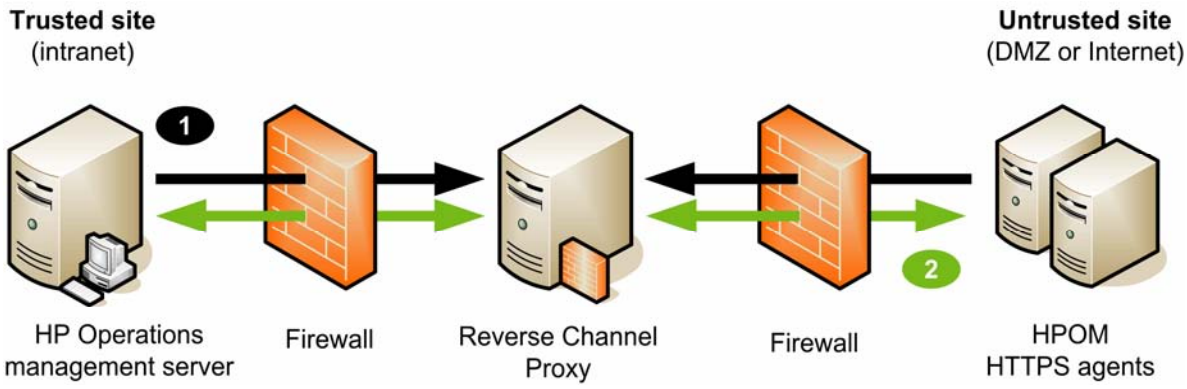


Figure 5 shows two different types of communication through a firewall:

1. Communication initiation
2. Data flow

High secure scenario

A setup with an RCP located between two firewalls works for a high secure scenario with a server behind one firewall and agents located behind another firewall. The server and agents are in trust zones with higher trust than the RCP.

Service provider scenario

The scenario in Figure 5 is also valid for service provider setups, where the HP Operations management server is run in a service provider intranet, and the HPOM HTTPS agents are located at the customer site. From the customer's perspective, the agents are located in a fully trusted site, but the server is not. From the service provider's perspective, the server is located in a fully trusted site, but the agents are not. The server as well as the agents use `ENABLE_REVERSE_ADMIN_CHANNELS`, `RC_CHANNELS` (or `RC_CHANNELS_CFG_FILES`), and `PROXY`.

Limitations of outbound-only communication

Outbound-only communication has the following limitations:

- **Windows**

  Outbound-only communication is supported on Windows. For Windows support, you need either PHSS_37679 or higher (HP-UX management server), or ITOSOL_00665 (Solaris management server). After installing the patch on the management server, you must install or update the agent software on the Windows systems that will host an RCP before starting the RCP on those systems.

- **Solaris 10 SPARC (global and local zone)**

  Outbound-only communication is supported on Solaris 10 SPARC. For Solaris 10 SPARC support, you need either PHSS_37677 or later (HP-UX management server), or ITOSOL_00663 (Solaris management server). After installing the patch on the management server, you must install or update the agent software on the Solaris systems that will host an RCP before starting the RCP on those systems. If you are using a Solaris 10 management server for outbound-only communication, you must update the agent software on that system as well.

- **Solaris (all versions)**

  When using outbound-only communication on a Solaris management server or RCP as concentrator, you should add a configuration setting using `` `ovconfchg -ns xpl.net -set SocketPoll=true` ``. This is a workaround for a known limitation on Solaris systems.

- **Tru64**

  Outbound-only communication is supported on Tru64, but RCP running on Tru64 is not supported. To use a Tru64 system with outbound-only communication, set `[bbc.http] PROXY` on the Tru64 system to use an RCP running on a supported platform.

- **Platforms**

  Outbound-only communication does not yet support all HPOM HTTPS agent platforms. For the most detailed and up-to-date platform support information, check the "HPOM for UNIX Support Matrix" at one of the following locations:

  http://h20230.www2.hp.com/sc/support_matrices.jsp

  http://partners.openview.hp.com/ovcw/pricing/config_matrix.jsp

  To access the "Operations" product support matrix, a user identification (HP Passport) is required. To use an HPOM HTTPS agent with outbound-only communication on a platform that does not support an RCP, you can use an RCP running on a supported platform and set `[bbc.http] PROXY` on the agent to use that RCP.

  Make sure that the platform support matrix really does contain information that is more up-to-date than this white paper. The platform support information must be from December 2006 or later.

- **Backup proxies**

  Outbound-only communication does not support backup proxies (HTTP and RCP). Third-party mechanisms (for example, Cisco Local Director) work for HTTP proxies but not for RCPs. If an RCP fails, you must restart it using `ovc -restart ovbbcrcp`.

The HPOM 8.25 for UNIX management server patch provides outbound-only support for the following scenario:

- HPOM 8 for UNIX manager-to-manager HTTPS communication

In most use cases of OVPM, OVPA, and HP Operations Service Reporter integrated with HPOM, communication is initiated from the trusted side (outbound from the HP Operations management server). In these use cases, no RCP is involved.

Outbound-only configuration

Configuring HPOM to handle outbound-only communication needs to be done at the HP Operations management server (trusted zone), RCP, and the client (untrusted zone). The RCP can be located on a separate dedicated machine, or it can be co-located on client machines.

Configuration variables

You can change configuration variables while processes are running.

CAUTION:
You must *not* change the `CHROOT_PATH` while the CB is running.

Client side (untrusted zone)

The client side is usually an HPOM HTTPS agent system in an untrusted zone. Clients must be configured to use an RCP for given targets (typically, HP Operations management servers).

The RCP entry must be configured as a list of RCPs in the `[bbc.http]` name space using `ovconfchg`. The syntax is identical to the syntax used for configuring communication using an HTTP proxy. For examples of how to apply this and other configuration settings, see "Getting started" on page 18.

IMPORTANT:
When running an RCP (`ovbbcrcp`) on an agent system that has been configured to run as non-root (using `ovswitchuser.sh`), you need to run the following command once:

```
# ovconfchg -ns bbc.rcp -set CHROOT_PATH /
```

The `chroot` command *cannot* be run by a non-root user on a UNIX or Linux system.

If the `CHROOT_PATH` parameter is not set, `ovbbcrcp` tries to `chroot` to `/var/opt/OV`, and produces the following error in the `System.txt` error log file every time the system starts up:

```
0: ERR: Thu Jul 19 09:21:27 2007: ovbbcrcp (2130/1):
(bbc-188) Cannot change the root directory for the
current process. See chroot man page for additional
detail. errno reason:
```

On a non-root agent, you should execute the following command as user root:

```
# /opt/OV/bin/ovcreg -add
/opt/OV/newconfig/DataDir/conf/bbc/ovbbcrcp.xml
```

You need to do this only once to register `ovbbcrcp` at `ovcd`.

```
[bbc.http]

PROXY=rcp1:port1+(a)-(b);rcp2:port2+(c)-(d);...
TARGET_FOR_RC=<OV Core ID>
TARGET_FOR_RC_CMD=<script | command>
```

Syntax

PROXY

Defines which proxy and port to use for a certain hostname.

Format:

```
PROXY=rcp1:port1+(a)–(b);rcp2:port2+(c)–(d);...
```

a Denotes a comma- or semicolon-delimited list of hostnames, IP addresses, or both with wildcards that use the proxy `rcp1`.

b Exclusions. Denotes a comma- or semicolon-delimited list of hostnames, IP addresses, or both that match a but do *not* use the proxy `rcp1`.

c Denotes a comma- or semicolon-delimited list of hostnames, IP addresses, or both with wildcards that use the proxy `rcp2`.

d Exclusions. Denotes a comma- or semicolon-delimited list of hostnames, IP addresses, or both that match c but do *not* use the proxy `rcp2`.

TARGET_FOR_RC

OV Core ID. If this parameter is set, the RCP validates against the core id of the target CB (typically, the CB of the HP Operations management server). This setting is useful in cases where the HP Operations management server hostname is not resolvable on the RCP (for example, because of firewalls located between the RCP and the server). An HPOM HTTPS agent uses TARGET_FOR_RC to uniquely identify the server that the agent is trying to reach using the RCP.

TARGET_FOR_RC_CMD

Script or command name. If this parameter is set, the RCP validates against the core id of the target CB. For this setting to work, the output of the script or command must be a valid OV Core ID. If both TARGET_FOR_RC and TARGET_FOR_RC_CMD are specified, TARGET_FOR_RC takes precedence.

Example

```
PROXY=pnode.net.hp.com:1025+(*.*.hp.com)–(pnode.net.hp.com,pnode,*.noallow.hp.com)
```

In this example, the RCP on system `pnode.net.hp.com` is used with port 1025 while trying to reach any host that matches `*.*.hp.com` (for example, `host1.dmz.hp.com`, but not `server1.noallow.hp.com`). It is also possible to use IP addresses instead of hostnames. For example, `16.*.*.*` could be specified when identifying hosts.

IMPORTANT:
For correct operation, you must specify the RCP system name itself in the exclude list, so communication using the RCP does not loop at the RCP itself. For this reason, `pnode.net.hp.com` is already inside the exclude list of the above example.

Server side (trusted zone)

The server side is usually the HP Operations management server's communication broker (CB). The CB settings described in this section also apply to the use case of running an HPOM HTTPS agent in a secure environment, with one RCP between the server and the agent, one firewall between the server and the RCP, and one firewall between the agent and the RCP. (For details, see "RCP communication through two firewalls" on page 7.) To enable inbound communication from clients, the server must be configured to enable communication using an RCP.

During the CB startup, and whenever the CB configuration is changed using `ovconfchg`, the CB loads the configuration. The CB establishes the necessary Admin Reverse Channels internally.

```
[bbc.cb]
ENABLE_REVERSE_ADMIN_CHANNELS=true/false  //Default = false
RC_CHANNELS=<RCProxy1>:<RCP1_port>[;<RCP1_OvCoreID>][;<RCP2>...]
RC_CHANNELS_CFG_FILES=<filename>
MAX_RECONNECT_TRIES=--1                   // default infinite (--1)
RETRY_INTERVAL = 60                       // default is 60 sec
CHROOT_PATH=/
```

Syntax

`ENABLE_REVERSE_ADMIN_CHANNELS`

Permanent Admin Reverse Channel to the RCPs given in `RC_CHANNELS` is established only if this is set to true. This parameter is mandatory for outbound-only communication.

`RC_CHANNELS`

List of RCPs to establish Admin Reverse Channels. This is a mandatory parameter for outbound-only unless `RC_CHANNELS_CFG_FILES` is used instead.

Format:

<rcp1>:*<rcp1_port>*[,*<rcp1_OvCoreID>*][;*<rcp2>*…..]

OV Core ID is optional, and is comma-separated. If this parameter is set, the CB validates against the core id of the RCP.

Set `RC_CHANNELS` using the following command:

"ovconfchg –ns bbc.cb –set RC_CHANNELS *<rcp>*:*<rcp_port>*"

A semicolon-separated list of additional RCPs can be appended.

Note that the `–ovrg server` option is necessary in the `ovconfchg` call only when you are running on a high-availability (HA) cluster. For stand-alone HP Operations management servers, do not use this option when setting `RC_CHANNELS`.

If the server runs as an HA resource group, use the following command:

"ovconfchg –ovrg server –ns bbc.cb –set RC_CHANNELS *<value>*"

RC_CHANNELS_CFG_FILES

Format: <*filename*>

The file with the specified name must be placed in the <*DataDir*>/conf/bbc directory. This file can contain a list of one or more RCPs. Each line can contain only one RCP name. For each RCP, a port number must be specified.

The OV Core ID is optional, separated from the port number by a comma:

<*rcp*>:<*port*>[,<*rcp_OvCoreID*>]

Blank lines and comment lines (# is the first character) are permitted. The CB attempts to contact RCPs, as specified in RC_CHANNELS and RC_CHANNELS_CFG_FILES. If you change RCP hostnames inside the file specified by RC_CHANNELS_CFG_FILES, you will need to use ovconfchg to trigger the CB to reread the configuration.

One way to trigger the CB to reread the configuration is to use the following:

```
"ovconfchg -ns bbc.cb -set ENABLE_REVERSE_ADMIN_CHANNELS true"
```

In general, if you are using many RCPs, where RCP hostnames are often changed, use RC_CHANNELS_CFG_FILES rather than the RC_CHANNELS setting.

MAX_RECONNECT_TRIES

Number of times that a CB attempts to establish an admin channel. When this number is reached, the CB stops attempting to establish the channels, and the failure is logged.

RETRY_INTERVAL

Time interval, in seconds, of each retry for establishing an Admin Reverse Channel to an RCP.

Set this interval using the following command:

```
"ovconfchg -ns bbc.cb -set RETRY_INTERVAL 120"
```

The default value is 60 seconds.

CHROOT_PATH

On UNIX and Linux systems, the CB runs in chroot context with /var/opt/OV/ as its root directory. The CB may not be able to resolve RCP hostnames specified in RC_CHANNELS or inside the file specified by RC_CHANNELS_CFG_FILES. An accessible DNS service or host file is needed for hostnames to be successfully resolved into IP addresses. These IP addresses must be known before TCP connections can be opened.

Example

```
[bbc.cb]
RC_CHANNELS=pnode.net.hp.com:1025
```

In this example, the HP Operations management server CB attempts to contact the RCP on agent pnode.net.hp.com on port 1025 when starting up.

IMPORTANT:
On UNIX and Linux systems, the CB runs in chroot context with /var/opt/OV/ as its root directory. It will not be able to create connections to RCPs because it cannot locate /etc, where the configuration files relevant to name services are located. These files are needed for opening TCP connections.

Workaround A

Workaround A is more secure than Workaround B, but requires more maintenance (the hosts file must be updated regularly).

1. Create the following directory:
   `/var/opt/OV/etc`

   (The CB is chroot-ed to `/var/opt/OV`. When chroot-ed (the initial default setting), the CB is unable to access the file system root directory. The directory `/var/opt/OV/etc` is viewed as `/etc` by the CB.)

2. Copy the files relevant to the name service to the following directory:

   `/var/opt/OV/etc`

   Examples:

   `/etc/resolv.conf`

   `/etc/hosts`

   `/etc/nsswitch.conf`

NOTE:
Using a symbolic link will not work. Also, it would defeat the purpose of using the chroot feature.

Workaround B

Workaround B is less secure than workaround A because, with the chroot feature disabled, the CB, the RCP, or both can access all files and directories on the host system.

Disable the `ovbbccb` chroot feature with the following:

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

CAUTION:
Before adding, removing, or changing the `CHROOT_PATH` setting, you must stop the CB using `ovc -kill`.

Workaround C

Workaround C works only on the HP Operations management server side, and only if all `RC_CHANNELS` entries are IP addresses and not hostnames.

Use the IP address instead of the hostname. No name resolution is needed. The CB does not need to know the RCP hostname.

NOTE:
For HPOM HTTPS agents that are located behind a firewall, an HTTP proxy, or both, you need to set the Polling Type to "RPC Only (for firewalls)." (In the administrator GUI, click **Actions→Node→Modify**.) Otherwise, heartbeat polling from the server to the agent does not work.

Reverse Channel Proxy

The Reverse Channel Proxy (RCP) provides the secure link between the HP Operations management servers and the HPOM HTTPS agents.

```
[bbc.rcp]
SERVER_PORT=0                    //Default='9090'
CHROOT_PATH=/
```

Syntax

SERVER_PORT

RCP port number. This is a mandatory parameter for outbound-only.

Set this parameter using the following command:

"ovconfchg –ns bbc.rcp –set SERVER_PORT <*RCP_port*>"

Before setting SERVER_PORT, *always* use `netstat -an` to make sure the port you intend to use is *not* already occupied by another process:

- UNIX and Linux

  Check `/etc/services` to make sure the port you intend to use is *not* listed. Also verify that `/etc/services` does *not* already contain an entry for another service.

  CAUTION:
  If you add an entry to `/etc/services`, be aware that the file is readable by all users on the system by default.

- Windows

  You must reserve a port using a Windows registry setting.

For details, see the following links:

- Windows TCP/IP Ephemeral, Reserved, and Blocked Port Behavior
  http://technet.microsoft.com/en-us/library/bb878133.aspx
- Information about TCP/IP port assignments
  http://support.microsoft.com/kb/174904/EN-US/
- Official IANA list of TCP/IP port assignments
  http://www.iana.org/assignments/port-numbers
- Information on reserved TCP/IP ports
  http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

CHROOT_PATH=/

On UNIX and Linux systems, the RCP runs in chroot context with `/var/opt/OV/` as its root directory. It may *not* be able to resolve management server hostnames provided to it by requests from agents trying to contact the management server via this RCP because it cannot locate `/etc`, where the configuration files relevant to name services are located. These files are needed for opening TCP connections.

Workaround A

Workaround A is more secure than Workaround B, but requires more maintenance (the hosts file must be updated regularly).

1. Create the following directory:
   `/var/opt/OV/etc`

   (The RCP is chroot-ed to `/var/opt/OV`. When chroot-ed (the initial default setting), the RCP is unable to access the file system root directory. The directory `/var/opt/OV/etc` is viewed as `/etc` by the RCP.)

2. Copy the files relevant to the name service to the following directory:

   `/var/opt/OV/etc`

   Examples:

   `/etc/resolv.conf`

   `/etc/hosts`

   `/etc/nsswitch.conf`

NOTE:
Using a symbolic link will not work. Also, it would defeat the purpose of using the chroot feature.

Workaround B

Workaround B is less secure than workaround A because, with the chroot feature disabled, the RCP can access all files and directories on the host system. However, using RCP running on a UNIX or Linux system under a non-root user account further enhances security. In this case, you should use Workaround B. Otherwise, each time you start up the RCP, an error message will be logged to the `System.txt` log file.

Disable the `ovbbcrcp` chroot feature with the following:

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

CAUTION:
Before adding, removing, or changing the `CHROOT_PATH` setting, you must stop the RCP using `` `ovc -stop ovbbcrcp` ``.

IMPORTANT:
By default, `ovbbcrcp` (RCP process) is not controlled by `ovcd` (OvCtrl, the OV Control Component).
You must explicitly register `ovbbcrcp` with `ovctrl`, as follows:

```
$OvInstallDir/bin/ovcreg -add \
$OvInstallDir/newconfig/DataDir/conf/bbc/ovbbcrcp.xml
```

For example, for Solaris, you would register `ovbbcrcp` as follows:

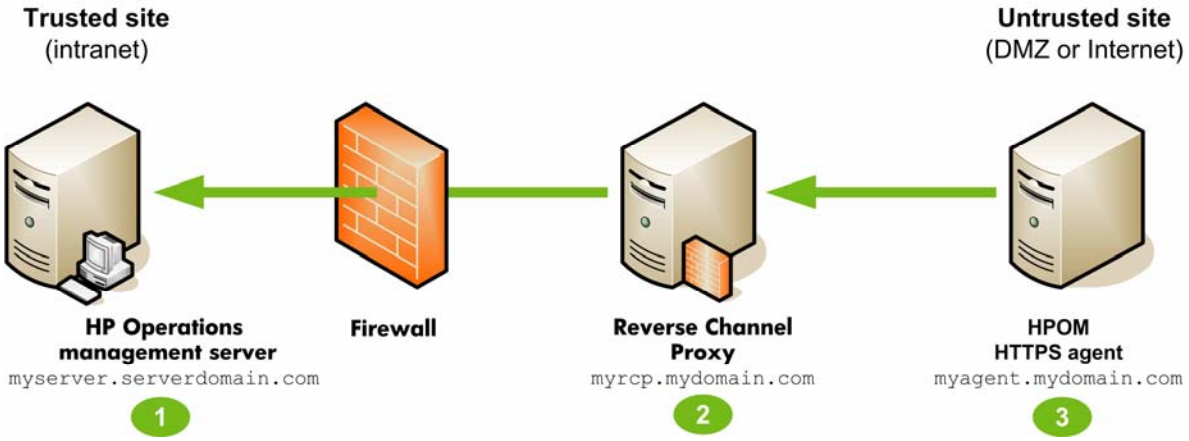
```
/opt/OV/bin/ovcreg -add \
/opt/OV/newconfig/DataDir/conf/bbc/ovbbcrcp.xml
```

For outbound-only, `ovc -start` should be used to start `ovbbcrcp`, together with the other registered processes. You must be user root to run the `ovcreg -add` command. A change request (QXCR1000781609) has been logged at HP for this problem.
For details about the `ovbbcrcp` command-line interface, see "Command-line interfaces" on page 17.

The system on which the RCP is running requires a "Trusted" and a "Node" certificate from the HP Operations management server (like any HPOM HTTPS agent).

A sample RCP configuration involving three machines is shown in Figure 6.

Figure 6. Sample RCP configuration



1. **OHP Operations management server** (`myserver.serverdomain.com`)

   ```
   [bbc.cb]
   RC_CHANNELS=myrcp.mydomain.com:1025
   ENABLE_REVERSE_ADMIN_CHANNELS=true
   ```

2. **Reverse Channel Proxy** (`myrcp.mydomain.com`)

   ```
   [bbc.rcp]
   SERVER_PORT=1025
   ```

3. **HPOM HTTPS agent** (`myagent.mydomain.com`)

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

Command-line interfaces

HPOM provides a command-line interface (CLI) tool, called `ovbbcrcp`, with the following functionality:

`ovbbcrcp`

Starts the RCP as a background process. Options include the following:

`-h|-help`

Displays and describes the available options for the `ovbbcrcp` command.

`-v|version`

Displays the version of the HPOM RCP in use.

`-kill`

Stops the RCP.

`-status`

Displays the RCP status.

Getting started

This section includes step-by-step instructions that show you how to set up outbound-only communication between an HP Operations management server and HPOM HTTPS agents using a Reverse Channel Proxy (RCP), as shown in Figure 3 in "RCP communication through one firewall" on page 5.

NOTE:
For outbound-only communication, the following minimum patch levels are required.

- HPOM for UNIX Management Server:
  A.08.23 Server Patch and A.08.16 Core Agent Patch

- HPOM HTTPS Agent RCP:
  A.08.16 (Core Agent)
  The A.08.16 Core Agent patch level includes HPOvBbc 06.00.052, HPOvConf 01.10.030, HPOvCtrl 01.50.240, HPOvSecCC 01.00.170, HPOvSecCo 02.20.070, and HPOvXpl 02.61.083.

If no RCP will be running on an agent system, no special patch level is required for that system. However, `[bbc.http] PROXY` must be set to route agent requests to a system with a running RCP that is able to connect to the server system.

Deploying the agent software to the HP Operations management server

To deploy the agent software to the server (or on a cluster, to all cluster nodes), follow these steps:

1. Open the Motif Administrator GUI Node Bank.
2. Select **Actions** → **Agents** → **Install / Update SW**.

   NOTE:
   Most of the time it is not necessary to activate the Force Update checkbox. Doing so greatly increases the time required to install the software.

3. Click **OK** to start the installation process.
4. Shut down all server processes completely using `ovstop` and restart them using `ovstart`.

Deploying software to HPOM HTTPS agent systems

Depending on the number of firewalls you have, or on your company procedures, it may not be possible to deploy agent software for new agents automatically. If you use manual agent installation, it is recommended that you use the `bbc.inst.defaults` mechanism to efficiently duplicate frequently used settings (for example, `[bbc.http] PROXY` and `[bbc.rcp] SERVER_PORT`) to multiple agents when installing them. For details, refer to the manual installation section of the *HP Operations Manager for UNIX HTTPS Agent Concepts and Configuration Guide* or the *HP Operations Manager for Windows Online Help*.

Setting up outbound-only communication

To set up outbound-only communication, follow these steps:

1. On the HP Operations management server system, use `ovconfchg -set` or `ovconfchg -edit` to set the `ENABLE_REVERSE_ADMIN_CHANNELS` and `RC_CHANNELS` configuration variables.

   In the examples below, 1025 is used as the RCP port number.

   Example 1:

   ```
   ovconfchg -ns bbc.cb -set ENABLE_REVERSE_ADMIN_CHANNELS true
   ovconfchg -ns bbc.cb -set RC_CHANNELS myrcp.mydomain.com:1025
   ```

   Example 2: (if your server is a cluster system)

   ```
   ovconfchg -ovrg server -ns bbc.cb -set ENABLE_REVERSE_ADMIN_CHANNELS \
   true
   ovconfchg -ovrg server -ns bbc.cb -set RC_CHANNELS \
   myrcp.mydomain.com:1025
   ```

   IMPORTANT:
   You must use the `-ovrg server` option for these two variables if your HP Operations management server is a cluster system.

2. Apply one of the workarounds described in "Server side (trusted zone)" on page 11.

   If you apply Workaround B, remember to stop the HP Operations management server CB before making the change.

3. On the HPOM HTTPS agent, set the `PROXY` configuration variable to use the RCP to communicate with the server.

   Example:

   ```
   ovconfchg -ns bbc.http -set PROXY \
   "myrcp.mydomain.com:1025+(*)-(myrcp.mydomain.com,myrcp)"
   ```

   In this example, the agent and RCP are on the same machine.

   NOTE:
   If the agent and RCP are running on separate systems, remember to add `",myagent.mydomain.com,myagent"` to the exclude part of the `PROXY` setting.

4. On the agent system, restart the message agent process with `ovc -restart opcmsga`.
5. On the RCP system, use `ovconfchg -set` or `ovconfchg -edit` to set the `SERVER_PORT` configuration variable.

   Example:

   ```
   ovconfchg -ns bbc.rcp -set SERVER_PORT 1025
   ```

   In this example, the RCP and agent are on the same machine.

6. On the RCP system, register `ovbbcrcp` with `ovc` so that this process will be started, stopped, and monitored by `ovc`.

Examples:

- UNIX or Linux

```
/opt/OV/bin/ovcreg –add \ /opt/OV/newconfig/DataDir/conf/bbc/ovbbcrcp.xml
```

- Windows 2000 or Windows XP

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

- Windows 2003 and later

```
cd "c:\documents and settings\all users\application data\hp\hp bto software\conf\bbc"
"c:\program files\hp openview\bin\ovcreg" -add ovbbcrcp.xml
```

7. On the RCP system, start the `ovbbcrcp` process with `ovc –start`.

   Use `ovbbcrcp -status` to check the status of the process. The output must include a line with `bbc.rcp` and the port number on which the RCP is listening.

   Also, within one minute, `ovbbcrcp -status` should list the accepted Admin Reverse Channel Connection from the HP Operations management server.

   On the server system, `ovbbccb -status` should list the successfully opened "HP OpenView HTTP Communication Reversal Channel Connection" to `myrcp.mydomain.com:myrcpportnumber`.

   If you run into problems, see "Troubleshooting" on page 22.

8. Test the connection on the agent using the following:

   - `bbcutil -gettarget myserver.serverdomain.com`

     The output should show that all agent communication will be routed using the proxy `myrcp.mydomain.com:myrcpportnumber`.

   - `bbcutil -ping myserver.mydomain.com`

     The output should include `status=eServiceOK` and the OV Core ID of the HP Operations management server. It is good practice to carefully verify that this OV Core ID is the correct OV Core ID.

   - Send a message (for example, using `opcmsg`). Verify that the message arrives in the message browser of the operator or administrator GUI.
   - Verify that the agent is not buffering messages. One way to do this is to run `/opt/OV/bin/opcagt` on UNIX or Linux. The output should state that the agent is not buffering messages. If it is buffering, wait two minutes, and run the command again. If it is still buffering, verify that all HP Operations management server processes are running.

9. Test the connection on the HP Operations management server using the following:
   - `bbcutil -gettarget myrcp.mydomain.com`

     The output should show that all communication will be routed directly to `myrcp.mydomain.com:383`. If the CB on `myrcp` has a different `[bbc.cb] SERVER_PORT` configured (for example, a non-root agent), the corresponding `[bbc.cb.ports] PORTS` must be set on the server. (To find out how to run agents under alternative users, refer to the *HP Operations Manager for UNIX HTTPS Agent Concepts and Configuration Guide* or the *HP Operations Manager for Windows Online Help*.) In this case, all communication will be routed to the `SERVER_PORT` configured for that agent.
   - `bbcutil -ping myrcp.mydomain.com`

     The output should include `status=eServiceOK` and the OV Core ID of the agent. It is good practice to carefully verify that this OV Core ID is the correct OV Core ID.
   - `/opt/OV/bin/OpC/opcragt myrcp.mydomain.com`

     The output should list all agent processes as running and the message agent as not buffering.

RCP performance considerations

To ensure proper performance, make sure that the RCP system can service incoming requests fast enough.

One RCP for one HPOM HTTPS agent

For a system hosting one RCP for one agent, meeting the minimum requirements for an agent system is sufficient. If you are planning to use one RCP for each agent (located on the same system), system performance will not be significantly impacted by this single additional process.

One RCP for more than one HPOM HTTPS agent (RCP as concentrator)

For a system hosting one RCP for more than one agent, meeting the minimum requirements for an agent system may not be sufficient. If you are planning to use one RCP for more than one agent system, you must ensure that the RCP system will be able to service all incoming requests fast enough.

Incoming requests are serviced on a first-come, first-served basis (FIFO queue). No additional disk space is required for the RCP system. Usage of CPU capacity by the RCP is roughly comparable to that of the HP Operations management server BBC message receiver process (`opcmsgrb`).

If an RCP has open Admin Reverse Channel Connections to more than one server, and if communication with one of the servers is interrupted, this interruption will not adversely affect communication with the other servers. If the RCP gets overloaded, message throughput will drop. However, sufficient safeguards are in place to ensure that no messages will be lost in transit (as long as the hard disks and file systems are functioning correctly).

HTTPS outbound-only communication between the agent and the server uses an end-to-end SSL handshake/authentication. No SSL stops occur between the server and the agent. As a result, no data is buffered by the RCP.

Troubleshooting

For additional troubleshooting information, refer to the following documents:

- HPOM for UNIX
  - *Firewall Concepts and Configuration Guide*
  - *HTTPS Agent Concepts and Configuration Guide*
- HPOM for Windows
  - *Firewall Concepts and Configuration Guide*
  - Online Help

Verifying RCP communication from an agent to the server

To verify that the agent system configuration correctly routes agent requests to the HP Operations management server using Reverse Channel Proxy (RCP), use the following command:

```
/opt/OV/bin/bbcutil -gettarget <management server hostname>
```

The output should look something like this:

```
HTTP Proxy: myrcp.mydomain.com:1025 (126.157.135.32)
```

NOTE:
The `bbcutil` command cannot differentiate between a regular HTTP proxy and an RCP. In this example, the RCP must be running on `myrcp.mydomain.com` using port 1025 for RCP communication to work correctly.

Verifying RCP-to-server communication through a firewall

To verify that an Admin Reverse Channel was correctly set up to the Reverse Channel Proxy (RCP), use the following command on the HP Operations management server:

```
/opt/OV/bin/ovbbccb –status
```

Check the last section of the output from this command, which is entitled "HP OpenView HTTP Communication Reverse Channel Connections."

The command output should look something like this:

```
HP OpenView HTTP Communication Reverse Channel Connections
 Opened:
  tcpc50.mydomain.com:1025    BBC 06.00.041; ovbbcrcp 06.00.041
  tcvm1119.mydomain.com:1025    BBC 06.00.041; ovbbcrcp 06.00.041
  ichthys.mydomain.com:1025    BBC 06.00.041; ovbbcrcp 06.00.041
  blauber.mydomain.com:1025    BBC 06.00.041; ovbbcrcp 06.00.041
 Pending:
  myrcp.mydomain.com:1025 Connection To Host Failed
  sagar.mydomain.com:1025 Connection To Host Failed
  tcdhcp1118.mydomain.com:1025 Connection To Host Failed
```

The `Opened` connections were established successfully. Some connections are pending because communication between the server and the RCP is not working. Such a communication problem can occur if a port is blocked by the firewall for this destination port (outbound, see Figure 1 in "Outbound-only communication in HPOM" on page 2), another application is listening on the same port, an agent system has no route to the server, and so on.

Verifying the connection to the RCP

If you run `ovbbccb -status`, and receive an error message with a status of `Error Unknown` or `Connection to Host Failed`, you need to verify the connection to the host. (For more about `ovbbccb -status`, see "Verifying RCP-to-server communication through a firewall" on page 22).

To verify the connection to the RCP, check the following:

- **RCP port number**

  Check the port number to which the CB on the HP Operations management server tries to connect. It is configured in `RC_CHANNELS` (or `RC_CHANNELS_CFG_FILES`) on the server.

  Is `:port number` attached after the hostname?

  – Correct: `myrcp.mydomain.com:1025`

  – Incorrect: `myrcp.mydomain.com`

  If the port number is configured correctly, check for the correct spelling of the RCP hostname, the fully qualified name, or the IP address (in case you specified an IP address instead of a hostname) configured in `[bbc.cb] RC_CHANNELS`. (If you used `RC_CHANNELS_CFG_FILES`, check the RCP name or IP address in the files).

  Try using telnet from the management server to the RCP system using the RCP port number (for example, **`telnet myrcp.mydomain.com 1025`**).

- **Firewall**

  Is the firewall open for this destination port (outbound, see Figure 1 in "Outbound-only communication in HPOM" on page 2)?

- **RCP port**

  On the RCP, check the RCP port using `ovbbcrcp -status`. Does this display the RCP as running on the same port number as configured for the `RC_CHANNELS` on the server?

  If `ovbbcrcp -status` takes a very long time and eventually times out with an error, this could be because another process is already using the port that you configured. You can check if this is the case by using **`netstat -an`**. Very likely, port 1025 is already occupied. Ports 1026 and 1027 may also be occupied. Disparate processes using the same port often causes problems. The RCP must have exclusive use of the configured port. For details, see "Reverse Channel Proxy" on page 14.

- **DNS setup**

  Depending on your DNS, it is possible that some agents may not be able to establish communication to the server. In this case, you can set `TARGET_FOR_RC` to the OV Core ID of the server. If the server is a cluster system, use the OV Core ID of the virtual node. For details, see "Client side (untrusted zone)" on page 9.

- **SSL certificates**

  Verify that SSL certificates and trust are set correctly between the RCP system and the management server. Search for all mentions of certificates in this white paper.

Verifying the OV Core IDs for agents

Another problem that causes communication between the HP Operations management server and the agent to fail is a null OV Core ID for the agent system in the HP Operations management server database. This null OV Core ID can occur when the agent software is installed manually or a node is added to the OVO Node Bank although it is already configured.

To check for an OV Core ID mismatch, follow these steps:

1. Open the HPOM Motif Administrator GUI.
2. Right-click the node in question.
3. From the shortcut menu, select **Modify**.
4. In the Modify Node window, click **Communication Options**.

The OV Core ID must match the OV Core ID as output by the `/opt/OV/bin/ovcoreid` command on the agent.

If the OV Core ID is all zeroes (`000...`), you must update the OV Core ID in the HP Operations management server database using this command:

```
/opt/OV/bin/OpC/utils/opcnode -chg_id node_name=myrcp.mydomain.com id="mycoreid"
```

Verifying the status of installed certificates on agents

A system running on the untrusted side of a firewall must have a valid HPOM certificate for HTTPS communication to work between the agent and the HP Operations management server.

To check the status of installed certificates on the agent, use the following:

```
/opt/OV/bin/ovcert -list
```

The output should look something like this:

```
+------------------------------------------------------------+
| Keystore Content                                           |
+------------------------------------------------------------+
| Certificates:                                              |
|     c731ede6-8061-7513-1d42-b85318b1d914 (*)               |
+------------------------------------------------------------+
| Trusted Certificates:                                      |
|     CA_03189d8a-d4bd-7510-1c23-90eb20297618                |
|     CA_3f1aa992-f8d9-750f-1259-91b920df5b5c                |
|     CA_fbc26e82-527b-7514-115b-df5797658102                |
+------------------------------------------------------------+
```

The `Certificates` section must contain a line with the OV Core ID of the agent system.

To see the OV Core ID, use the following:

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

The `Trusted Certificates` section must contain a line with the OV Core ID of the HP Operations management server. If the server is a cluster, the OV Core ID of the virtual node must appear in this list.

In a MoM environment, you will see a certificate authority (CA) certificate for each of the MoM servers, as shown in the example.

For details on how to correctly issue and install certificates on agents, refer to the *HP Operations Manager for UNIX HTTPS Agent Concepts and Configuration Guide* or the *HP Operations Manager for Windows Online Help*.

Verifying the certificate authorities for RCPs and agents

When the agent is on a different system than the RCP, and the RCP was installed from another HP Operations management server (MoM environment), it is possible for communication to fail with SSL-related errors reported in the `System.txt` error log file. Verify that both certificate authorities (CAs) are among the trusted certificates of the agent and the RCP.

To get the Issuer CA of a certificate, use the following command:

```
ovcert -certinfo `ovcoreid`| grep "Issuer CN"
```

Verify that the Issuer CA is listed in the Trusted Certificates section of `ovcert -list` on the other node:

```
ovcert –list
```

If the trusted certificate is not known on one of the two systems, exchange the trusted certificates from the agent to the RCP system, and from the RCP system to the agent.

To export the trusted certificates from the agent to the RCP system, follow these steps:

1. Export the trusted certificates from the agent:

   ```
   ovcert -exporttrusted -file /tmp/trusted
   ```

2. Copy the file `/tmp/trusted` to the RCP system and import the certificates:

   ```
   ovcert -importtrusted -file /tmp/trusted
   ```

To export the trusted certificates from the RCP system to the agent, follow these steps:

1. Export the trusted certificates from the RCP system:

   ```
   ovcert -exporttrusted -file /tmp/trusted
   ```

2. Copy the file `/tmp/trusted` to the agent and import the certificates:

   ```
   ovcert -importtrusted -file /tmp/trusted
   ```

For more information about security in MoM environments, refer to the *HP Operations Manager for UNIX HTTPS Agent Concepts and Configuration Guide* or the *HP Operations Manager for Windows Online Help*.

Verifying the trusted certificates of the server

Verify that the server can communicate with the agent:

```
/opt/OV/bin/OpC/opcragt myrcp.mydomain.com
```

If you get SSL errors, run this command:

```
ovcert -list
```

Verify that all of the trusted certificates from the keystore OVRG server are also available in the agent keystore (first section).

If they are not, update the trusted certificates:

```
ovcert -updatetrusted
```

For a server in a cluster environment, repeat this step on all of the physical nodes of the cluster.

Sample customer setups

This section shows how some customers have set up HP Operations with outbound-only communication.

Figure 7 shows a sample customer setup with an HP Operations management server cluster.

Figure 7. HP Operations management server cluster

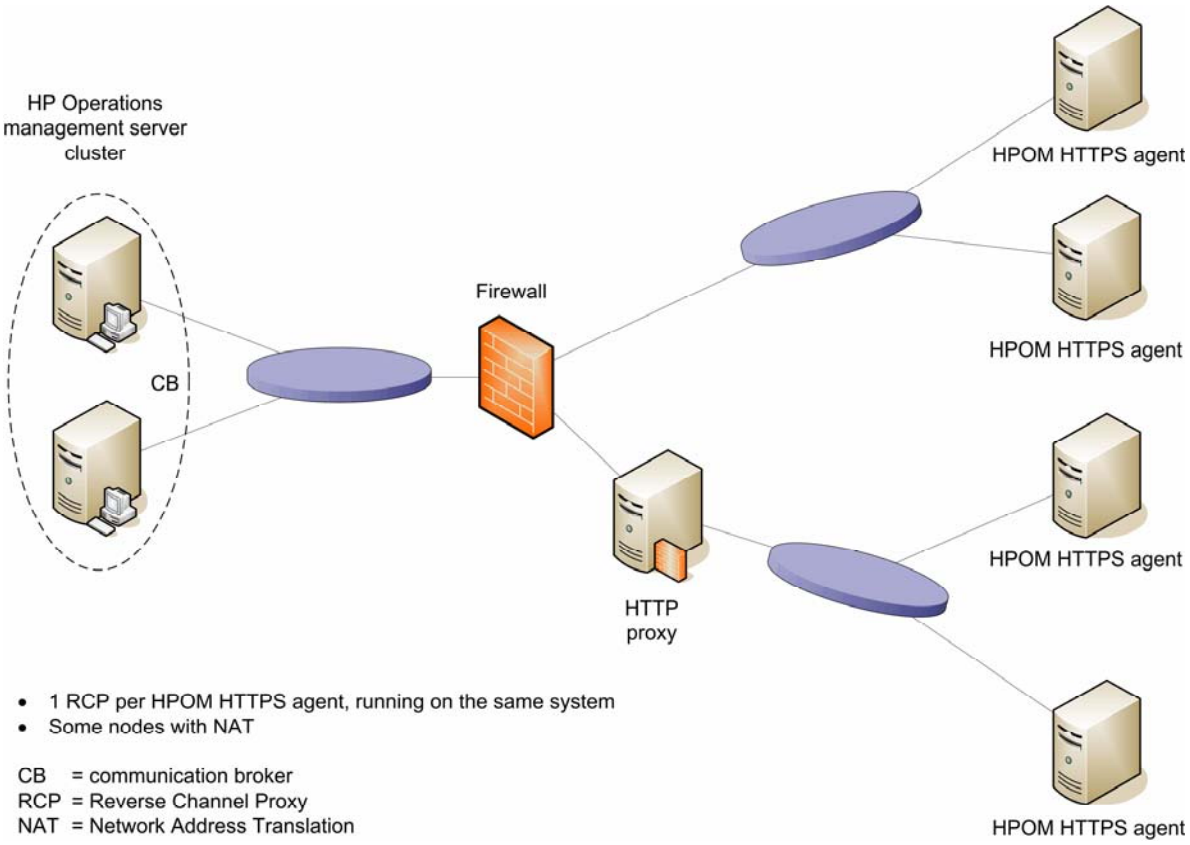
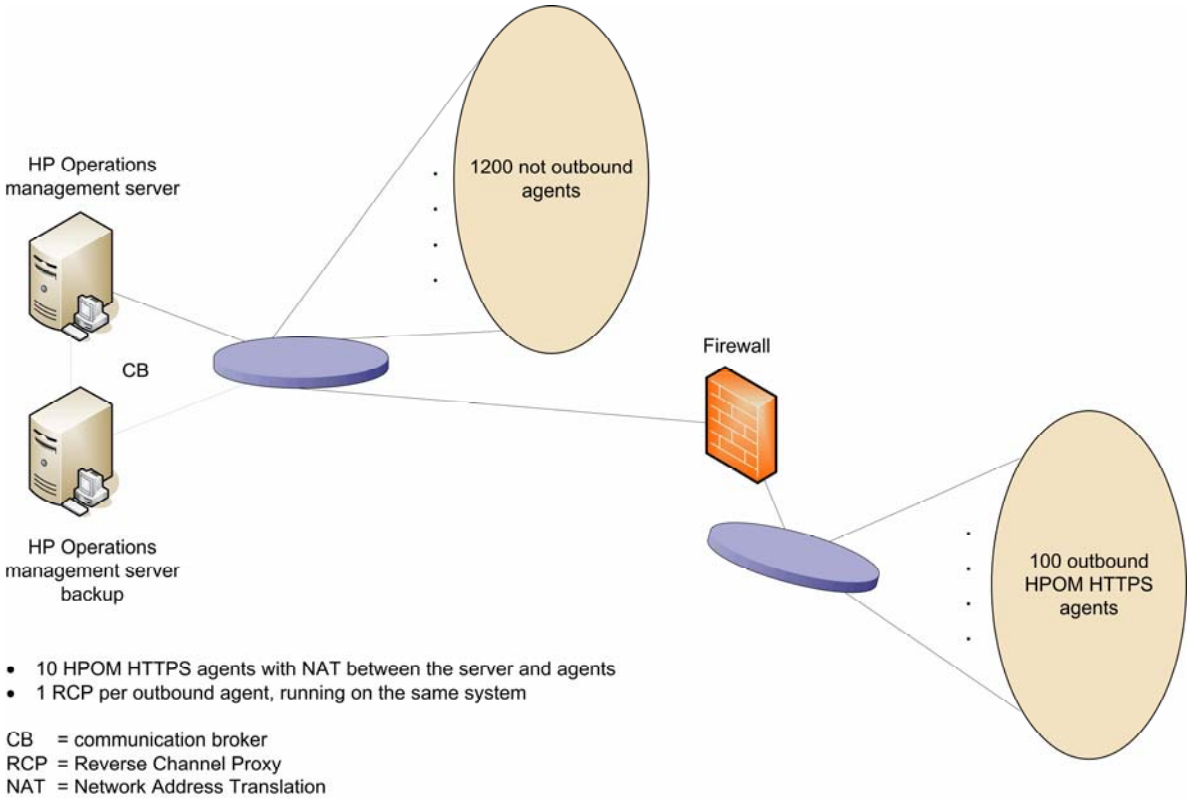


Figure 8 shows a sample customer setup with an HP Operations management server, a backup server, and 100 outbound HPOM HTTPS agents.

Figure 8. HP Operations management server, backup server, and outbound HPOM HTTPS agents



Glossary

Admin Reverse Channel Connection

HTTPS connection initiated by a CB in a high trust zone through a firewall to a RCP in a low or medium trust zone. The connection remains open until it is closed by the CB or the RCP. The connection is used by the RCP to "tunnel" connections from systems in the low or medium trust zone to the CB in the high trust zone.

CB

communication broker. HP Operations process that enables other processes to communicate with nodes through a single TCP port.

HTTP Tunneled Connection

HTTPS connection from a system in a medium or low trust zone to a CB in a high trust zone, through a firewall. An RCP in the medium or low trust zone "tunnels" this connection through the firewall. An HTTP Tunneled Connection can be established only if the CB in the high trust zone has an open Admin Reverse Channel Connection to the RCP.

outbound-only communication

TCP/IP communication through a firewall. For this type of communication, the firewall is configured such that a trusted system is able to send data out through the firewall, typically using any TCP port. After this specific port is opened by the trusted system, the untrusted system on the other side of the firewall can send data back to the trusted system on the open port. The trusted system controls when and for how long ports are opened. If no ports are open, no untrusted system can send data through the firewall to the trusted system.

ovbbcrcp

Command-line utility that starts and stops the RCP as a background process on an HPOM HTTPS agent system.

OVIS

HP Internet Services

OVPA

HP Performance Agent

OVPM

HP Performance Manager

RCP

Reverse Channel Proxy. HP Operations process (`ovbbcrcp`) that can provide a secure link between two systems, using the HTTPS protocol. Used to allow outbound-only communication through firewalls.

trust zone

Network separated from other networks by at least one firewall. Network traffic originating from a low trust zone is normally blocked by the firewall, and is thus normally unable to reach systems in a high trust zone on the other side of the firewall.

trusted site

Site that is trusted by another communications party. It can contain multiple trust zones.

Document updates

The first page of this document contains the version number, which indicates the software version.

The last page of this document contains the publish date, which changes each time the document is updated.

To check for recent updates, or to verify that you are using the most recent edition, visit the following URL:

http://support.openview.hp.com/selfsolve/manuals

1. In the Product list, click the product name (for example, **Operations Manager for UNIX**).
2. In the Product Version list, click the version number (for example, **8.0**).
3. In the Operating System list, click the operating system type (for example, **HP-UX**).
4. In the Optional text box, enter keyword text (for example, **outbound**) to restrict the search.
5. To retrieve a list of matching documents, click **Search** or press **Enter**.
6. In the list of results, click the appropriate link to open the document.

NOTE:
To view files in PDF format (*.pdf), Adobe Acrobat Reader must be installed on your system. To download Adobe Acrobat Reader, go to the following URL:
http://www.adobe.com

12/2008