HP Operations Manager on Linux

HTTPS Agent
Concepts and Configuration Guide

Software Version: 9.01

Manufacturing Part Number: n/a

September 2009

Legal Notices

Warranty.

Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices.

Trademark Notices.

Adobe® is a trademark of Adobe Systems Incorporated.

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

Java™ is a US trademark of Sun Microsystems, Inc.

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

1. HP Operations HTTPS Agent Overview

2. Concepts of HTTPS Communication

3. Security Concepts

4. Concepts of Managing HTTPS Nodes

5. Working with HTTPS Managed Nodes

6. Working with Certificates

7. Virtual Nodes in HPOM

B. Tracing HPOM

C. Configuring HTTPS-Based Communication

D. HTTPS Communication Architecture

E. Firewalls and HTTPS Communication

Printing History

The printing date and part number of the manual indicate the edition of the manual. The printing date will change when a new edition is printed. Minor changes may be made at reprint without changing the printing date. The part number of the manual will change when extensive changes are made.

Manual updates may be issued between editions to correct errors or document product changes. To ensure that you receive the updated or new editions, you should subscribe to the appropriate product support service. See your HP sales representative for details.

Table 1

First Edition:	September 2009

Conventions

The following typographical conventions are used in this manual:

Table 2 Typographical Conventions

Font	Meaning	Example
Italic	Book or manual titles, and manpage names	See the *HPOM Administrator's Reference* and the *opc(1M)* manpage for more information.
	Emphasis	You *must* follow these steps.
	Variable that you must supply when entering a command	At the prompt, enter **`rlogin`** ***`username`***.
	Parameters to a function	The *`oper_name`* parameter returns an integer response.
Bold	New terms	The **HTTPS agent** tracks...
`Computer`	Text and other items on the computer screen	The following system message displays: `Are you sure you want to remove current group?`
	Command names	Use the `grep` command ...
	Function names	Use the `opc_connect()` function to connect...
	File and directory names	`/opt/OV/bin/OpC/`
	Process names	Check to see if `opcmona` is running.
	Window names	In the `Add Logfile` window...
	Menu name followed by a colon (`:`) means that you select the menu, then the item. When the item is followed by an arrow (`->`), a cascading menu follows.	Select `Actions: Filtering -> All Active Messages` from the menu bar.

Table 2 Typographical Conventions (Continued)

Font	Meaning	Example
`Computer Bold`	Text that you enter	At the prompt, enter **`ls -l`**
Keycap	Keyboard keys	Press **Return**.
`[Button]`	Buttons in the user interface	Click `[OK]`.

HPOM Documentation Map

HP Operations Manager (HPOM) provides a set of manuals and online help that help you to use the product and to understand the concepts underlying the product. This section describes what information is available and where you can find it.

Electronic Versions of the Manuals

All the manuals are available as Adobe Portable Document Format (PDF) files in the documentation directory on the HPOM product CD-ROM.

With the exception of the *HPOM Software Release Notes*, all the manuals are also available in the following HPOM web-server directory:

`http://<management_server>:3443/ITO_DOC/<lang>/manuals/*.pdf`

In this URL, <*management_server*> is the fully qualified hostname of your management server, and <*lang*> stands for your system language, for example, `C` for the English environment.

Alternatively, you can download the manuals from the following website:

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

Watch this website regularly for the latest edition of the *HPOM Software Release Notes*, which is updated every two to three months with the latest news (for example, additionally supported operating system versions, the latest patches and so on).

HPOM Manuals

This section provides an overview of the HPOM manuals and their contents.

Table 3 HPOM Manuals

Manual	Description	Media
HPOM Installation Guide for the Management Server	Designed for administrators who install HPOM software on the management server and perform the initial configuration. This manual describes the following: • Software and hardware requirements • Software installation and de-installation instructions • Configuration defaults	PDF only
HPOM Concepts Guide	Provides you with an understanding of HPOM on two levels. As an operator, you learn about the basic structure of HPOM. As an administrator, you gain an insight into the setup and configuration of HPOM in your own environment.	PDF only
HPOM Administrator's Reference	Designed for administrators who install HPOM on the managed nodes and are responsible for HPOM administration and troubleshooting. Contains conceptual and general information about the HPOM managed nodes.	PDF only
HPOM HTTPS Agent Concepts and Configuration Guide	Provides platform-specific information about each HTTPS-based managed node platform.	PDF only
HPOM Reporting and Database Schema	Provides a detailed description of the HPOM database tables, as well as examples for generating reports from the HPOM database.	PDF only
HPOM Java GUI Operator's Guide	Provides you with a detailed description of the HPOM Java-based operator GUI and the Service Navigator. This manual contains detailed information about general HPOM and Service Navigator concepts and tasks for HPOM operators, as well as reference and troubleshooting information.	PDF only

Table 3 HPOM Manuals (Continued)

Manual	Description	Media
Service Navigator Concepts and Configuration Guide	Provides information for administrators who are responsible for installing, configuring, maintaining, and troubleshooting the HP Operations Service Navigator. This manual also contains a high-level overview of the concepts behind service management.	PDF only
HPOM Software Release Notes	Describes new features and helps you: • Compare features of the current software with features of previous versions. • Determine system and software compatibility. • Solve known problems.	PDF only
HPOM Firewall Concepts and Configuration Guide	Designed for administrators. This manual describes the HPOM firewall concepts and provides instructions for configuring the secure environment.	PDF only
HPOM Web Services Integration Guide	Designed for administrators and operators. This manual describes the HPOM Web Services integration.	PDF only
HPOM Security Advisory	Designed for administrators. This manual describes the the HPOM security concepts and provides instructions for configuring the secure environment.	PDF only
HPOM Server Configuration Variables	Designed for administrators. This manual contains a list of the HPOM server configuration variables.	PDF only

Additional HPOM-Related Products

This section provides an overview of the HPOM-related manuals and their contents.

Table 4 Additional HPOM-Related Manuals

Manual	Description	Media
HP Operations Manager on Linux Developer's Toolkit If you purchase the HP Operations Manager on Linux Developer's Toolkit, you receive the full HPOM documentation set, as well as the following manuals:		
HPOM Application Integration Guide	Suggests several ways in which external applications can be integrated into HPOM.	PDF
HPOM Developer's Reference	Provides an overview of all the available application programming interfaces (APIs).	PDF

HPOM Online Information

The following information is available online.

Table 5 HPOM Online Information

Online Information	Description
HPOM Java GUI Online Information	HTML-based help system for the HPOM Java-based operator GUI and Service Navigator. This help system contains detailed information about general HPOM and Service Navigator concepts and tasks for HPOM operators, as well as reference and troubleshooting information.
HPOM Manpages	Manpages available online for HPOM. These manpages are also available in HTML format. To access these pages, go to the following location (URL) with your web browser: `http://<management_server>:3443/ITO_MAN` In this URL, the variable <*management_server*> is the fully qualified hostname of your management server. Note that the manpages for the HP Operations HTTPS agents are installed on each managed node.

HPOM Online Help

This preface describes online documentation for the HP Operations Manager (HPOM) Java operator graphical user interface (GUI).

Online Help for the Java GUI and Service Navigator

The online help for the HP Operations Manager (HPOM) Java graphical user interface (GUI), including Service Navigator, helps operators to become familiar with and use the HPOM product.

Types of Online Help

The online help for the HPOM Java GUI includes the following information:

- **Tasks**

  Step-by-step instructions.

- **Concepts**

  Introduction to the key concepts and features.

- **References**

  Detailed information about the product.

- **Troubleshooting**

  Solutions to common problems you might encounter while using the product.

- **Index**

  Alphabetized list of topics to help you find the information you need, quickly and easily.

Viewing a Topic

To view any topic, open a folder in the left frame of the online documentation window, then click the topic title. Hyperlinks provide access to related help topics.

Accessing the Online Help

To access the help system, select `Help: Contents` from the menu bar of the Java GUI. A web browser opens and displays the help contents.

NOTE To access online help for the Java GUI, you must first configure HPOM to use your preferred browser.

Support

Please visit the HP Software support 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 online software 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 valuable support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit enhancement requests online
- Download software patches
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter 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 log in. Many also require a support contract.

To find more information about access levels, go to:

http://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

http://www.managementsoftware.hp.com/passport-registration.html

1 HP Operations HTTPS Agent Overview

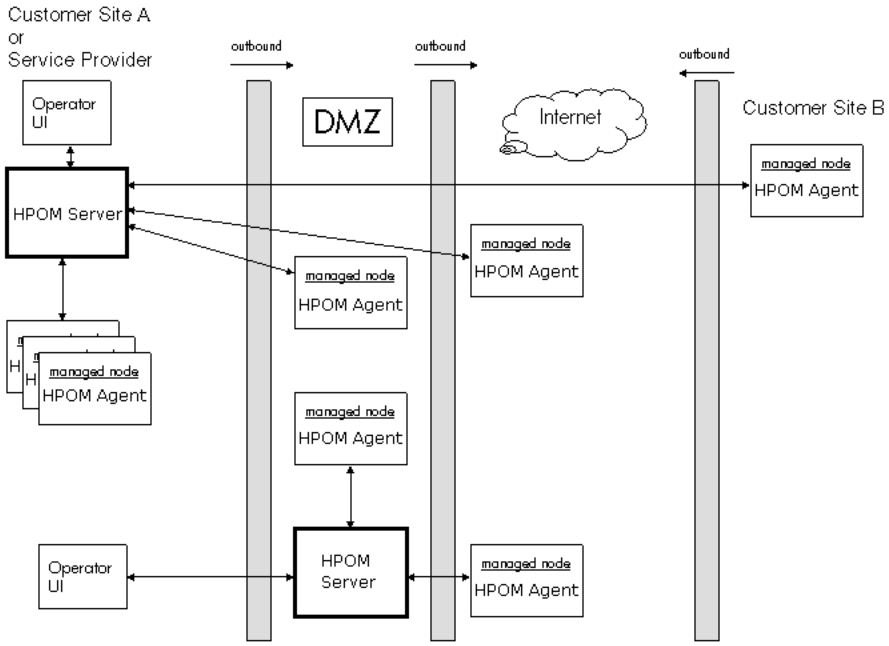
Introduction

HTTPS agent software provides highly secure communication between HP Operations management servers and their managed nodes.

Figure 1-1 illustrates a typical environment managed by HP Operations Manager.

Advantages and benefits of using the HTTPS agents are described in the following chapters.

Figure 1-1 A Typical HPOM Managed Environment



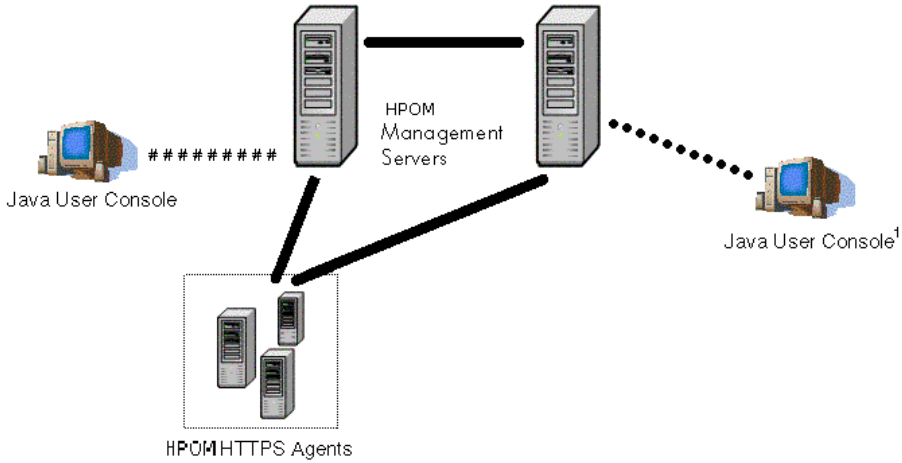
HTTPS-based communication provides you with the following major advantages:

- Simple management through firewalls with configurable, single-port, secure communication using, open, HTTPS-based communication techniques. Restrict outside access to dedicated HTTP proxies and reduce port usage by multiplexing over HTTP proxies.

- Out-of-the-box Internet Secure Communication using SSL/PKI encryption with server and client certificates for authentication.
- Communication is based on standard Web technologies (HTTP, SOAP, Proxies, SSL, …), available in every environment today, and familiar to every IT administrator.
- HPOM message format based on XML and SOAP used for message security from the HTTPS agent to the HP Operations management server.
- IP independence/dynamic IP (DHCP). Managed nodes can be identified by their unique `OvCoreID` and not necessarily by their IP addresses.
- No need for additional investments (training, additional software).
- HP Operations standard control and deployment mechanism.
- HP Operations standard logging capability.
- HP Operations standard tracing capability.

Figure 1-2 illustrates an example of the different communication types in HPOM.

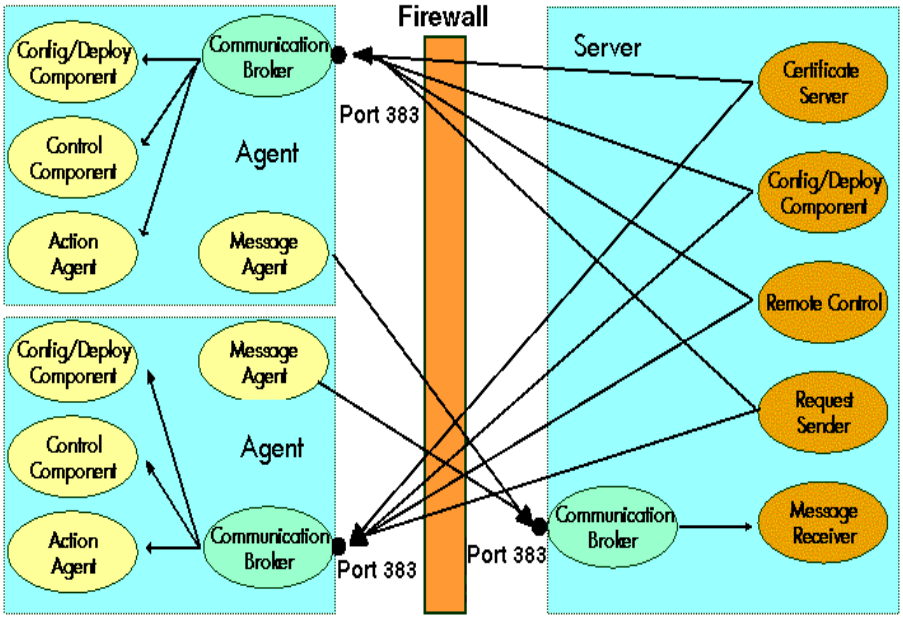
Figure 1-2 Communication Overview in HP Operations Manager



HP Operations HTTPS Agent Architecture

The following graphics illustrate the architecture of the HTTPS communication in HPOM.

Figure 1-3 **HTTPS Agent Components and Responsibilities**



HTTPS Agent Platforms Supported with HPOM 9.xx

- AIX
- HP-UX (PA-RISC)

  HP-UX (Itanium IA64)
- Linux (Intel x86)
- Microsoft Windows (Intel x86)

  Microsoft Windows (Intel x64)
- Sun Solaris (Intel x86)

  Sun Solaris (SPARC)

For the most up-to-date list of supported managed node platforms, see the latest version of the *HPOM Software Release Notes*. This document is available in PDF format from: `http://support.openview.hp.com/selfsolve/manuals` under *Operations Manager on Linux*, version *9.x*.

Organization of HTTPS Managed Nodes

Generic Directory Structure on a Managed Nodes

The files associated with the HTTPS agent are found in the following directory structures by default:

- **<OvInstallDir>**

  HP-UX, Solaris, Linux `/opt/OV/`

  AIX `/usr/lpp/OV/`

  Windows `%ProgramFiles%\HP\HP BTO Software`

  This directory contains static files that are installed from the product media and never change, for example, executables. Since these files never change, you can mount <*InstallDir*> as “read-only” for increased security in highly sensitive environments. It is not necessary to back up these files as they can be re-installed from the product media.

  All other files change during operation and must be backed up regularly.

- **<OvDataDir>**

  HP-UX, Solaris, AIX, Linux

  ```
  /var/opt/OV
  ```

  Windows Server 2008, Windows Vista

  ```
  %AllUsersProfile%\HP\HP BTO Software
  ```

  Windows Server 2003, Windows XP

  ```
  %AllUsersProfile%\Application Data\HP\HP
  BTO Software
  ```

  This directory contains configuration and runtime data files that are used only on the local system. The most important directory contains the instrumentation files such as actions, commands and monitors:

  <*OvDataDir*>/bin/instrumentation

The *<OvInstallDir>*/newconfig/inventory/*.xml files contain a list of all the directories and files that are created and installed with the agent software.

HPOM Agent User and the opc_op Accounts

The HPOM agent runs by default as `root` on UNIX, and as `system` on Windows. It is assumed that the HPOM agent account already exists on a managed node, when the agent is installed. At HPOM agent installation time, an additional minimal-rights account is created—the `opc_op` account. Its main purpose is to execute actions with minimal rights.

Table 1-1 shows the HPOM agent accounts on UNIX managed nodes.

Table 1-1 HPOM Accounts on UNIX Managed Nodes

Account Characteristics	HPOM Agent Account	Additional Minimal-rights Account
User Name	`root`	`opc_op`[a]
Password	Defined for user `root`	Defined during installation
Group	`sys`	`opcgrp`
Login Shell	Korn Shell (`/bin/ksh`)	POSIX Shell (`/bin/sh`)
home directory	`/.root`	`/home/opc_op`

a. It is not possible to log into the system directly using the `opc_op` account (enter `*` in `/etc/passwd`).

NOTE HPOM software on UNIX managed nodes systems can be configured to run under a user that does not have full root permissions, often referred to as “running as non-root”. For details, see “Agents Running Under Alternative Users” on page 86.

If the managed node is a Network Information Service (NIS or NIS+) client, you must add the `opc_op` account as a member of the `opcgrp` group on the NIS server before installing the HPOM software on a managed node. This ensures that the `opc_op` account is used by HPOM and is consistent on all systems.

If you do not add the `opc_op` account on the NIS server, the installation creates a user `opc_op` with the group `opcgrp` locally on the managed node.

Table 1-2 shows the HPOM agent accounts on Windows managed nodes.

Table 1-2 HPOM Agent Accounts on Windows Managed Nodes

Account Characteristics	HPOM Agent Account
User Name	Built-in system
Password	N.A.
Rights	`Local Administrator`

UNIX System Resources

HPOM applies changes in the following system resource files:

`/etc/passwd`	Default HPOM operator entry.
`/etc/group`	Default HPOM operator group entry.
<BootDir>`/OVCtrl`	HPOM startup and shutdown.
<BootDir>`/TrcSrv`	HP Operations Tracing start and stop.

Value of *<BootDir>*:

AIX	`/etc/rc.d`
HP-UX	`/sbin/init.d`
Linux	`/etc/rc.d/init.d`
Solaris	`/etc/init.d`

NOTE If you are working with Network Information Services (NIS or “yellow pages”), you should adapt the user registration accordingly.

Symbolic links <*BootDir*>/OVCtrl and <*BootDir*>OVTrcSrv to define the start and stop sequences at boot time of the https agent:

HP-UX

Start Trace Daemon.	/sbin/rc3.d/S900VTrcSrv
Start HPOM Agent.	/sbin/rc3.d/S920VCtrl
Stop Agent.	/sbin/rc2.d/K010VCtrl
Stop Trace Server.	/sbin/rc2.d/K020VTrcSrv

AIX

Start Trace Daemon	/etc/rc.d/rc2.d/S90OVTrcSrv
Start HPOM Agent	/etc/rc.d/rc2.d/S92OVCtrl
Stop Agent	/etc/rc.d/rc<*num*>.d/K02OVTrcSrv
Stop Trace Server	/etc/rc.d/rc<*num*>.d/K01OVCtrl
	Where <*num*> = 3, 4, 5, ...8, 9.

Solaris

Start Trace Daemon	/etc/rc3.d/S90OVTrcSrv
Start HPOM Agent	/etc/rc3.d/S92OVCtrl
Stop Agent	/etc/rc<*key*>.d/K01OVCtrl
Stop Trace Server	/etc/rc<*key*>.d/K01OVTrcSrv
	/etc/rc<*key*>.d/K02OVTrcSrv
	Where <*key*> = 0 | 1 | 2 | S.

Linux

Start Trace Daemon	/etc/rc.d/rc<*num*>.d/S90OVTrcSrv
Start HPOM Agent	/etc/rc.d/rc<*num*>.d/S92OVCtrl
	<*num*> = 3 | 4 | 5
Stop HPOM Agent	/etc/rc.d/rc<*num*>.d/K01OVCtrl
Stop Trace Server	/etc/rc.d/rc<*num*>.d/K02OVTrcSrv
	<*num*> = 0 | 1 | 2 | 6

Windows System Resources

User Environment Variables

HPOM sets the following user environment variables, which can be used in scripts, for example, when setting up automatic actions in policies:

Table 1-3 Windows User Environment Variables

Variable	Location and Explanation
`OvDataDir`	The directory for HP Software configuration and runtime data files.
`OvInstallDir`	The installation directory for the HP BTO Software.
`OvPerlADir`	Directory that contains the agent's Perl interpreter.

Starting and Stopping the Windows Agent

`ovcd` starts the components after reboot if the value of `START_ON_BOOT` is set to `true` in the `[ctrl]` namespace (common to both Windows and UNIX platforms). To set this value, enter the following command:

```
ovconfchg -ns ctrl -set START_ON_BOOT true
```

The `Control` service startup should be configured to startup automatically after reboot. To configure a service, open the `Services` window:

Click **Start** –> **Control Panel** –> **Administrative Tools** –> **Services**

Open the properties window of the `Control` service, and select **Automatic** from the **Startup type** drop down menu.

Registry Keys

HPOM inserts several keys in the Windows Registry.

The keys and their associated values can be viewed with the Registry Editor, using the following command:

```
%SystemRoot%\System32\regedt32.exe
```

There are many registry changes that happen during the installation of the agent. They can be generally classified as follows:

- Registry keys which contain configuration settings for the agent software that is installed added under:

  `HKLM\SOFTWARE\HEWLETT-PACKARD`

- Registry keys added when HP BTO Software registers a Windows service under the name `HP ITO Agent`.
- Keys added to register `.dll` and `.exe` files.
- Keys related to de-installing agent software.

For example, the Windows Registry includes the following keys for HPOM:

❑ ***<OvInstallDir>***

`HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView`

Value Name: `InstallDir`

Value Type: `string`

❑ ***<OvDataDir>***

`HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\data`

Value Name: `DataDir`

Value Type: `string`

If on a domain controller, the Windows Registry Editor also shows:

`HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\Services\`
`HP ITO Installation Server`

Path Variables

Following values are added to the PATH variable.

<OvInstallDir>\bin;
<OvInstallDir>\bin\OpC;
<OvDataDir>\bin\instrumentation;

Libraries

Consider the following requirements:

- On operating systems for which the agent provides both 64 bit and 32 bit libraries, link the appropriate libraries for your program. For example, link the 32 bit libraries to a 32 bit program, even if the program runs on a 64 bit operating system.
- HTTPS agents on Linux kernel 2.6 for x86 and x64 processors require the standard C++ library (`libstdc++.so`). Please install the latest version of the package that came along with the installation CD of the Linux operating system.
- The 64 bit libraries that are included with 32 bit Linux agents do not support message stream interface functions. To compile a 64 bit application that uses message stream interface functions, link the 64 bit libraries from a 64 bit Linux agent.

Lightweight libraries for agents HP BTO Software shared component libraries

HTTPS agents version 8.60 or higher provide lightweight libraries, which use less memory and provide better performance than previous libraries. Link the lightweight libraries if you develop new applications that use HP Operations Agent APIs.

The lightweight libraries provide the same interfaces as the previous libraries. Therefore, you can recompile existing applications to link the lightweight libraries.

Examples of how to use the lightweight libraries are available in the following folder on nodes that have the HTTPS agent version 8.60 or higher:

`<OvInstallDir>/examples/copcagtapi`

AIX	`/usr/lpp/OV/lib/libopcagtapi.a`
HP-UX PA-RISC	`/opt/OV/lib/libopcagtapi.sl`
HP-UX Itanium	`/opt/OV/lib/hpux32/libopcagtapi.so`
Linux 32 bit	`/opt/OV/lib/libopcagtapi.so`
Linux 64 bit	`/opt/OV/lib64/libopcagtapi.so`

Solaris	`/opt/OV/lib/libopcagtapi.so`

Legacy HTTPS agent libraries

On UNIX and Linux operating systems, you must also link the HP BTO Software shared libraries, which are in the same directory as the HTTPS agent library.

AIX	`/usr/lpp/OV/lib/libopc_r.a` `/usr/lpp/OV/lib/libnsp.a`
HP-UX PA-RISC	`/opt/OV/lib/libopc_r.sl` `/opt/OV/lib/libnsp.sl`
HP-UX Itanium	`/opt/OV/lib/hpux32/libopc_r.so` `opt/OV/lib/hpux32/libnsp.so`
Linux 32 bit	`/opt/OV/lib/libopc_r.so` `/opt/OV/lib/libnsp.so`
Linux 64bit	`/opt/OV/lib64/libopc_r.so` `/opt/OV/lib64/libnsp.so`
Solaris	`/opt/OV/lib/libopc_r.so` `/opt/OV/lib/libnsp.so`

On Windows operating systems, `libopc.dll` is the agent library, and `opcapi.dll` is the agent API library.

Windows 32 bit	*<OvInstallDir>*`\bin\opcapi.dll` *<OvInstallDir>*`\bin\libopc.dll` *<OvInstallDir>*`\bin\opcauth.dll` *<OvInstallDir>*`\bin\pdh.dll` *<OvInstallDir>*`\bin\lOpCWbemInterceptor.dll`
Windows 64 bit	*<OvInstallDir>*`\bin\win64\opcapi.dll` *<OvInstallDir>*`\bin\win64\libopc.dll` *<OvInstallDir>*`\bin\win64\opcauth.dll` *<OvInstallDir>*`\bin\win64\pdh.dll` *<OvInstallDir>*`\bin\win64\lOpCWbemInterceptor.dll`

HP BTO Software shared component libraries

To use the lightweight libraries for HTTPS agent APIs on UNIX and Linux operating systems, you should also link the following shared libraries:

HP-UX PA-RISC	`/opt/OV/lib/libOvXpl.sl`
HP-UX Itanium, Solaris, Linux 32 bit	`/opt/OV/lib/libOvXpl.so`
Linux 64 bit	`/opt/OV/lib64/libOvXpl.so`
AIX	`/usr/lpp/OV/lib/libOvXpl.so`

To use the legacy libraries for HTTPS agent APIs on UNIX and Linux operating systems, you should also link the following shared libraries:

HP-UX PA-RISC	`/opt/OV/lib/libOvBbc.sl`
	`/opt/OV/lib/libOvConf.sl`
	`/opt/OV/lib/libOvCtrl.sl`
	`/opt/OV/lib/libOvCtrlUtils.sl`
	`/opt/OV/lib/libOvDepl.sl`
	`/opt/OV/lib/libOvSecCm.sl`
	`/opt/OV/lib/libOvSecCore.sl`
	`/opt/OV/lib/libOvXpl.sl`

HP-UX Itanium, Solaris, Linux 32 bit	`/opt/OV/lib/libOvBbc.so`
	`/opt/OV/lib/libOvConf.so`
	`/opt/OV/lib/libOvCtrl.so`
	`/opt/OV/lib/libOvCtrlUtils.so`
	`/opt/OV/lib/libOvDepl.so`
	`/opt/OV/lib/libOvSecCm.so`
	`/opt/OV/lib/libOvSecCore.so`
	`/opt/OV/lib/libOvXpl.so`

Linux 64 bit	`/opt/OV/lib64/libOvBbc.so`
	`/opt/OV/lib64/libOvConf.so`
	`/opt/OV/lib64/libOvCtrl.so`
	`/opt/OV/lib64/libOvCtrlUtils.so`
	`/opt/OV/lib64/libOvDepl.so`
	`/opt/OV/lib64/libOvSecCm.so`
	`/opt/OV/lib64/libOvSecCore.so`
	`/opt/OV/lib64/libOvXpl.so`

AIX	/usr/lpp/OV/lib/libOvBbc.so /usr/lpp/OV/lib/libOvConf.so /usr/lpp/OV/lib/libOvCtrl.so /usr/lpp/OV/lib/libOvCtrlUtils.so /usr/lpp/OV/lib/libOvDepl.so /usr/lpp/OV/lib/libOvSecCm.so /usr/lpp/OV/lib/libOvSecCore.so /usr/lpp/OV/lib/libOvXpl.so

Include Files

On supported managed node platforms, use the appropriate include file:

AIX	`/usr/lpp/OV/include/opcapi.h`
HP-UX	`/opt/OV/include/opcapi.h`
Linux	`/opt/OV/include/opcapi.h`
Solaris	`/opt/OV/include/opcapi.h`
Windows	`<`*`OvInstallDir`*`>\include\opcapi.h`

An example of how the API functions are used is available in the following file on the management server:

`/opt/OV/OpC/examples/progs/opcapitest.c`

Makefiles

The following directory on the management server contains the makefiles for building executables:

`/opt/OV/OpC/examples/progs`

The build an executable with correct compile and link options, use the following makefiles:

AIX	`Makef.aix`
HP-UX	`Makef.hpux11` `Makef.hpuxIA32`
Linux	`Makef.linux`
Solaris	`Makef.solaris`
Windows	To built an executable, use Microsoft Developer Studio 6.0 or higher.

For more information about the managed node makefile, see the ReadMe file:

`/opt/OV/OpC/examples/progs/README`

HTTPS Communication Administration Commands in HPOM

HTTPS Communication can be controlled using the following commands.

On the HP Operations Management Server and Managed Nodes:

- **ovcoreid** (Unique System Identifier)

  The `ovcoreid` command is used to display existing `OvCoreId` value and, in addition, create and set new `OvCoreId` values on the local system.

  For details of how to use this tool, refer to the *ovcoreid(1)* man page.

- **ovc** (Process Control)

  `ovc` controls starting and stopping, event notification, and status reporting of all components registered with the Control service, `ovcd`. A component can be a server process, an agent (for example, the Performance Agent or the Discovery Agent), an event interceptor, or an application delivered by an integrator.

  For details of how to use this tool, refer to the *ovc(1)* man page.

- **bbcutil**

  The `bbcutil` command is used to control the HP Communication Broker.

  For syntax information and details of how to use this tool, refer to the *bbcutil(1)* man page.

  Communication parameters are set in the file:

  `<OVDataDir>/conf/confpar/bbc.ini`

- **ovconfget**

  Installed HP BTO Software components have associated configuration settings files that contain one or more namespaces and apply system wide or for a specified High Availability Resource Group. A namespace is a group of configuration settings that belong to a component. All configurations specified in the settings files are duplicated in the `settings.dat` configuration database.

For each specified namespace, `ovconfget` returns the specified attribute or attributes and writes them to `stdout`. Used without arguments, `ovconfget` writes all attributes in all namespaces to `stdout`.

For details of how to use this tool, refer to the *ovconfget(1)* man page.

- **ovconfchg**

  Installed HP BTO Software components have associated configuration settings files that contain one or more namespaces. A namespace is a group of configuration settings that belong to a component.

  `ovconfchg` manipulates the settings in either the system-wide configuration file or the configuration file for the specified `High Availability Resource Group`, updates the configuration database, and triggers notification scripts.

  For details of how to use this tool, refer to the *ovconfchg(1)* man page.

- **ovpolicy**

  `ovpolicy` manages local policies and policies. A policy is a set of one or more specifications, rules and other information that help automate network, system, service, and process management. Policies can be deployed to managed systems, providing consistent, automated administration across the network. Policies can be grouped into categories. Each category can have one or more policies. Each category can also have one or more attributes, an attribute being a name value pair.

  You use `ovpolicy` to install, remove, enable, and disable local policies. For details of how to use this tool, refer to the *ovpolicy(1)* man page.

On Managed Nodes:

- **ovcert**

  The `ovcert` command is used to manage certificates on an HTTPS node through the Certificate Client. You can execute tasks such as initiating a new certificate request to the Certificate Server, adding managed node certificates and importing the private keys, adding certificates to the trusted root certificates, and checking the certificate status.

  For details of how to use this tool, refer to the *ovcert(1)* man page.

On the HP Operations Management Server:

- **opccsacm** (Certificate Server Adapter Control Manager)

  The `opccsacm` command is used to issue new node certificates and installation keys manually on the HP Operations server. It also modifies the HP Operations database to reflect the changes made by certificate management actions.

  For details of how to use this tool, refer to the *opccsacm(1m)* man page.

- **opccsa** (Certificate Server Adapter)

  The `opccsa` command is used to list the pending certificate requests, map certificate requests to target nodes from the HP Operations database, grant, deny and delete specified certificate requests.

  For details of how to use this tool, refer to the *opccsa(1m)* man page.

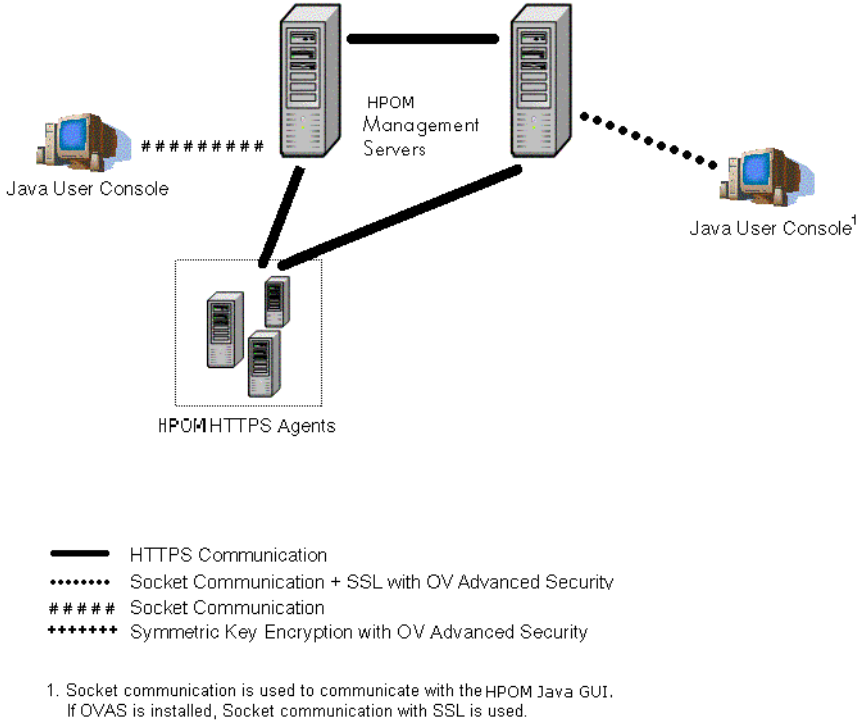
2 Concepts of HTTPS Communication

HTTPS Communication in HPOM

HTTPS based communications is the latest communication technology used by HP BTO Software products and allows applications to exchange data between heterogeneous systems.

HP BTO Software products using HTTPS communication can easily communicate with each other, as well as with other industry-standard products. It is also now easier to create new products that can communicate with existing products on your network and easily integrate with your firewalls and HTTP-proxies. Figure 2-1 illustrates an example of HTTPS communication.

Figure 2-1 Communication Overview in HP Operations Manager



Advantages

HTTPS communication provides the following major advantages:

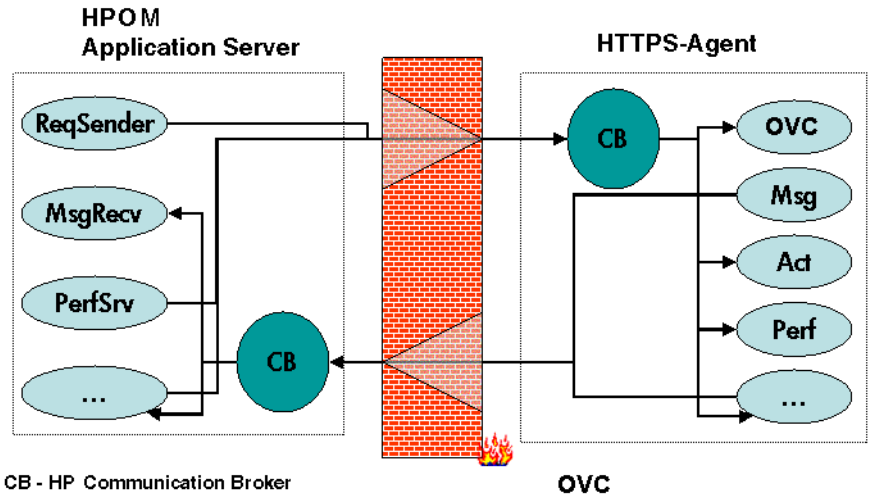
- Firewall Friendly
- Secure
- Open
- Scalable

Firewall Friendly

More and more organizations need to cross firewalls in a safe, secure, and easily manageable way. Most of these organizations are very familiar and comfortable with HTTP, HTTP proxies, and firewalls. Their IT environments are already configured to allow communication through HTTP proxies and firewalls. By focusing on technology that is already a part of most IT infrastructures, it helps you to be more efficient and effective, without the need for new training. The end result reduces support and maintenance costs, while simultaneously creating a highly secure environment without significant effort.

Figure 2-2 illustrates crossing a firewall using HTTPS-communication.

Figure 2-2 Crossing a Firewall with HTTPS Communication



Secure

HP Operations HTTPS communication is based on the TCP/IP protocol, the industry standard for reliable networking. Using the Secure Socket Layer (SSL) protocol, HTTPS communication uses authentication to validate who can access data, and encryption to secure data exchange. Now that businesses are sending and receiving more transactions across the Internet and private intranets than ever before, security and authentication assume an especially important role.

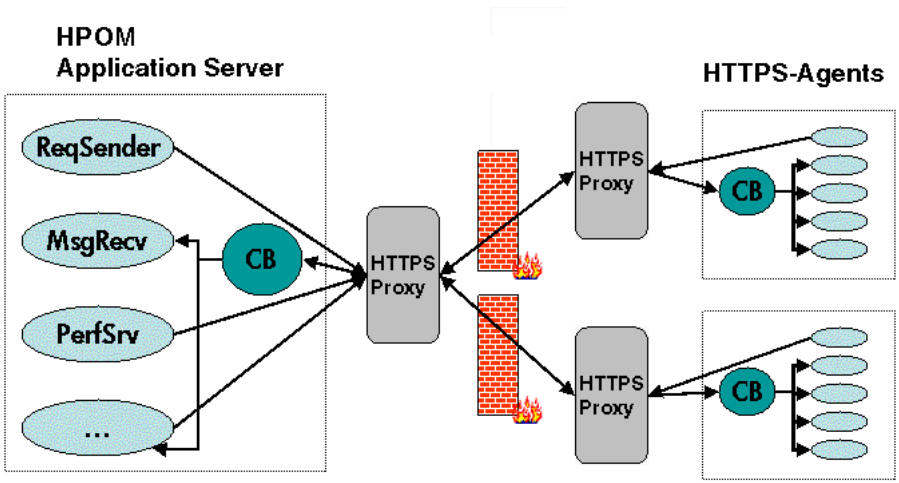
HP Operations HTTPS communication meets this goal through established industry standards. HTTP protocol and SSL encryption and authentication insure data integrity and privacy. By default, data is compressed, ensuring that data is not transmitted in clear text format, even for non-SSL connections.

In addition:

- All remote messages and requests arrive through the Communication Broker, providing a single port entry to the node.
- Restricted bind port range can be used when configuring firewalls.
- Configure one or more standard HTTP proxies to cross a firewall or reach a remote system when sending messages, files or objects.

Figure 2-3 illustrates crossing firewalls using standard HTTP proxies.

Figure 2-3 Crossing a Firewall using External HTTPS Proxies



To work with HTTPS communication and proxies, you will need to:

- Configure HTTP proxy servers.
- Implement SSL encryption.
- Establish server side authentication with server certificates.
- Establish client side authentication with client certificates.

How you do this in HP Operations is described in the following sections.

Open

HP Operations HTTPS communication is built on the industry standard HTTP 1.1 protocol and SSL sockets. HP Operations adherence to open standards, such as HTTP, SSL and SOAP, allows you to maximize the use of your current HTTP infrastructure.

NOTE Content filtering for HPOM agents is not supported.

HTTP proxies are widely used in today's networks. They are workhorses to help safely bridge private networks to the Internet. The use of HTTP allows HP Operations to slot into and take advantage of current infrastructures.

Scalable

HP Operations HTTPS communication is designed to perform well, independent of the size of the environment and the number of messages sent and received. HP Operations HTTPS communication can be configured to suit the environment within which it is to work. Large applications are able to handle many simultaneous connections while consuming the minimum of resources. If the maximum number of configured connections is exceeded, an entry in a logfile is created from which a warning message can also be raised.

3 Security Concepts

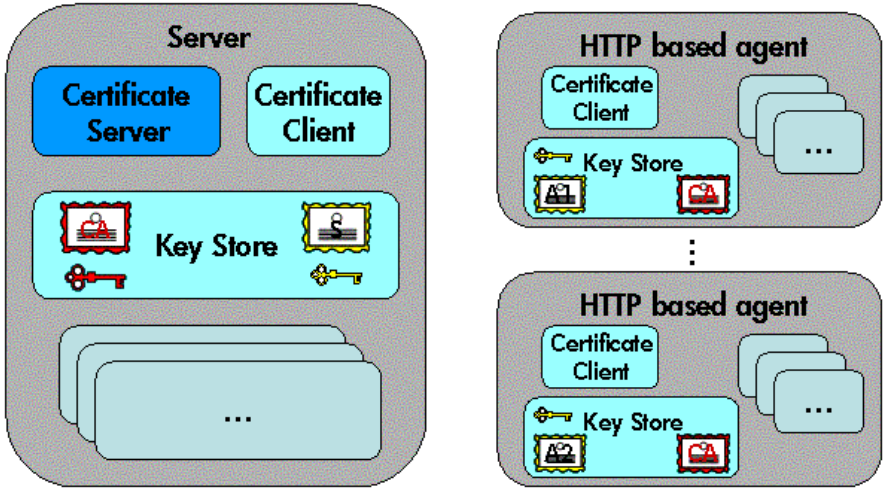
HTTPS-Based Security Components

Managed nodes must have a valid, industry standard, X509 certificate issued by the HP Certificate Server to be able to communicate with HP Operations management servers. Certificates, signed by 1024 bit keys, are required to identify managed nodes in a managed environment using the Secure Socket Layer (SSL) protocol. The “SSL handshake” between two managed nodes only succeeds if the issuing authority of the certificate presented by the incoming managed node is a trusted authority of the receiving managed node. The main communication security components responsible for creating and managing certificates are:

- HP Certificate Server
- HP Key Store
- HP Certificate Client

Figure 3-1 illustrates these components:

Figure 3-1 Components of Authenticated Communication



Each system hosting an HTTPS agent is allocated a unique identifier value for the parameter, `OvCoreId`, created during installation of the HP Operations software on that system.

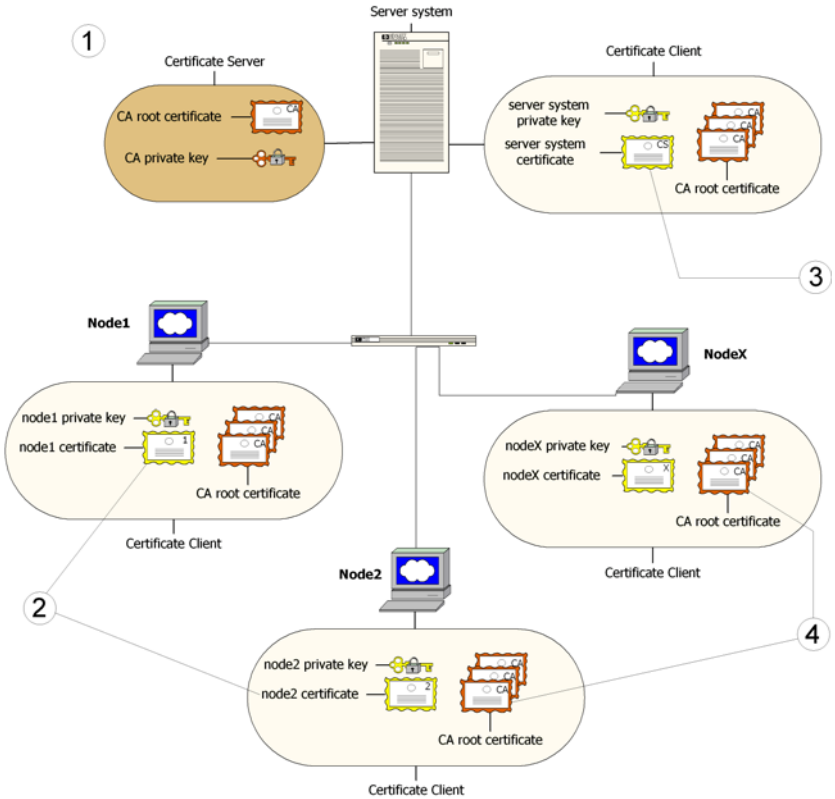
NOTE

After the `OvCoreId` for an HTTPS managed node has been created, it does not change, even if the hostname or the IP address, for example through DHCP, of the system is changed.

For each HP Operations system (managed node or server) `OvCoreId` is used as a unique identifier and is contained in the corresponding managed node certificate. `OvCoreId` is allocated its value during installation.

Figure 3-2 illustrates an environment for authenticated communication:

Figure 3-2 Environment for Authenticated Communication



1. A server system hosts the Certificate Server, which contains the needed certification authority (CA) functionality.
2. Every system has a certificate that was signed by the Certificate Server with the certification authority private key.
3. The server system also needs a certificate to prove its identity.
4. Every system has a list of trusted root certificates, which must contain at least one certificate. The trusted root (CA) certificates are used to verify the identity of the communication partners; a communication partner is only trusted if the presented certificate can be validated using the list of trusted certificates.

A list of trusted root certificates is required, when the certificate client is being managed by more than one HP Operations management server. For instance, when a managed node is managed simultaneously by multiple HP Operations management servers.

Certificates

There are two types of certificates:

- Root certificates
- Managed node certificates

A root certificate is a self-signed certificate, containing the identity of the certification authority of the certificate server. The private key belonging to the root certificate is stored on the certificate server system and protected from unauthorized access. The certification authority uses its root certificate to digitally sign all certificates.

Every HTTPS managed node in the managed environment receives a managed node certificate issued by a certificate server, a corresponding private key stored in the file system and the root certificates valid in its environment. The certificate client running on the managed node ensures this.

NOTE

A managed node certificate contains the unique identity `OvCoreId`. The following is an example of an `OvCoreId`:

```
d498f286-aa97-4a31-b5c3-806e384fcf6e
```

Each managed node can be securely authenticated through its managed node certificate. The managed node certificate can be verified by all other managed nodes in the environment using the root certificate(s) to verify the signature.

Managed node certificates are used to establish SSL-based connections between two HTTPS managed nodes that use client and server authentication, and can be configured to encrypt all communication.

The `ovcert` tool provided by the certificate client can be used to list the contents of the Key Store or to show information about an installed certificate. The `ovcert` tool is described in the `ovcert` man page.

HP Certificate Server

The certificate server is responsible for the following:

- Creating and installing self-signed root certificates.
- Importing self-signed root certificates from the file system.
- Storing the private keys of root certificates.
- Granting or denying certification requests.
- Creating a new certificate and a corresponding private key or creating an installation key for manual certificate installation.
- Offering a service for clients to automatically retrieve trusted root certificates.

Certification Authority

NOTE Every HP Operations management server is automatically configured as a Certificate Authority. The default setting for `sec.cm.client:CERTIFICATE_SERVER` for every agent is its own HP Operations management server.

The certification authority is part of the certificate server and is the center of trust in certificate management. Certificates signed by this certification authority will be regarded as valid certificates and therefore be trustworthy. The certification authority must be hosted in a highly secure location. By default, it is installed on the system hosting the HP Operations management server.

Since the certification authority is the root of trust, it operates with a self-signed root certificate. This root certificate and the corresponding private key are created and stored on the file system with the level of protection to allow the certification authority to operate. After the certification authority is successfully initialized, it is responsible for signing granted certificate requests using its root certificate.

Certificate Client

The certificate client runs on a managed node and acts as the counterpart of the certificate server's certificate request handler.

The certificate client operates as follows:

- The certificate client checks whether the managed node has a valid certificate.
- If the managed node has no certificate, the certificate client generates a new public and private key pair and creates a certificate request based on the unique identity (`OvCoreId` value) of the managed node. This certificate request is sent to the certificate server together with any additional managed node properties and the certificate client waits for a response.

  The additional managed node properties, for example DNS name and IP address of the managed node are intended to be used as additional information that, on the certificate server, should help to determine from which system in the environment a certificate request comes and to decide whether this request should be granted.
- After receiving the new certificate, it is installed on the managed node. After being installed, the certificate client can ensure that all HTTPS-based communication uses this certificate.

  If the request is not successfully processed, a descriptive error is logged and the associated status is set.

In addition, the certificate client does the following:

- It can be triggered to contact a certificate server to update its trusted root certificates, for example, using the command line tool `ovcert`. Refer to the `ovcert` man page for details.
- It supports the import of a managed node certificate and the corresponding private key from the file system with its command line interface `ovcert`. For more details see “Generating Certificate for Manual Certificate Deployment” on page 158 and “Deploying Manual Certificate with Installation Key” on page 163. Manual certificate installation is used to improve security on sensitive systems.
- It supports the import of trusted root certificates.
- It provides status information. Status includes `OK`, `valid certificate`, `no certificate`, `certificate requested`, and `certificate request denied`.

Root Certificate Update and Deployment

It may be necessary to update the trusted root certificates of one or more managed nodes, for example, in environments hosting several HP certificate servers.

It is possible to supply all currently trusted root certificates to certificate clients in a secured way. It is usually sufficient to supply the root certificate of the certification authority. However, it may be necessary to deploy one or more additional root certificates to selected certificate clients, for example when there is more than one certification authority in the environment.

The certificate client allows triggering the “trusted root certificates update” through the command line tool `ovcert`. Refer to the `ovcert` man page.

Security in Manager of Manager (MoM) Environments

The use of certificate servers in Manager of Manager environments can be divided into the following two types:

- “Environments Hosting Several Certificate Servers”
- “Establish a Shared CA in MoM Environments”

Environments Hosting Several Certificate Servers

It is possible that a managed environment has more than one certificate server. This situation would arise if two existing managed environments, both having an operating certificate server are joined to form a single environment. This is termed **merge**.

Both certificate servers are each using a self-signed root certificate. As a result, all clients belonging to one certificate server do not trust any client belonging to the other. This is solved by adding the root certificate of each certificate server to the trusted root certificates of the other certificate server. Finally, all clients in the managed environment are triggered to receive the updated root certificate list from their certificate server.

If an agent is managed by multiple management servers some certificate management configuration must be made. By default, every HP Operations server has its own Certificate Authority and the agent trusts only certificates subscribed by this authority. For MoM environments, you must establish a trust between two or more managers so that their environments are able to communicate with each other.

The common scenarios are:

- “Merge Two Existing MoM Environments”
- “Certificate Handling for a Second HP Operations Management Server”
- “Establish a Shared CA in MoM Environments”

These scenarios are discussed in greater detail in the following sections.

Merge Two Existing MoM Environments

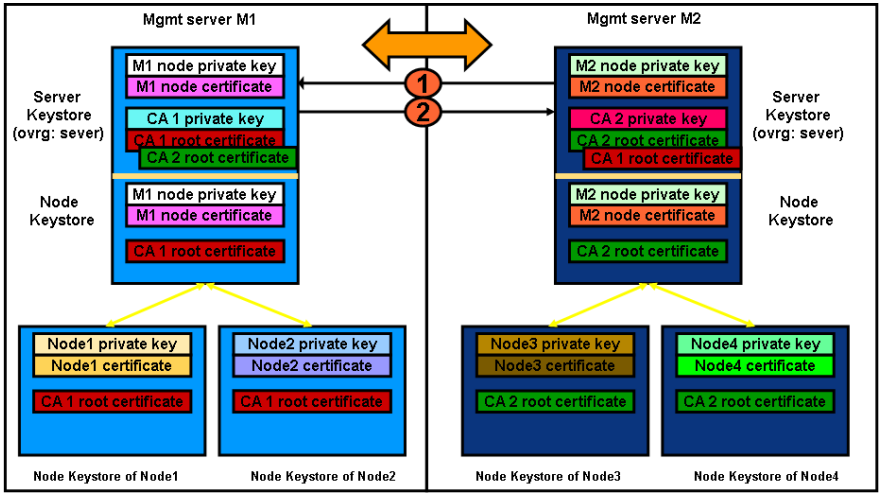
Assume you have an environment belonging to server M1 with the agents AM1 and the second of M2 with AM2. Assume that each server has its own Certificate Authority.

Complete the following steps to merge the environments:

NOTE HA environments and non-HA environments are handled in the same way. The following steps are valid for both types of installations.

1. Synchronize the trusted certificates on the management servers: M1 gets the root certificates of M2 and M2 the root certificate of M1.

Figure 3-3 Synchronizing the Trusted Certificates on the Management Servers



a. On HP Operations management server M1, enter the command:

```
ovcert -exporttrusted -ovrg server -file <my_file>
```

b. Copy *<my_file>* to the management server M2, for example using `ftp`.

c. Enter the following command on M2:

```
ovcert -importtrusted -ovrg server -file <my_file>
```

d. Repeat the procedure for management server M2.

e. To verify that M1 and M2 have the root certificate of the other, on both management server systems, execute the command:

```
ovcert -list
```

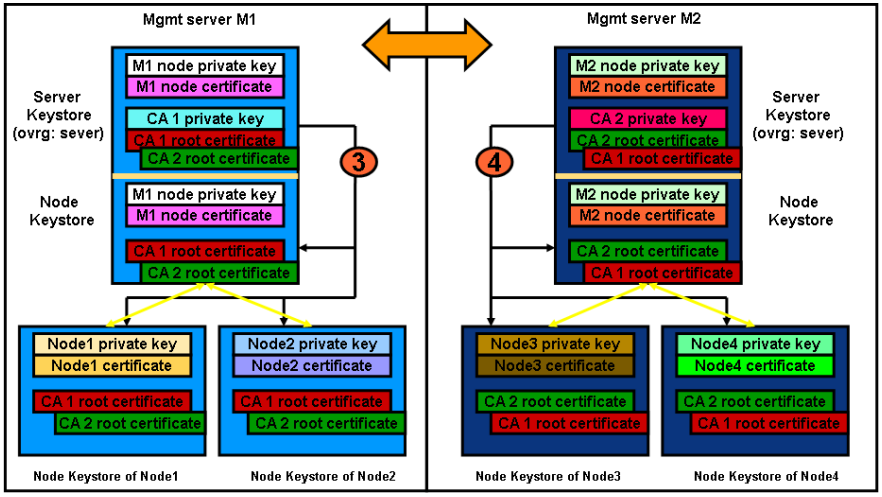
Two trusted certificates should be listed.

2. Update the local root certificates on each managed node.

To trigger this action on the managed node, execute the command:

```
ovcert -updatetrusted
```

Figure 3-4 Updating the Local Root Certificates on Each Managed Node



NOTE In cluster installations, the local certificates for the agents and the server are not the same.

On each management server (M1 and M2), select all required managed nodes and execute the application. The agents contact their certificate server and ask for new root certificates.

You can verify this on all managed nodes by executing command:

```
ovcert -list
```

Two trust certificates should be displayed.

3. Configure other management server as regular nodes in the HPOM node bank. M1 must be added to the node bank of M2 with its `OvCoreId` and M2 must be added to the node bank of M1 with its `OvCoreId`.

   a. Add node M1 in the node bank of M2 and M2 in the node bank of M1 as follows:

      On node M1, enter the command:

      ```
      opcnode -add_node node_name=<M2> \
      net_type=<network_type> mach_type=<machine_type> \
      group_name=<node_group_name>
      ```

      On M2, enter the command:

      ```
      opcnode -add_node node_name=<M1> \
      net_type=<network_type> mach_type=<machine_type> \
      group_name=<node_group_name>
      ```

   b. M1's `OvCoreId` must be stored in M2's database:

      On M1, call the `ovcoreid` command to display its `OvCoreId`:

      ```
      ovcoreid -ovrg server
      ```

      Note down the displayed value.

      On M2, call the `opcnode` command to add M1's `OvCoreId` into M2's database:

      ```
      opcnode -chg_id node_name=<M1> id=<core_id_of_M1>
      ```

   c. M2's `OvCoreId` must be stored in M1's database:

      On M2, call the `ovcoreid` command to get `OvCoreId` of M2:

      ```
      ovcoreid -ovrg server
      ```

      Note down the displayed value.

On M1, call the `opcnode` command to add M2's `OvCoreId` into M1's database:

```
opcnode -chg_id node_name=<M2> id=<core_id_of_M2>
```

You can verify that the nodes have been correctly added to the databases by executing the following commands:

a. On M1, enter the command:

```
opcnode -list_id node_list=<M2>
```

The `OvCoreId` of node M2 should be displayed.

b. On M2, enter the command:

```
opcnode -list_id node_list=<M1>
```

The `OvCoreId` of node M1 should be displayed.

NOTE Do not forget to add uploaded nodes to `Node Group` by using the `opcnode` tool so that you are able to see messages.

4. Create or enhance the responsible manager policy on both servers and deploy it to their own agents.
5. Synchronize the node banks using `opccfgupld` and `opccfgdwn`. M1 gets the entries of M2, M2 gets the entries of M1 including their OvCoreIds.

   By default, in the merged MoM environment all automatic and operator initiated actions are allowed on both management servers because both management servers have root certificates installed and a trust relationship established. To restrict actions on management server A from agents belonging to other management servers, set the following configuration setting:

   ```
   ovconfchg -ovrg server -ns opc -set \
   OPC_RESTRICT_ACTIONS_WITH_FOREIGN_SIGNATURE TRUE
   ```

   In case there are more than just two servers in the MoM environment and you want to allow actions from agents belonging to these servers, set the following configuration setting:

   ```
   ovconfchg -ovrg server -ns opc -set \
   OPC_ACCEPT_ACTION_SIGNATURES_FROM
   <List_of_allowed_srv_COREIDs>
   ```

where <List_of_allowed_srv_COREIDs> is a comma-separated list of other servers' CORE IDs.

NOTE This action restriction cannot be configured by using the `remactconf.xml` file because a trust relationship is established between servers through installed root certificates.

Certificate Handling for a Second HP Operations Management Server

Assume the second HP Operations management server has its own Certificate Authority and is used as a backup management server or competence center. Assume that server M1 owns the agents AM1 and that the server M2 initially has no agents.

1. Synchronize the trusted certificates on the management servers: M1 gets the root certificates of M2 and M2 the root certificate of M1.

   a. On HP Operations management server M1, enter the command:

      ovcert -exporttrusted -ovrg server -file *<my_file>*

   b. Copy *<my_file>* to the management server M2, for example using `ftp`.

   c. Enter the following command on M2:

      ovcert -importtrusted -ovrg server -file *<my_file>*

   d. Repeat the procedure for management server M2.

   e. To verify that M1 and M2 have the root certificate of the other, on both management server systems, execute the command:

      ovcert -list

      Two trusted certificates should be listed.

2. Update the root certificate on M1.

   To trigger this action on the managed node, execute the command:

   ovcert -updatetrusted

   On M1 select AM1, and execute the application. The agent contacts its certificate server and asks for a new root certificate.

3. Configure other management server as regular nodes in the HPOM node bank. M1 must be added to the node bank of M2 with its `OvCoreId` and M2 must be added to the node bank of M1 with its `OvCoreId`.

   a. Add node M1 in the node bank of M2 and M2 in the node bank of M1 as follows:

      On node M1, enter the command:

```
opcnode -add_node node_name=<M2> \
net_type=<network_type> mach_type=<machine_type> \
group_name=<node_group_name>
```

On M2, enter the command:

```
opcnode -add_node node_name=<M1> \
net_type=<network_type> mach_type=<machine_type> \
group_name=<node_group_name>
```

b. M1's `OvCoreId` must be stored in M2's database:

On M1, call the `ovcoreid` command to display the `OvCoreId` of M1:

```
ovcoreid -ovrg server
```

Note down the displayed value.

On M2, call the `opcnode` command to add M1's `OvCoreId` into M2's database:

```
opcnode -chg_id node_name=<M1> id=<core_id_of_M1>
```

c. M2's `OvCoreId` must be stored in M1's database:

On M2, call the `ovcoreid` command to get `OvCoreId` of M2:

```
ovcoreid -ovrg server
```

Note down the displayed value.

On M1, call the `opcnode` command to add M2's `OvCoreId` into M1's database:

```
opcnode -chg_id node_name=<M2> id=<core_id_of_M2>
```

You can verify that the nodes have been correctly added to the databases by executing the following commands:

a. On M1, enter the command:

```
opcnode -list_id node_list=<M2>
```

The `OvCoreId` of node M2 should be displayed.

b. On M2, enter the command:

```
opcnode -list_id node_list=<M1>
```

The `OvCoreId` of node M1 should be displayed.

NOTE

Do not forget to add uploaded nodes to `Node Group` by using the `opcnode` tool so that you are able to see messages.

4. Create or enhance the responsible manager policy on both servers and deploy it to their own agents. M1 must deploy a responsible manager policy to all its managed nodes, in this case, they are M1 and AM1. M2 must deploy a responsible manager policy to its local agent if it was not already a part of M1's environment.
5. Synchronize the node banks using `opccfgupld` and `opccfgdwn`. Now M2 receives all agents of M1 and M1 loads the local agent of M2, if not already present in the database.

Switch CAs in MoM Environments

Assume that a MoM environment is already established. For example:

- Management server A is active CA.
- Management server B is alternative CA.
- Systems are managed as HPOM nodes.
- Responsible manager template has been created and distributed to all managed nodes.

To change the CA in the above MoM environment:

1. Set management server B as a primary manager for a managed node by executing the following command on management server B system:

   opcragt -primmgr *<node hostname>*

2. Remove all templates from this managed node that were distributed from management server A.
3. Stop the agent software on the managed node:

   ovc -kill

4. Remove the agent certificate from the managed node:

   ovcert -remove *<alias>*

5. Remove the trusted management server A certificate from the managed node:

   ovcert -remove *<alias>*

NOTE Management server B must present on node (**ovcert -list**).

6. Issue a new node certificate manually from management server B:

   opccsacm -issue -name *<nodename>* -file *<filename>* -coreid *<OvCoreId>*

7. Transfer the newly created certificate to the managed node.
8. Import the new certificate to the managed node:

   ovcert -importcert -file *<filename>*

9. Change the configuration settings on the managed node to reflect the change to the new CA (management server B):

   ```
   ..
   [sec.cm.client]
   CERTIFICATE_SERVER=<management server B hostname>
   [sec.core.auth]
   MANAGER=<management server B hostname>
   MANAGER_ID=<management server B OvCoreId>
   ...
   ```

   The configuration settings are changed with the following commands:

   ovconfchg -ns sec.cm.client -set CERTIFICATE_SERVER *<management server B hostname>*

   ovconfchg -ns sec.core.auth -set MANAGER *<management server B hostname>*

   ovconfchg -ns sec.core.auth -set MANAGER_ID *<management server B OvCoreId>*

10. Start the agent software on the managed node:

    ovc -start

11. Distribute templates to the managed node.

12. *Optional*. Do not allow automatic or operator-initiated actions to be executed on management server A.

    By default, in merged MoM environments, automatic and operator-initiated actions are allowed on both management servers because both have each other's root certificate installed and hence trust each other.

    Set the following variable on management server A to prevent actions from nodes belonging to other management servers from being executed:

    ovconfchg -ovrg server -ns opc -set OPC_RESTRICT_ACTIONS_WITH_FOREIGN_SIGNATURE TRUE

13. *Optional*. Allow automatic and operator-initiated actions from nodes belonging to selected management servers to be executed on management server A.

    In MoM environments with more than two management servers, you can specify a list of management servers whose nodes are allowed to execute automatic and operator-initiated actions:

    ovconfchg -ovrg server -ns opc -set OPC_ACCEPT_ACTION_SIGNATURES_FROM *<List_of_allowed_server_COREIDs>*

    <List_of_allowed_server_COREIDs> is a comma-separated list of core IDs of the management servers whose nodes are allowed to execute actions on management server A.

NOTE

Preventing actions from being executed on a management server cannot be configured in the remote action configuration file `remactconf.xml` because the management servers have each other's root certificate installed and hence trust each other.

Establish a Shared CA in MoM Environments

The scenarios described above show how to merge environments with separate Certificate Authorities. It is also possible to work with only one Certificate Authority. However, this should be considered before setting up an HP Operations MoM Managed environment.

NOTE If you have an existing environment with two certificate authorities, it is not recommended to use the shared CA scenario, as this would require you to replace all certificate that have been granted by one of the CAs.

In addition, consider that all HP Operations management servers and their managed nodes are dependent on one Certificate Authority.

Assume that server M1 has a Certificate Authority and M2 should not have one.

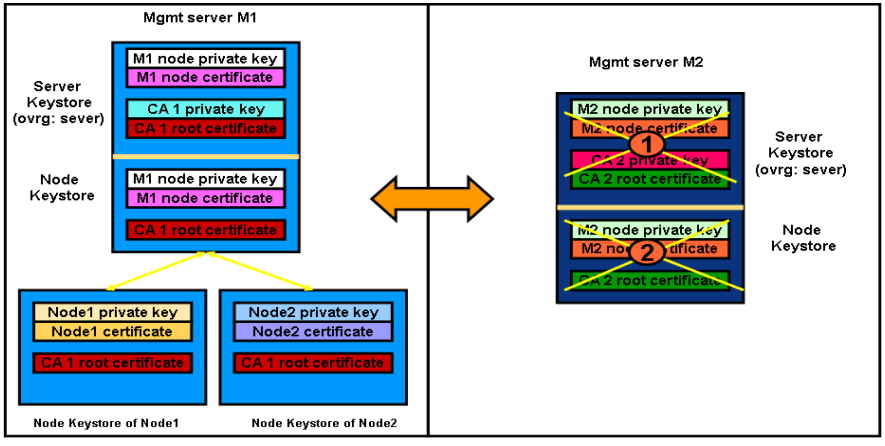
Execute the following steps:

1. Immediately after the installation of M2, remove the local certificates with the following commands:

   ```
   ovcert -remove <cert_id>

   ovcert -remove -ovrg server <cert_id>
   ```

Figure 3-5 Removing Certificates from the M2 Management Server



2. Add M2 to the node bank of M1.

   On node M1, enter the command:

   ```
   opcnode -add_node node_name=<M2> \
   net_type=<network_type> mach_type=<machine_type> \
   group_name=<node_group_name>
   ```

3. Create a certificate for M2 on M1 with the following commands:

   ```
   opccsacm -issue -name <M2> -coreid <core_ID_M2> \
   -file <M2_cert> -pass <password>
   ```

NOTE

To display the `OvCoreId` of M2, on the M2 system, enter the command:

```
ovcoreid -ovrg server
```

`opccsacm` also adds the `OvCoreId` of M2 to the database.

4. Copy the certificate to M2 (HA server) and install it as the server certificate:

   ```
   ovcert -importcert -ovrg server -file <my_cert> \
   -pass <password>
   ```

   If M2 is not an HP Operations HA cluster server, call the same command as above but without the resource group `server` option to install a node certificate:

   ```
   ovcert -importcert -file <my_cert> -pass <password>
   ```

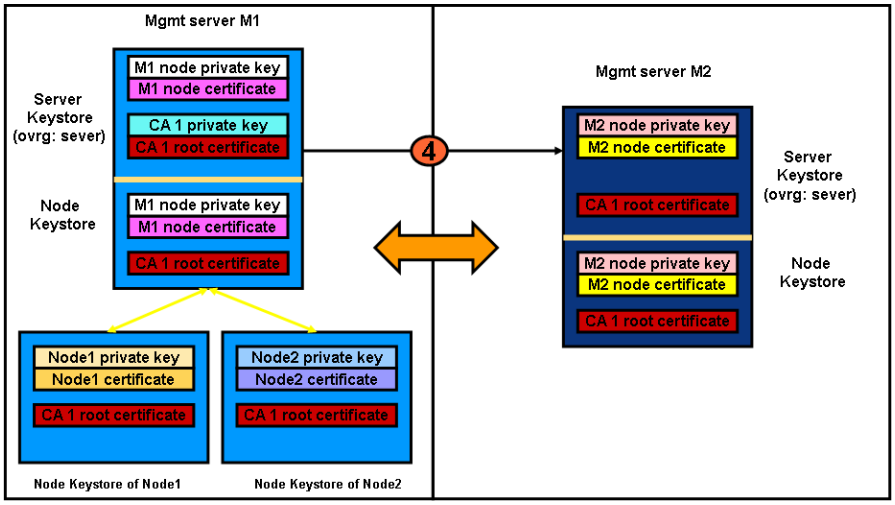
   If M2 is an HA system, create an extra node certificate for each physical node. On M1 call:

   ```
   opccsacm -issue -name <hostname_M2_cluster_node> \
   -coreid <OvCoreId_M2_cluster_node> -file <my_cert> \
   -pass <password>
   ```

   Copy the node certificates to the M2 cluster nodes and install using the command:

   ```
   ovcert -importcert -file <my_cert> -pass <password>
   ```

Figure 3-6 Issuing Certificate for M2 on M1 and Installing it on M2



5. Instruct every managed node which will be installed by M2 that its certificate server is M1 by placing an entry into the `bbc_inst_defaults` file. This file is used to automatically generate profiles for the agent installation. The location of the file is:

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

NOTE

If this file does not exist, create it now using the following sample file as a template:

`/etc/opt/OV/share/conf/OpC/mgmt_sv/bbc_inst_defaults.sampl`

Add the namespace and certificate server specifications to your `bbc_inst_defaults` file as follows:

```
[sec.cm.client]
CERTIFICATE_SERVER <hostname_M1>
```

For the local agent on M2 call:

```
ovconfchg -ns sec.cm.client -set \
CERTIFICATE_SERVER <hostname_M1>
```

6. On M1, specify the OvCoreId of M2 as a trusted OvCoreId:

   ```
   ovconfchg -ovrg server -ns opc -set \
   OPC_TRUSTED_SERVER_COREIDS <M2's OvCoreId>
   ```

   If you have more than two management servers in your Shared-CA environment, you need to complete some additional steps. Let us assume that you have three management servers: M1, M2, and M3. On M1, the CA root certificate is installed. M2 and M3 receive a shared CA which is issued by M1. The followings steps must also be be completed:

   a. On management server M1, which has a Certificate Authority, specify a trusted OvCoreId list which contains a comma separated list of all management server OvCoreIds in your MoM environment, excluding the OvCoreId from management server M1.

      On M1, specify the OvCoreIds of M2 and M3 as trusted OvCoreIds:

      ```
      ovconfchg -ovrg server -ns opc -set \
      OPC_TRUSTED_SERVER_COREIDS
      <OVCoreID>_M2>,<OVCoreID_M3>
      ```

   b. On all other management servers (for example, M2 and M3) which have a shared CA, specify a trusted OvCoreId list which contains a comma separated list of management server OvCoreIds. This list contains all management server OvCoreIds in this MoM environment, excluding the OvCoreIds from:

      - Local management server where the following command is executed.
      - Management server (M1) which has the Certificate Authority.

      On M2, specify the OvCoreId of M3 as a trusted OvCoreId:

      ```
      ovconfchg -ovrg server -ns opc -set \
      OPC_TRUSTED_SERVER_COREIDS <OVCoreID_M3>
      ```

      On M3, specify the OvCoreId of M2 as a trusted OvCoreId:

      ```
      ovconfchg -ovrg server -ns opc -set \
      OPC_TRUSTED_SERVER_COREIDS <OVCoreID_M2>
      ```

7. Unregister the Certificate Server (`ovcs`) component from system M2 using the command:

   `ovcreg -del ovcs`

8. Create or enhance the responsible manager policy on both servers and deploy it to their own agents. M1 must deploy a responsible manager policy to all of its agents which are to be managed by M2. M2 must deploy a responsible manager policy to its local agent, if it was not already a part of M1's environment.

9. Download the node bank configuration on M1 and upload to M2 by using the `opccfgupld` and `opccfgdwn` tools.

Remote Action Authorization

From the point of view of security, remote actions are a very special case in HPOM managed environments. It must be ensured that it is not possible to send a faked remote action to a management server that is then executed on the specified remote system in the environment. In particular, this is sensitive since it is not possible to regard any managed system as a secure system. It is assumed that root access to a managed node is available to unauthorized users.

In addition, one HP Operations management server of a service provider must be able to manage the environments of several of its customers, while ensuring that no system located in one customer segment is allowed to trigger any actions in any other customer segment.

HPOM ensures that action strings, for example, a specific command, cannot be tampered with by a malicious user. On the HP Operations management server, it is possible to configure:

- On which systems the HP Operations management server is allowed to execute an action.
- Whether only "signed actions" originating from an HTTPS agent are accepted.

Action requests contained in HPOM messages which specify a target system for the action other than the sender of the message are remote actions and must be handled securely. These remote actions are subjected to additional security checks described in the following section. Remote actions are only executed if they pass these security checks.

The following general rules apply:

- A remote action is defined as an automatic action or operator-initiated action which is defined within an HPOM message sent by Managed Node A and configured to run on Managed Node B. The execution of such actions can be controlled with the file

  `/etc/opt/OV/share/conf/OpC/mgmt_sv/remactconf.xml`.

- Whenever a message containing a remote action arrives on the HPOM management server, this file is re-loaded if modified and the message will be processed against the rules contained in the remote action configuration file.

- If the remote action configuration file does not exist, is empty, unreadable or does not contain rules, all remote actions are disabled.
- A message containing remote actions will be matched against the rules in the same sequence as configured. The first match determines the result - a `deny` clause disables the remote actions within the message and adds an appropriate annotation to the message. Other than this, the actual message is processed normally. An `allow` clause leaves the message unmodified.
- If the message does not match any rule, the remote actions will be disabled in the same way as if it had matched a `deny` rule.
- A rule matches if all rule elements match in an AND-logic fashion. If a possible rule element is omitted, for example no `<target>` tag is specified, any appropriate message value matches. However, this does not apply to the `<certified>` tag - if this is not specified, a default of `true` applies (*).
- If the remote action configuration file contains syntax errors or other logical errors, such as a non-existing node group, parsing stops and all subsequent rules are ignored (*).
- The `trust` section is not supported (*).
- The `certified` tag has the `true` (default) value. The meaning is whether the message originates from a certified source and the message certificate has been verified. A rule containing the clause `<certified>true</certified>` matches messages from HTTPS nodes.

Server Configuration of Remote Action Authorization

The message manager uses a file-based configuration on the HP Operations management server to specify authorization of remote actions. The configuration contains a trust section that defines which systems are trusted as action signers, and a list of rules, each of which consist of a condition and an action. Each action request is checked against all condition in the order of their definition. If a condition matches, processing of the action request the action is stopped.

The conditions allow checking properties on an action request, such as source node, target node, or signature. There are only two possible actions: `allow` and `deny`. An `allow` action means that the action request is authorized. A `deny` action means that the action request is rejected.

Authorization data is logged with the reason for denying authorization. If an action is unauthorized, it is automatically deleted from the message and details about the match and the signature status are added as an annotation to the message. Unauthorized messages never appear in the GUI and therefore cannot be accidentally executed.

Source and target nodes are matched against node groups or single nodes. A dedicated keyword can be used for the management server.

If the new configuration file is missing or contains no rules, all remote actions are disabled. A default configuration file that contains the `OvCoreId` of the management server is installed with the product. The default configuration file also contains some examples in comments.

During startup, the message manager reads the file:

`/etc/opt/OV/share/conf/OpC/mgmt_sv/remactconf.xml`

It may also be triggered at runtime to re-read the file.

The syntax of the configuration file is XML based, and according with the following schema:

Figure 3-7 Remote Action Configuration File Syntax

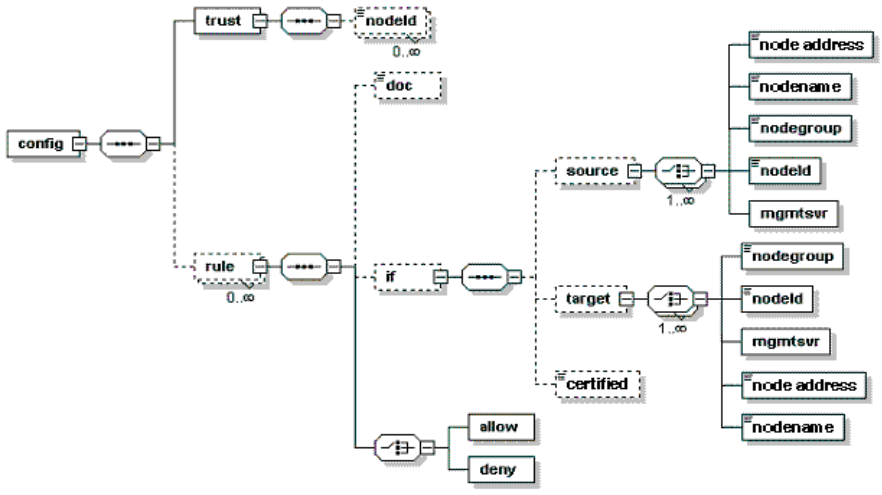


Table 3-1 Remote Action Configuration File Components

Elements	Description
`config`	`config` consists of a trust element and of a list of rule elements.
`trust`	The `trust` element consists of a list of `nodeId` element, each containing the `OvCoreId` of a trusted node.
`rule`	Each `rule` consists of the following components: • `doc` (optional) containing a description. string • `if` (optional) containing a `condition`. • An `allow` or a `deny` action. The `allow` and `deny` actions are empty and define if action execution is allowed or denied.
`condition`	A condition consists of a sequence of optional checks. A condition matches only if all contained checks match. If no check is defined, or if no condition is defined, a match is always successful. The checks are: • `source` • `target` • `certified`

Table 3-1 Remote Action Configuration File Components (Continued)

Elements	Description

`source`
 	
`target`
	Used to check the source node of an action request.
	
	Used to check against the target node of an action request.
	
	Both source and target consist of a set of choices. These checks match if any of the elements match.
	
	• `nodegroup`
	
	The `nodegroup` element contains the name of a node group from the HPOM database. It matches if the request's node is a member of that node group.
	
	• `nodeId`
	
	The `nodeId` element contains an `OvCoreId`. It will mach if this `OvCoreId` is the ID of the request's node.
	
	• `mgmtsrv`
	
	The `mgmtsrv` element is empty. It matches if the request's node is the management server.
	
	• `nodeAddress`
	
	• `nodename`

`certified`	The certified check allows the values `valid` and `invalid`. `Valid` matches only if a signature and a certificate are provided, with the signature being signed by the certificate's owner, and when the `OvCoreId` of the certificate's subject is listed in the trust element. `Invalid` matches all other cases.

The following is an example of a remote action configuration:

```
<?xml version="1.0"?>
<config xmlns="http://openview.hp.com/xmlns/Act/Config/2002/08">
  <rule>
    <doc>Actions from Group2 to Group1 are always allowed</doc>
    <if>
      <source>
        <nodegroup>Group2</nodegroup>
      </source>
      <target>
      <nodegroup>Group1</nodegroup>
      </target>
    </if>
    <allow/>
  </rule>
  <rule>
    <doc>No actions from Group3 are allowed</doc>
    <if>
      <source>
        <nodegroup>Group3</nodegroup>
      </source>
    </if>
    <deny/>
  </rule>
  <rule>
    <doc>Actions to Group3 are allowed if certified</doc>
    <if>
      <target>
        <nodegroup>Group3</nodegroup>
      </target>
      <certified>true</certified>
    </if>
    <allow/>
  </rule>
</config>
```

Agents Running Under Alternative Users

HPOM processes normally run under user `root` on UNIX systems and under the `System` account on Windows systems. The root/administrative privileges enable the processes to:

- Access HPOM resources. HPOM files are normally also restricted to privileged access only.
- Allow a switch user for application specific access rights.
- Directly access operating system resources such as log files and configuration files.
- Start application or operating system specific commands and executables.
- Access remote systems over the network.

There may be systems within IT environments that are highly security sensitive and it is necessary to limit the number of processes that have full root permissions to a small, well defined and tested group. In addition, it is desirable to be able to identify the precise process that manipulated critical system resources. This is not possible if many applications are running under the privileged user.

HPOM software on managed nodes can be configured to run under a user that does not have full `root` permissions, often referred to as “running as non-root”. To run an agent as non-root, access to non-HPOM files and executables must be specifically given to the HPOM processes on the managed node.

To configure HTTPS agents on UNIX systems to run under a user other than root using the `ovswitchuser` tool. See “Configure an Agent to Run Under an Alternative User on UNIX” on page 87.

The `ovswitchuser` command is not supported by the HTTPS agent on Windows platforms. To configure HTTPS agents on Windows systems to run under a privileged user, see “Changing the User of an HTTPS Agent on Windows” on page 95.

Limitations of Running HTTPS Agents Under Alternative Users

Agents running under alternative users have the following limitations:

WARNING **The HP Operations management server processes must always run under the user `root`. The `ovswitchuser` tool must not be called on the HP Operations management server system.**

- Actions can only be executed if the account under which the agent runs has suitable privileges.
- It is not possible to access files or any other operating system resources unless the agent account has suitable privileges.

NOTE It is possible to circumvent access restrictions by implementing a sudo program, which gives the agent user additional capabilities for specific operations. For further details, refer to “Working with Sudo Programs on UNIX Agents” on page 99.

Configure an Agent to Run Under an Alternative User on UNIX

The `ovswitchuser` tool allows the UNIX HTTPS agent on an HPOM managed node to run under a user other than the privileged root user. The `ovswitchuser` tool makes the following changes:

- Perform change group ownership on:
  - All registered files of all installed component packages.
  - All files and directories of *<OVDataDir>* recursively.
- Change operating system daemon/service registration to start HPOM processes under the new user.

Consider the information below before performing the configuration changes:

- The HTTPS agent has file access rights opened for the assigned user and all other users which belong to the same group as the user of the HTTPS agent.
- The HTTPS agent has the `group-id` bit set on its base directories.

  The `group-id` bit guarantees that all files created under such directories will belong to the agent's group. This also works if the primary group of the user under which the agent is running is different from the group of the agent files and directories.

  For example, the primary group of user `HPOM_Agent` is `Security`, agent files and directories belong to group `Security2`. Now also add `HPOM_Agent` to group `Security2` (`Security` remains the primary group of `HPOM_Agent`) and run the agent under user `HPOM_Agent`. All files created by the agent running under the user `HPOM_Agent` will belong to `Security2`. This mechanism allows HPOM components to run under different users but share common files.
- The `set group-id` bit may cause warnings of security check tools like medusa, which can be safely ignored.
- On HTTPS agent, you call `ovswitchuser` only once after bootstrap installation. Later you call `ovswitchuser` only when you want to change the group/user of the agent, for example, back to root.

Prepare the System Environment

WARNING **Do not use ovswitchuser.sh on the HP Operations management server system. The HTTPS agent on the HP Operations management server must run under the user root.**

NOTE After the change of user has been made using the `ovswitchuser` command, the agent processes must be run under this newly assigned user and no longer under the user `root`.

For HTTPS agents, you must select a UNIX group for the agent. All users under which the agent is to run must belong to this group.

umask Setting on UNIX The non-root concept relies on the user under which the agent runs belonging to a specific UNIX group. Therefore the group bits of any files that are created by HP Operations applications must be set. This allows applications to be run under dedicated users if required, while sharing the same resources, for example log files. Therefore, it is recommended to set the `umask` to suit the users that are used to run HP Operations applications.

A `umask` setting of 02 is preferable. 022 would cause problems when multiple applications are run under different users.

If only the HTTPS agent is installed or if all applications run under the same user, the `umask` does not need to be set.

Install an Agent Using an Alternative User on UNIX Managed Nodes

Complete the following steps to run a managed node under an alternative account to `root`:

1. Install the HPOM software on the desired managed node as usual.
2. Stop the agent with the command:

   `ovc -kill`

NOTE

Do not use the command:

`ovc -stop`

This stops the agent processes but not the core HPOM processes. When you later start the agent processes with the command:

`ovc -start`

as the core processes are already running under the `root` user, all other process are also started under the `root` user.

3. Set the `umask` of the user to grant `Group Permissions`.
4. Call the `ovswitchuser` command:

   `/opt/OV/bin/ovswitchuser.sh -existinguser <my_user> \`
   `-existinggroup <my_trusted_group>`

5. By default the HTTPS agent uses port 383 for network communication. This is a privileged port which can only be opened by user `root`.

   To configure the non-root agent to communicate over the network, you must select one of the following port configuration alternatives.

   If you want to continue using the reserved, privileged port `383`, set the `SUID` bit as described in the first point below. However, if you wish to use an alternative port, reset it using the following `ovconfchg` command as described in the second point.

WARNING **Only apply one of the following approaches: `setuid` OR change the `PORTS` setting.**

- It is possible to continue using the reserved, privileged port `383` by setting the `SUID` bit on the communication broker executable. Then, the communication broker only uses root privileges to open up the port and then switches back to the agent user for all other activities.

  Set the `setuid` bit of the `ovbbccb` binary with the following command:

  ```
  chmod 4550 /opt/OV/bin/ovbbccb
  ```

  Enter the following configuration command so that the root directory can be changed:

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

- Select a non-privileged `ovbbccb` port. Change the port from `383` to a desired port with a value greater than `1024`.

  For HTTPS agents, the communication broker port on a system where the HTTPS agent is not running under user `root` is changed to a non-privileged port. As a result, all other applications using the communication broker on this managed node experience the same limitation. If you want to use an alternative port, refer to “Configure the HPOM for UNIX Management Server for Agents Running Under Alternative Users” on page 91.

On a managed node, use the commands:

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

ovconfchg -ns bbc.cb.ports -set PORTS \
<FULL_DNS_NODE_NAME>:<NEW_PORT_NUMBER>
```

6. Restart the agent using the command:

```
ovc -start
```

Configure the HPOM for UNIX Management Server for Agents Running Under Alternative Users

If you use a different port than the default 383 on a managed node, you must also configure this on the HP Operations management server. In addition, the port to be used for a particular managed node must be known to all HP Operations management servers that need to contact that managed node. This is done by setting the `bbc.cb.ports PORTS` variable on HP Operations management servers.

For example, let us assume that we have a managed node with hostname `HPOM_node.sales.mycom.com`, the HP Operations management server hostname is `ovo_srv.sales.mycom.com`. The new `ovbbccb` port on `HPOM_node.sales.mycom.com` is `8001`.

This port value must be set on the managed node and the HP Operations management server.

To set an alternative value for the `ovbbccb` port, enter the following command on both HP Operations management server and the managed node:

```
ovconfchg -ns bbc.cb.ports -set PORTS \
"HPOM_node.sales.mycom.com:8001"
```

Individually setting the new port values for each managed node is inefficient and error-prone. Wildcards are recognized and should be used to specify groups of managed nodes as used in the following examples.

Let us now assume that all managed nodes of domain `sales.mycom.com` should use port `8001`. To set this port for all systems in this domain, enter the following command on both HP Operations management server and the managed nodes:

```
ovconfchg -ns bbc.cb.ports -set PORTS \
"*.sales.mycom.com:8001"
```

However, it is recommended that HP Operations management servers always use port 383. So we should modify the previous step and enter the following command on both HP Operations management server and the managed nodes:

```
ovconfchg -ns bbc.cb.ports -set PORTS \
"HPOM_srv.sales.mycom.com:383,*.sales.mycom.com:8001"
```

It is important that the `bbc.cb.ports:PORTS` entries on HP Operations management servers are always up-to-date. It is not normally important for a managed node to know which port is used by another managed node. Therefore, only the setting on the HP Operations management server and the setting on a newly installed managed node agent must be considered. No update of the `PORTS` setting on existing agents is needed.

Changing the Default Port

It is recommended that you maintain the `PORTS` setting in a central place on the HP Operations management server system and use wildcards to reduce the need to make changes on the management server.

A sample configuration file with examples of how to set up parameters is available:

`/etc/opt/OV/share/conf/OpC/mgmt_sv/bbc_inst_defaults.sampl`

Take a copy of the `bbc_inst_defaults.sampl`, rename it `bbc_inst_defaults`, and modify it as follows:

Make a `bbc_inst_defaults` file entry of the form:

```
[bbc.cb.ports]
PORTS = HPOM_srv.sales.mycom.com:383,*.sales.mycom.com:8001
```

As a result, all newly installed agents are automatically provided with the information that `HPOM_srv.sales.mycom.com` uses port `383`, while all agents matching `*.sales.mycom.com` use port `8001`. The `bbc_inst_defaults` file is the basis for the “Agent Profile”, which is installed with every new managed node. The “Agent Profile” is explained in more detail on page 93.

If a new managed node system belongs to the domain `*.sales.mycom.com`, the HP Operations management server is correctly configured and port 8001 is used. You can check this by entering the following command on the HP Operations management server:

```
ovconfget bbc.cb.ports
```

If the HP Operations management server does not have the correct settings, take the value from the bbc_inst_defaults file and call ovconfchg to update the HP Operations server with a command of the following form:

```
ovconfchg -ns bbc.cb.ports -set PORTS \
"<HPOM_server>:383,<system1>:<port1>,<system2>:<port2>, \
*.<domain1>:<port3>,*.<domain2>:<port4>"
```

Agent Profile

An agent profile maintained on the HPOM is a list of configuration settings which is copied to the agent at install time. The profile contains some default values which do not need to be configured in the bbc_inst_defaults file. Any settings defined in the bbc_inst_defaults file are also added to the agent profile.

The profile is concerned in ALL types of agent initial installations.

Use of the bbc_inst_defaults file is optional. If it exists, it is processed and the agent profile is enriched with data from the file.

In case of manual agent installation, you can create the agent profile using the command:

```
/opt/OV/bin/OpC/opcsw -create_inst_info <node>
```

The profile is located at:

```
/var/opt/OV/share/tmp/OpC/distrib/<hex_IP_addr_of_node>.i
```

NOTE When opcsw is called, it prints the <hex_IP_addr_of_node> to stdout.

Copy the profile together with the software packages to the managed node and enter a command of the following form:

```
opc_inst -configure <profile_name> ...
```

The utility opcsw includes the option:

```
create_inst_info
```

If you call **opcsw -create_inst_info <node_specifier>**

For each managed node specified in <node_specifier>, a file is created at:

/var/opt/OV/share/tmp/OpC/distrib/<hex_IP_addr>.i

This file contains the installation defaults for the managed node with IP address <hex_IP_addr>. The file is automatically copied to the target managed node during remote agent installation using inst.sh, or you can use it for manual agent installation.

The opcsw -create_inst_info command creates agent profiles using configuration data from the file:

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

on the management server and the following additional information from the HPOM database:

- **CORE_ID**: OvCoreId of managed node. An optional parameter which is added to the profile if a value for CORE_ID is available in the HPOM database under the namespace sec.core. If the CORE_ID parameter is not present in the database nor on the managed node, one is automatically created on the agent.
- **MANAGER**: Long hostname of primary HP Operations management server in namespace sec.core.auth.

  Only managed node MANAGER is authorized to perform config-, deployment-, message-, or action-execution related tasks after initial installation.
- **MANAGER_ID**: OvCoreId of MANAGER in namespace sec.core.auth.

  MANAGER_ID corresponds to MANAGER and is needed to perform the authorization checks.
- **CERTIFICATE_SERVER**: Long hostname of the system where a certificate request is issued (certificate authority) in namespace sec.cm.client.

  If no valid managed node certificate is present on the managed node, one is requested from CERTIFICATE_SERVER using the CORE_ID as the identifier.
- **PROXY**

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

These five parameters are the minimum initial settings required on a managed node. It is possible to overwrite them in the `bbc_inst_defaults` file, for example, if you have one dedicated certificate authority for several HP Operations management servers.

Changing the User of an HTTPS Agent on Windows

You must test whether the user account has appropriate rights to run the agent and manage the node correctly. You assign these user rights in the local Windows security settings on the node, or a group policy object in Active Directory. The user rights that you assign depend on your requirements. Consider assigning the following user rights:

User rights to run the agent

- Log on as a service
- Manage auditing and security log

User rights to manage the node

- Shut down the system

  This allows the agent to shut down the system (for example, when a user starts the shutdown tool in the console).

- Debug programs

  This allows the agent to collect information about processes, and to kill processes. For example, when a user starts the list processes or kill process tool in the console.

User rights to allow the agent to start commands and tools as a user other than the agent user

- Act as part of the operating system.
- Adjust memory quotas for a process (also called Increase quotas in some versions of Windows.)
- Replace a process-level token.

Additional rights for the management tasks that you need to perform

- To be able to monitor a log file using a policy, the agent user must have permission to read that log file.

- To be able to start a program using an automatic command, the agent user must have permission to start that program.

Permissions for registry entries

- The user must have full control for this registry key and all child objects:

  `HKEY_LOCAL_MACHINE/Software/Hewlett-Packard/OpenView`

- The user must have permission to read this registry key for the agent to access performance data:

  `HKEY_LOCAL_MACHINE/Software/Microsoft/WindowsNT/CurrentVersion/Perflib`

Before changing the user of the HTTPS agent, you can optionally create a new user you want to use to run the agent and create a new user group to add this user.

You can change the user as follows:

1. On the node, open the command prompt and type:

   cscript "*<OvInstallDir>*\bin\ovswitchuser.vbs" -existinguser *<DOMAIN\USER>* -existinggroup *<GROUP>* -passwd *<PASSWORD>*

   where:

   - `<DOMAIN\USER>` is the domain and user name, for example `EXAMPLE\AgentUser`. For a local user, specify just the user name, for example `AgentUser`.
   - `<GROUP>` is the name of a group that the user belongs to, for example `AgentGroup`. The command gives this group full control of all files in the agent data directory (*<OvDataDir>*), and also full control of all installed packages. If you previously started the command and specified a different group, the command removes control of the files for the previous group.
   - `<PASSWORD>` is the user's password.

2. Type the following commands:

   a. **ovc -kill**

   b. **ovc -start**

The control service and agent processes now run as the user that you specified.

Changing the default user for commands

By default, the agent starts automatic or operator-initiated commands under the user account that the agent is currently running under. If you want to configure an HTTPS agent to start commands under a different user account, set the OVO_STD_USER parameter in the eaagt name space on the nodes. You can do this in the following ways:

- Configure the values in the HTTPS agent installation defaults. This is recommended if you need to configure the user for large numbers of nodes. You must plan and configure the installation defaults before you create or migrate your nodes.
- Use ovconfchg or ovconfpar at a command prompt. For more information on the commands, see the respective man pages.

Specify the value of OVO_STD_USER in the format *<user>*/|*<encrypted password>*

where:

- <user> is the name of the user. For a domain user, specify the domain and user name, for example EXAMPLE\AgentUser. For a local user, specify just the name, for example AgentUser.
- <encrypted password> is output from the command opcpwcrpt *<password>*. You can start this command from a command prompt on the management server.

It is also possible to use the OVO_STD_USER when you configure or launch a tool. Specify the user name $OVO_STD_USER and leave the password blank.

CAUTION

You must test whether the user account has appropriate rights to run commands and tools correctly.

If the agent fails to start a command or tool as the OVO_STD_USER, the agent starts the command under the same user account that the agent is currently running under. This can happen, for example, if you specify an incorrect user or password.

Upgrading and Patching an Agent Running Under an Alternative User

Copy to Managed Node and Manually Install Later

It is possible that an HPOM administrator does not have root access to a system and the HTTPS agent is running under a non-root user. However, for HTTPS agents, if the communication broker is running on a system, you do not need to enter passwords, as data transfer works without them. Without root access, the complete remote installation of the agent, as described in the section “Installing HTTPS Managed Nodes Manually” on page 131, cannot be performed. It is only possible to copy the agent packages to the managed node system and a manual installation must be done at the managed node system itself. Native installer calls, such as `pkgadd` on Solaris, `rpm` on Linux, or `swinstall` on HP-UX need superuser privileges. This HTTPS node concept can be viewed as “copy to managed node and manually install later”.

If you run a non-root agent and you want to deploy a sub agent, a patch or a complete upgrade package which requires native installer access, the following is done automatically:

1. The bits are copied to `/tmp/<pkg_name>`.
2. The installation cannot proceed further, because the deployer is not able to call a native installer as this requires root capabilities.

   It finishes with `OK` but generates a warning message.
3. Inform an authorized person on the target managed node that the packages are locally available. This administrator can then continue with the installation by calling the `opc_inst` script in the same way as for a manual agent installation.

NOTE

HTTPS-transfer is preferred to bootstrap transport methods. This means that a remote sub-agent, patch or upgrade installation of a non-root agent will not ask for passwords but on the other hand it will terminate after copying the bits. You are not prompted for the root password and the installation must be triggered explicitly. However, the additional manual installation step respects the current agent user.

Working with Sudo Programs on UNIX Agents

One way to get the required rights is to configure a tool like sudo and configure the OV_SUDO setting. Sudo allows a permitted user to execute a command as the superuser or another user, as specified in the sudoers file. The real and effective uid and gid are set to match those of the target user as specified in the passwd file. The group vector is also initialized when the target user is not root. By default, sudo requires that users authenticate themselves with a password. By default this is the user's password, and not the root password. After a user has been authenticated, a timestamp is updated and the user may then use sudo without a password for a short period of time. By default, 15 minutes unless overridden in the sudoers file.

TIP

Sudo is free software and it is distributed under BSD-style licence. It can be obtained from http://www.sudo.ws.

Sudo software is not packaged as part of the HPOM software.

Let us take an HTTPS agent running on a Solaris managed node as a non-root user, ovo_user.

The procedure is as follows:

1. Open the /etc/sudoers file.
2. Add the following line into /etc/sudoers file. Use vi /etc/sudoers or visudo command.

   ```
   ovo_user ALL =(root) = NOPASSWD: /var/opt/OV/\
   installation/incoming/bundles/HPOM-Client/opc_inst
   ```

   Only the installation script opc_inst is called under a superuser, root.

NOTE

This command is valid for remote installation using opc_inst. In all other cases, the actual path for opc_inst must be substituted.

If NOPASSWD is not specified, you should enter your own password, for example for the user ovo_user, and not superuser (root) password.

How to Set Up a Sudo Program

NOTE The bootstrap installation does not support OV_SUDO.

HP Operations installation utilities that make native installer calls contain code of the form:

```
${OV_SUDO} opc_init
```

If the OV_SUDO variable is not set, it is interpreted as an empty string and ignored.

If the OV_SUDO variable is set, the variable is either exported from the non-root user's login shell, or it is read using `ovconfget ctrl.sudo` and then added to the environment by the install scripts.

NOTE Reading the OV_SUDO variable using `ovconfget ctrl.sudo` has higher priority than exporting its value from the non-root user's login shell.

A typical bootstrap installation of a non-root agent with sudo requires the following steps:

- Install agent as root.
- Call `/opt/OV/bin/ovswitchuser` to set the preferred user and group.
- Set preferred sudo program using the command:

  **ovconfchg -ns ctrl.sudo -set OV_SUDO **
  <my_sudo_with_full_path>

- Set preferred sudo user using the command:

  ovconfchg -ns ctrl.sudo -set OV_SUDO_USER *<my_sudo_user>*

- Set preferred sudo group using the command:

  ovconfchg -ns ctrl.sudo -set OV_SUDO_GROUP *<my_sudo_group>*

NOTE The benefit of setting a sudo allows automatic sub-agent, patch and upgrade installation of non-root environments without entering passwords. Conversely, a remote bootstrap installation requires that an HPOM administrator knows a super-user password of the managed node.

The remote agent installation first checks as which user an agent is running and whether `OV_SUDO` is setup. It decides then, whether “copy to managed node and manual install later” is needed. Depending on this bootstrap installation with password prompting or automatic installation is chosen.

Roles and Access Rights

In general, a role grants the right to perform a certain task; for example, in HPOM environments, the rights to execute actions, deploy files, or configure settings. Each preconfigured HPOM role described below has a default set of access rights that can be changed as explained in “Restricting Access Rights” on page 103.

About Roles

An HP Operations management server can assume a preconfigured HPOM role. The mapping between management servers and roles is defined in the `sec.core.auth` namespace and, in MoM environments, in the responsible manager policy.

An HPOM environment includes the following preconfigured roles:

- **Local User Role**

  The local user has all rights, assuming appropriate system rights are given, for example `root`.

- **Initial or Authorized Manager Role**

  This manager has all rights and is set up at install time. This role is defined by the `MANAGER` and `MANAGER_ID` settings in the security namespace `sec.core.auth`. There can be only one initial manager.

- **Secondary Manager Role** (MoM environments only)

  A secondary manager has all rights including action execution and configuration deployment. There can be multiple secondary managers defined in the responsible manager policy. The initial manager and the secondary managers make up the group of possible configuration servers.

- **Action-allowed Manager Role** (MoM environments only)

  An action-allowed manager has no other rights than the action execution right. There can be multiple action-allowed managers defined in the responsible manager policy.

About Access Rights

Access rights are the rights to, for example, execute actions, deploy files, and configure settings. The rights are mapped to the HP Operations management server roles described in “About Roles” on page 102.

It is possible to alter the mappings by changing configuration settings under the namespace `sec.core.auth.mapping.<HPOM_mgr_role>`, where `<HPOM_mgr_role>` is the role of the HP Operations management server. For example, to avoid accidental or unauthorized configuration deployment, you may want to disallow policy and instrumentation deployment from the initial HP Operations management server.

Restricting Access Rights

You can restrict access from the HP Operations management server processes to the HTTPS agents and thereby limit or disallow the operations a management server can perform on a managed node.

You can grant specific access rights either locally on each individual HTTPS managed node using the `ovconfchg` command-line tool, or remotely from the HP Operations management server at agent installation time, by adding the required settings to the `bbc_inst_defaults` file.

TIP

If you add the settings to the `bbc_inst_defaults` file, you do not need to change settings on individual HTTPS agents. You can limit these settings to subnets, individual nodes, and so on within the `bbc_inst_defaults` file.

See also “Avoiding Unattended Configuration Deployment” on page 105 and “Denying Remote Access” on page 106 for more information about two common scenarios.

When you use the `ovconfchg` command-line tool or the `bbc_inst_defaults` file to change access rights, you must replace the following variables with one of the possible values listed below:

Variable	Description and values

`sec.core.auth.mapping.<HPOM_mgr_role>`	Namespace of the initial HP Operations manager: `sec.core.auth.mapping.manager`
	MoM environments only:
	`sec.core.auth.mapping.secondary`
	`sec.core.auth.mapping.actionallow`
	See "About Roles" on page 102 for more information about each role.

<comp_name>	Agent component names:
	`ctrl`
	`conf`
	`depl`
	`eaagt.actr`

<dec_value>	Sum of the decimal values representing the access rights of an HP Operations manager for a particular agent component. The default values are: `ctrl` 15 `conf` 511 `depl` 2047 `eaagt.actr` 1 See Table 3-2 on page 108 for a detailed list of access rights and their corresponding values.

To restrict access to HTTPS agents, do one of the following:

- **Locally on individual HTTPS nodes**

  On the HTTPS-based managed node, use the `ovconfchg` command-line tool:

  ```
  ovconfchg -ns sec.core.auth.mapping.<HPOM_mgr_role> \
  -set <comp_name> <dec_value>
  ```

  Then restart the HTTPS agent processes.

- **Remotely from the management server at installation time**

  Specify the desired settings in the `bbc_inst_defaults` file:

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

  ```
  [sec.core.auth.mapping.<HPOM_mgr_role>]
     <comp_name> = <dec_value>
     <comp_name> = <dec_value>
     ...
  ```

Avoiding Unattended Configuration Deployment

To avoid unattended configuration deployment, you can deny configuration deployment from the HP Operations management servers by setting the following values for one or more of the HP Operations manager roles:

`conf`	496
`depl`	2044

For example, use the `ovconfchg` command-line tool on a managed node to deny configuration deployment from the initial HP Operations manager, enter:

```
ovconfchg -ns sec.core.auth.mapping.manager -set conf 496 \
-set depl 2044
ovc -kill
ovc -start
```

You can also deny configuration deployment from the initial HP Operations management server to all nodes within a specified subnet (192.168.10 in the following example) so that only authorized experts can update these security-sensitive nodes locally. Add the following lines to the `bbc_inst_defaults` file before installing the nodes:

```
[sec.core.auth.mapping.manager]
   192.168.10.* : conf = 496
   192.168.10.* : depl = 2044
```

An error message is generated when a configuration distribution request is triggered accidentally (or without authorization) on the management server.

Denying Remote Access

To completely deny remote access to an HTTPS agent, set the following values for one or more of the HP Operations manager roles:

`ctrl`	0
`conf`	0
`depl`	0
`eaagt.actr`	0

For example, use the `ovconfchg` command-line tool locally on an HTTPS managed node, enter

```
ovconfchg -ns sec.core.auth.mapping.manager - set ctrl 0 \
-set conf 0 -set depl 0 -set eaagt.actr 0
ovc -kill
ovc -start
```

Or add the following lines to the `bbc_inst_defaults` file before installing the nodes:

```
[sec.core.auth.mapping.manager]
   192.168.10.* : ctrl = 0
   192.168.10.* : conf = 0
   192.168.10.* : depl = 0
   192.168.10.* : eaagt.actr = 0
```

The management server will still be able to receive messages from the managed node but will not be able to access the node from remote. To revert this setting, use the `ovconfchg` command-line tool locally on the managed node.

Authorization Mappings

The following table lists the individual default access rights for each HPOM management server role.

Table 3-2 Authorization Mapping

Component	Right	Value	Initial Manager	Secondary Manager	Action-allowed Manager
<comp_name>		*<dec_value>*	*<HPOM_mgr_role>*		
Control (ctrl)	Start	1	yes	yes	no
	Stop	2	yes	yes	yes
	Status	4	yes	yes	no
	Notify	8	yes	yes	no
	Default value:	**15**	**15**	**15**	**2**
Config (conf)	Install policy	1	yes	yes	no
	Remove policy	2	yes	yes	no
	Enable policy	4	yes	yes	no
	Disable policy	8	yes	yes	no
	List policies	16	yes	yes	yes
	Update policy header	32	yes	yes	no
	Read configuration setting	64	yes	yes	yes
	Write configuration setting	128	yes	yes	no
	Sign policy	256	yes	yes	no
	Default value:	**511**	**511**	**511**	**80**

Table 3-2 Authorization Mapping (Continued)

Component	Right	Value	Initial Manager	Secondary Manager	Action-allowed Manager
<comp_name>		*<dec_value>*	*<HPOM_mgr_role>*		
Deploy (depl)	Deploy file	1	yes	yes	no
	Remove file or directory	2	yes	yes	no
	Get file	4	yes	yes	no
	Execute file	8	yes	yes	no
	Deploy package	16	yes	yes	no
	Remove package	32	yes	yes	no
	Upload package	64	yes	yes	no
	Download package	128	yes	yes	no
	Get inventory	256	yes	yes	yes
	Modify inventory	512	yes	yes	no
	Get node information	1024	yes	yes	yes
	Default value:	**2047**	**2047**	**2047**	**1280**
Action agent (eaagt.actr)	Execute action	1	yes	yes	yes
	Default value:	**1**	**1**	**1**	**1**

4 Concepts of Managing HTTPS Nodes

Controlling HTTPS Nodes

The HP Operations management server can perform the following functions on HTTPS nodes:

- Remote control of HTTPS agents.
- Remote and manual installation of HTTPS agents.
- Remote and manual patch installation and agent upgrade.
- Remote and manual configuration deployment.
- Support of multiple parallel configuration servers for HTTPS agents.
- Heartbeat polling.
- Security management of HTTPS nodes.
- Support of HTTPS nodes through the HP Operations management server APIs and utilities.

The following sections explain some new concepts for HTTPS nodes.

- “Configuration Deployment to HTTPS Nodes” on page 113
- “Heartbeat Polling of HTTPS Nodes” on page 118
- “Remote Control of HTTPS Nodes” on page 120
- “HP Operations Server Components and Processes” on page 344

Configuration Deployment to HTTPS Nodes

The following sections explain the configuration management concepts introduced with the HTTPS agents.

Policy Management

Policy is a configuration element in which data and meta information are strictly separated. It contains an agent configuration, a set of rules for generating the messages on the managed node where the policy is distributed to. Related policies configure a unit, which is referred to as a policy type. To learn more about policies and policy types, refer to the *HPOM Concepts Guide*.

The HPOM policies are managed in a way which allows the generic policies to be registered in the database, assigned to managed nodes, and distributed to them. For information about administration tasks related to policies, such as adding policies, registering policies and policy types, and so on, refer to the *HPOM Administrator's Reference*.

Policies can have multiple versions on the HPOM 9.0x management server, and are organized in a tree-like structure. Refer to the *HPOM Concepts Guide* and the *HPOM Administrator's Reference* for more information.

Policies can also contain category assignments. **Categories** unify the related instrumentation files and make their distribution to the managed nodes easier. For more details, refer to the *HPOM Administrator's Reference*.

Instrumentation Management

On HTTPS nodes, the actions-, commands-, and monitor directories are replaced with:

```
$OVDataDir/bin/instrumentation
```

which can have one level of sub directories. All instrumentation programs are installed at this location.

NOTE

The directory for executables on the HP Operations management server is located under:

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

No `instrumentation` directory is created and the directories actions, commands, and monitors are used, unless the categories for the instrumentation data are created. Refer to the *HPOM Administrator's Reference* for more on category-based distribution.

Typically, action, command, and monitor executables are referenced in HPOM policies. As long as these executables are not referred with their full path in policies, this change is transparent, because the new locations of the binaries is also added to the path variables of utilities like the HPOM action agent, monitor agent and logfile encapsulator.

Files from the monitor directory on the HP Operations management server are installed on the agent with the rights `744`, all others with the rights `755`.

The configuration management process can also update running executables. Scripts and binaries of running executables are renamed and allowed to complete their tasks. Subsequent execution of these programs use the newly installed files.

Manual Installation of Policies and Instrumentation

It is not possible to copy policy data directly to a managed node because the agent must receive the configuration data in a secured format. This is required to avoid illegal manipulation of configuration data by unauthorized persons on the managed nodes.

The `opctmpldwn` tool is used to prepare the manual installation of policies on the HP Operations management server. The output data is stored in a directory on the management server system dedicated to the managed node.

`opctmpldwn` handles HTTPS nodes in the following way:

- The `nodeinfo` and `mgrconf` data are regarded as policies and therefore contained in the directory mentioned above.
- A policy is encrypted with a node-specific key.

HTTPS Agent Distribution Manager

`opcbbcdist` is the configuration management adapter between the HP Operations management server and the HTTPS agents. Its main functions are:

- Convert templates into policies.
- Create instrumentation from existing actions, commands, and monitors.
- Convert ECS templates into policies and their associated circuits.
- Switch `nodeinfo` settings into the XPL format used on HTTPS nodes.

`Opcbbcdist` uses the internal file system interface:

`/var/opt/OV/share/tmp/OpC/distrib`

to get the information about what data should be deployed. It distinguishes between the four configuration categories:

- Policies/templates
- Instrumentation actions/commands/monitors
- nodeinfo
- mgrconf

`opcbbcdist` only accepts requests from other HP Operations management server components of the form `deploy configuration types xyz to node abc`. These requests may be issued by a configuration API or by `opcragt -update` and `opcragt -distrib`.

`opcbbcdist` possesses an automatic retry mechanism which is started if it was not possible to reach a node and new data is present for it. You can also manually trigger a retry by calling `opcragt -update`.

When `opcbbcdist` completes a task for a certain node, you get a message in the browser confirming correct distribution of configuration data. If tasks are not completed, messages, such as `Node Unreachable`, are displayed.

`Opcbbcdist` transfers instrumentation data first, then policies. This is done to avoid synchronization issues when an executable is referenced in a template. In addition `opcbbcdist` follows a simple transaction model: only if all data of a certain configuration type is successfully deployed, is the next category processed. The distribution of one configuration type is

regarded as one transaction. If a transaction fails, it is rolled back and retried later. This schema is also applied when `opcbbcdist` is stopped due to HP Operations server shutdown.

Configuration Push

The HP Operations management server triggers all configuration deployment tasks to HTTPS nodes. The HP Operations server pushes configuration data down to the agent and there is only out-bound communication. The more secure HP Operations management server triggers the managed nodes.

A disadvantage is that a managed node must run with old data in the case of the system not being reachable when new configuration was distributed. The HP Operations management server must poll all nodes for which configuration is present but could not be delivered. The HP Operations management server does this task:

- at least once an hour per pending node.
- when the server is restarted.
- when the configuration push is explicitly triggered by `opcragt -update`, `opcragt -distrib`, or by directly calling the API associated with the command.

A monitor called `dist_mon.sh` checks for pending distributions. If any data in the configuration transfer directory:

`/var/opt/OV/share/tmp/OpC/distrib`

is older than 30 minutes, a message is displayed that specifies the managed node where a distribution is pending.

Delta Distribution

By default in HPOM, the distribution process, known as delta-distribution, only deploys data which has been modified or added since the last configuration transfer. This minimizes the amount of data transferred and reduces the number of reconfiguration requests for interceptors and other sub agents. If required, the complete configuration can be re-deployed to the managed node.

In the delta-distribution mode, the HP Operations management server requests the policy inventory of the managed node and time stamps of the last instrumentation distribution. The policy inventory is compared

with the policy assignment list and `opcbbcdist` computes and executes the required policy removal and installation tasks for the node. For instrumentation deployment, the time stamp of the last deployment is compared with the time stamps in the management server instrumentation directories. All files on the HP Operations management server that are newer than the corresponding file on the managed node are distributed. No instrumentation data is ever removed from the managed node, except if the `opcragt -purge` command line command and option is applied.

Heartbeat Polling of HTTPS Nodes

Heartbeat polling of managed nodes checks for following things:

- Does the managed node respond to ping.
- Is `ovbbccb` (HTTPS) reachable.
- Is `ovcd` (HTTPS) reachable.
- Is the message agent (`opcmsga`) reachable.

NOTE

Other agent processes, such as `opcmona`, `opcle`, and `opcacta`, are not checked by the heartbeat polling but are monitored by the agent's health check.

If any of these processes dies and is not disabled, `ovcd` issues a message and automatically re-start the process.

Heartbeat polling of HPOM managed nodes is driven by the HPOM request sender process `ovoareqsdr` and is divided into three phases:

- The request sender `ovoareqsdr` sends ping packages to check whether the node is reachable.
- The HTTPS agent communication broker is polled.
- HP Control RPC server is requested.

TIP

You can use the `RPC_only` mode, where the ping phase is omitted, to get through firewalls which have the ICMP filter enabled. In `RPC_only` mode, less checks are executed. Should a problem arise, the detail available from the error messages is reduced.

You can set different polling intervals per node.

Reduce Network and CPU Load

To reduce CPU load, HTTPS node heartbeat-polling does not use SSL.

Heartbeat polling includes the option `agent_sends_alive_packages`. When enabled, the agent regularly informs the HP Operations management server that it is working correctly by sending ping packages. The HP Operations management server only starts polling when it has not received an alive package from one or more managed nodes in the last period.

The server plays an active role only in failure cases and the alive packages are very small. This results in an extreme reduction of network and CPU load. This feature is of great benefit when large environments are managed with no firewalls between managed nodes and the HP Operations management server.

Remote Control of HTTPS Nodes

The `opcragt` utility is used to control agents from the HP Operations management server. The operations includes start, stop, get status, primary manager switch, get and set configuration variables, as well as configuration distribution.

There is a wrapper called `opcagt` on HTTPS nodes. This utility can be used to perform remote control tasks by application launch from the operator's desktop. It allows to setup a common action definition for any kind of managed nodes.

Subagents are identified by names on HTTPS nodes. Therefore, you can specify aliases of the form:

<alias> <maps_to>

in the configuration file:

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

The entries `1 EA` and `12 CODA` are pre-defined. To automatically transform the `-id 1` into `-id EA` for HTTPS managed nodes, enter the command:

opcragt -status -id 1 *<node_list>*

5 Working with HTTPS Managed Nodes

Configure HTTPS Nodes

HTTPS nodes are configured by using the `opcnode(1m)` command line tool.

As HPOM administrator, do the following for HTTPS nodes:

- Specify a new communication type `HTTP-Based` for supported platforms.
- Specify whether a node's IP address is static or dynamically assigned using DHCP. See “Managing HTTPS Agents on DHCP Client Systems” on page 229.

Security of HTTPS communication is achieved by using certificates which results in some new steps being required to install HTTPS agents. The steps that you must complete are:

1. Install the HTTPS agent software on the managed node by using the `inst.sh` script. The node automatically sends a certificate request to the certificate server which is automatically granted. If auto-grant is disabled, the next two steps are also required.
2. The `ovcm -listpending` command is used to display the pending certificate request IDs. If you want that detailed information on every pending request is listed, use the `-l` option:

   `ovcm -listpending [-l]`

   For more information, see the *ovcm* man page.
3. To grant the certificate requests to the nodes, enter the following command:

   `ovcm -grant <requid>`

   The nodes for which certificates have been granted are added to the `Holding Area` (default) or in the configured layout group as specified in the configuration setting `OPC_CSA_LAYOUT_GROUP` in the namespace `opc`.

Install HPOM Software on HTTPS Nodes

To install the HPOM software on HTTPS nodes, perform the following steps:

1. Use the `opcnode` command line utility to add a node:

   ```
   opcnode -add_node node_name=<node_name> \
   net_type=<network_type> mach_type=<machine_type> \
   group_name=<group_name> node_type=<node_type>
   ```

NOTE

In a NAT environment (management server IP address is translated on the managed node side) the Windows HTTPS agent installation may hang. This is caused by ftp which is used during installation. The ftp connection to Windows hangs.

Install the HTTPS agent software manually. FTP is unlikely to work. Therefore, another file transport mechanism must be used.

2. To specify that the IP address of the selected HTTPS node is dynamic, use the `opcnode` command line utility with the `dynamic_ip=yes` attribute. This is most useful when the node uses DHCP to get its IP address. If DHCP is selected, HPOM automatically deals with managed node IP address changes without causing any problems, without losing any messages or without creating an inconsistent or undefined state.
3. Select the type of managed node by using `opcnode` with the `node_type` attribute. `CONTROLLED` is the default.

NOTE

On the managed node set to `MONITORED`, automatic actions will execute, however, operator-initiated action will not.

Setting `MESSAGE ALLOWED` as the node type prevents the distribution of software and instrumentation to that node.

4. Enter the desired heartbeat polling settings (optional) by using the `opchbp` command line utility, for example:

```
opchbp -interval 0h12m1s <nodename>
```

5. Use the `inst.sh` script to install the HPOM software on HTTPS nodes.
6. Information about HTTPS-based High Availability clustered systems that make up a virtual node can be gained by entering the following command:

   ```
   /opt/OV/bin/OpC/utils/opcnode \
   -list_virtual node_name=<virtual_node_name>
   ```

   To set the virtual node, enter the command:

   ```
   /opt/OV/bin/OpC/utils/opcnode \
   -set_virtual node_name=<virtual_node_name> \
   cluster_package=<package name> \
   node_list=<list of physical nodes>
   ```

NOTE The character set is always set to `Unicode`.

NOTE Only HP Operations management server features are available for virtual nodes and one agent feature: distribution of policies and instrumentation to the virtual node. Automatically distributes policies and instrumentation to all physical nodes of the virtual node.

The following options cannot be used for virtual nodes:

- `mgrconf` cannot be distributed.
- `Agent Sends Alive Packets`.
- All software installation and related options.
- Node Type `Message Allowed`.
- `Limit Buffer Size`.

After installing the HPOM software on a managed node, you must make sure that the certificates required by HTTPS communication are created and distributed. The default is for these to be generated automatically. These steps are explained in Chapter 6, “Working with Certificates.”

Define Common Settings for Managed Nodes

You can define settings on the management server, which are deployed to the managed nodes at installation time. Basic parameters, such as communication ports or http proxy settings, that are used by many nodes can be define this way. Common scenarios include:

- Need to install many HPOM agents on a subnet or domain. Due to firewall restrictions, the default port of the Communication Broker (383) cannot be used and you want to avoid having to manually set the Communication Broker port on every node during agent installation.
- Configure default settings for installation of managed nodes at a central point as the nodes of a subnet or domain share many settings.
- HPOM agents are manually installed on a subnet behind a firewall. Common parts of the installation can be automated.

You can maintain these common settings on the HP Operations management server using the file:

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

A sample configuration file with examples of how to set up parameters is available at:

`/etc/opt/OV/share/conf/OpC/mgmt_sv/bbc_inst_defaults.sampl`

Take a copy of `bbc_inst_defaults.sampl`, rename it `bbc_inst_defaults`, and modify in accordance with the syntax specified in the sample file.

Allocate a Specific OvCoreId to a Managed Node

If you want to allocate a specific OvCoreId for a new node, manually add it as follows before starting the agent software installation:

On the HP Operations management server, enter one of the following commands:

`opcnode -chg_id ... id=<id>`

or

`opcnode -add-node ... id=<id>`

During agent installation, the OvCoreId from the HPOM database is used for the specified managed node.

This is recommended when reinstalling a node managed by many management servers. Reusing the original OvCoreId avoids having to update all the HP Operations management servers.

When installing certificates manually, everything is prepared on the HP Operations management server before an agent is installed, including creating an OvCoreId, generate a certificate, add the node with the new OvCoreId to the database. Only after these steps can the agent software be installed on the managed node. Finally the certificate must be copied to the managed node.

Installing on Windows Managed Nodes

Set Startup Type on Windows Managed Nodes

Windows does not have a boot startup system comparable to UNIX. To start `ovcd` on Windows independent of user login, `ovcd` is registered as a service. Based on the default `START_ON_BOOT` value, the installation sets the service startup to `Automatic` or `Manual`. However, subsequent changes to the `START_ON_BOOT` flag have no effect on the `ovcd` service registration.

Change the service startup manually as follows:

1. Go to `Start` -> `Settings` -> `Control Panel` -> `Administrative Tools` -> `Services`
2. Double-click the `HP OpenView Ctrl Service` and from the `General` tab of the `Properties` window, set the required `Startup Type`.

This behavior can be noticed in the following use cases:

Agent Installation Using the CLI
When installing the agent on the managed node, you can set the `Automatically update system resource files` option to `yes` while running the `inst.sh` script. If you set this option for a Windows node, the `ovcd` control service is registered with start-up type Automatic, and the agent starts automatically after a reboot. If you do not set this option, the ovcd service is registered with start-up type `Manual`. In this case, you must manually start the agent after each reboot.

Manual Agent Installation
Using `opcactivate`, you can specify the `-nb` option (or an equivalent option), which has the same effect as setting `Automatically update system resource files`.

Settings set during the agent installation cannot be changed using HPOM. To change these settings, use the Windows Control Panel.

Installation Log File on Windows Managed Nodes

The Windows agent install script `opc_inst.vbs` creates the `opc_inst.log` log file. Installation steps and results are automatically records in this file. While the script is running it resides in `%TMP%` of the user under which the installation is run. The default is `Administrator`.

It is copied, after a successful installation, to *<OVInstDir>*`\data\log`.

Configure a Windows Installation Server

HTTPS agents can be fully automatically installed onto Windows systems using an installation server system. An installation server is a regular Windows managed node with an HTTPS agent installed. Once the HTTPS agent is installed, you can install any further Windows HTTPS nodes using `inst.sh` on the HP Operations management server without the need to manually execute the `opc_inst.vbs` utility on the target nodes.

NOTE It it is necessary to set the installation server of the target nodes.

The following guidelines describe the specific configurations required for the HTTPS agent acting as installation server:

- The Windows system hosting the HTTPS agent which acts as installation server must be in the HPOM node bank and must be of the same communication type (HTTPS) as the target nodes.
- It is recommended to use a dedicated system as an installation server system because it is necessary that the HTTPS agent acting as the installation server runs with extensive capabilities (see below). This means that this agent should not receive any policies or instrumentation to avoid accidental or malicious start of functionality with these capabilities.
- The HTTPS agent must run as a user who is able to access the target systems using standard Windows access mechanisms. In particularly it must be able to copy files to the target system as the software is transferred to the Windows nodes using a windows share.

To configure a managed node to act as a Windows Installation Server, complete the following steps:

1. Install and start a Windows service on the target system. This can be accomplished by making this agent run as either:
   - A domain administrator
   - Any other user who has:
     - Networking capabilities.
     - Windows pass-through authentication is in place (identical user/password on both nodes).
     - Administrative capabilities on the target nodes.

TIP

For information about Windows user rights and privileges, see the Microsoft documentation at the following location:

`http://www.microsoft.com/technet/security/prodtech/`

To install Windows agent software using an installation server, the HTTPS agent acting as the installation server cannot run as SYSTEM (which is the default) because it is not able to access remote systems. Instead, this agent must run under an identity, which is able to access the target managed node using regular Windows access mechanisms to the admin drive.

To change the user under which the HTTPS agent acting as an installation server runs, perform the following steps:

2. Stop the HTTPS agent with the command:

   ```
   ovc -kill
   ```

3. Create the Windows user account to be used.
4. Make the following user and permission changes to the selected Windows user account to make sure that the agent is running with the appropriate privileges as well as the agent directory structure has the appropriate privileges set:
   - Changes the start-up user of the Windows Service.
   - Change the permissions of HPOM data files.

Entering the following command:

```
cscript <InstallDir>\bin\ovswitchuser.vbs -existinguser
<user> -existinggroup <group> -passwd <user_pwd>
```

This command requires a few minutes to execute.

5. Due to a limitation in `ovswitchuser.vbs` , complete the following steps:

   a. Open the `Control Panel` -> `Administrative Tools` -> `Services`

   b. Change the Windows user to one which is configured to run the service `HP OpenView Ctrl Service` and re-enter the user password.

NOTE

The `SYSTEM` account is not sufficient to do the install-server tasks as it does not have the appropriate network rights. Because of this, you must change the agent user on the installation server to an existing administrative account with sufficient network rights. This user is not created automatically.

   c. Confirm that the user has been given the `Start as service` capability.

6. Start the agent with the command:

   `ovc -start`

7. Verify that the processes are running and note the user under which they are running as follows:

   a. **`ovc -status`**

   b. Open the `Task Manager` and display the user.

Installing HTTPS Managed Nodes Manually

In some situations, you may want to install the HTTPS agent software without using the management server. This manual installation enables you to prepare the system to become an HPOM managed node when it is later connected to the network. Manual installation is useful if you are preparing many systems in a central location, or if you want to avoid the network connection necessary for standard installation. Manual installation may be necessary for systems behind a firewall or behind an HTTP proxy.

Certificate Installation Tips

If an agent is installed before it is added to the HP Operations management server node bank, a certificate request is issued from the node, but it remains in the list of pending certificate requests listed by using the `ovcm -listpending` command, because it cannot be automatically mapped to any node from the node bank.

When a node is uploaded or added by using the command line tool, it is added to the `Holding Area`. Certificate requests are then automatically mapped to that node, but they are not granted. An administrator must manually grant the certificate requests as required.

When a certificate request is granted, the certificate server signs the certificate and sends it to the certificate client. The certificate client now installs the certificate on the node.

NOTE Remote certificate deployment type can be used during manual agent installation.

After the certificate is installed on the node, either by using remote certificate deployment or by manually importing the certificate to the node, the certificate client notifies the certificate server that the certificate has been successfully installed. The certificate server notifies the certificate server adapter and certificate server adapter then sets the `Node Certificate State` in the database to `Installed`.

For more detailed information about handling certificates, refer to Chapter 6, “Working with Certificates,” on page 151.

For troubleshooting certificates handling, refer to “Certificate Deployment Problems” on page 291.

Install an Agent Manually from Package Files

For an agent installation, you need superuser rights, for example, `root` on UNIX and `Administrator` on Windows. This is required because native installers, such as `swinstall` on HP-UX and MSI on Windows, which are used for the HP Operations agent installation, need super-user rights to work.

To install an agent manually from package files, complete the following steps:

1. **Check node status and select configuration**
   - Check if the system is already added to the node bank. Add the system to the node bank if desired.
   - Decide whether the managed node installation should have:
     — No configuration (only if system is not yet in the node bank)
     — Customized configuration (system must already be in the node bank)
     — Default configuration

     The type of managed node installation that you select determines which of the following steps you are required to complete.
2. **Create a default profile**

NOTE This step is required only if the managed node is already in the node bank and the configuration has been customized.

On the HP Operations management server system, create a default profile with the command:

`/opt/OV/bin/OpC/opcsw -create_inst_info <nodenames>`

For each managed node from *<nodenames>*, the following file is created:

`/var/opt/OV/share/tmp/OpC/distrib/<hex_IP_addr>.i`

The file contains the installation defaults for the managed node with IP address *<hex_IP_addr>*. The file is automatically copied to the target managed node via remote agent installation (`inst.sh`) or you can use it for manual agent installation.

To check the mapping between managed node name and its hex_IP_addr use:

`/opt/OV/bin/OpC/install/opc_ip_addr <nodename>`

This will print you the resulting hex_IP_addr for the specified managed node.

After the system is added to the node bank, copy the `/var/opt/OV/share/tmp/OpC/distrib/<hex_IP_addr>.i` profile file to the managed node system.

3. **Copy the HP Operations agent components to the managed node**

   Copy the HPOM managed node packages, installation script and package description to a temporary directory on the managed node.

   The files on the HP Operations management server that you require are:

   - `HPOvBbc.<platform>`

     `HPOvBbc.xml`
   - `HPOvConf.<platform>`

     `HPOvConf.xml`
   - `HPOvCtrl.<platform>`

     `HPOvCtrl.xml`
   - `HPOvDepl.<platform>`

     `HPOvDepl.xml`
   - `HPOvEaAgt.<platform>`

     `HPOvEaAgt.xml`
   - `HPOvPCO.<platform>`

     `HPOvPCO.xml`
   - `HPOvPacc.<platform>`

     `HPOvPacc.xml`

- `HPOvPerlA.<platform>`

  `HPOvPerlA.xml`
- `HPOvSecCC.<platform>`

  `HPOvSecCC.xml`
- `HPOvSecCo.<platform>`

  `HPOvSecCo.xml`
- `HPOvXpl.<platform>`

  `HPOvXpl.xml`
- `opc_inst` (UNIX) or `[cscript] opc_inst.vbs` (Windows)

The following are the optional language packages:

- `HPOvLcja.<platform>`

  `HPOvLcja.xml`
- `HPOvEaAja.<platform>`

  `HPOvEaAja.xml`
- `HPOvEaAes.<platform>`

  `HPOvEaAes.xml`
- `HPOvEaAko.<platform>`

  `HPOvEaAko.xml`
- `HPOvEaAzS.<platform>`

  `HPOvEaAzS.xml`

The `.xml` files are common to all architectures.

The depot files for the supported platforms are identified with a platform-specific extension *<platform>*. The value of *<platform>* is as follows:

`depot.Z.`	Files for HP-UX nodes
`sparc.Z.`	Files for Solaris (Sparc) nodes
`i86pc.Z`	Files for Solaris (Intel x86) nodes
`rpm.gz`	Files for Linux nodes
`msi`	Files for Windows nodes

The files are located in the following directory on the management server:

```
/<OvDataDir>/share/databases/OpC/mgd_node/vendor/ \
<vendor>/<newarch>/<ostype>/<HPOM_version>/RPC_BBC/
```

where *<vendor>/<newarch>/<ostype>* is, for example:

```
hp/ia64-32/hpux1122

ms/x86/winnt

linux/x86/linux24

linux/x86/linux26

ibm/rs6000/aix5

sun/x86/solaris10
```

where *<HPOM_version>* is, for example, `9.00`

4. **Install the agent software**

   On UNIX systems, you may need to change the permissions of the agent installation script to ensure that it can be executed. If you need to change the permissions, enter the command:

   ```
   chmod +x ./opc_inst
   ```

   There are three methods of installing and configuring an agent manually:

   - Default configuration
   - No configuration (to be configured later)
   - Customized configuration (configuration file must be specified)

   Select the type of configuration and complete the steps from the appropriate section below.

- **Managed nodes with default configuration**

  For managed nodes to be installed with the default configuration, go to the temporary directory to which you have copied the packages and start the agent installation script `opc_inst` by entering the command appropriate for your operating system:

  For UNIX systems:

  `./opc_inst -srv <management_server_name> -cert_srv <certificate_server_name>`

  For Windows systems:

  `[cscript] opc_inst.vbs -srv <management_server_name> -cert_srv <certificate_server_name>`

  Wait until installation and configuration on the remote managed node are finished.

- **Install, configure, and activate customized managed nodes**

  To configure a customized configuration and activate the profile created in step 2 for systems already in the node bank, use one of the following commands:

  — **`opc_inst -configure <hex_IP_addr>.i`**

  — **`opcactivate -configure <hex_IP_addr>.i`**

  Wait until installation and configuration on the remote managed node are finished.

  The settings are placed under `local_settings` and have highest priority.

  You can maintain these common settings on the HP Operations management server using the file:

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

  A sample configuration file with examples of how to set up parameters is available at:

  `/etc/opt/OV/share/conf/OpC/mgmt_sv/bbc_inst_defaults.sampl`

  Take a copy of the `bbc_inst_defaults.sampl`, rename it `bbc_inst_defaults`, and modify in accordance with the syntax specified in the sample file.

- **Pre-install managed node software without configuration**

  If you want to pre-install the managed node software on a system with no immediate configuration and prepare the system for later use, for example, by another department, enter the following command and do not specify an HP Operations management server:

  `./opc_inst -no_start`

  The software is installed but the processes are not started.

  When the node needs to be activated and the processes started, enter one of the following commands, depending on the type of configuration you want to apply.

  To apply the default configuration, enter the command:

  `./opcactivate -srv <management_server_name> \`
  `-cert_srv <certificate_server_name>`

  To apply a customized configuration, enter the command:

  `opcactivate -configure <hex_IP_addr>.i`

  Wait until installation on the remote managed node is finished.

TIP

If you want to reset the `MANAGER_ID` parameter after a failed `opcactivate` call, manually set the `MANAGER_ID` or establish communication between the HP Operations management server and the managed node and run `opcactivate` again. These methods are described below.

— On the management server system, enter the command:

`/opt/OV/bin/ovcoreid -ovrg`
`<management_server_name>`

On the managed node, enter the following command and specify the value of the `OvCoreId` of the HP Operations management server:

`ovconfchg -ns sec.core.auth -set MANAGER_ID`
`<management_server_ovcoreid>`

— Make sure that the following command from the managed node is successful:

`bbcutil -ping http://<management_server_name>`

Call `opcactivate` again.

This might not be possible in all types of environments, for example where HTTP without SSL is not possible from the managed node to the management server.

5. **Examine the managed node logfile**

   If any errors occurred during installation, correct the problems and reinstall. Errors are written to the native installer logfile for the managed node. For example, on HP-UX, the logfile is at the following location:

   `/var/adm/sw/swagent.log`

   Alternatively, `opc_inst` creates a logfile on all platforms in:

   `/<OvDataDir>/log/opc_inst.log`

6. **Map the certification request**

   On the HP Operations management server, if necessary, map the certification request to the newly installed managed node.

   a. If the pending certificate is not mapped, no output is returned after typing the following command:

      ```
      opccsa -list_pending_cr -format hrm
      ```

      For more information, see the *opccsa* man page.

   b. If the certificate request from the newly installed managed node is not mapped, enter the following command:

      ```
      opccsa -map_node <hostname|CertReqID>= \
      <nodebank_hostname>
      ```

7. **Grant the certification request**

   On the HP Operations management server, grant the certification request for the newly installed node by entering the following command:

   ```
   opccsa -grant <hostname|CertReqID>
   ```

8. **Add pre-installed nodes to the node bank**

   Only pre-installed nodes from the HP Operations management server should be added to the node bank.

a. Use the `opcnode` tool:

   For example, for an HP-UX 11 node, enter the command:

   ```
   /opt/OV/bin/OpC/opcnode -add_node
   mach_type=MACH_BBC_HPUX_PARISC \
   net_type=NETWORK_IP group_name=<node_group> \
   node_name=<node_name> node_label=<node_label>
   ```

   See the *opcnode* man page for further details.

b. If the message browser is already open, request a `Browser Reload`.

   All messages from the node should be displayed.

9. **Update the database and start heartbeat polling for the node**

   After the node is connected to the network:

   From the command line, enter the following command on the HP Operations management server:

   ```
   /opt/OV/bin/OpC/opcsw -installed <node>
   ```

10. **Verify that the HP Operations agent is running on the managed node**

    Enter the following:

    ```
    /opt/OV/bin/OpC/opcragt -status <node>
    ```

NOTE Valid certificates must be installed on the managed node, otherwise the agent will not run and the verification will fail.

Specify Folders for Agent Installation and Data

When you install an HTTPS agent, the installation creates two main folders on the node: an installation folder and a data folder.

“Generic Directory Structure on a Managed Nodes” on page 33 lists the default installation and data folders for the agent, which vary according to the node's operating system.

On new nodes that run a Windows operating system, you can manually install the agent into different folders. It is not possible to specify different folders in any other scenario:

- Remote or manual agent installations on UNIX and Linux nodes always use the default folders.
- Remote agent installations on Windows nodes always use the default folders.
- Upgrades of existing HTTPS agents always use the same folders as the existing agent.

NOTE To specify a different data folder on Windows nodes you need HTTPS agent version 8.53 or higher.

To specify agent installation and data folders, prepare the manual agent installation as described in"Install an Agent Manually from Package Files" on page 132, but add the options `-inst_dir` and `-data_dir` when you start `-opc_inst.vbs` as follows:

- Managed nodes with default configuration

  cscript opc_inst.vbs -srv <*management_server_host_name*> -cert_srv <*certificate_server_host_name*> -inst_dir <*installation_folder*> -data_dir <*data_folder*>

- Install, configure, and activate customized managed nodes

  cscript opc_inst.vbs -configure <*profile_filename*> -inst_dir <*installation_folder*> -data_dir <*data_folder*>

- Pre-install managed node software without configuration

  cscript opc_inst.vbs -no_start -inst_dir <*installation_folder*> -data_dir <*data_folder*>

The script installs the agent into the installation and data folders that you specify. You can then continue with the node setup as normal. For example, if you preinstall an agent, you must later start the agent. In all cases, you must ensure that the node receives a certificate.

Comparing `opc_inst` and `opcactivate`

- Manually installing the agent software using `opc_inst` also activates the node. The `opc_inst` tool installs the software packages and calls `opcactivate`. `opcactivate` sets some initial configuration parameters. A separate activation step is not necessary.
- The purpose of `opcactivate` is to configure the agent by establishing the three fundamental configuration settings:

  sec.core.auth: MANAGER

  Corresponds to the `-srv` option of `opc_inst` and `opcactivate`.

  sec.cm.client: CERTIFICATE_SERVER

  Corresponds to `-cert_srv` option of `opc_inst` and `opcactivate`.

  sec.core.auth: MANAGER_ID

  The `MANAGER_ID` setting defines who is allowed to access the agent from outside. By default, this is the OVO management server and therefore you need its `core_ID`.

  The is no equivalent `opc_inst` or `opcactivate` option for this parameter. Instead `opcactivate` tries to contact the OVO management server (`MANAGER_ID` setting) using `bbcutil -ping` (no SSL). If it cannot reach the management server, the `MANAGER_ID` parameter cannot be set and management server - agent communication is not possible even not if you have a valid certificate on the agent.
- When working with agent profiles:
  - All 3 settings from above are automatically included.
  - Any settings available for the managed node in the following defaults file are included:

    `/etc/opt_OV/share/conf/OpC/mgmt_sv/bbc_inst_defaults`
  - The `core_ID` of the managed node is included if it is available from the management server database.

Install Managed Nodes Using Clone Images

When installing a large number of similar managed nodes, it may be advantageous to create a clone image of a typical system configuration and use this as the basis for installing the other systems. This section provides basic information on using cloned images. If you require further details, refer to the white paper *HPOM Installing Agents Using Clone Images*. It is available from the following web site:

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

From an HPOM point of view, there are two levels of clones that could be created:

- Agent software installed on HPOM managed node system.
- Agent software installed with policies deployed to HPOM managed node system.

The clone image should not contain the unique identifier of the original managed node, the `OvCoreId`. If all cloned systems contain the same identifier, there will be a significant amount of manual reconfiguration required before these systems are recognized as individual managed node with no confusion.

To install the managed node software using a cloned image, complete the following steps:

1. Install the managed node software and configure a system that will be cloned.
2. Stop all managed node processes with the command:

   `ovc -kill`

3. Display all installed certificates from the managed node to be cloned by executing the following command:

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

The output of the following form is displayed:

```
+---------------------------------------------+
| Keystore Content                            |
+---------------------------------------------+
| Certificates:                               |
|     edb87a09-1511-75ff-13c1-f6aef454aa2b (*) |
|     edb...                                  |
+---------------------------------------------+
| Trusted Certificates:                       |
|     CA_edb66a23-1422-04ff-77c1-f1aef555aa1b  |
|     CA_edb...                               |
+---------------------------------------------+
```

4. Remove all installed certificates from the managed node to be cloned by executing the following command:

   /opt/OV/bin/ovcert -remove *<certificate name>*

   For example:

   ```
   /opt/OV/bin/ovcert -remove \
   edb87a09-1511-75ff-13c1-f6aef454aa2b \
   CA_edb66a23-1422-04ff-77c1-f1aef555aa1b
   ```

5. Check that the `CERT_INSTALLED` parameter is set to `FALSE` with the following command:

   /opt/OV/bin/ovconfget

   If the parameter is not correctly set, set it with the command:

   **/opt/OV/bin/ovconfchg -ns sec.cm.certificates **
   -set CERT_INSTALLED FALSE

6. Remove the `OvCoreID` value of the managed node to be cloned by executing the following command:

   /opt/OV/bin/ovconfchg -ns sec.core -clear CORE_ID

7. Make a clone image of the system without certificates and the `OvCoreID` value.

8. Copy the image to the new managed node system.

9. Create a new the `OvCoreID` value on the new managed node:

   ovcoreid -create

NOTE Use the **-force** option if the `OvCoreID` value was not deleted and it needs to be overwritten.

10. Run the `opcactivate` command to send a certificate request to the HP Operations management server:

    ./opcactivate -srv *<srv_name>*

NOTE Care must be taken if policies were already deployed to the managed node that was cloned. If new managed nodes created from the clone are configured to report to a different HP Operations management server than that managing the original managed node, the policies will no longer be trusted and they are signed by the Certificate Authority of the original HP Operations management server. To trust these policies, add the hostname of the original HP Operations management server as a secondary manager in the `mgrconf` file on the new managed node.

Installing Agent Hotfixes

HP Software Support may provide you with hotfixes for the HTTPS agent to address specific change requests. Agent hotfixes normally include several updated files, which you can install on affected agents immediately (without having to wait for the next version of the agent package to become available).

HPOM provides several tools that enable you to install and manage agent hotfixes remotely from the management server. These tools enable you to perform the following tasks:

- Install agent hotfixes
- List installed agent hotfixes
- Remove agent hotfixes
- Roll back agent hotfixes

Install Agent Hotfixes

1. Extract the hotfix files to a temporary directory on the management server called `/tmp/hotfix` (or, if necessary, any other temporary directory).
2. Start the tool `Tools` → `Hotfix Deployment - HPOvEaAgt` → `Copy Hotfix`.

   The tool copies the hotfix files from the temporary directory `/tmp/hotfix` to a target directory on the management server. If you extracted the hotfix files to any other directory, specify the directory in the tool parameters before you launch the tool:

   a. Right-click `Copy Hotfix`, and then click `Start Customized`. The `Start Tools - Customized Wizard (Step 2 of 3)` dialog box opens.

   b. Click `Next`, and then type the path to the temporary directory in the `Additional Parameters` field.

   c. Click `Finish`.

NOTE

The Copy Hotfix tool creates a target directory based on information in the hotfix files. If previous hotfixes already exist in the target directory, the tool overwrites the files. However, hotfixes are cumulative, and contain all the fixes for a particular version of the agent.

3. Right-click `Tools` → `Hotfix Deployment - HPOvEaAgt` → `Select Hotfix`, and then click `Start Customized`. The `Start Tools - Customized Wizard (Step 1 of 3)` dialog box opens. Select the nodes or node groups where you intend to install the hotfixes, and then click `Finish`.

   The Select Hotfix tool creates a configuration file for each combination of operating system, binary format, and agent version. If you want to install only a subset of available hotfixes, you can edit the configuration files:

   a. Navigate to the following folder:

      `/var/opt/OV/conf/eaagt`

      The name of each configuration file consists of the operating system, binary format, and agent version. For example:

      `HP-UX_IPF32_08.53.006.conf`

   b. Each configuration file contains a list of change request numbers for which hotfixes exist on the management server. If you want to install a subset of available hotfixes to nodes with a particular platform and agent version, open the corresponding configuration file in a text editor.

   c. Remove the change request numbers of the hotfixes that you do not want to install, and then save the configuration file.

4. Right-click `Tools` → `Hotfix Deployment - HPOvEaAgt` → `Deploy Hotfix`, and then click `Start Customized`. The `Start Tools - Customized Wizard (Step 1 of 3)` dialog box opens. Select the nodes or node groups where you intend to install the hotfixes, and then click `Finish`.

The Deploy Hotfix tool copies the hotfixes to each node and starts an installation script on the node. An output dialog box opens, and shows the results of the hotfix installation. The following log files also contain details of the results:

- On the management server:
  `/var/opt/OV/log/Agt_Hotfix_Install.log`
- On nodes with a Windows operating system:
  `%OvDataDir%\log\hotfix_inst.log`
- On nodes with a UNIX or Linux operating system:
  `/var/opt/OV/log/hotfix_inst.log`

NOTE If more recent hotfixes already exist on a node, the tool does not install the currently selected hotfixes to that node.

List Installed Agent Hotfixes

1. Right-click `Tools` → `Hotfix Deployment - HPOvEaAgt` → `List Inventory`, and then click `Start Customized`. The `Start Tools - Customized Wizard (Step 1 of 3)` dialog box opens.
2. Select the nodes or node groups for which you want a list of installed hotfixes, and then click `Finish`. An output dialog box opens, and shows the inventory of each node that you selected.

The inventory log file is available in the following location:
`/var/opt/OV/log/Agt_inventory.log`

Remove Agent Hotfixes

1. Right-click `Tools` → `Hotfix Deployment - HPOvEaAgt` → `Remove Hotfix`, and then click `Start Customized`. The `Start Tools - Customized Wizard (Step 1 of 3)` dialog box opens.
2. Select the nodes or node groups from which you want to remove the hotfixes, and then click `Finish`. An output dialog box opens, and shows the results of the hotfix removal.

Roll Back Agent Hotfixes

1. Right-click `Tools` → `Hotfix Deployment - HPOvEaAgt` → `Rollback Hotfix`, and then click `Start Customized`. The `Start Tools - Customized Wizard (Step 1 of 3)` dialog box opens.
2. Select the nodes or node groups on which you want to roll back the hotfixes, and then click `Finish`. An output dialog box opens, and shows the results of the hotfix roll back.

De-installing Agents

To de-install an agent from an HTTPS managed node, execute the following steps.

For UNIX managed nodes:

1. Go to the installation directory:

   cd /opt/OV/bin/OpC/install

2. Enter the following command:

   ./opc_inst -r

For Windows managed nodes:

1. Stop all HPOM agents running on the managed node.
2. Enter the following command:

   cscript "%OvInstallDir\bin\OpC\install\opc_inst.vbs" -r

De-installation Errors

If errors occur during the de-installation, check the local de-installation log files. Errors are written to the native installer logfile for the node. For example on HP-UX, the logfile is at the following location:

`/var/adm/sw/swagent.log` and `/var/adm/sw/swremove.log`

For Windows managed nodes, the logfile is:

`%SYSTEMROOT%\temp\inst.log`

Alternatively, `opc_inst` creates a logfile on all platforms in:

`/<OvDataDir>/log/opc_inst.log`

6 Working with Certificates

Creating and Distributing Certificates

Certificates are needed for network communication using the Secure Socket Layer (SSL) protocol with encryption. Server and client authentication are enabled. Managed nodes of the managed environment are identified using certificates. The “SSL handshake” between two managed nodes only succeeds if the issuing authority of the certificate presented by the incoming managed node is a trusted authority of the receiving managed node.

You can install certificates automatically, and manually. Refer to the following sections for further information.

- “Deploying Certificates Automatically” on page 154.
- “Generating Certificate for Manual Certificate Deployment” on page 158.
- “Deploying Manual Certificate with Installation Key” on page 163.

Certificate installation is monitored with HPOM messages. After a certificate request has been granted automatically, a notification message confirming the successful deployment of a certificate is sent to the message browser. If a certificate request is not automatically granted, a message in the message browser indicates the reasons for request denial and the steps that an administrator must take to solve the problem.

Certificates are managed with the `ovcm` and `opccsa` command line utilities. You can either grant, deny, list, or delete certificate requests, or map certificate requests with the corresponding node from the node bank.

Node Information

For detailed information about the node, enter the following command:
`opccsa -list_pending_cr -format rhiomp`

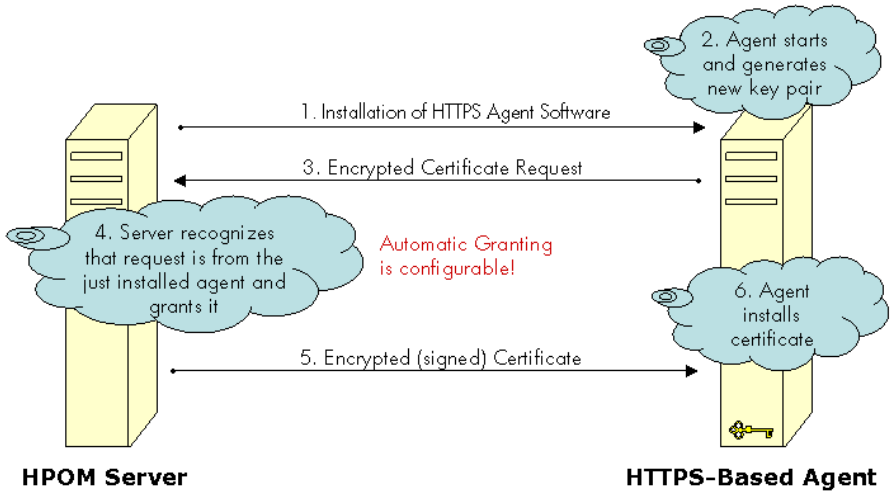
Where `rhiomp` stands for:

h	Hostname: the hostname of the node that initiated the certificate request (not a unique identifier).
i	IP address: the IP address of the node that initiated the certificate request (not a unique identifier).
o	`OVCoreID`: the only unique identifier of an HPOM HTTPS node. When you grant a request, you also grant all communication originating from the node with this `OvCoreID`. The hostnames can be changed, but the `OVCoreID` remains the unique identifier of the node.
m	Mapped to: the hostname of the node to which listed certificate requests are mapped.
p	Platform: the operating system of the HPOM managed node.

Deploying Certificates Automatically

The most common certificate deployment method is to let HPOM create, grant and distribute certificates automatically. Figure 6-1 illustrates how HPOM issues certificates to HTTPS managed nodes.

Figure 6-1 Certificate Deployment Process



After the HTTPS agent software is installed on a managed node system, the certificate management client on the node system creates a private key and a certificate request. A secret key is used to encrypt the certificate request which is sent over the network to the server system. Automatic granting is the default configuration and the autogrant interval is set to 30 minutes. If a request arrives after the allowed time interval, it must be handled by using the `ovcm -grant` command. If you wish to change this interval, use the following command:

```
ovconfchg -ovrg server -ns opc -set \
OPC_CSA_AUTOGRANT_INTERVAL <time interval in minutes>
```

If the message is encrypted with the correct key, the receiving management server trusts the sender. This does not provide full security, and is not recommended for highly secure environments but is more

secure than transmitting the requests as plain text. This mode is only used for transmitting the certificate request and the signed certificate, which should be a short period of time.

In secure environments, it is recommended that automatic granting of certificate requests is disabled and that an administrator assesses each request before granting those that are valid. You can do this with the command:

```
ovconfchg -ovrg server -ns opc -set \
OPC_CSA_USE_AUTOGRANT <TRUE|FALSE>
```

However, manual installation of certificates is the only fully secure method.

NOTE

A secret key is part of the HTTPS security software and is used by default for all HP Operations HTTPS-based applications. Every installation uses the same secret key.

A configurable secret key is a user configured key that replaces the secret key. This can be done before the management environment is setup. Ensure that every system that may request a certificate is using the same secret key as the certificate server.

Using a configured secret key ensures that a client system is not able to request a certificate from a foreign certificate server system, for example another HP Operations installation.

NOTE

The Certificate Server system must be setup and active before certificates can be generated and distributed.

To automatically deploy certificates, install the HTTPS agent software on a managed node system. After the installation, the following steps are executed by HPOM:

1. A new public/private key pair is generated on the managed node system by the certificate management client.
2. The managed node system initiates a certificate request on the node system.
3. The generated private key is stored in an encrypted file.

4. The certificate request is encrypted with the secret key and sent to the Certificate Server system (using a non-SSL connection as the node system does not yet have a valid certificate).
5. After the certificate request has been decrypted successfully on the Certificate Server it is added to the pool of pending certificate requests and a notification is sent to all registered components, and corresponding entry in the HPOM Event Browser is also displayed.
6. The certificate request is either granted or denied by matching certain preconfigured criteria. For example, the request was made within 2 minutes of the HTTPS agent software being installed on the node system.

NOTE

Granting of a certificate request is the most security sensitive step in this process. The instance that grants the request should have a good reason to do this. An example would be an administrator who is waiting for a request after deploying a package to the node that now requests a certificate from the certificate server.

7. If the request is granted, the certificate request is signed by the Certificate Server. The signed certificate is then encrypted with the secret key and sent to the node system.

   If the certificate request is denied, the server system sends a message to the node system indicating that the request has been rejected and corresponding entry in the HPOM Event Browser is also displayed.
8. The Certificate Client on the node system receives the response. If the request has been granted, it installs the new certificate and is now ready to use SSL for authenticated connections.

   If the certificate request has been denied, the Certificate Client stores this information to prevent an automatic retry.

Managing Certificates for HTTPS Managed Nodes

Certificate management is handled by using either the `ovcm` or `opccsa` command line tool.

Actions Available by Using `ovcm` or `opccsa`:

- `grant` — Used for granting the certificate request determined by `<hostname>` or `<OVCoreID>`. You can only grant mapped certificate requests.
- `deny` — Used for denying the certificate request determined by `<hostname>` or `<OVCoreID>`. You can deny any certificate request, mapped or not.
- `delete` — Used for deleting the certificate request determined by `<hostname>` or `<OVCoreID>`. You can delete any certificate request.

NOTE After any of these operations is completed, the certificate server automatically refreshes the hostname list.

Action Available by Using `opccsa`:

- `map` — Used for mapping the certificate request containing `<CertReqID>` to the node with `<nodebank_hostname>` from the node bank.

For detailed information, refer to the corresponding manpage.

Generating Certificate for Manual Certificate Deployment

Certificates can be deployed totally manually. This avoids sending any certificate-related information over the network before SSL communication is established. The public/private key pair is generated on the certificate server and then transported to the managed node system. This method is often chosen for highly secure environments where it is undesirable to transmit certificate and key data over a network.

NOTE The Certificate Server system must be setup and active before certificates can be generated and distributed.

To manually deploy certificates that have been generated on the Certificate Server:

1. If you are dealing with a particularly large environment, you can create the `bbc_inst_defaults` file to maintain common settings for managed node on the HP Operations management server. The file should be located as follows:

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

   In the namespace `sec.cm.client`, set the deployment type for your managed nodes to manual by adding an entry of the following type for each managed node:

   <IP address> `: CERTIFICATE_DEPLOYMENT_TYPE = MANUAL`

   for example:

   `192.168.10.17 : CERTIFICATE_DEPLOYMENT_TYPE = MANUAL`

   The IP address can accept wildcards to specify ranges of managed node.

   For further information, refer to the file:

   `/etc/opt/OV/share/conf/OpC/mgmt_sv/bbc_inst_defaults.sampl`

See “Changing the Default Port” on page 92 and “Agent Profile” on page 93 for some examples of how to use the `bbc_inst_defaults` file.

2. If installing the HTTPS agent software manually, create a default profile as described in point 2 of “Install an Agent Manually from Package Files” on page 132.
3. Install the HTTPS agent software on the selected managed node system, manually or remotely.
4. Make a note of the `OvCoreId` value assigned to the selected managed node. `OvCoreId` can be retrieved by calling one of the following commands:

   - **`ovcoreid`**
   - **`ovconfget sec.core`**

   When an agent is newly installed by using the `inst.sh` script, a new OvCoreId is created. However, if an OvCoreId is already present in the HPOM database for the managed node system, this is used in preference.

   When installing the agent software manually, you must create a profile, copy it and the software packages to the managed node system. The profile includes the original OvCoreId from the HPOM database. Install the profile with the command:

   `opc_inst -configure <profile>`

NOTE

The `OvCoreId` stored on a remote system can be determined by using the command:

`bbcutil -ping http://<remote system>`

provided that the Communication Broker is running on the remote system.

The `OvCoreId` can also be locally displayed with the command:

`ovcoreid`

The `OvCoreId` value stored for the managed node in the HPOM database can be displayed with the command:

`opcnode -list_id node_list=<nodename>`

5. On the HP Operations management server system, ensure that the selected managed node is added to the node bank.
6. As an HPOM administrator, create a signed certificate and the corresponding private key for a specific managed node manually on the Certificate Server system using the `opccsacm` command line tool. You must provide a password to encrypt the created data.

NOTE

If certificates must be created before the HTTPS agent software is installed on the selected managed node, it is possible to specify the `OvCoreId` (`coreid` parameter) in the following command. A `OvCoreId` is still created and it is stored in the database. The `OvCoreId`, which is part of the certificate file name, can be retrieved with the command if the managed node is already stored in the HPOM database:

opcnode -list_id node_list=*<node name>*

This value must then be set on the corresponding node system after the HTTPS agent software is installed with the command:

ovcoreid -set *<id>* -force

If no `OvCoreId` is already stored, use the value from the managed node:

The `OvCoreId` stored on a remote system can be determined by using the command:

bbcutil -ping http://*<remote system>*

provided that the Communication Broker is running on the remote system.

Alternatively, the `OvCoreId` can be locally displayed with the command:

ovcoreid

To create a certificate for the selected managed node, on the HP Operations management server system, enter the command:

**opccsacm -issue -file *<filename>* [-pass *<password>*] **
-name *<full_qual_hostname>* -coreid *<OvCoreId>*

The tool asks you to specify a password to encrypt the created certificate. This is later required to decrypt the certificate when importing the certificate to the managed node system.

7. Set the installation type to `MANUAL`, either in the `bbc_inst_defaults` file or with the command:

   ```
   ovconfchg -nssec.cm.client -set \
   CERTIFICATE_DEPLOYMENT_TYPE MANUAL
   ```

   Copy the file containing the signed certificate, its corresponding private key and the root certificate onto a floppy disk or other portable media.

   The default file location directory if the `-file` option was omitted is:

   `/<OvDataDir>/temp/OpC/certificates`

   The file name takes the following form:

   `<hostname>-OvCoreId.p12`

8. Go to the managed node system and stop the agent locally with the command:

   ```
   ovc -stop
   ```

9. Install the certificate, the trusted root certificates and the private key from the portable media using the `ovcert` command line tool. Specify the password used in step 5 when requested during installation of the certificate.

   To import the certificate, enter the following command:

   ```
   ovcert -importcert -file <file created in step 5>
   ```

   The tool will ask for the password that was provided in step 5.

NOTE Access to the medium that contains private keys should be tightly controlled to ensure that only authorized people can use them.

10. After installation, delete the certificate installation file from the managed node, and delete the data on the portable medium or store it in a secured place.
11. Start the agent locally with the command:

    ```
    ovc -start
    ```

12. Delete the file created for the certificate import from the certificate server system.

Deploying Manual Certificate with Installation Key

Manual certificate deployment with installation key offers the advantage that the private key never leaves the system to which it belongs. However, it requires that some security-related data is transmitted over the network before the certificate can be installed on the managed node system.

NOTE The Certificate Server system must be setup and active before certificates can be generated and distributed.

To manually deploy certificates using an installation key:

1. Manually install the HTTPS agent software on the managed node system. For further information, refer to “Installing HTTPS Managed Nodes Manually” on page 131.
2. As an HPOM administrator, initiate the creation of a new installation key on the Certificate Server system. Provide a password to encrypt the created key.

   opccsacm -geninstkey -file *<filename>* [-pass *<password>*]

   The Certificate Server adds the key to its installation key repository and writes it, together with some management information to a file.
3. Copy the file with the installation key information onto a floppy disk or other portable media.
4. Go to the managed node system and, using the `ovcert` command line tool, initiate a new certificate request. A new public/private key pair is generated. Use the following command:

   ovcert -certreq -instkey *<filename>*

   The encrypted request is sent to the Certificate Server.

The Certificate Server decrypts the request with the key from its repository. If the correct installation key was used, the Certificate Server automatically grants the request and sends the signed certificate back to

the managed node. Then it removes the installation key from the repository. If an invalid installation key was used, the request is automatically denied.

Displaying Certificate States

To display the certificate states of nodes, use this Certificate State Report:

```
/opt/OV/bin/OpC/call_sqlplus.sh cert_state
```

Certificate States Overview

These are two different scenarios that might possibly happen with node certificate states.

Depending on the actions, the certificate states change as follows:

Table 6-1 Certificate States Workflow Scenario 1

Certificate State	Action	Description
NO	A node is added to the node bank.	There is no agent installed. The certificate was not requested yet.
PENDING	The agent is installed manually.	The certificate request is granted, but the certificate is not yet installed on the agent. The certificate is not granted yet. The agent is installed and activated and therefore the certificate server got certificate request from it.

Table 6-1 Certificate States Workflow Scenario 1 (Continued)

Certificate State	Action	Description
GRANTED	The certificate request is granted.	The certificate request is granted, but the certificate is not yet installed on the agent. Once the certificate request is granted, the certificate is installed automatically on the agent. The state is changed to YES. Note that the state might not be visible.
GRANTED	The agents are stopped with `ovc -kill`.	The certificate state remains granted only if the managed node is unreachable. For example the agents were stopped. The certificate server tries to send the certificate to an unreachable managed node every minute after it is granted. After the time limit of two hours, the certificate request is removed from the queue. This means a new certificate request needs to be created on the managed node with `ovcert -certreq`.
YES	The certificate is installed.	The certificate is installed on agent.

Table 6-2 Certificate States Workflow Scenario 2

Certificate State	Action	Description
PENDING	The agent is activated and thus the certificate is requested.	The certificate request is PENDING.
PENDING	The agent processes are stopped using `ovc -kill`.	Since the processes are not running, the certificate cannot be delivered or installed. The certificate state remains PENDING in the GUI, it is not GRANTED yet.
GRANTED	The certificate is granted in the GUI.	Now the certificate is GRANTED in the GUI, but since the Core processes on the agent are not running, the certificate cannot be delivered and installed yet. Therefore the state remains GRANTED.
GRANTED	The agents are started with `ovc -start`.	The certificate is requested. The state is still GRANTED. The certificate state remains GRANTED until certificate server tries to install the certificate again.

Table 6-2 Certificate States Workflow Scenario 2 (Continued)

Certificate State	Action	Description
YES	The certificate server tries to send the certificate to the node.	The certificate server tries to send the certificate to an unreachable managed node every minute after it is granted. After the time limit of two hours, the certificate request is removed from the queue. This means a new certificate request needs to be created on the managed node with `ovcert -certreq`. After a while, the certificate is successfully installed and the state changes to YES.

7 Virtual Nodes in HPOM

Virtual Nodes in HPOM

Clusters are multiple systems, or nodes, that operate as a unit to provide applications, system resources, and data to users. In modern cluster environments such as Veritas Cluster, Sun Cluster or TruCluster, applications are represented as compounds of resources. Those resources construct a resource group, which represents the application running in cluster environment. Each resource has a special function in this compound.

There is a common mechanism to model applications running in cluster environments.

Terminology

The following High Availability terms and abbreviations are used in HPOM.

General High Availability Terms

HA (High Availability)

High availability is a general term used to characterize environments that are business critical and which are therefore protected against downtime through redundant resources. Very often, cluster systems are used to reach high availability.

HA Cluster (High Availability Cluster)

High availability clusters are hardware resources grouped together by a cluster management application such as HP ServiceGuard (HP/SG), Veritas Cluster, and Sun Cluster. Redundant resources are used to guarantee high availability through, for example, multiple computers, redundant network connections, and mirrored storage devices.

HA package | HA resource group | Cluster package | HARG

These terms are all used to denote a resource defined in the 'cluster world' which can be linked to an application instance. It runs on a cluster and can be switched from one cluster node to another. A cluster package is usually also linked to an element from the 'networking world' known as a virtual node.

Virtual Node

A virtual node is the network representation of an application package running on an HA cluster. A virtual node typically has a hostname and an IP address, is known to the name resolution and can be addressed like an ordinary system.

Physical Node | Cluster Node

This is one single system belonging to the cluster hardware and acting as a potential host for the HARG. A set of physical nodes makes up the cluster.

Switch-over

Controlled switch of a cluster package from one cluster node to another, for example, due to load balancing.

Fail-over

Unplanned switch of a cluster package from one cluster node to another, for example, due to an application error.

Cluster Terms used in HPOM

HPOM Virtual Node

An HPOM virtual node is a concept to represent HA packages in the HPOM database. A virtual node is assigned the hostname and IP address belonging to the HA package. An HPOM virtual node has an `HARG Name` attribute. Typically, the value of this attribute is the HA resource group name. An HPOM virtual node is comprised of the physical nodes where the HA resource group can run on the cluster.

ClAw (Cluster Awareness)

Cluster awareness is HPOM functionality which is used to monitor start and stop events of cluster packages. The ClAw module must be installed on each physical node of a cluster that is to be monitored, as the cluster awareness software only monitors start and stop events on the LOCAL node. The ClAw module is part of the HPOM HTTPS agent and the functionality is located in the `ovconfd` process.

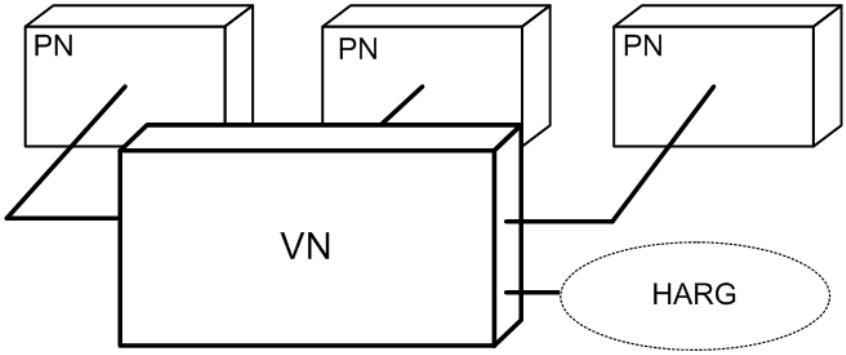
HARG Name (High Availability Resource Group Name)

HARG Name is a string attribute which can be assigned to an HPOM virtual node in the HPOM database. A HARG name in HPOM must be identical to the HA resource group's name in a cluster. This name is the link between the HPOM world (HPOM database) and the cluster world.

Virtual Node Concepts

An HPOM virtual node can be regarded a group of physical nodes linked by a common `HA Resource Group` name. The Cluster Awareness (ClAw) extension of the agents on these physical nodes can switch the policies on a physical node as the package itself switches within the virtual node.

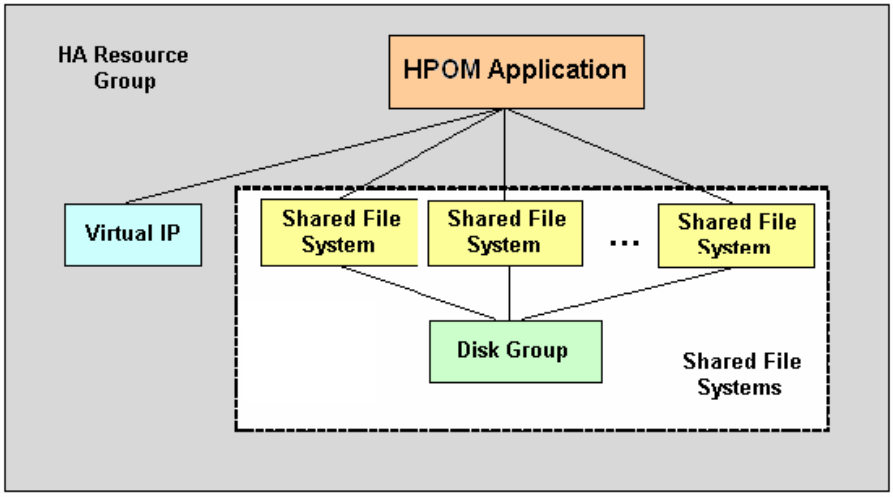
Figure 7-1 Virtual Nodes



The `HA Resource Group` name linking the managed node provides the following advantages:

- Events detected in the scope of the `HA Resource Group`, for example, by policies assigned to the virtual node, may receive that name as the originating node.
- Correct filtering and highlighting on the management station GUI.
- Provide appropriate service names and message key correlations for true management of the cluster.

Figure 7-2 HA Resource Group



NOTE This functionality is only available for HTTPS nodes.

A virtual node can be associated with just one HA resource group name.

An HA resource group name can be assigned to more than one virtual node, but these virtual nodes should not share any common physical nodes. This is because any policy assigned to both virtual nodes would receive the same HARG a second time and the cluster awareness of the agent would not be able to distinguish the virtual nodes.

Working with Virtual Nodes

The following sections describe how to work with virtual nodes in HPOM:

Adding Virtual Nodes to HPOM

Virtual nodes can be configured in a node bank by uploading them with the `opccfgupld(1m)` utility or the `opcnode(1m)` utility.

The new call parameters added to opcnode(1m):

```
-set_virtual

node_list = "node1 node2 …"

cluster_package = HARG_name
```

Example:

```
./opcnode -set_virtual node_name=ovguest3 node_list="talence
ovguest3" cluster_package=HARG_name
```

NOTE

All nodes that are to be a part of a cluster must also be members of the node bank. They must all share the same node type characteristics (platform, operating system, communication type).

The virtual node must not be a DHCP node.

The physical nodes of a cluster must not be virtual nodes themselves.

Modifying Virtual Nodes in HPOM

To modify the virtual node-related information, enter the following commands:

- To change the HA Resource Group name:

```
opcnode -set_virtual node_name=<virtual host> \
cluster_package=<HA resource group> \
node_list=<physical nodes>
```

- To change the list of physical nodes:

```
opcnode -set_virtual node_name=<virtual host> \
node_list=<physical nodes>
```

NOTE

All nodes that are to be a part of a cluster must also be members of the node bank. They must share the same node type characteristics (platform, operating system, communication type).

The physical nodes of a cluster must not be virtual nodes themselves.

Assigning Policies to Virtual Nodes in HPOM

Assigning policies to virtual nodes is done in the same way as assigning policies to physical nodes, that is, by using the `opcnode` command line utility. For example:

```
opcnode -assign_pol node_name=<virtual_node> \
net_type=NETWORK_IP pol_name=<policy_name> \
pol_type=<policy_type> [ version=<version> ]
```

For more information about the policy assignment, refer to the *HPOM Concepts Guide* and the *opcnode(1M)* man page.

Deploying Policies to Virtual Nodes in HPOM

To deploy policies to virtual nodes, use the `opcragt` command line utility. For example:

```
opcragt -dist <virtual_node>
```

NOTE The HPOM agent software cannot be deployed to a virtual node. It must be installed on all physical nodes, which make up the virtual node.

For more information about the policy deployment, refer to the *HPOM Concepts Guide* and the *opcragt* man page.

Modifying Policy Configuration on Virtual Nodes in HPOM

To modify a policy:

1. Download the policy by using the `opctempl` tool with the `-download` command line argument.

   For more information, refer to the *opctempl(1M)* man page.

2. Edit the policy body by using your favorite editor.
3. Make modifications according to the policy body grammar.

   For detailed information about the policy body grammar for the default policy types, refer to the *HPOM Concepts Guide*.

4. After you have made modifications, save the policy body and upload the policy by using `opctempl -upload`.

NOTE Make sure that you do not make changes to the policy header, otherwise the upload might fail. When the policy is uploaded, a new version with the modified policy body is created.

Deassigning Policies from Virtual Nodes in HPOM

To deassign policies from virtual nodes, use the `opcnode` command line utility. For example:

```
opcnode -deassign_pol node_name=<virtual_node> \
net_type=NETWORK_IP pol_name=<policy_name> \
pol_type=<policy_type> [ version=<version> ]
```

Deleting Virtual Nodes from HPOM

To delete a virtual node from the node bank, use the `opcnode` command line utility. For example:

```
opcnode -del_node node_name=<virtual_node> \
net_type=<network_type>
```

Configuring Agents Running under Alternative Users

HPOM agents running under alternative users do not by default have the correct permissions to issue cluster commands such as HP Serviceguard `cmviewcl` or `cmgetconf`. To grant non-root agents the required permissions, configure them to use a security program such as `sudo` or `.do` when issuing cluster commands.

For example, use the following command to configure HPOM agents running under alternative users to use the `.do` tool when issuing cluster commands:

```
ovconfchg -ns ctrl.sudo -set OV_SUDO /usr/local/bin/.do
```

If you are using a configuration file to specify which users can run which commands, add the cluster commands listed in Table 7-1 to this file.

Table 7-1 Cluster Commands Used by ClAw

Cluster Application	Cluster Command
AIX Cluster (HACMP	/usr/es/sbin/cluster/clstat
	/usr/es/sbin/cluster/utilities/clRGinfo
	/usr/es/sbin/cluster/utilities/clgetip
HP Serviceguard	/usr/sbin/cmviewcl
	/usr/sbin/cmgetconf
Microsoft Cluster Server	ClAw uses APIs instead of command-line tools.
Red Hat Cluster Suite (Red Hat Enterprise Linux 2.1)	/sbin/cluadmin
Red Hat Cluster Suite (Red Hat Enterprise Linux 3)	/usr/sbin/redhat-config-cluster-cmd
	/usr/sbin/clustat

Table 7-1 Cluster Commands Used by ClAw (Continued)

Cluster Application	Cluster Command
Red Hat Cluster Suite (Red Hat Enterprise Linux 4)	/sbin/cman_tool
	/usr/sbin/clustat
Red Hat Cluster Suite (Red Hat Enterprise Linux 5)	/usr/sbin/cman_tool
	/usr/sbin/clustat
Sun Cluster	/usr/cluster/bin/scha_cluster_get
	/usr/cluster/bin/scha_resource_get
	/usr/cluster/bin/scha_resourcegroup_get
TruCluster	/usr/sbin/clu_get_info
Veritas Cluster Server (VCS)	/opt/VRTSvcs/bin/haclus
	/opt/VRTSvcs/bin/hasys
	/opt/VRTSvcs/bin/hagrp
	/opt/VRTSvcs/bin/hares

Configuring Agents on Multi-homed Hosts

For some physical nodes, for example for multihomed nodes, the standard hostname may be different from the name of the node in the cluster configuration. If this is the case, the agent cannot correctly determine the current state of the resource group.

Configure the agent to use the hostname as it is known in the cluster configuration:

1. On the physical node, run the command `ovclusterinfo -a` to obtain the name of the physical node as it is known in the cluster configuration:

   `ovclusterinfo -a`

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

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

3. Replace *<name>* with the name of the node as reported in the output of `ovclusterinfo -a`.

4. Restart the agent:

   a. Stop the agent:

      ```
      ovc -stop AGENT
      ovc -stop COREXT
      ```

   b. Start the agent:

      ```
      ovc -start COREXT
      ovc -start AGENT
      ```

Using ClAw

Cluster awareness can be very helpful to:

- Monitor applications which are running as HA packages.
- React on HA package switch-over or fail-over.
- Represent HA-related information for operators.

These scenarios are discussed in more detail in the following sections.

Monitoring Applications Running as HA Packages

ClAw monitors package existence and package switch-over and fail-over, enabled and disabled through HPOM configuration.

Derived from HA Package events, policies which monitor application instances running on cluster nodes are enabled or disabled. A policy is enabled on a node, as soon as an HA package is running on the cluster node. It is disabled when the last package switches to another node or if none was present when the HPOM agent was started.

React to HA Package Switch-Over or Fail-Over

ClAw can be configured to run customizable start and stop actions at package switch-over or fail-over time.

Representing HA-Related Information for Operators

ClAw can be used to represent HA-related information for operators. For example, messages for a clustered application should go to the virtual node in the browser and they should color the service graph representing this application.

HA-related information for operators is handled using HPOM message enrichment to represent clustered applications.

ClAw can link the application world and cluster world. The HPOM interceptors with their policies and related instrumentation, such as monitor scripts, logfile pre-processors, and automatic actions, work on application level. For example, `opcle` monitors the logfile of an Oracle instance. Typically, such policies and instrumentation are not aware of

any underlying cluster on which the application instance runs. ClAw can link an application instance to a virtual node. Messages that are generated for a certain application or application instance, are associated with the virtual node instead of the physical node. This helps to more clearly model clustered applications in service graphs and message browsers.

ClAw and the HTTPS agent are policy-based.

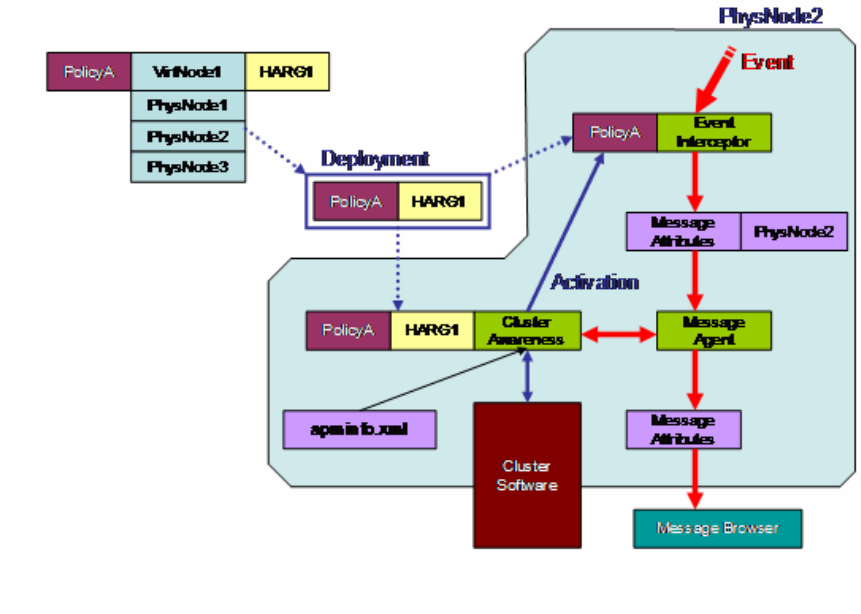
The Virtual Node Concept, ClAw, and Message Enrichment

There are three important concepts in managing clustered applications:

- ClAw
- Virtual Node Concept in HPOM
- Message Enrichment Using ClAw

The relationships between these concepts are used to represent clustered applications. Let us take a closer look at these three concepts.

Figure 7-3 Virtual Node Concept with ClAw



ClAw

ClAw reads the `apminfo.xml` file. This is the link between the application layer, for example, Oracle instances and Exchange instances, and the cluster layer (HA resource groups).

The cluster layer should be transparent for application instances.

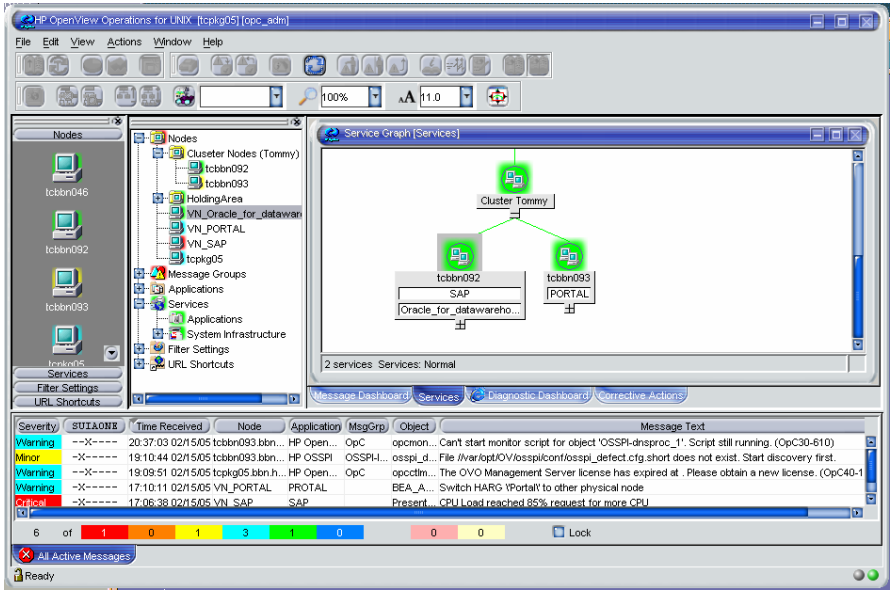
Applications like HPOM do not run as multiple instances. Applications like Oracle can support multiple instances. When there is more than one instance, the instance name from `apminfo.xml` file is important.

Virtual Node Concept in HPOM

For every monitored HA resource group, you need one virtual node.

The most important attribute of a virtual node is the `HARG name`; the name of the monitored HA resource group.

Figure 7-4 HA Concept with ClAw in HPOM



Policies inherit the HARG name attribute from the virtual nodes at policy deployment time. While stored in the database, a policy has no HARG name attribute. If the policy is assigned to several virtual nodes and the virtual nodes share physical nodes (several HA packages running on the same cluster) then the policies deployed to such physical nodes inherit the HARG name attributes from all concerned virtual nodes.

The HARG name attributes are then stored in the policy header and ClAw accesses them to perform enable/disable operations accordingly.

Example:

Two Oracle instances db_app1 and db_app2 run on the same cluster. They are linked to the HA resource groups HA_pkg_db_app1 and HA_pkg_db_app2. A single logfile policy HA_pkg_db monitors both logfiles of both instances.

You need two virtual nodes, one with HARG name HA_pkg_db_app1 the other with HA_pkg_db_app2. The policy must be assigned to both virtual nodes.

The policy exists once per cluster node after deployment. It is enabled on the nodes where HA_pkg_db_app1 or HA_pkg_db_app2 is currently running and it is disabled on any nodes where neither HA resource group is running.

NOTE

Policies are NOT installed on the shared disk of an HA resource group. Instead they are installed on all physical nodes of a cluster, which belong to a HA resource group.

If HPOM could install on the shared disk of a HA resource group, the enabling and disabling of policies would not be necessary. However, HPOM does not have the rights to install on the shared disk of any HA capable application.

Message Enrichment Using ClAw

There are two main types of ClAw message enrichment:

- Message enrichment using Custom Message Attributes (CMA).
- Message enrichment to obtain the virtual node of an application instance.

Message Enrichment Using Custom Message Attributes

There are two pre-defined custom message attributes (CMAs) which can be set in policies. These are CMA names:

- `namespace`
- `instance`

Both must map to entries in the `apminfo.xml` file. `namespace` maps to `application namespace`, and `instance` maps to `instance`. The two CMAs can be populated as follows.

- For policies:

```
  ...
CONDITION ...
  ...
  SET
    ...
    CUSTOM "namespace" "<$OPTION(my_ns)>"
    CUSTOM "instance" "<$OPTION(my_instance)>"
```

NOTE

Policies may be defined to include the user variable *<$MSG_GEN_NODE_NAME>*. For policies assigned to an HTTPS virtual node, *<$MSG_NODE_NAME>* represents the virtual node name and *<$MSG_GEN_NODE_NAME>* the physical node name of the event, if the Custom Message Attributes values for `namespace` and `instance` are set.

- For monitor scripts or the `opcmsg` command line interface:

  ```
  opcmsg ... -option my_ns=<my_appl_ns> -option \
  my_instance=<my_instance>
  ```

  or respectively

  ```
  opcmon ... -option my_ns=<my_appl_ns> -option \
  my_instance=<my_instance>
  ```

The interceptors feed the namespace, `instance CMA` into the matched messages. Next `opcmsga` reads the special CMAs and requests the HA resource group (IP address and nodename) from ClAw for *<my_appl_ns>* and *<my_instance>*. The physical name, as added by the interceptors and stored in the following message attributes, is replaced by the virtual name and corresponding IP address as received from ClAw: `node_name`, `msg_key`, `msg_key relation`, `service_name`, `auto-perator action node_name` and `operator action node_name`. This is useful, for example, if you want to show a service graph in Service Navigator, which represents a clustered application.

If an action should be executed on the physical node where the message was created, use `<$MSG_GEN_NODE_NAME>` in the action node field of the corresponding policy.

The CMAs instance and namespace are visible in the Java message browser. In addition, a further CMA is automatically added to such messages, denoting the HA resource group, called `harg`.

Configuring Custom Message Attributes

To configure custom message attributes, perform as follows:

1. Download the policy by using the `opctempl` tool with the `-download` command line argument.

   For more information, refer to the *opctempl(1M)* man page.

2. Edit the policy body by using your favorite editor.

3. Make modifications according to the policy body grammar.

   For detailed information about the policy body grammar for the default policy types, refer to the *HPOM Concepts Guide*.

4. After you have made modifications, save the policy body and upload the policy by using `opctempl -upload`.

NOTE Make sure that you do not make changes to the policy header, otherwise the upload might fail. When the policy is uploaded, a new version with the modified policy body is created.

Message Enrichment to obtain the Virtual Node of an Application Instance

ClAw incorporates the `ovappinstance` tool, located in the `$OvBinDir` directory, which can be used on command line level to get information about application instances and their related HARGs. For example, the following command prints the virtual IP address of the instance *<instance>*:

```
ovappinstance -i <instance> -host
```

Configuring ClAw and APM

ClAw and APM can be configured with exactly the same configuration files.

NOTE Some of the configuration elements are supported by ClAw only for backward compatibility. ClAw can work in `APM-mode` and in `ClAw-mode`, where the `ClAw-mode` needs no configuration on the agent in the case where you want to enable and disable policies.

There are two configuration file types:

- `$OvDataDir/conf/conf/apminfo.xml`
- `$OvDataDir/bin/instrumentation/conf/<appl_name>.apm.xml`

The following sections introduce how to use these configuration files and present some examples.

NOTE The directories `$OvDataDir/conf/conf/` and `$OvDataDir/bin/instrumentation/conf/` do not exist by default. When you are configuring apminfo.xml for the first time, you must first manually create these directories.

$OvDataDir/conf/conf/apminfo.xml

The `apminfo.xml` file is used to define the mappings between HA resource groups and application instances.

There must only be one `apminfo.xml` file per node. There is no special distribution mechanism to transport the `apminfo.xml` file from the HP Operations management server to the managed nodes. Typically, the `apminfo.xml` file is installed manually on the agents. There is no merge mechanism to add further entries to the `apminfo.xml` file. You must update it manually, for example, if you want to add another application instance -> HA resource group link.

apminfo.xml Syntax

```
<APMClusterConfiguration>
       <Application>
              <Name> ... </Name>
                 <Instance>
                       <Name> ... </Name>
                       <Package> ... </Package>
                 </Instance>

       </Application>
</APMClusterConfiguration>
```

apminfo.xml Examples

Example 1: In the following example, one application, `HP_Application`, is defined. It defines one instance with the name `HP` and an HA Resource Group with the name `ov-server`.

```
<?xml version="1.0"?>
<APMClusterConfiguration>
       <Application>
              <Name>HP_Application</Name>
              <Instance>
                       <Name>HP</Name>
                       <Package>ov-server</Package>
              </Instance>
       </Application>
</APMClusterConfiguration>
```

Example 2: In the following example, two applications, `SQL_Server` and `Exchange`, are defined. Each application defines two instances with a name and corresponding HA Resource Group name.

```
<?xml version="1.0"?>
<APMClusterConfiguration>
       <Application>
               <Name>SQL_Server</Name>
               <Instance>
                       <Name>Instance1</Name>
                       <Package>sqlsrvpkg1</Package>
               </Instance>
               <Instance>
                       <Name>Instance2</Name>
                       <Package>sqlsrvpkg2</Package>
              </Instance>
       </Application>
       <Application>
               <Name>Exchange</Name>
               <Instance>
                       <Name>Instance1</Name>
                       <Package>msexpkg1</Package>
               </Instance>
               <Instance>
                       <Name>Instance2</Name>
                       <Package>msexpkg2</Package>
               </Instance>
       </Application>
</APMClusterConfiguration>
```

$OvDataDir/bin/instrumentation/conf/ <*appl_name*>.apm.xml

The `<appl_name>.apm.xml` file is used to specify start and stop hooks used by APM and ClAw. These are used to execute additional tasks at HA package switch or fail over. Policy enable and disable operations are not handled from this file.

NOTE

With ClAw you do not need to define policy to resource group mappings in `<appl_name>.apm.xml`. Instead, you can perform these mappings by assigning HARG names to virtual nodes on the management server.

Nevertheless, the policy name to HA resource group mappings are understood by ClAw.

Usage of <appl_name>.apm.xml:

As for the `apminfo.xml` file, there are no special deployment mechanisms to distribute the configuration files to the agents.

`<appl_name>` must be defined in the `apminfo.xml` file so that the link between `apminfo.xml` entries and `<appl_name>.apm.xml` files can be made by APM and ClAw.

`<appl_name>.apm.xml` policy name to resource group mappings do not interfere with virtual node HARG names, if both are used together. It is effectively a type of redundancy; a policy mentioned in both methods is enabled or disabled twice.

NOTE

`<appl_name>.apm.xml` is dependent on the application namespace. It is not dependent on the instance level. Therefore, the start and stop actions are provided with the associated instance name as their first parameter when they are executed at package switch time (see the `$instanceName` in example 2 below). The environment variable `$instanceName` is set by ClAw when start or stop tasks are performed.

<appl_name>.apm.xml Syntax

```
<APMApplicationConfiguration>
       <Application>
               <Name> ... </Name>
               <Template> ... </Template>
               <Template> ... </Template>
               <StartCommand> ... </StartCommand>
               <StopCommand> ... </StopCommand>
       </Application>
</APMApplicationConfiguration> ?
```

Application (or application namespace)	`Application` or `Name`
Policies (or templates)	`Template`
Start Actions (or start commands)	`StartCommand`
Stop Actions (or start commands)	`StopCommand`

<appl_name>.apm.xml Examples

`<appl_name>.apm.xml` must be located at:

`/var/opt/OV/bin/instrumentation/conf`

Example 1:

The following example application configuration, `OpenView_Application`, defines the start action `/tmp/test_clawstart.sh clawstart` and the stop action `/tmp/test_clawstop.sh clawstop`.

The application configuration file should be located as follows:

`/var/opt/OV/bin/instrumentation/conf/Openview_Application.apm.xml`

```
<?xml version="1.0"?>
<APMApplicationConfiguration>
   <Application>
     <Name>OpenView_Application</Name>
     <StartCommand>/tmp/test_clawstart.sh clawstart</StartCommand>
     <StopCommand>/tmp/test_clawstop.sh clawstop</StopCommand>
   </Application>
</APMApplicationConfiguration>
```

Example 2:

The following example application configuration, `SQL_Server`, defines two policies `SQLTemplA` and `SQLTemplB` with start action `C:\startSQLSrv.bat $instanceName` and stop action `C:\stopSQLSrv.bat $instanceName`.

The application configuration file should be located as follows:

`/var/opt/OV/bin/instrumentation/conf/SQL_Server.apm.xml`

```
<?xml version="1.0"?>
<APMApplicationConfiguration>
   <Application>
     <Name>SQL_Server</Name>
     <Template>SQLTemplA</Template>
     <Template>SQLTemplB</Template>
     <StartCommand>C:\startSQLSrv.bat $instanceName</StartCommand>
     <StopCommand>C:\stopSQLSrv.bat $instanceName</StopCommand>
   </Application>
</APMApplicationConfiguration>
```

Example 3:

The following example application, `Exchange`, defines one policy `ExchangeTempl` and one custom agent or subagent `ExchangeSubAgent`.

The application configuration file should be located as follows:

`/var/opt/OV/bin/instrumentation/conf/Exchange.apm.xml`

```
<?xml version="1.0"?>
<APMApplicationConfiguration>
   <Application>
        <Name>Exchange</Name>
        <Template>ExchangeTempl</Template>
        <Subagent>ExchangeSubAgent</Subagent>
   </Application>
</APMApplicationConfiguration>
```

Syntax check tool for `apminfo.xml` and *<appl_name>*`.apm.xml` is located at:

`/opt/OV/bin/ovappinstance -vc`

where `-vc` = verify Configuration

This tool can be called on the managed node where the configuration files are used.

Command Line Utilities of ClAw

1. `$ovBinDir/ovclusterinfo` prints cluster related information.

2. **`$OvBinDir/ovappinstance`** provides information about application instances and their related HA resource groups (based on the data available in the `apminfo.xml` configuration file).

For further information, refer to the man pages for these commands.

Command Line Utilities of APM

`<HPOM_bin_dir>/opcclustns` provides information about application instances and related resource groups.

Customizing ClAw to Monitor Cluster States

ClAw checks the state of a cluster to decide whether policies have to be enabled or disabled. If a state maps to `online` then a policy is enabled, if it maps to `offline` or `unknown`, then it is disabled.

For certain use cases it can make sense to modify the mapping. For example, with Veritas Cluster Server, an administrator decides that the cluster state `|PARTIAL|` should also be regarded as `online`. This means that the administrator wants to monitor HA resource groups even if they are only partially running. A partially running HARG could mean that a minor subservice did not start, but the main service is operational.

For Veritas Cluster Server, this can be performed with the command:

```
ovconfchg -ns conf.cluster.RGState.VCS -set _PARTIAL_ online
```

NOTE

HPOM configuration setting names can only contain alpha-numeric characters and the underscore character (A ... Z, a ... z, 0 ... 9 and _).

For example, the Veritas Cluster state `|PARTIAL|` is translated by HPOM as `_PARTIAL_`.

The `ovconfchg` call must be executed on all cluster nodes.

Cluster Application Default States

The following is a list of the default states and their meaning for different cluster applications.

The term [`conf.cluster.RGState.`*<HA_Application>*], for example `[conf.cluster.RGState.MCSG]`, defines the namespace where a configuration setting is made.

Any state which is not defined in this namespace is treated as being offline. However, you can specify entries for additional states to the configuration settings with command of the following form:

```
ovconfchg -ns conf.cluster.RGState.<HA_Application> \
-set <New_State_Name> <State>
```

For HP Service Guard, Red Hat Advanced Server, Sun Cluster and Veritas Cluster Server, you can directly add the states with their value (offline or online) using the `ovconfchg` command under the appropriate name space. ClAw uses cluster commands to get the current state and then refers to the configuration settings to find whether this state is online or offline. So, while adding a new state in the configuration settings, the state string should be the same as the string returned by the cluster command used to retrieve its state.

However, this is not the case with Microsoft Cluster Server. ClAw uses Microsoft Cluster Server APIs instead of CLI tools and Microsoft Cluster Server APIs return enumerated values for its state instead of a state string.

At the time of writing, all the possible states for Microsoft Cluster Server are supported. If Microsoft Cluster Server introduces new states, it will be necessary to update ClAw to incorporate these modifications.

NOTE

The settings are not HA resource group specific. They impact the monitoring of all configured HARGs. As a result, you cannot configure resource group A so that state S maps to `online`, while for resource group B, state S maps to `offline`. The will both be `online` or `offline`.

HP Service Guard

```
[conf.cluster.RGState.MCSG]
down=offline
halting=unknown
starting=unknown
unknown=unknown
up=online
```

Microsoft Cluster Server:

```
[conf.cluster.RGState.MSCS]
ClusterGroupFailed=offline
ClusterGroupOffline=offline
ClusterGroupOnline=online
ClusterGroupPartialOnline=offline
ClusterGroupStateUnknown=unknown
```

Red Hat Advanced Server

[conf.cluster.RGState.RHAS]
started=online

Sun Cluster

```
[conf.cluster.RGState.SC]
ERROR_STOP_FAILED=unknown
OFFLINE=offline
ONLINE=online
PENDING_OFFLINE=unknown
PENDING_ONLINE=unknown
UNMANAGED=unknown
```

Veritas Cluster Server

NOTE HPOM configuration setting names can only contain alpha-numeric characters and the underscore character (A ... Z, a ... z, 0 ... 9 and _).

For example, the Veritas Cluster state |PARTIAL| is translated by HPOM as _PARTIAL_.

```
[conf.cluster.RGState.VCS]
OFFLINE=offline
ONLINE=online
_OFFLINE_=offline
_ONLINE_=online
_PARTIAL_=unknown
_UNKNOWN_=unknown
```

Getting the First Message for a Virtual Node

This is an example to generate a message for a virtual node. Prerequisite is an HA cluster on which one or more HA resource groups are running. For simplicity, just select one of the existing resource groups and model it in HPOM as a virtual node. You need to know the resource group name, either the IP address or nodename to do this.

1. Make sure that the HPOM agent software is installed on each physical node of the cluster.
2. Add the virtual node into the node bank.
3. Add the physical nodes belonging to the virtual node.
4. Specify the HA resource group name associated with the virtual node.

   In the following steps, the HA resource group name is referred to as *<my_resource_group>*.
5. Configure CMAs in the policy.

   a. Download the policy by using the `opctempl` tool with the `-download` command line argument.

      For more information, refer to the *opctempl(1M)* man page.

   b. Edit the policy body by using your favorite editor.

   c. Make modifications according to the policy body grammar.

      For detailed information about the policy body grammar for the default policy types, refer to the *HPOM Concepts Guide*.

   d. After you have made modifications, save the policy body and upload the policy by using `opctempl -upload`.

NOTE

Make sure that you do not make changes to the policy header, otherwise the upload might fail. When the policy is uploaded, a new version with the modified policy body is created.

6. Assign the `opcmsg(1|3)` policy to the virtual node.

7. Distribute the `opcmsg(1|3)` policy to the virtual node.
8. Check if the policy is installed on the agent using the `ovpolicy` command.

   On each physical node, enter the command:

   `ovpolicy -l -level 4`

   The following information is displayed:

```
msgi       "opcmsg(1|3)"   <enabled or disabled> 1
policy id : "15012f6e-ab2a-71d9-1d2e-0a110b850000"
owner     : "HPOM:<full_qualified_virtual_node_name>"
category  : <no categories defined>
attribute : "HARG:<my_resource_grp_name>" "no_value"
```

NOTE

If the policy is assigned to the virtual node only, on the node where the HA package is running, this policy is enabled. On the node where the HA package is not running, this policy is disabled.

You can obtain policy status information (enabled or disabled) using the command `ovpolicy -l`.

For example, to list installed policies for the local agent, enter the command:

`ovpolicy -l`

The information is displayed in the following form:

```
Type              Name              Status     Version
-------------------------------------------------------
configsettings    "HPOM settings"    enabled     1
msgi              "opcmsg(1|3)"     enabled    1
monitor           "mondbfile"       disabled   1
```

9. Check whether the `apminfo.xml` file is already installed on each physical node.

   On the management server, execute the following command for each of your physical nodes:

```
"
for node in <all your physical nodes>
do
opcdeploy -cmd "ls"  -par "\$OvConfDir/conf/apminfo.xml"
-node $node
done
"
```

10. If the `apminfo.xml` file is NOT installed, edit the `apminfo.xml` file on the management server and install it on each physical node as follows:

    a. **`cd /tmp`**

    b. **`vi apminfo.xml`**

    c. Put the following contents into the `apminfo.xml` file and save the file:

```
"
<?xml version="1.0"?>
<APMClusterConfiguration>
      <Application>
            <Name>OpenView_Application</Name>
            <Instance>
                  <Name>openview</Name>
                  <Package>ov-server</Package>
            </Instance>
      </Application>
</APMClusterConfiguration>
"
```

NOTE

The extract for the `apminfo.xml` file mentioned above is an example, and the application `OpenView_Application` is defined, which is mapped to `my_ns` defined in a CMA. It also defines the mapping between the application instance `openview` and the HA Resource Group `ov-server`. Instance `openview` is mapped to `my_instance` defined in the CMA.

d. Install the `apminfo.xml` file on each physical node as follows:

```
"
for node in <all of your physical node names>
do
opcdeploy -deploy -file /tmp/apminfo.xml -node $node
-targetdir "conf/conf" -trd data
done
"
```

11. If the `apminfo.xml` file is already installed on the agent, you must edit the existing `apminfo.xml` file manually as follows:

    a. Log on to the system where the `apminfo.xml` file is installed.

    b. **`cd \$OvConfDir/conf/`**

    c. **`vi apminfo.xml`**

    d. Keep the existing application definitions and define your application:

```
"
<?xml version="1.0"?>
<APMClusterConfiguration>
    <Application>
        <Name>Existing_Application</Name>
        <Instance>
            <Name>Existing_instance</Name>
            <Package>Existing_resource_group_name
                                        </Package>
        </Instance>
    </Application>
    <Application>
        <Name>OpenView_Application</Name>
        <Instance>
            <Name>openview</Name>
            <Package>ov-server</Package>
        </Instance>
    </Application>
</APMClusterConfiguration>
"
```

12. Configure the file:

    `$OvDataDir/bin/instrumentation/conf/<appl_name>.apm.xml`

This file should be created in the directory:

`$OvDataDir/bin/instrumentation/conf`

on each physical node and it should take the form of the following example:

```
<?xml version="1.0"?>
<APMApplicationConfiguration>
    <Application>
        <Name>OpenView_Application</Name>
        <Template>opcmsg(1|3)</Template>
    </Application>
</APMApplicationConfiguration>
```

For more detailed information about configuring the `<appl_name>.apm.xml` file, see "$OvDataDir/bin/instrumentation/conf/ <appl_name>.apm.xml" on page 192.

13. If the `opcmsg(1|3)` policy is installed on the agent and `enabled`, and if the `apminfo.xml` file is installed, execute the following command from this agent:

    `opcmsg a=a o=testcma msg_t="I want to test CMA" \`
    `-option my_ns=OpenView_Application \`
    `-option my_instance=openview`

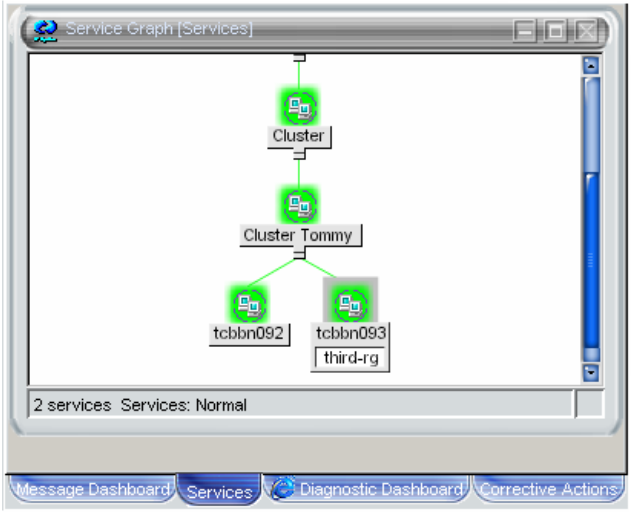
    You should receive a normal message for the virtual node with the following details in the browser:

    `Node:<virtual_nodename>`
    `Application: "a"`
    `Object: "testcma_result"`
    `Message Text: "Receive enriched message from CMA"`

Monitoring HARGs in the Java UI

Clusters and their nodes can be monitored in the `Services Graph` window. You can configure the cluster so that the active node is labelled with, for example, the application that it is hosting. When this node is no longer active, the label is switched to the new active node.

Figure 7-5 Cluster Displayed in the Services Graph



To monitor HA resource groups in the Java UI, the following configurations need to be made:

- Create an APM definition file to define the mappings between HA resource groups and application instances.
- Create or configure a command, script or executable, which is run when an HA resource group is started or stopped.
- Specify start and stop hooks used by APM and CLAw to execute additional tasks at HA package switch or fail over.
- Configure the custom message attributes.
- Create policies to label and unlabel the system in the Java GUI on which the HA resource group is active or inactive when an HA resource group is started or stopped.

Our example is based on a cluster `tommy2`, consisting of two physical nodes, `tcbbn092` and `tcbbn093`. Three HARGs are installed on this cluster; `OpenView_Application`, `second-rg` and `third-rg`. This example concentrates on the `third-rg` application. To be able to monitor HARGs in the Java GUI, the following steps need to be provided.

1. Create the APM definition file to define the mappings between HA resource groups and application instances. In the following example, for simplicity, we configure the application name and instance name to be the same as the HARG name for HA resource group "`second_rg`" and "`third_rg`". For further information, see “$OvDataDir/conf/conf/apminfo.xml” on page 189.

```
# more /var/opt/OV/conf/conf/apminfo.xml

<?xml version="1.0"?>
<APMClusterConfiguration>
      <Application>
            <Name>OpenView_Application</Name>
            <Instance>
                  <Name>openview1</Name>
                  <Package>ov-server</Package>
            </Instance>
      </Application>
      <Application>
            <Name>second-rg</Name>
            <Instance>
                  <Name>second-rg</Name>
                  <Package>second-rg</Package>
            </Instance>
      </Application>
      <Application>
            <Name>third-rg</Name>
            <Instance>
                  <Name>third-rg</Name>
                  <Package>third-rg</Package>
            </Instance>
      </Application>
</APMClusterConfiguration>
```

2. Create a shell script which will be executed when a HARG is started or stopped. It will log the start and stop information to the logfile `/tmp/clawapplication_log` and send a status message to the browser. The shell script should look like the following example:

```
# more /tmp/test_clawst.sh

application=$1
label=$2
start_stop=$3
echo "app=$application st=$start_stop label=$label"
>>/tmp/clawapplication_log
echo "$application $start_stop at:" >>/tmp/clawapplication_log
date >>/tmp/clawapplication_log
echo "HPOM_instance is $application" >>/tmp/clawapplication_log
echo "Sending $start_stop message..."
>>/tmp/clawapplication_log
/opt/OV/bin/OpC/opcmsg a=a o=o msg_t="$application $start_stop"
-option label=$label -option my_instance=$application -option
my_ns=OpenView
echo "$application ends at:" >>/tmp/clawapplication_log
date >>/tmp/clawapplication_log
echo "=======================" >>/tmp/clawapplication_log
```

3. Specify start and stop hooks used by APM and CLAw to execute additional tasks at HA package switch or fail over. For further information, see the section titled “$OvDataDir/bin/instrumentation/conf/ <appl_name>.apm.xml” on page 192.

   In the following example, we specify start and stop hooks for `third-rg`. When `third-rg` is started, the shell script `/tmp/test_clawst.sh` which we defined in the previous step is executed with input parameters `$instanceName ov_label3 starts`. A message with text `third-rg starts` is then sent to the browser and the value of `label` is set to `ov_label3`. When `third-rg` is stopped, the same shell script is executed with input parameters `$instanceName ov_label3 stops` and a message with text `third-rg stops` is then sent to the browser and the value of `label` is set to `ov_label3`.

   The start and stop definitions should be specified as in the following example:

```
# more /var/opt/OV/bin/instrumentation/conf/third-rg.apm.xml

<?xml version="1.0"?>
<APMApplicationConfiguration>
   <Application>
      <Name>third-rg</Name>
      <StartCommand>
         /tmp/test_clawst.sh $instanceName ov_label3 starts
      </StartCommand>
      <StopCommand>
         /tmp/test_clawst.sh $instanceName  ov_label3 stops
      </StopCommand>
   </Application>
</APMApplicationConfiguration>
```

4. Configure custom message attributes. For more information, see “Configuring Custom Message Attributes” on page 187.

5. Create a policy to check if an HARG is started and to label the system in the Java UI on which the HARG is active. Deploy this policy to the virtual node.

   The following policy example checks the message text for a running HARG. On finding one, it runs an automatic action to label the active cluster node with the package name, `third-rg` on node `tcbbn093` in our example.

```
OPCMSG "opcmsg(1|3)

DESCRIPTION "starts HARG"
      CONDITION_ID
"96a679b2-b59c-71d9-1ed2-c0a801020000"
      CONDITION
            TEXT "<*> starts<*>"
      SET
            SERVICE_NAME "<$MSG_GEN_NODE_NAME>"
            MSGKEY "<$OPTION(my_instance)>"
            MSGKEYRELATION ACK  "<$OPTION(my_instance)>"
            CUSTOM  "instance"  "<$OPTION(my_instance)>"
            CUSTOM  "namespace"  "<$OPTION(my_ns)>"
            CUSTOM  "orig_nodename"
"<$MSG_GEN_NODE_NAME>"
            AUTOACTION "/opt/OV/bin/OpC/opcsvcattr
svc_id=<$MSG_GEN_NODE_NAME> name=<$OPTION(label)>
value=<$OPTION(my_instance)>" ACTIONNODE IP 0.0.0.0
```

```
"<$OPC_MGMTSV>"
ANNOTATE
                SIGNATURE "EAJHjRr9vq48…
```

Enter the following command to run the `third-rg` HARG on the node `tcbbn093`:

`/usr/sbin/cmrunpkg -n tcbbno93 third-rg`

The `third-rg` HARG is started, the message `third-rg starts` is received and the icon of the node `tcbbn093` in the Java UI is labeled with the active package name, `third-rg`.

Figure 7-6 Cluster Status Showing third-rg Running on tcbbn093

Cluster status confirms that `third-rg` has been started on node `tcbbn093`

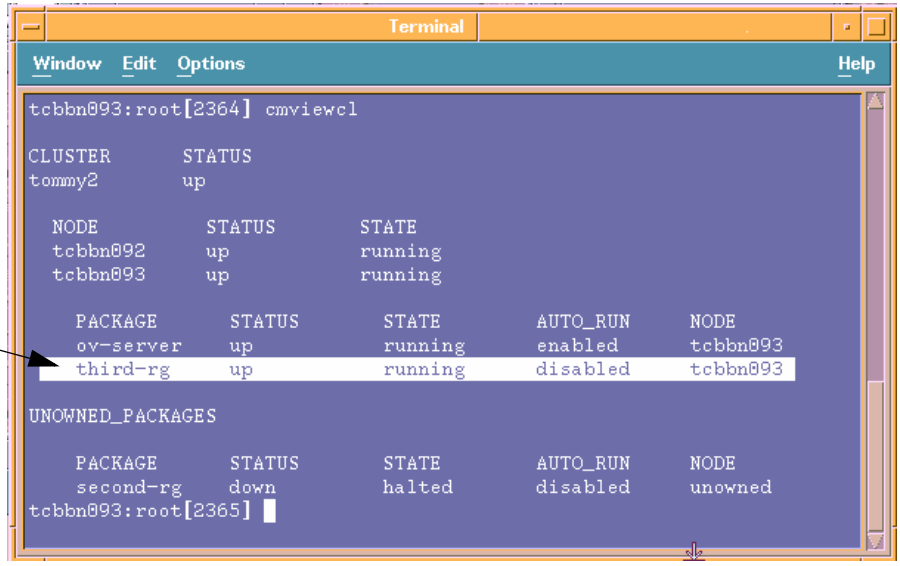
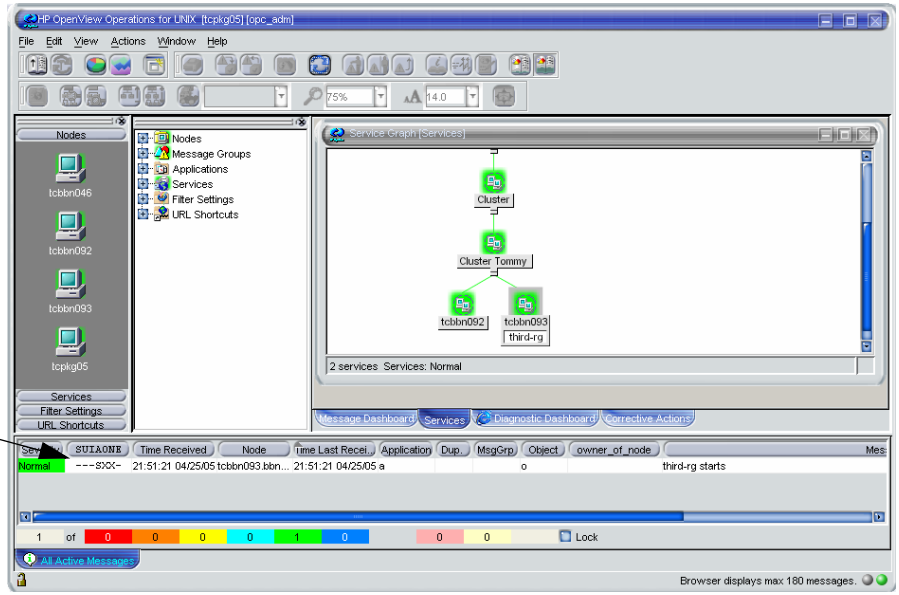


Figure 7-7 Cluster Service View Showing third-rg Running on Node tcbbn093



Message confirms that `third-rg` has been started on node `tcbbn093`

6. Create a policy to check if an HARG is stopped and to remove the label from the system in the Java UI on which the HARG was active. Deploy this policy to the virtual node.

   The following policy example checks the message text for a stopped HARG. On finding one, it runs an automatic action to remove the label from the now no longer active cluster node, `tcbbn093` in our example.

```
OPCMSG "opcmsg(1|3)

    DESCRIPTION "default interception of messages
            submitted by opcmsg(1) and opcmsg(3)"
    FORWARDUNMATCHED
    MSGCONDITIONS
    DESCRIPTION "stops HARG"
        CONDITION_ID "8070b36c-b5b3-71d9-1ed2-c0a801020000"
        CONDITION
            TEXT "<*> stop<*>"
        SET
            SEVERITY Warning
            SERVICE_NAME "<$MSG_GEN_NODE_NAME>"
```

```
                MSGKEY "<$OPTION(my_instance)>"
                MSGKEYRELATION ACK  "<$OPTION(my_instance)>"
                CUSTOM  "instance"  "<$OPTION(my_instance)>"
                CUSTOM  "namespace"  "<$OPTION(my_ns)>"
                CUSTOM  "orig_nodename"  "<$MSG_GEN_NODE_NAME>"
                AUTOACTION "/opt/OV/bin/OpC/opcsvcattr -remove
svc_id=<$MSG_GEN_NODE_NAME> name=<$OPTION(label)>" ACTIONNODE
IP 0.0.0.0  "<$OPC_MGMTSV> ANNOTATE
                SIGNATURE "RgUMFg...
```

Enter the following command to stop the `third-rg` HARG on the node `tcbbn093`:

```
/usr/sbin/cmhaltpkg -n tcbbno93 third-rg
```

The `third-rg` HARG on the node `tcbbn093` is stopped. The message `third-rg stops` is received and the label of the package name, `third-rg`, is removed.

Figure 7-8 HARG third-rg is Stopped on Node tcbbn093

Cluster status confirms that `third-rg` has been stopped on node `tcbbn093`

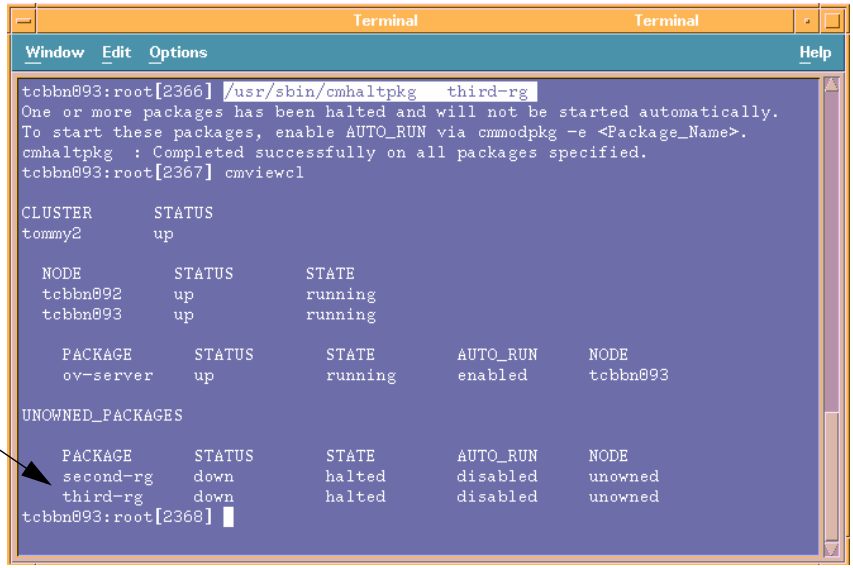
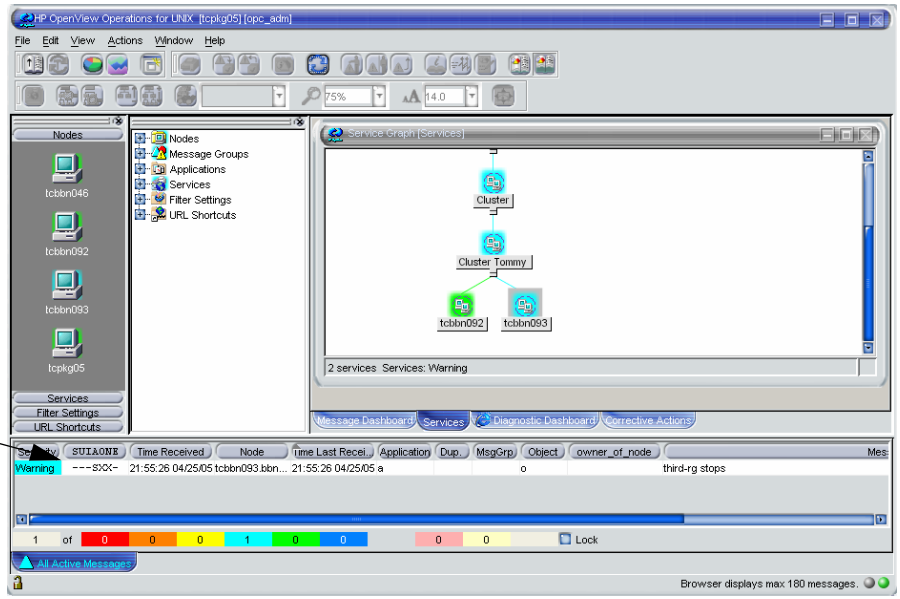


Figure 7-9 Cluster Service View with third-rg No Longer Running on Node tcbbn093

Message confirms that `third-rg` has been stopped on node `tcbbn093`



On switching the `third-rg` HARG to the node `tcbbn092`, the node icon in the `Service Graph` is labeled with the application name `third-rg`.

Figure 7-10 HARG third-rg is Started on Node tcbbn092

Cluster status confirms that `third-rg` has been started on node `tcbbn092`

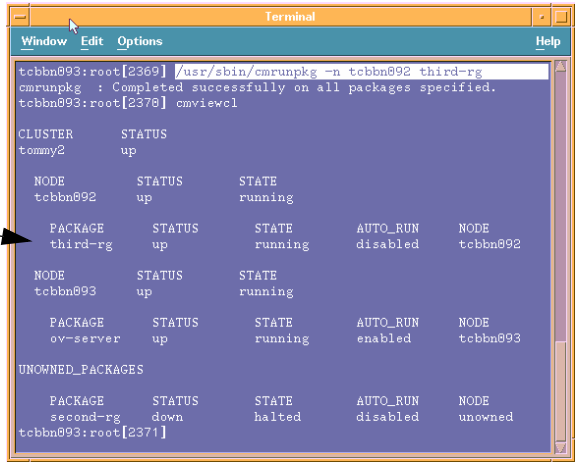
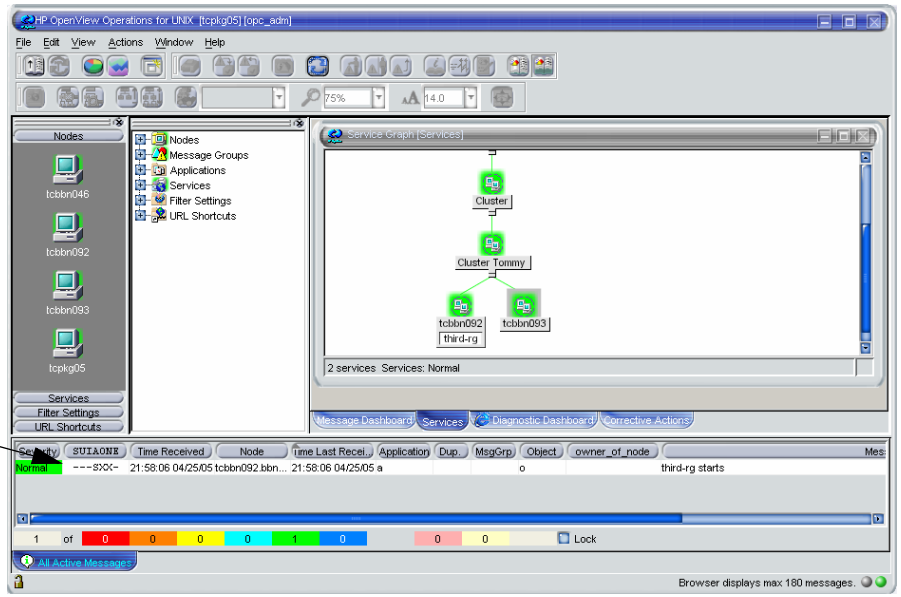


Figure 7-11 Cluster Service View Showing third-rg Running on Node tcbbn092



Message confirms that `third-rg` has been stopped on node `tcbbn092`

Virtual Node FAQs

1. Do I need to configure anything on the agent when using ClAw only for policy enabling and disabling?

   Answer:

   No. The `apminfo.xml` configuration file is not needed for policy enabling and disabling. The ClAw module is designed to monitor ALL resource groups.

2. How can I check which policies on the agent are *cluster-aware*?

   Answer:

   Enter the command:

   `/opt/OV/bin/ovpolicy -list -level 4`

   Check the output for lines with `attribute` and `HARG:`.

3. What happens if a policy is assigned to a virtual node and also assigned to a physical node belonging to that virtual node?

   Answer:

   The policy remains enabled even when the HA package is switched away from the physical node, because there is still the explicit assignment of the policy to the physical node.

4. Can I permanently disable a policy on a cluster? For example, when problems such as message storms arise?

   Answer:

   There is no completely effect method. After a package switch, the policy is normally enabled automatically. Remember that several cluster nodes are concerned and that the policy is duplicated on all cluster nodes.

   A short-term solution can be achieved with the following commands:

   On the managed node:

   `ovpolicy -disable -polname <name>`

   `ovpolicy -remove -polname <name>`

From the HP Operations management server, you can wrap the same calls into `opcdeploy`:

```
opcdeploy -cmd "ovpolicy -..." -node <virtual_nodename>
```

5. How should a model for an HTTPS-agent-monitored cluster look like in the HPOM database?

   Answer:

   Define one virtual node per monitored HA resource group.

   In addition you can have a normal node group containing the physical nodes of a cluster. This node group can be used to:

   - Assign policies only for the physical nodes.
   - Execute broadcast commands or application calls on ALL cluster nodes instead of only on the active node of an HA package.

6. What happens when I execute an action on a virtual node?

   Answer:

   The task is only executed on the node to which the virtual address refers.

7. Does APM-style (`apminfo.xml` and `<appl_name>.apm.xml` based) policy enabling and disabling collide with virtual node based enabling and disabling when both are defined for the same policy?

   Answer:

   No.

8. How can I switch off ClAw? I do not want to monitor any HA applications on a specific cluster.

   Answer:

   By default, CLAW monitors all resource groups on a system.

   Enter the following command on each cluster node:

   ```
   /opt/OV/bin/ovconfchg -ns conf.cluster -set MONITOR_MODE false
   ```

   This will reduce some CPU load on each system.

9. Can I install or patch the HPOM agent software on a cluster by deployment to the virtual node?

Answer:

No. You must install or patch each physical node individually.

10. Is the HP Operations management server running on a HA cluster also modelled as a virtual node?

Answer:

Yes. The HA resource group running HPOM is added as a virtual node to the node bank.

Limitations

Status from HPOM Patch Level 8.51:

- CMAs are supported for SNMP Trap Interceptor (`trapi`) and Scheduled tasks. Though, such CMAs can be only configured on HPOM for Windows management server, the corresponding HPOM messages can be correctly displayed and processed by the HPOM for UNIX and HPOM on Linux management server.

Status Before HPOM Patch Level 8.51:

- CMAs are not supported for `trapi`.
- `-option` approach only possible for `opcmon`, and `opcmsg`. Therefore, it is currently not possible to dynamically set CMAs with `opcle`. You can only set the CMAs in logfile policies to hard-coded values or variables from HPOM pattern matching. But it is difficult, for example, to subtract an instance name from a directory path of a logfile.

Supported Platforms

See latest *HPOM Software Release Notes*.

8 Proxies

Proxies in HPOM

Firewall programs and their associated policies, located at a network gateway server, are gateways that are used to protect the resources of a private network from external users. Users of an intranet are usually able to access the approved parts of the Internet while the firewall controls external access to the organization's internal resources.

There are two basic categories of firewalls:

- IP packet filters that work on the network level.
- Proxy servers that work on the application level, for example, a web proxy.

A proxy is a software application that examines the header and contents of Internet data packets and takes necessary action required to protect the systems to which the data is directed. In conjunction with security policies, proxies can remove unacceptable information or completely discard requests.

There are significant security-related advantages of using Application Proxies. These include:

- A fine granularity of security and access control can be achieved as proxies examine packets at the application level. For example, it is possible to restrict specific types of file transfer such as `.exe` files.
- Proxies can provide protection against “Denial of Service” attacks against the firewall.

There are two commonly cited disadvantages of using proxies:

- Proxies require large amounts of computing resources in the hose system but this is no longer a practical issue as powerful computers are now relatively inexpensive.
- Proxies must be written for specific application programs and there may be programs for which proxies are not easily available.

A proxy server stops and inspects all information before letting it access the internal network. Therefore, by using a proxy, there is no direct connection between an internal network and the “outside” world. Users must authenticate to the proxy to be able to send out information. When a client within the intranet attempts to make a request to the Internet,

the proxy actually receives that request. Using Network Address Translation (NAT), the proxy changes the source IP address of the packet to that of the proxy server, which hides the identity of the users on the internal network from the outside. If the request meets the requirements of any established policies, the proxy server forwards this request to the desired address. When a response is received, the process is reversed. As long as the incoming request is deemed to be safe, the request is forwarded to the target client on the network. The source address of the response remains unchanged but the destination address is changed back to that of the requesting machine within the firewall. This confers a dramatic increase in security for the network because there is no direct, uncontrolled route to any network systems.

There are two basic types of proxy servers:

- **Single-Homed Host**

  The proxy server has only one network card and address, and it is the responsibility of the Internet router to forward requests to the proxy server and block all other information to the network.

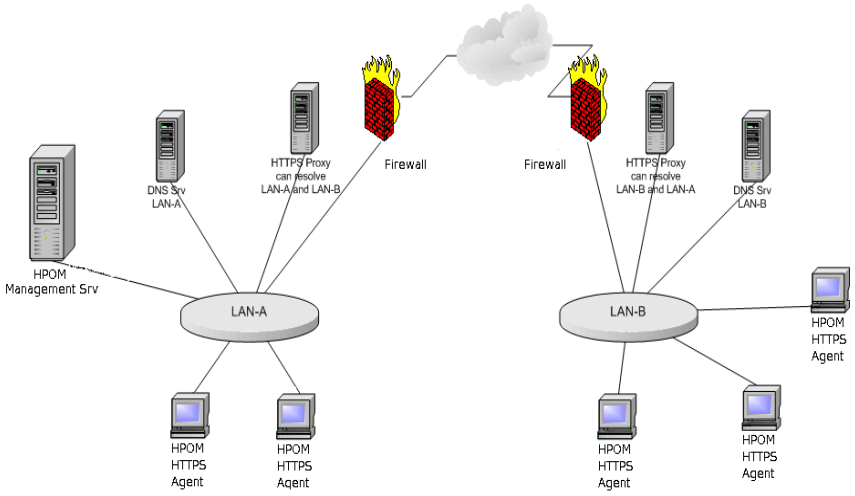
- **Dual-Homed or Multi-Homed Host**

  The proxy server is associated with more than one network card. Requests from the internal network are directed to one of the network cards. Information that comes from the Internet is received by the other network card. There is no routing setup between the network cards, so there is no direct connection between the incoming and outgoing information. The proxy server is responsible for deciding what is sent and to where it is sent.

Configuring Proxies

Most LAN-Internet-LAN architectures can be represented by the following diagram or a subset of the illustration.

Figure 8-1 HTTP Proxy Schematic



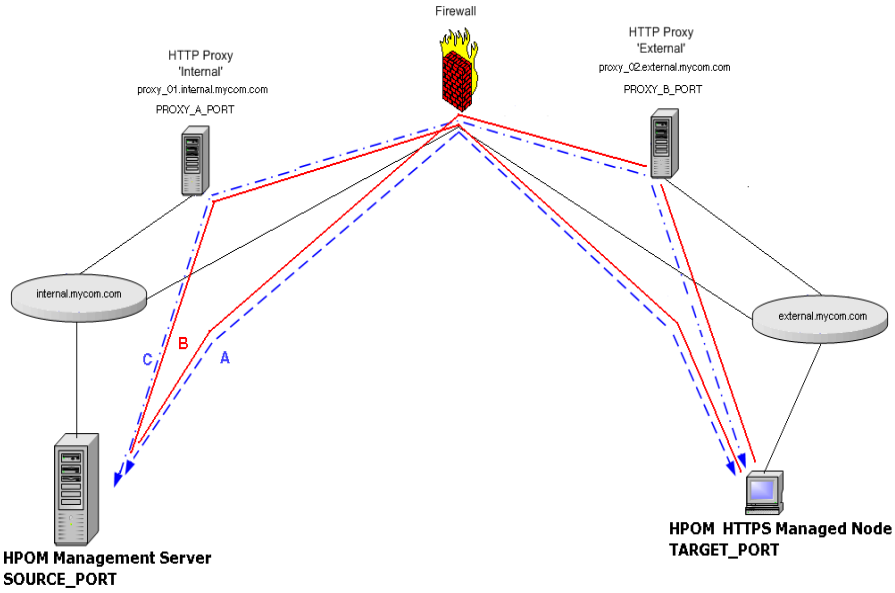
Internal LAN-A includes the HP Operations management server and an HTTP proxy.

A firewall separates the internal LAN from the Internet and the outside world.

A external LAN-B includes HTTPS managed nodes and an HTTP proxy.

The proxy communication can be represented by the following diagram or a subset of the illustration.

Figure 8-2 HTTP Proxy Infrastructure



A: Direct communication; no Proxy. Firewall must accept all connections from `*.internal.mycom.com:*` to `*.external.mycom.com:TARGET_PORT` and all connections from `*.external.mycom.com.*` to `*.internal.mycom.com:SOURCE_PORT`.

B: `proxy_01` is the proxy in domain `internal.mycom.com` and can access domain `external.mycom.com`. Firewall must accept all connections from `proxy_01.internal.mycom.com:*` to `*.external.mycom.com:TARGET_PORT`.

`proxy_02` is the proxy in domain `external.mycom.com` and can access domain `internal.mycom.com`. Firewall must accept all connections from proxy_01.internal.mycom.com to `*.internal.mycom.com:SOURCE_PORT`.

C: `proxy_01` is the proxy in domain `internal.mycom.com`. `proxy_02` is the proxy in domain `external.mycom.com`. `proxy_01` can access `proxy_02` and `proxy_02` can access `proxy_01`. Firewall must accept all connections from proxy_01.internal.mycom.com:* to

proxy_02.external.mycom.com:PROXY_B_PORT and proxy_02.external.mycom.com:* to proxy_01.internal.mycom.com:PROXY_A_PORT.

The proxies through which a managed node is to communicate must be specified for each system. This is set in the namespace `bbc.http` and stored in the `bbc.ini` file using the `ovconfchg` command. `bbc.ini` must not be edited manually.

Syntax

`ovconfchg -ns <namespace> -set <attr> <value>`

where:

`-ns <namespace>` Sets a namespace for following options.

`-set <attr> <value>` Sets an attribute (proxy) and values (port and addresses) in current namespace.

For example:

```
ovconfchg -ns bbc.http -set PROXY
"web-proxy:8088-(*.mycom.com)+(*.a.mycom.com;*)"
```

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

Format:
`proxy:port +(a)-(b);proxy2:port2+(a)-(b); ...;`

`a`: list of hostnames separated by a comma or a semicolon, for which this proxy shall be used.

`b`: list of hostnames separated by a comma or a semicolon, for which the proxy shall *not* be used.

The first matching proxy is chosen.

It is also possible to use IP addresses instead of hostnames so `15.*.*.*` or `15:*:*:*:*:*:*:*` would be valid as well, but the correct number of dots or colons MUST be specified. IP version 6 support is not currently available but will be available in the future.

`PROXY=web-proxy:8088-(*.hp.com)+(*.a.hp.com;*)`

The proxy `web-proxy` is used with port `8088` for every server `(*)` except hosts that match `*.hp.com`, for example `www.hp.com`. If the hostname matches `*.a.hp.com`, for example, `merlin.a.hp.com` the proxy server will be used.

Manual Agent Installation Behind an HTTP Proxy

Manual agent installation where the system is behind a proxy must follow the dedicated sequence of steps:

1. Take all necessary files to the system where you want to install the HTTPS agent software. See “Installing HTTPS Managed Nodes Manually” on page 131 for instructions on manual installation of HTTPS agent software.
2. Start the agent installation script by entering:

   `./opc_inst`

   You can also add server and certificate server options to this command.
3. Set the proxy parameters. For example:

   ```
   ovconfchg -ns bbc.http -set PROXY
   "web-proxy:8088-(*.mycom.com)+(*.a.mycom.com;*)"
   ```
4. When the node needs to be activated and the agent started, enter the command:

   `./opcactivate -srv <srv_name>`

Set Proxies on a Managed Node

To set proxies on a managed node:

1. Manually install the agent software on the managed node system. It will probably not be possible to do a remote installation as the target system cannot yet be reached. See “Installing HTTPS Managed Nodes Manually” on page 131 for instructions on manual installation of HTTPS agent software.
2. Set the proxies over which the HP Operations agent will communicate with the HP Operations management server. For example:

   ```
   ovconfchg -ns bbc.http -set PROXY
   "web-proxy:8088-(*.mycom.com)+(*.a.mycom.com;*)"
   ```

3. Stop all agent processes with the command:

   ovc -kill

4. Restart the agent with the command to register the proxy changes:

   ovc -start

Set Proxies on the HP Operations Management Server

To change the proxy settings on the HP Operations management server:

1. Set the proxies over which the management server will communicate with its HTTPS managed nodes. For example:

   ```
   ovconfchg -ns bbc.http -set PROXY
   "web-proxy:8088-(*.mycom.com)+(*.a.mycom.com;*)"
   ```

2. Stop all HP Operations processes with the following commands:

   opcsv -stop

   /opt/OV/bin/OpC/ovc -kill

3. Restart the processes with the following commands to register the proxy changes:

   opcsv -start

   /opt/OV/bin/OpC/opcagt -start

Manual Agent Installation Behind an HTTP Proxy with No Name Resolution

In some cases agent and server nodes are not able to resolve each other's node names. This can be caused by a system configuration where DNS is disabled and `/etc/hosts` file does not introduce other node names. This can be the case with systems behind a proxy which can only resolve the both node names: agent's and management server's.

To install the agent manually on a system behind a proxy, complete the following steps:

1. On the management server, provide a dummy IP address and the real hostname for this managed node in `/etc/hosts` and then add the managed node to the node bank.

   Without this name service entry you cannot add this managed node to the node bank nor grant a certificate for it.

2. In the node bank for this agent, set the Heartbeat Polling (HBP) type by using the `opchbp` command line utility.

3. Configure the proxy settings on the HP Operations management server to enable HPOM to contact the managed node system. See "Set Proxies on the HP Operations Management Server" on page 225" for instructions.

4. Copy all necessary files to the system where you want to install the HTTPS agent software. See "Installing HTTPS Managed Nodes Manually" on page 131" for instructions on manual installation of HTTPS agent software.

5. Start the agent installation script with the command:

   `./opc_inst`

   You can also add server and certificate server options to this command and skip step 6.

6. Set the proxy parameter on the agent. For example:

   ```
   ovconfchg -ns bbc.http -set PROXY
   "web-proxy:8088-(*.mycom.com)+(*.a.mycom.com;*)"
   ```

If the agent is already running, restart it:

```
ovc -kill
```

```
ovc -start
```

7. When the node needs to be activated and the agent started (in the case it is not yet started in step 4), enter the command:

   ```
   ./opcactivate -srv <srv_name> -cert_srv \
   <certificate_server_name>
   ```

8. If the certificate has not been manually installed on the agent, trigger certificate request from this managed node system with the command:

   ```
   ovcert -certreq
   ```

9. Grant the certificate for this agent:

   ```
   ovcm -listpending [-l]
   ```

   ```
   ovcm -grant <reqid>
   ```

10. Optionally remove *<agent_node>* from `/etc/hosts` on the management server.

9 Managing HTTPS Agents on DHCP Client Systems

HP Operations Agents and DHCP

Dynamic Host Configuration Protocol, or DHCP, enables a DHCP server to dynamically allocate network configurations to computers on an IP network. The primary purpose of this is to reduce the work necessary to administer a large IP network and distributed IP addresses to computers as they are required.

DHCP is a client-server application. When a computer connects to a DHCP server, the server temporarily allocates the computer an IP address. The computer uses this address until the lease expires, at which point it can be replaced with a new IP address.

The main advantage of DHCP is that its addressing scheme is fully dynamic. With a DHCP server running on your network, you can add or move computers around on your network and not have to worry about re-configuring your IP settings.

You can manage HTTPS agents running on DHCP-Client systems. The HPOM solution is not dependent on any specific DHCP or DNS product and is based on the following assumptions:

- System names must not change. The system name can be used as an identifier of a system, even in a manager-of-manager (MoM) environment.
- DHCP and DNS are synchronized.
- There are a relatively small number of IP address changes per day so no IP Address Change Event (IPCE) Storm strategy is necessary. An HP Operations agent sends this event, when it detects an IP address change on one of its network interfaces.
- The Java GUI processes do not automatically update the IP address changes.
- DHCP support of agents is configurable for each agent and server.
- Dynamic IP address changes at runtime, not only at startup.

  The time between two IP address change checks can be configured by setting the `IPADDR_CHECK_INTERVAL` variable on the system.

DHCP Settings in HPOM

Variables for DHCP

The following variables are used to configure the DHCP-specific behavior of the management server processes.

`OPC_DUMMY_IP_RANGE 1.1.1.*`

If the HPOM for UNIX management server detects an IP address conflict while processing an IP change request, the next free IP address out of the `OPC_IP_DUMMY_IP_RANGE` is used. The format of this string is `[1-9*].[1-9*].[1-9*].[1-9*]`. At least one number must be specified. The default is `1.1.1.*`.

`OPC_IPCE_RETRY_NUM 10`

If none of the IP addresses reported by t he system matches those of DNS, the IP address change event is buffered. Each event is processed with a maximum number of retries as specified by the `OPC_IPCE_RETRY_NUM` variable. The default is `10`.

`OPC_IPCE_RETRY_INTERVAL 180`

After the `OPC_IPCE_RETRY_INTERVAL` time period has elapsed, all buffered IP change events are processed again. The default is `180` seconds.

Using opcnode for DHCP

You can use the `opcnode` command to specify the DHCP. To configure the HP Operations management server to accept IP address change events, set `dynamic_ip` to `yes` as follows:

- When adding a new node:

  $ opcnode -add_node node_name=*<node name>* dynamic_ip=yes net_type=*<net_type>* mach_type=*<mach type>* group_name=*<group name>*

- When modifying a system:

  $ opcnode -chg_iptype dynamic_ip=yes -node_name=*<node_name>* | -node_list='*<list>*'

NOTE The network type of all specified nodes must be `NETWORK_IP`. It is not possible to specify another network type with `net_type`.

Enabling Management of Agents on DHCP Clients

Complete the following steps to enable management of HTTPS agents on DHCP Clients:

1. Ensure that DHCP and DNS are synchronized, for example by updating from the DHCP Server. If synchronization is not achieved, the HP Operations management server cannot process any IP address change events and it will decrease the overall performance of the system.
2. Customize `/opt/OV/contrib/OpC/dhcp_postproc.sh`

   Customize the script to suit your environment. The following entries are of particular interest:

   ```
   NETMASK="255.255.248.0" # netmask

   MAXRETRY=5     # number of retries for opctranm

   SLEEP_TIME=10  # sleep this amount of seconds
                  # before the next retry

   TRACE="off"    # on=do (or off=do not) create
                  # lots of tracefiles in /tmp

   NETMON_TOPO_FIX="OFF" #off is highly recommended

   FORCE_NODEINFO_DIST #off
   ```

   You may add `opcmsg` or `opcwall` calls.

10 MoM Environments

Environments with Multiple HP Operations Management Servers (MoM)

For detailed information about the MoM concepts for the HTTPS agent, refer to the chapter titled *Scalable Architecture for Multiple Management Servers* in the *HP Operations Concepts Guide*. Configuration information is available from the *HP Operations Administrator's Reference*.

Message target rules that specify where messages go to and remote access rules that specify which HP Operations server is allowed to do which tasks are configured on the agent. Both message target rules and remote access rules are defined in the responsible manager policy (formally known as the `mgrconf` file). On the HP Operations management server, you must set up the responsible manager policy.

For details, refer to the steps in "Environments Hosting Several Certificate Servers" on page 63 to first establish a trust between the multiple configuration servers.

For more information about multiple configuration servers, refer to "Configuring Multiple Configuration Servers" on page 239.

For an explanation of the roles an HP Operations management server can assume in a MoM environment, see "About Roles" on page 102.

Message Target Rules (OPC_PRIMARY_MGR Setting)

There is a setting called OPC_PRIMARY_MGR in the HTTPS agent namespace eaagt. It specifies the hostname of the HP Operations management server to which HPOM messages are sent by default. This agent setting is modified by HP Operations management servers using the command:

```
opcragt -primmgr
```

If OPC_PRIMARY_MGR is not set or is invalid, the HP Operations management server is denoted by the MANAGER setting. Invalid means that the OPC_PRIMARY_MGR is not specified as a secondary manager nor as an action-allowed manager, nor is it the initial manager. The OPC_PRIMARY_MGR is only a message related setting and it maps to the $OPC_PRIMARY_MGR variable which may be used in message target rules of the responsible manager policy so that messages are sent to that HP Operations management server.

Multiple Parallel Configuration Servers

Multiple parallel configuration servers are supported for HTTPS nodes. The HP Operations policy concept allows multiple HP BTO Software products to independently work with policies on an agent by providing an owner concept for policies. The policy header includes an attribute `owner`, which can be set by the HP Operations management server. This is a logical association using a concept of agreements between management servers to decide which management server is responsible for which configuration (policies) on an agent. Normally all policies associated with an HP Operations management server can be modified by this management server. This means that two different management servers will not interfere when distributing policies to the same agent, because they have a different name.

Let us now understand when multiple parallel configuration servers could used. For example, a service provider manages the hardware and operating systems of a set of customer systems. The customer himself manages an application on the same set of nodes. Both the service provider and the customer each use their own HP Operations management server to manage these systems. The implementation of a solution could be as follows:

- Service provider and customer create their own certificates but agree on a trust, so that the agent accepts action and configuration requests from both HP Operations management servers.
- Service provider and customer agree on a responsible manager policy (`mgrconf` policy). In this case, the service provider acts as the primary manager, and the customer as a competence center. Both HP Operations management servers must be listed in the `mgrconf` policy.
- The competence center is also allowed to deploy configurations. It provides all policies with a specific attribute which can be matched by the message target rules of the responsible manager file. Related messages are then sent to the competence center, all others to the primary manager.

Configuring Multiple Configuration Servers

Multiple configuration servers can be used in two different scenarios:

- **Backup Server**

  Typically in a backup scenario, two HP Operations management servers are configured identically. The main installation is referred to as the primary management server and the other as a backup server.

- **Competence Center**

  In a competence center scenario, the management responsibilities are split between different HP Operations management servers. Typically, the competence center management server is responsible for dedicated applications, such as SAP, and the primary management server is responsible for the rest of the duties.

When policies are deployed to HTTPS agents, they are provided with an owner string. This owner string is fetched from a configuration setting on the management server (`OPC_POLICY_OWNER in the` namespace `opc`). Default value is HPOM : *<server_fully_qualified_name>*).

Primary- and backup management servers should share the same owner string.

In the competence center scenario, normally all parties retain their default owner strings.

When a backup management server is desired, you can overwrite the default owner string by using the following command on the backup management server:

```
ovconfchg -ovrg server -ns opc -set \
OPC_POLICY_OWNER <HPOM:primary_server_fully_qualified_name>
```

NOTE You can also change the `OPC_POLICY_OWNER` string to any desired value but they must be identical on both management servers.

NOTE Be aware that only one owner string can be set per management server. If a manager acts as backup for a certain HPOM domain, but as competence center for another one, this will not work.

NOTE If the backup management server is not setup in exactly the same way as the primary management server, the agent may be configured differently when policies and instrumentations are deployed. Instrumentation files from the primary management server remain, if not overwritten by the backup management server. Additional instrumentation files from the backup management server will be deployed and cumulated on the agent. Policies are only replaced, if the primary and backup management server use the same owner string or if policies are identical. All other policies on the agent will remain unchanged, because they belong to different owners.

mgrconf and nodeinfo Policies in Multiple Configuration Server Environments

`mgrconf` and `nodeinfo` policies are treated as special cases. The rules described in the section “Dealing with Identical Policies Deployed by Different Management Servers” on page 241 are not applicable to these two policies.

For HPOM on UNIX and on Linux, there can only be one instance of either of these policies per manage node. The management server which deploys either of these policies first will permanently remain the owner. The second management server will not overwrite the existing policy. Therefore, it is recommended that in competence center scenarios, only one server is used to deploy `mgrconf` policies.

If it is really necessary to change the owner attribute for `mgrconf` and `nodeinfo` on a managed node, execute the appropriate following commands:

If you are at a management server system, execute the following command:

For nodeinfo:

```
opcdeploy -cmd "ovpolicy -setowner \
HPOM:<your_full_qualified_mgmt_server_name> -poltype \
configsettings" -node <your_managed_node_name>
```

For mgrconf:

```
opcdeploy -cmd "ovpolicy -setowner \
HPOM:<your_full_qualified_mgmt_server_name> -poltype \
mgrconf" -node <your_managed_node_name>
```

If you are at a managed node system, execute the following command:

For `nodeinfo`:

```
ovpolicy -setowner \
HPOM:<your_full_qualified_mgmt_server_name> -poltype \
configsettings
```

For `mgrconf`:

```
ovpolicy -setowner \
HPOM:<your_full_qualified_mgmt_server_name> -poltype \
mgrconf
```

Dealing with Identical Policies Deployed by Different Management Servers

Policies are identified using their Ids and policy name, type and version. If an ID is present, it has a higher priority than a name plus policy type and version.

Identical policies are determined in the following way:

- The same policy ID
- The same policy name, type and version, but different policy ID.

Identical policies can be modified by multiple management servers, independent of the policy owner. This avoids many instances of the same policy being installed on an agent and avoids multiple messages being created for the same issue.

If multiple servers are used to deploy the same configuration data, they are acting as backup management servers, and their data should be synchronized.

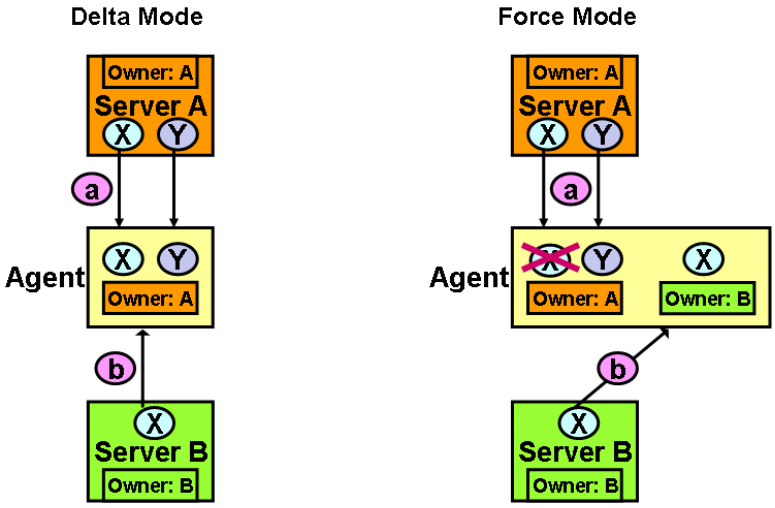
With regards to the owner concept, the following examples show you how the policies are handled between multiple configuration servers.

Let us assume that we have management server A and management server B, policy X and policy Y. Policy X is assigned to the agent from both management server A and management server B. Policy Y is assigned to the same agent only from management server A.

Server A and server B use different owner string. Server A use owner string “A”. Server B use owner string “B”.

1. Trigger configuration distribution.

Figure 10-1 Policy Handling Between Multiple Configuration Servers, Server A Has a Different Owner than Server B.



a. From server A, in delta mode and force mode:

   Policy X and Policy Y are deployed and have owner “A”.

b. From server B, in delta mode:

   Nothing is changed for policy X. Since policy X is already installed, it will remain the same and has owner “A”. Nothing is changed for policy Y. It still has owner “A”.

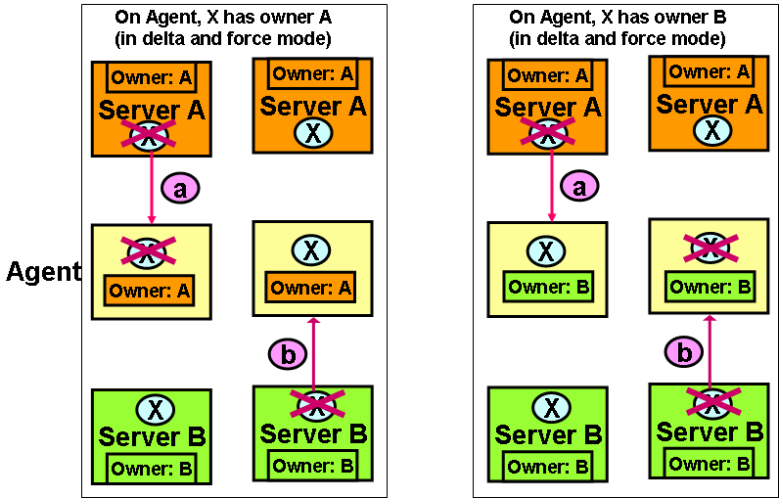
   From server B, in force mode:

   Policy X is overwritten and has owner “B”.

   Nothing is changed for policy Y. It still has owner “A”.

2. De-assign policy X and trigger distribution.

Figure 10-2 Policies Handling Between Multiple Configuration Servers, Server A Has a Different Owner than Server B.



a. If from server A, in delta mode and force mode:

   If policy X has owner “A”, it is removed from the agent.

   If policy X has owner “B”, it remains the same, because of the different owner string.

b. If from server B, in delta mode and force mode:

   If policy X has owner “A”, it remains the same, because of the different owner string.

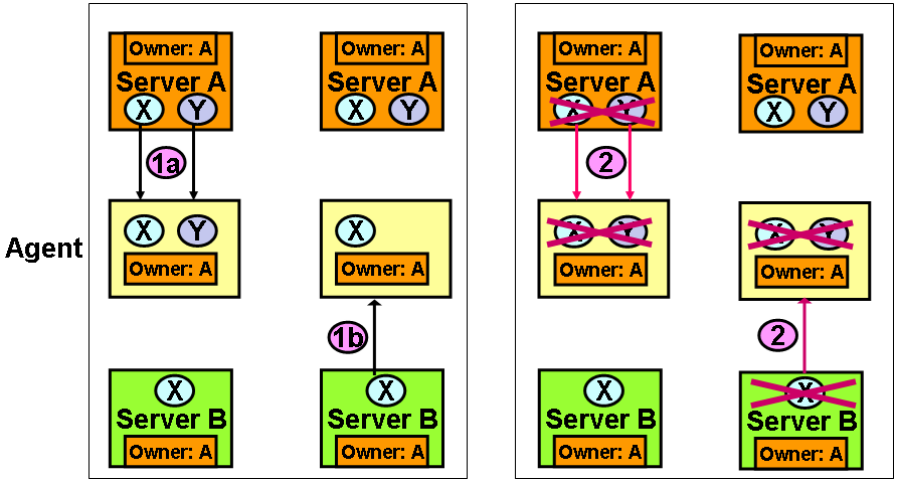
   If policy X has owner “B”, it is removed from the agent.

3. De-assign policy Y from server A, in delta mode and force mode:

   Policy Y is removed.

Server A and server B use same owner string “A”.

Figure 10-3 **Policies Handling Between Multiple Configuration Servers, Same Owner for Servers A and B, and Delta or Force Modes**



1. Trigger configuration distribution.
   a. From server A, in delta mode and force mode:

      Policy X and Policy Y are deployed and has owner “A”.

   b. From server B, in delta mode:

      Nothing is changed for policy X. It still has owner “A”. Policy Y is removed.

      In force mode:

      Policy X is overwritten and still has owner “A”. Policy Y is removed.
2. De-assign policy X and trigger distribution.
   a. If from server A, in delta mode and force mode:

      Policy X is removed.

   b. If from server B, in delta mode and force mode:

      Policy X is removed.

3. De-assign policy Y from server A, in delta mode and force mode:

   Policy Y is removed.

A policy can only be removed by its owner. With regards to policy removal, the following important scenario must be considered:

Let us assume that we have a backup management server scenario. Initially, the primary management server (A) deploys policy (PA) to agent (G). Then policy (PA) has owner (A).

Next, the backup management server (B) deploys the same policy (PA) to the same agent (G). Because the policy is identical, the already installed policy (PA) with owner (A) is removed and re-installed from the backup management server B. Now, the reinstalled policy (PA) has owner (B).

Finally, on the primary management server (A), de-assign policy (PA) and issue policy distribution to the same agent (G).

The result is that policy (PA) is NOT removed from agent (G), because policy (PA) has owner (B). Thus only the backup management server (B) can remove it.

The `delta` and `force` distribution modes are also available for multiple server environments. `force` replaces all policies of the calling owner and all identical policies, even though they are owned by different management servers.

For non-identical policies, in delta and force mode, a de-assigned policy is only removed by the same owner.

How to List and Modify Policy Owners on the Agent

The local policy utility `ovpolicy` can modify all policies on a system by default. Specify the `-owner` option to select policies belonging to a specific owner.

To list all policies of any owner, use the command:

`ovpolicy -l`

For example, to only list the policies for `my_srv`, use the command:

`ovpolicy -l -owner HPOM:<my_srv_full_qualified_name>`

`ovpolicy` can also be used to modify owner strings of policies, for example, if the owner string of an HP Operations management server must be changed without the need to redeploy the configuration for a managed node. For details, refer to the `ovpolicy` man page.

Cleaning-up the Agent

To remove and re-deploy all policies from all HP Operations applications from HTTPS nodes, use the command:

```
opcragt -distrib -purge -templates <nodename>
```

Instrumentation deployment is cumulative. Neither the `delta` nor the `force` installation removes any file on the agent, but only updates existing configurations and adds new ones.

If you want to cleanup and re-install all configuration data in the instrumentation directory on the agent, use the command:

```
opcragt -distrib -purge -actions -monitors -commands \
<nodenames>
```

11 Variables in HPOM

Setting Variables in HPOM

To set variables on the HP Operations management server:

1. Enter the command:

   ```
   /opt/OV/bin/ovconfchg -ovrg server -ns opc -set \
   <var_name> <value>
   ```

2. Restart server processes.

All relevant variables that were available in the `opcsvinfo` files are also used by HPOM.

The HPOM schema uses namespaces (the parameter `-ns` from the example above). All former `opcsvinfo` variables now have the namespace `opc`, all former `opcinfo/nodeinfo` variables on HTTPS nodes have the namespace `eaagt`.

You can suffix the namespace by the process name if required. For example, to set the maximum number of simultaneous connections to `opcuihttps`, enter the following command:

```
ovconfchg -ovrg server -ns opc.opcuihttps -set \
MAX_CONNECTIONS 200
```

To set a variable on a managed node, use `ovconfchg` without the `-ovrg server` option.

```
/opt/OV/bin/ovconfget [ <namespace> [ <var_name> ] ]
```

Reading Variables

To read the variables on the HP Operations management server, enter the command:

```
/opt/OV/bin/ovconfget -ovrg server \
[ <namespace> [ <var_name> ] ]
```

This either prints all settings, all settings of a namespace, or one variable.

To read variables on a managed node, use the `ovconfget` command, but without the `-ovrg server` option.

Customizing XPL config Variables Locally

HTTPS agent provides the possibility to customize threshold policy locally on the node. The use of threshold parameters allows to deploy the same policy on all agents and to overwrite the thresholds of the policy system specific using XPL config parameters locally.

It is now possible to have one policy that contains the default thresholds that are used on most systems. To change the thresholds for some specific systems it is no longer necessary to copy and change the threshold policy. You just need to update XPL config policies with the changed thresholds on the agent system. The concept can be used also on older measurement threshold policies without the need to modify them.

It is possible to set the thresholds direct in XPL config on the agent system by using the XPL config command `ovconfchg`. For information on this command, see the *ovconfchg(1)* man page.

Before checking a measurement threshold the monitor agent now first checks whether overwrite of a threshold is defined in XPL config. If no overwrite is defined, the threshold defined in the measurement threshold policy is used. If the threshold is defined in XPL config, the monitor agent uses this threshold.

To enable the threshold overwrite for threshold policies it is necessary to set a XPL config variable `OPC_OPCMON_OVERRIDE_THRESHOLD` to `TRUE` on the agent system. If this variable is not set the monitor agent ignores all thresholds defined in XPL config.

After the threshold overwrite is enabled on a node, the monitor agent checks always before evaluating a threshold condition, whether the XPL config namespace `eaagt.thresholds` contains a threshold for the policy and condition. The XPL config variable has the following syntax:

<name>=<policy name>/<condition description>/<threshold value>:<reset value>

`name` Specify the variable name, it has to follow the syntax of XPL config variables and to be unique on the system.

`policy name` Specify the policy name you want to customize.

`conditions description` Specify the condition you want to customize.

`threshold value` Specify the threshold value you want to use on this system.

`reset value` Specify the reset value. Even if the reset value is the same as the threshold value, it is necessary to define it.

For example:

```
DiskUsage_1=DiskUsage/Critical Threshold/5:10
```

NOTE The predefined file handles `STDIN`, `STDOUT`, and `STDERR` are not available for Perl scripts in scheduled task and measurement threshold policies. It is also not possible to open file handles that use command pipes or capture the standard output from commands within backticks (`).

Pattern Matching for Variables

HPOM enables you to test a string or variable against a pattern, and define an output string that is conditional on the result. You can do this using `$MATCH` operator. Whenever an HTTPS agent processes a policy, the agent evaluates any `$MATCH` expressions that the policy contains. Use the following syntax:

```
$MATCH(string, pattern, true[, false])
```

Specify the parameters as follows:

`string` Specify a literal string (for example, `TEST STRING`) or an HPOM variable (for example `<$LOGPATH>`).

`pattern` Specify a pattern, using HPOM pattern matching syntax. You can create user-defined variables in the pattern to use in the parameters `true` and `false`. The pattern is case-sensitive.

`true` Specify a string to return if the string and pattern match. You can specify a literal string, a user-defined variable, or an HPOM variable.

`false` Optional. Specify a string to return if the string and pattern do not match. You can specify a literal string, a user-defined variable, or an HPOM variable.

Separate each parameter with a comma (,). To specify a comma within a parameter, you must precede it with two backslashes (\\).

You can use $MATCH within your policies in the following message attributes:

- Service Name
- Message Type
- Message Group
- Application
- Object
- Message Text
- Automatic Command
- Custom message attribute (CMA)

NOTE You can use $MATCH only once in each message attribute. You cannot use $MATCH recursively.

A logfile entry policy can monitor a number of log files. The path name is available in the HPOM variable <$LOGPATH>. If part of the log file path corresponds to an application name, you can use $MATCH to set the application message attribute as follows:

```
$MATCH(<$LOGPATH>,<@.application>.log, <application>,
Unknown)
```

NOTE The predefined file handles STDIN, STDOUT, and STDERR are not available for Perl scripts in scheduled task and measurement threshold policies. It is also not possible to open file handles that use command pipes or capture the standard output from commands within backticks (`).

Deleting Variables

You can delete variables with the ovconfchg -clear option.

```
/opt/OV/bin/ovconfget -clear [ <namespace> [ <var_name> ] ]
```

Example for Configuration Settings

You can find more documentation and examples about configuration settings under:

```
/opt/OV/misc/xpl/config/defaults/*.ini
```

12 Agent Message Stream Interface

Enabling the Agent MSI

The agent-based message stream interface (MSI) enables external applications to read and change incoming messages on the managed node before they are sent to the management server. This can help to reduce the amount of network traffic considerably. A typical external application might be an event correlation engine, for example HP Event Correlation Services.

If you develop your own MSI applications using the APIs provided, you must install the applications on the managed node. You must then enable the agent MSI on the managed node and specify for each policy that generates a message whether the agent should divert or copy the message to the MSI. Otherwise, the message bypasses the MSI.

NOTE The agent MSI supports C APIs only. For more information about the APIs, see the documentation provided with the HPOM Developer's Toolkit.

To enable the agent MSI, use the `ovconfchg` command-line tool on the node:

```
ovconfchg -ns eaagt OPC_AGTMSI_ENABLE TRUE
```

Table 12-1 contains a list of parameters that configure the agent MSI.

Table 12-1 Agent MSI Configuration Parameters

Parameter	Default Value	Description
OPC_AGTMSI_ENABLE	FALSE	Enables the agent MSI.
OPC_AGTMSI_ALLOW_AA	FALSE	Allows automatic commands in messages. If set to FALSE, the agent discards the commands in the messages.
OPC_AGTMSI_ALLOW_OA	FALSE	Allows operator initiated commands in messages. If set to FALSE, the agent discards the commands in the messages.

Table 12-1 Agent MSI Configuration Parameters (Continued)

Parameter	Default Value	Description
OPC_MSI_CREATE_NEW_MSGID	2	Determines how message IDs are created when messages are sent to the agent MSI. 1 = Create a new message ID each time a message attribute is changed or the API copy-operator is called. 2 = Do not create a new message ID when message attributes change if this message was diverted and sent to only one instance. If you apply the API copy-operator to a message, the copy is no longer diverted and later attribute changes lead to a new message ID. For changed messages, the attribute OPCDATA_ORIGMSGID contains the original message ID (otherwise it contains a null ID). 3 = Same as 2, except that the API copy-operator immediately creates a new message ID for the copy. 4 = Do not modify message IDs. The API-user is responsible for modifying the message IDs.

Specifying the Order of Access to the Agent MSI

You can control the order in which application instances can read and change the stream of incoming messages. An application instance with a lower order number is able to read, change, and delete messages before an application instance with a higher order number.

To specify the order in which application instances access the message stream, create a text file called `msiconf` on the managed node. List all registered MSI application instances in this file and assign an appropriate order number to each application instance. Registered MSI applications that are not listed in the `msiconf` file are given an order number of zero (0).

1. On the managed node, create a text file that specifies each application instance and the corresponding order number:

   <application_instance> <order_number>

   <application_instance> corresponds to the name of the MSI application registered with the HP Operations agent. The instance name can contain up to 13 alphanumeric characters.

   <order_number> specifies the order in which the registered MSI application receives a message from the HP Operations agent (lowest to highest). Specify an order number in the range -127 to 127.

   Use new lines to separate application instances, and use spaces or tabs to separate application instances from order numbers.

   If multiple application instances have the same order number, the management server forwards messages to all the application instances at the same time.

CAUTION

Forwarding messages to multiple application instances at the same time can have undesirable results with diverted messages, because there will be two messages in the message stream with the same message ID.

The same problem can also occur with messages that are copied to the MSI, if at least two application instances receive the same message in parallel and do not modify it.

2. *Optional.* Add comments on lines that begin with the number sign (#).
3. Save the file in the following directory on the managed node:
   - On nodes with a Windows operating system:

     `%OvDataDir%\conf\OpC\msiconf`
   - On nodes with a UNIX or Linux operating system:

     `/var/opt/OV/conf/OpC/msiconf`

The HP Operations agent reads the `msiconf` file whenever an MSI instance opens or closes a connection to the agent MSI.

msiconf Example

```
counter -10
evtcorr   0
proca    10
procb    10
enhtt    20
```

A Troubleshooting HTTPS Agents

Troubleshooting HTTPS-based Communication

If communication between an HP Operations management server and an HTTPS agent appears to be interrupted, for example, messages do not arrive at the Message Browser, or software or instrumentation is not distributed, execute the appropriate troubleshooting steps as described in the following sections.

Before you continue with the described actions, you should be familiar with the new HTTPS agent and the underlying communication concepts such as certificates.

This guideline describes possible actions to identify and solve HTTPS communication problems between HP Operations management servers, Certificate Authority Servers and managed nodes.

It is assumed, that the HPOM agent software is installed, but there is a problem in the communication between HP Operations managed nodes and HP Operations management servers in one or both directions.

In most installations, the HP Operations management server and Certificate Authority servers are installed on the same system.

Troubleshooting problems encountered with the communication between an HP Operations management server and an HTTPS agent is split into the following areas:

- Troubleshooting Tools
- Logging
- Troubleshooting Processes

Troubleshooting Tools

Ping an HTTPS-Based Application

HTTPS-based applications can be pinged to test if the application is active and responding. A ping may be executed against an application whether or not it has SSL enabled.

The `bbcutil` utility supports a `-ping` command line parameter that can be used to ping an HP Operations HTTPS-based application.

Use the following command to ping a specified HTTPS-based application:

From an HP Operations managed node:

```
<OvInstallDir>/bin/bbcutil -ping [<hostname_or_ip_addr>] [count]
```

From an HP Operations management server:

```
<OvInstallDir>/bin/bbcutil -ovrg server -ping \
[<hostname_or_ip_addr>] [count]
```

For example:

HTTP `bbcutil -ovrg server -ping http://...`

HTTPS `bbcutil -ovrg server -ping https://...`

Checks whether the communication service on the managed node specified by *<hostname_or_ip_addr>* is alive. If the hostname or IP address is omitted, localhost is assumed. An optional loop count can be specified after the hostname or IP address which causes the ping command to be repeated by the number of times specified.

See the `bbcutil` man page for details of the command line parameters.

In general, all `bbcutil` calls from an HP Operations management server to a managed node should include the `-ovrg server` parameter. for example:

```
bbcutil -ovrg server -ping https://...
```

If the HP Operations management server is a stand-alone system, the `-ovrg server` parameter maybe omitted. However, if the HP Operations management server is installed on an HA cluster, the `-ovrg server` parameter is required because a managed node certificate and a server

certificate including two OvCoreIds are installed on each HP Operations management server. While on stand-alone systems, the managed node certificate and server certificate, including the OvCoreIds, are identical, they differ on cluster installations. The agent is only aware of the management server OvCoreId. It is not aware of the OvCoreId value of the management server.

Display the Current Status of an HTTPS-Based Application

An HTTPS-based application at a specified location can be requested to display its current status.

Use the following command to query a specified application:

bbcutil -status *<hostname_or_ip_addr:port>*

Queries the communication server located at the hostname and port specified by *<hostname_or_ip_addr:port>* for details about the current state of the server.

See the bbcutil man page for details of the command line parameters. If a port is not specified, the port number of the Communication Broker is used.

Display All Applications Registered to a Communication Broker

The Communication Broker at a specified location can be requested to display all applications that are registered to it.

Use the following command to list all applications that are registered to the specified Communication Broker:

bbcutil -registrations|-reg *<hostname_or_ip_addr>*

Queries a Communication Broker on the managed node specified by *<hostname_or_ip_addr>* and displays a list of all registered applications. If the hostname or IP is omitted, localhost is assumed.

See the bbcutil man page for details of the Communication Broker command line parameters.

Use What String

All executables contain a detailed UNIX-style `what` string that can be used to determine the precise version of the HTTPS-based communication software installed. Microsoft Windows executables also contain standard property strings.

List All Installed HP BTO Software Filesets on an HTTPS Managed Node

The `ovdeploy` tool can be used to list the installed HP BTO Software products and components. The following three levels of information can be displayed:

- Basic inventory
- Detailed inventory
- Native inventory

The following sections illustrate how to list the inventory and show examples of the output.

Basic Inventory

To display basic inventory information, enter the following command:

From a managed node:

`ovdeploy -inv -host <hostname>`

From an HP Operations management server:

`ovdeploy -ovrg server -inv -host <hostname>`

For example:

```
ovdeploy -ovrg server -inv -host hp_System_002

NAME                                          VERSION    TYPE
ARCHITECTURE
HP OpenView HTTP Communication                05.00.070  package
Windows 4.0 5.0 5.1 5.2
HP OpenView Deployment                        02.00.070  package
Windows 4.0 5.0 5.1 5.2
HP OpenView Security Certificate Management   01.00.070  package
Windows 4.0 5.0 5.1 5.2
```

```
HP OpenView Security Core                    02.00.070  package
Windows 4.0 5.0 5.1 5.2
...
```

Detailed Inventory

To display detailed inventory information, enter the following command:

From a managed node:

ovdeploy -inv -all -host *<hostname>*

From an HP Operations management server:

ovdeploy -ovrg server -inv -all -host *<hostname>*

For example:

```
ovdeploy -ovrg server -inv -all -host hp_System_002
```

```
<?xml version='1.0' encoding='UTF-8' standalone='yes'?> <inventory
    xmlns=">http://openview.hp.com/xmlns/depl/2003/inventory">
  <host>hpspi002.bbn.hp.com</host>
  <date>Thursday, October 30, 2003 12:24:48 PM</date>
  <package>
    <name>HP OpenView HTTP Communication</name>
    <version>05.00.070</version>
    <systemtype>IA32</systemtype>
    <ostype>Windows</ostype>
    <osvendor>MS</osvendor>
    <osversion>4.0 5.0 5.1 5.2</osversion>
    <osbits>32</osbits>
    <nativeinstallertype>msi</nativeinstallertype>
  </package>
  <package>
    <name>HP OpenView Deployment</name>
    <version>02.00.070</version>
    <systemtype>IA32</systemtype>
...
```

Native Inventory

To display native inventory information, enter the following command:

From a managed node:

ovdeploy -inv -it native -host *<hostname>*

From an HP Operations management server:

ovdeploy -ovrg server -inv -it native -host *<hostname>*

For example:

```
ovdeploy -ovrg server -inv -it native -host hp_System_002

NAME                                          VERSION
WebFldrs XP                                   9.50.5318
HP OpenView Core Library                      2.50.70
HP OpenView Certificate Management Client     1.0.70
HP OpenView HTTP Communication                5.0.70
ActivePerl 5.6.1 Build 633                    5.6.633
HP OpenView Deployment                        2.0.70
Microsoft FrontPage Client - English          7.00.9209
```

Standard TCP/IP Tools

If SSL is not enabled, standard TCP/IP tools such as telnet can be used to contact HTTPS-based application. To use telnet to ping an HTTPS-based application execute the following commands:

Two carriage returns are required after the `PING` input line to telnet.

To end the telnet session, enter **`control-D`** and **Return**:

```
telnet <host> <port>
PING /Hewlett-Packard/OpenView/BBC/ping HTTP/1.1
```

The output takes the following form:

```
HTTP/1.1 200 OK
content-length: 0
content-type: text/html
date: Thu, 08 Aug 2008 08:20:24 GMT
senderid: fd7dc9c4-4626-74ff-9e5a09bffbae
server: BBC X.05.00.01.00; ovbbccb 05.00.100
```

`HTTP status 200 OK` indicates the HTTPS-based application has recognized the request and successfully responded. Other status may indicate a failure in the request or other error.

For a list of error codes, refer to :

`http://www.w3.org/Protocols/rfc2616/rfc2616.html`

RPC Calls Take Too Long

If an RPC call takes longer than the default timeout of 5 minutes, the following error messages may be displayed, for example, for a policy installation:

```
ERROR:   General I/O exception while connecting to host '<hostname>'.
           (xpl-117) Timeout occurred while waiting for data.
```

or

```
ERROR:  The Configuration server is not running on host '<hostname>'.
Check
        if the Configuration server is in state running.
        (bbc-71) There is no server process active for address:
        https://<hostname>/com.hp.ov.conf.core/bbcrpcserver
```

This may happen if 1000 policies are installed using the `PolicyPackage` interface from `OvConf` or if the connection or target-machine is slow.

To prevent this the communication timeout (response timeout) can be changed using the following commands with the required time out value:

On the target system:

`ovconfchg -ns bbc.cb -set RESPONSE_TIMEOUT <seconds>`

On the HP Operations management server:

`ovconfchg -ovrg server -ns bbc.http.ext.conf -set \`
`RESPONSE_TIMEOUT <seconds>`

NOTE The `RESPONSE_TIMEOUT` parameter must be set on both managed nodes.

A similar situation can arise when running any command that takes over 5 minutes to complete. The timeouts should be extended as follows.

On the managed node enter the commands:

NOTE The unit is milliseconds in the second case.

`ovconfchg -ns bbc.cb -set RESPONSE_TIMEOUT <seconds>`

`ovconfchg -ns depl -set CMD_TIMEOUT <milliseconds>`

On the HP Operations management server, enter the command:

```
ovconfchg -ovrg server -ns bbc.http.ext.depl -set \
RESPONSE_TIMEOUT <seconds>
```

Logging

Errors in violation of security rules are recorded in a logfile. For HTTPS-based servers, all client access can be additionally logged, if enabled.

To enable logging of all client access, set the following parameter value using the command:

```
ovconfchg -ns bbc.cb -set LOG_SERVER_ACCESS true
```

This will log all access to the Communication Broker. To view the logs, open on of the following files:

***<OvDataDir>*/log/System.txt** (ASCII)

***<OvDataDir>*/log/System.bin** (Binary)

You can additionally log access to all HP Communication Broker servers using the command:

```
ovconfchg -ns bbc.http -set LOG_SERVER_ACCESS true
```

You can additionally log all client access to the configuration and deployment application using the command:

```
ovconfchg -ns bbc.http.ext.conf -set LOG_SERVER_ACCESS true
```

Communication Problems Between Management Server and HTTPS Agents

The most likely areas where communication problems may be experienced are divided into the following sections:

Network Troubleshooting Basics

Basic network troubleshooting uses the following commands:

`ping`	**`<SYSTEMPATH>/ping`**
`nslookup`	**`<SYSTEMPATH>/nslookup`**
`telnet`	**`<SYSTEMPATH>/telnet`**
`ovgethostbyname`	**`<INSTALLDIR>/bin/ovgethostbyname`** (for use on Solaris systems only in place of `nslookup`)

NOTE

The actions described below may not work if communication between an HP Operations management server or Certificate Authority server and HP Operations managed node has to pass:

- Firewalls
- NATs
- HTTP Proxies

Contact your Network Administrator for more information.

To check for basic network problems, complete the following steps:

1. Check if the name resolution for the HP Operations management server, Certificate Authority server and HP Operations managed node is consistent on all affected systems.

   Use `ping`, and `nslookup` (on Solaris: `ovgethostbyname`) with the Fully Qualified Domain Name (FQDN) on all systems with all systems as targets.

   `bbcutil -gettarget <nodename>`

2. Check if all systems (HP Operations management server, Certificate Authority server and managed node) are accessible.

   Use one of the following commands:

   - **`<OvInstallDir>/bin/bbcutil -ping <FQDN>`**
   - **`telnet <FQDN>`**

3. Check if HTTP communication is working by using a Web browser to connect to the Communication Broker. The Communication Broker, `ovbbccb`, must be running for this check.

   To retrieve the assigned *<AGENT-BBC-PORT>* value, enter the command:

   `bbcutil -getcbport <agenthostname>`

   For example, if you enter the command:

   ```
   bbcutil -getcbport mysystem.mycom.com
   ```

   Output of the following form is displayed:

   ```
   mysystem.mycom.com:8008
   ```

   On the HP Operations management server system, open a Web browser and enter the following URL:

   `http://<HPOM managed node>:<AGENT-BBC-PORT>/ \`
   `Hewlett-Packard/OpenView/BBC/`

   The default port number for *<AGENT-BBC-PORT>* is 383.

   Repeat this step from the managed node to the HP Operations management server:

   `http://<HPOM management server>:<AGENT-BBC-PORT>/ \`
   `Hewlett-Packard/OpenView/BBC/`

The `HP OpenView BBC Information Modules` page should appear and allow you to check `ping` and `status` or list registered services and HPOM resource groups (ovrg).

HTTP Communication Troubleshooting Basics

Basic HTTP communication troubleshooting uses the following commands:

`ovc`	**<*INSTALLDIR*>/bin/ovc**
`ovconfget`	**<*INSTALLDIR*>/bin/ovconfget**
`ovbbccb`	**<*INSTALLDIR*>/bin/ovbbcutil**
`ps`	**<*SYSTEMPATH*>/ps**

NOTE Even if the communication between HP Operations management server or Certificate Authority server and managed node has to pass:

- Firewalls
- NATs
- HTTP Proxies

the following actions must work! If they do not, contact your Network Administrator for more information.

NOTE If the communication between HP Operations management server or Certificate Authority server and managed node is not allowed to pass through the firewalls, one or more HTTP Proxies must be used (see the corresponding sections).

To check for HTTP communication problems, complete the following steps:

1. On all systems, the HP Operations management server, Certificate Authority server and managed node, check if:

   The HP Communication Broker ovbbccb is running with the following commands:

   ovc -status

   The ovbbccb process must be listed as running. The output takes the following form:

```
ovcd      OV Control                CORE       (2785)  Running
ovbbccb   OV Communication Broker    CORE       (2786)  Running
ovconfd   OV Config and Deploy       CORE       (2787)  Running
ovcs      OV Certificate Server      SERVER     (3024)  Running
coda      OV Performance Core        AGENT      (2798)  Running
opcmsga   OMU Message Agent          AGENT,EA   (2799)  Running
opcacta   OMU Action Agent           AGENT,EA   (2800)  Running
opcmsgi   OMU Message Interceptor    AGENT,EA   (2801)  Running
opcle     OMU Logfile Encapsulator   AGENT,EA   (2805)  Running
opcmona   OMU Monitor Agent          AGENT,EA   (2806)  Running
opctrapi  OMU SNMP Trap Interceptor  AGENT,EA   (2810)  Running
```

   ps *<OPT>* | grep ovbbccb

   ovbbccb must be listed.

   ***<OvInstallDir>*/bin/bbcutil -status**

   Status of ovbbccb must be ok.

NOTE

Make a note of the ports listed using the command:

bbcutil -getcbport *<hostname>*

- on managed node as *<AGENT-PORT>*
- on management server as *<MGMT-SRV-PORT>*
- on Certificate Authority server as *<CA-SRV-PORT>*

Alternatively, you can use the command:

ovconfget bbc.cb.ports PORTS

You can start the Communication Broker with the command:

ovc -start

No error messages should be displayed.

If the ovbbccb process is not running:

a. Check the logfile for error messages in the appropriate file:

<*OvDataDir*>/log/System.txt (ASCII)

<*OvDataDir*>/log/System.bin (Binary)

b. Start the Communication Broker with the command:

<*OvInstallDir*>/bin/bbcutil -nodaemon -verbose

If there is any problem, errors are displayed in detail at startup. The port number it uses is also displayed on startup.

c. For more detailed output use the command:

```
OVBBC_TRACE=true <OvInstallDir>/bin/ \
bbcutil -nodaemon -verbose
```

This displays a very significant amount of detailed information. This detail can also be obtained using HPOM tracing.

2. Check the configuration of the Communication Broker port settings with the following commands:

a. Lists all Communication Broker ports:

bbcutil -getcbport *<hostname>*

b. Check if the default `DOMAIN` parameter is correctly set for the managed nodes using the command:

ovconfget bbc.http DOMAIN

This should be set to the default domain, for example, `myco.com`. This parameter may be used to find a match for the parameters configured in step 2.a above.

c. Check if a process has the Communication Broker port open and is listening for connections using the command:

netstat -an | grep \.383

You should see something similar to (varies on each platform):

```
tcp        0      0  *.383          *.*          LISTEN
```

`LISTEN` verifies that a process is listening on the specified port. If this is displayed and the Communication Broker is not running, another process is using the port and the Communication Broker will not startup. This can be verified with steps 1.a and 1.b.

3. Check the HTTP Communication capabilities by entering the following commands.

On the HP Operations management server and the Certificate Authority server:

**<*OvInstallDir*>/bin/bbcutil -ovrg server -ping **
http://<HPOM managed node>[:<*AGENT-PORT*>]/

On the managed node:

**<*OvInstallDir*>/bin/bbcutil -ping **
http://HPOM management server[:<*MGMT-SRV-PORT*>]/

**<*OvInstallDir*>/bin/bbcutil -ping **
http://Certificate Authority server[:<*CA-SRV-PORT*>]/

NOTE If no port is specified in these command, the default port 383 is used.

Each call should report:

`status=eServiceOK`

4. Check if the managed nodes have the correct Communication Broker port configuration. Do *not* specify a port number in the URI. OV communication *must* be able to resolve the Communication Broker port number on its own. If the ping works with the port number, but does not work without the port number, the local managed node is not correctly configured. Go back to step 2.
5. Check if the HTTP Proxy is correctly configured using the command:

   bbcutil -gettarget <*nodename*>

   For example, if you enter the command:

   ```
   bbcutil -gettarget mysystem.mycom.com
   ```

   Output of the following form is displayed:

   ```
   Node: mysystem.mycom.com:8008 (14.133.123.10)
   ```

   If a proxy is configured, it will be displayed.

   For example, if you enter the command:

   ```
   bbcutil -gettarget www.mycom.com
   ```

   Output of the following form is displayed:

   ```
   HTTP Proxy: web-proxy:8008 (14.193.1.10)
   ```

   ovconfget bbc.http PROXY

   Although not recommended, applications may set their own private PROXY setting. The above setting is valid for the whole managed node. An individual application may override this value in its own private namespace:

   ovconfget bbc.http.ext.<*comp id*>.<*appname*>

   If the <*comp id*> or <*appname*> is not known, check using `ovconfget` the entire configuration for all proxy settings in the namespaces starting with:

   bbc.http.ext
6. Check on the HP Operations management server and the Certificate Authority server systems that the proxy is working and supports the `CONNECT` command.

NOTE

The blank lines are important.

On some platforms, it may not be possible to echo commands typed into telnet.

Enter the command:

telnet *<proxy>* *<proxy port>*
CONNECT *<AGENT>*:*<AGENT PORT>* HTTP/1.0

PING /Hewlett-Packard/OpenView/BBC/ HTTP/1.0

To exit telnet, enter **Control-D**

The output should be similar to the following. If the Communication Broker is up and running on the target managed node, the HTTP status should be `200 OK`.

```
HTTP/1.1 200 OK
cache-control: no-cache
content-type: text/html
date: Fri, 06 Feb 2004 15:15:02 GMT
senderid: fd7dc9e4-4626-74ff-084a-9e5a09bffbae
server: BBC 05.00.101; ovbbccb 05.00.101HP OpenView BBC
Information Modules:

    Node:         ping.bbn.hp.com
    Application:  ovbbccb
    Version:      05.00.101
    Modules:      ping
                  status
                  services
                  ovrg

Connection closed by foreign host.
```

7. Check on the HP Operations managed node that the proxy is working and supports the CONNECT command.

NOTE

The blank lines are required.

On some platforms, it may not be possible to echo commands typed into telnet.

Enter the command:

```
telnet <proxy> <proxy port>
CONNECT <MGMT-SRV>:<MGMT-SRV PORT> HTTP/1.0

PING /Hewlett-Packard/OpenView/BBC/ HTTP/1.0
```

or

```
telnet <proxy> <proxy port>
CONNECT <CA-SRV>:<CA-SRV PORT> HTTP/1.0

PING /Hewlett-Packard/OpenView/BBC/ HTTP/1.0
```

To exit telnet, enter **Control-D**

See the previous point for a sample output.

8. Enable logging for HTTP access to the Communication Broker.

   ```
   ovconfchg -ns bbc.cb -set LOG_SERVER_ACCESS true
   ```

   This will log all access to the Communication Broker. To see the logs use:

   ```
   ovlogdump <OvDataDir>/log/System.txt
   ```

   You can additionally log access to all HP Operations servers using:

   ```
   ovconfchg -ns bbc.http -set LOG_SERVER_ACCESS true
   ```

Authentication and Certificates Troubleshooting for HTTP Communication

Troubleshooting Basic HTTP communication uses the following commands:

ovc	**<INSTALLDIR>/bin/ovc**
ovconfget	**<INSTALLDIR>/bin/ovconfget**

ovconfchg	**<*INSTALLDIR*>/bin/ovconfchg**
ovcoreid	**<*INSTALLDIR*>/bin/ovcoreid**
ovcert	**<*INSTALLDIR*>/bin/ovcert**
bbcutil	**<*INSTALLDIR*>/bin/bbcutil**

To check for authorization and certificate related HTTP communication problems, complete the following steps:

1. Check the OvCoreID of each system.

   On the HP Operations management server or the Certificate Authority server, enter the command:

   ovcoreid -ovreg server

   On the managed node, enter the command

   ovcoreid

   Make a note of each of the displayed OvCoreID values:

   - *<MGMT-SRV-COREID>*
   - *<CA-SRV-COREID>*
   - *<AGENT-COREID>*

2. Check the certificates on the HP Operations management server or Certificate Authority server and on managed node using the following command:

   ovcert -list

NOTE

There are 3 certificates on the HP Operations management server system or Certificate Authority system:

- HP Operations management server certificate
- Certificate authority certificate
- Managed node certificate

When an HP Operations management server is installed on a cluster (high availability environment), the certificates of the HP Operations management server and the agent on the management server are not the same. On non-cluster installations, the certificates must be identical.

On each system there must be at least following Certificates.

On the managed node:

```
| Certificates:                                    |
|     <AGENT-COREID>                  (*)          |
```

On the management server or the Certificate Authority server:

```
| Certificates:                                    |
|     <MGMT-SRV-COREID>|<CA-SRV-COREID>    (*)     |
```

On all systems:

```
| Trusted Certificates:                            |
|     <CA-SRV-COREID>                              |
```

NOTE

The `(*)` signifies that the private key for the certificate is available.

If one of the certificates is missing, refer to Chapter 6, “Working with Certificates,” on page 151 and generate the required certificates.

To get more detailed info about the installed certificates, use the following commands:

On the managed node:

ovcert -check

On the management server:

ovcert -check -ovrg server

An example of the output is shown below:

```
OvCoreId set                        : OK
Private key installed               : OK
Certificate installed               : OK
Certificate valid                   : OK
Trusted certificates installed      : OK

Check succeeded.
```

To check that the installed certificates are valid, use the following command and make sure that the current date is between the `valid from` and `valid to` dates of the installed certificates:

ovcert -certinfo *<CertificateID>*

NOTE

The CertificateID of a trusted certificates is the OvCoreID of the certificate server prefixed with a `CA_`.

An example of the output is shown below:

```
# ovcert -certinfo 071ba862-3e0d-74ff-0be4-b6e57d0058f2

Type        :  X509Certificate
Subject CN  :  071ba862-3e0d-74ff-0be4-b6e57d0058f2
Subject DN  :  L:  alien2.ext.bbn.com
               O:  Hewlett-Packard
               OU: OpenView
               CN: 071ba862-3e0d-74ff-0be4-b6e57d0058f2

Issuer CN   :  CA_99300c4e-f399-74fd-0b3d-8938de9900e4
Issuer DN   :  L:  tcbbn054.bbn.hp.com
               O:  Hewlett-Packard
               OU: OpenView
               CN: CA_99300c4e-f399-74fd-0b3d-8938de9900e4
Serial no.  :  04
Valid from  :  01/27/04 12:32:48 GMT
Valid to    :  01/22/24 14:32:48 GMT
Hash (SHA1):   60:72:29:E6:B8:11:7B:6B:9C:82:20:5E:AF:DB:D0: ...
```

NOTE

An HTTPS agent is also installed on an HP Operations management server system.

If calling `ovcert -list` on a management server system, you are given the certificate details of the agent on the management server system as well as the details of the certificate for the management server and the CA.

3. Check the HTTPS communication capabilities using the following commands.

NOTE

The following actions must work even if communication between an HP Operations management server or a Certificate Authority server and an managed node has to pass:

- Firewalls
- NATs
- HTTP Proxies

If they do not, contact your Network Administrator for more information.

NOTE

If the communication between HP Operations management server or Certificate Authority server and HP Operations managed node is not allowed to pass through the firewalls, one or more HTTP Proxies must be used (see the corresponding sections).

On an HP Operations management server or Certificate Authority server:

```
<OvInstallDir>/bin/bbcutil -ovrg server -ping \
https://<HPOM managed node name>[:<AGENT-PORT>]/
```

On a managed node:

```
<OvInstallDir>/bin/bbcutil -ping \
https://<HPOM management server name>[:<MGMT-SRV-PORT>]/
```

```
<OvInstallDir>/bin/bbcutil -ping \
https://Certificate Authority server[:<CA-SRV-PORT>]/
```

Each call should report:

```
status=eServiceOK
```

The reported OvCoreID must match with the OvCoreIDs that you noted in the first step:

```
coreID=<COREID>
```

HPOM Communication Troubleshooting

Troubleshooting HPOM communication uses the following commands:

ovc	**<INSTALLDIR>/bin/ovc**
ovconfget	**<INSTALLDIR>/bin/ovconfget**
ovconfchg	**<INSTALLDIR>/bin/ovconfchg**
ovcoreid	**<INSTALLDIR>/bin/ovcoreid**
ovpolicy	**<INSTALLDIR>/bin/ovpolicy**
ovcs	**<INSTALLDIR>/bin/ovcs**
opcagt	**<INSTALLDIR>/bin/OpC/opcagt**
opcragt	**<INSTALLDIR>/bin/OpC/opcragt**
opccsa	**<INSTALLDIR>/bin/OpC/opccsa**
opcssam	**<INSTALLDIR>/bin/OpC/opccsam**
opcsv	**<INSTALLDIR>/bin/OpC/opcsv**
opcnode	**<INSTALLDIR>/bin/OpC/opcnode**

opc **/usr/bin/OpC/opc**

To check for HPOM communication problems, complete the following steps:

1. HP Operations managed nodes must be in the node bank.
2. The Fully Qualified Domain Name (FQDN) of the HP Operations managed node must match.
3. The communication type of the managed node must be HTTPS.
4. The OvCoreID of the managed node must match.

   Check the value of the managed node OvCoreID stored in the HPOM database using the command:

   opcnode -list_id node_list=*<HPOM managed node>*

   It must match the *<AGENT-COREID>*.

   To check, on the managed node call the command:

   ***<OvInstallDir>*/bin/ovcoreid**

   You can change the managed node OvCoreID from the HP Operations management server using the command:

   **opcnode -chg_id node_name=*<HPOM managed node>* **
   id=*<AGENT-COREID>*

   You can change the OvCoreID on the managed node using the command:

   ovcoreid -set *<NEW-AGENT-COREID>*

NOTE

Changing the OvCoreId of a system is an operation that must be done with great care because it changes the identity of a managed node. All managed node-related data, such as messages, are linked by the OvCoreId of a managed node. Changing the value of the OvCoreID should only be executed by experienced users who know exactly what they want to do and what is being affected by attempting this change, especially on the HP Operations management server.

5. Check, that all HP Operations management server processes are running using the commands:

opcsv -status

All registered processes must be in the state `running`.

ovc -status

All registered core processes must be in state `running`.

6. Make sure that the operator is responsible for the:
   - HP Operations managed node and its node group
   - Message group

   Reload the Message Browser.
7. Check for pending certificate requests.

   On the Certificate Authority server enter the command:

   opccsa -list_pending_cr

   Check if the managed node is listed by nodename, IP address or `OvCoreID` and whether all parameters are consistent.

   Manually grant pending certificate requests with the command:

   opccsa -grant *<NODE>*|*<Certificate_Request_ID>*

   If the parameter are not consistent, change the values on the HP Operations management server and managed node, as required.

   On the HP Operations managed node, stop and restart all processes with the commands:

   ovc -kill

   Verify, that all processes are stopped with the command:

   ps *<OPT>* | grep /opt/OV

   ovc -start

NOTE

To manually trigger a Certificate Request, first check that there is no certificate already installed with the command:

ovcert -status

If no certificate is installed, enter the command:

ovcert -certreq

The ovcd process of the HTTPS agent must be running for the ovcert -certreq call to work. Certificate requests are automatically sent during agent startup, so just the agent startup is sufficient, unless the CERTIFICATE_DEPLOYMENT_TYPE is set to Manual. This is done with the command:

```
ovconfchg -ns sec.cm.client -set \
CERTIFICATE_DEPLOYMENT_TYPE Manual
```

Therefore, the ovcert -certreq command is only of interest if Manual certificate deployment type is chosen, or if the certificate was removed while the agent was running. For example, no ovc -kill command run before removing the certificate.

If a certificate is already installed, the following error message is displayed:

```
ERROR:   (sec.cm.client-125) There is already a valid
certificate for this node installed.
```

8. If there are no managed node messages in the Message Browser on a managed node, execute the following checks:

   - Check if all processes are running:

     ovc -status

     All registered processes must be running and no process should run twice.

   - Check if the expected policies are deployed:

     ovpolicy -list

   - Check the MANAGER, MANAGER_ID, and CERTIFICATE_SERVER settings:

     ovconfget sec.cm.client CERTIFICATE_SERVER

     This must match the Certificate Authority server.

     ovconfget sec.core.auth MANAGER

     This must match the HP Operations management server.

     ovconfget sec.core.auth MANAGER_ID

     This must match the OvCoreID of the HP Operations management server.

To check the OvCoreId of the management server, on the management server enter the command:

```
ovcoreid -ovrg server
ovconfget eaagt OPC_PRIMARY_MGR
```

This setting is optional, but when set, it must match the HP Operations management server.

NOTE If the HP Operations management server is not the primary manager, additional checks have to be performed.

The HP Operations management server must appear with consistent values in the file:

<OvDataDir>/datafiles/policies/mgrconf/*<ID>*_data

- Check the settings of message suppression.
- Check the settings of message buffering.
- Check if the message buffer file is growing:

  ls -l *<OvDataDir>*/tmp/OpC/msgagtdf

  or on HP Operations management server:

  opcragt -status *<nodename>*

- Send a message to be forwarded to the server:

  opcmsg a=appl o=object msg_t=*<my_text>*

- Check if messages appear in the message manager queue file:

  ```
  strings /var/opt/OV/share/tmp/OpC/mgmt_sv/ \
  msgmgrq | grep <my_text>
  ```

9. If DEPLOYMENT, ACTIONS or HBP to a managed node fails, on the managed node, check the status of the agent with the command:

   opcragt -status

   If this reports no problems, the problem is not HTTPS communication dependent.

HTTPS Communication and Time Zones

ovbbccb provides increased security on UNIX operating systems by using a feature known as chroot(). A chroot on UNIX operating systems is an operation which changes the root directory. Whenever the ovbbccb process starts up, it is rooted to *<OvDataDir>* in UNIX. This ensures that it can access files only under *<OvDataDir>*. It cannot access any other files.

For time zone conversions, the system files for time zone are needed, which are located in a now inaccessible directory. ovbbccb cannot access the time zone file and writes the date information in UTC(GMT) format rather than actual time zone set for the system.

To establish the correct time zone, create a similar directory structure under *<OvDataDir>* as is available under . . . /zoneinfo/*<TZ>* and copy the actual time zone file:

1. Stop all the HPOM processes:

   /opt/OV/bin/ovc -kill

2. Check the /etc/TIMEZONE file for the current time zone (TZ value), for example:

   TZ=US/Eastern

3. Create the following directory based on the TZ value.

   mkdir -p *<OvDataDir>*/usr/share/lib/zoneinfo/*<TZ>*

   If the TZ value contains entries separated by a /, as in our example with TZ=US/Eastern, create the directory structure up to the last slash:

   mkdir -p *<OvDataDir>*/usr/share/lib/zoneinfo/US

NOTE

Substitute *<OvDataDir>* with path used by the managed node platform. For details refer to “Generic Directory Structure on a Managed Nodes” on page 33.

For example: *<OvDataDir>* on Solaris is: /var/opt/OV

Make sure that the directory structure under *<OvDataDir>* is exactly same as that of /usr/share/lib/zoneinfo/<TZ>.

4. Copy the timezone resource file to the newly created directory:

   ```
   cp /usr/share/lib/zoneinfo/<TZ> \
   <OvDataDir>/usr/share/lib/zoneinfo/<TZ>
   ```

   On HP-UX systems, also copy the following file:

   usr/lib/tztab

5. Start all the HPOM processes:

   ```
   /opt/OV/bin/ovc -start
   ```

All the messages subsequently logged by `ovbbccb` should have the correct timestamp.

Certificate Deployment Problems

During certificate deployment, the situation may arise that there are two pending certificate requests for the same managed node in the Certificate Server Adapter's list of pending certificate requests.

For example, this can occur if the certificate request is triggered from the managed node. This certificate request is not granted and remains pending in the Certificate Server Adapter's internal list. If you now de-install the agent software and re-install it, another certificate request is triggered. The new request also contains a new `OvCoreID`, because re-installing the managed node generates a new `OvCOreID`. This certificate also remains in the list of pending certificate requests.

The listing of the pending certificate requests also contain a time stamp of when the certificate request was received by the HP Operations management server. It is clear which certificate request is newer and valid. Grant the newest one and remove any older requests.

Alternatively, there are two further ways of removing unwanted certificate requests:

- Log in as an HPOM administrator and remove all certificate requests for a “problematic” managed node and then issue a new certificate request from the managed node with the command:

  `ovcert -certreq`

NOTE

The `ovcd` process of the HTTPS agent must be running for the `ovcert -certreq` call to work. Certificate requests are automatically sent during agent startup, so just the agent startup is sufficient, unless the `CERTIFICATE_DEPLOYMENT_TYPE` is set to `Manual`.

Therefore, the `ovcert -certreq` command is only of interest if `Manual` certificate deployment type is chosen, or if the certificate was removed while the agent was running. For example, no `ovc -kill` command run before removing the certificate.

This results in a single certificate request for the managed node which can then be mapped and granted in the usual way. See Chapter 5, “Working with HTTPS Managed Nodes,” on page 121.

- If as administrator, you cannot execute the `ovcert -certreq` command on the managed node and so cannot issue a new certificate request, then retrieve the valid `OvCoreID` from the managed node by executing the command:

  `<OvInstallDir>/bin/bbcutil -ovrg server -ping <nodename>`

  List all certificate requests and grant the certificate request that contains valid `OvCoreID` and remove any others.

Change the Management Server Responsible for a Managed Node

It is sometimes necessary to change the management server which manages a managed node. In the following steps, we concentrate on the changes required on the managed node. With HTTPS agents, the following topics must be taken into consideration:

1. **Policy Cleanup on the Managed Node**

   If the new server has a different certificate authority than the old one and the new and old server do not have a trust setup, the agent needs a new certificate. This also means that the policies on the agent become unreadable as soon as the agent gets a certificate from the new CA.

   Remove all policies, because they cannot be read anymore, using the command:

   `ovpolicy -remove all`

   If the CAs are the same or a trust exists, then the policies are basically readable, but the `OvCoreId` of the old server, which is contained in the certificates as part of the policy header files, must still be authorized. This is achieved by entering the name of the old management server in the `mgrconf` policy. The following file must exist and the old manager must be mentioned in it:

   <OvDataDir>`/datafiles/policies/mgrconf/*data`

   If this is not the case, enter the command:

   `ovpolicy -remove all`

   An alternative to running the command `ovpolicy -remove all`, you can also remove all files from the following directory:

   <OvDataDir>`/datafiles/policies`

2. **Stop the Agent**

   The agent should be stopped before doing further modifications:

   `ovc -kill`

3. **Certificate Cleanup on the Agent**

   If the new target server shares the same certificate authority as the old one or there is a trust setup between new and old servers, then the certificates can remain as they are. If not, then you must create new certificates.

   Remove the existing ones using the command:

   ovcert -remove *<all_certs_listed_in_ovcert_-list_output>*

4. **Configuration Settings Cleanup**

   Change some basic settings on the agent. The `OvCoreId` can remain unchanged:

   - If the certificate authority has changed, enter the following command to specify the new certificate authority:

     ovconfchg -ns sec.cm.client -set CERTIFICATE_SERVER \ *<new_CA>* (typically the fully qualified hostname)

   - Set the new management server using the following command:

     ovconfchg -ns sec.core.auth -set MANAGER *<new_mgmtsv>* (typically the fully qualified hostname)

   - Obtain the management server `OvCoreId` value with the command:

     ovcoreid -ovrg server

     Set the `OvCoreId` of the new management server on the agent:

     ovconfchg -ns sec.core.auth -set MANAGER_ID \ *<new_manager_core_id>*

   - For MoM environments only, check if the `OPC_PRIMARY_MGR` setting is already set. If it is set, you can clear it or set it to the new management server (both actions have the same effect).

     ovconfchg -ns eaagt -clear OPC_PRIMARY_MGR

5. **Create New Certificates**

   If the old certificates were removed, request new certificates. Restart the agent, and it will make a request for a new certificate (except when the `CERTIFICATE_DEPLOYMENT_TYPE` setting under namespace `sec.cm.client` is set to `Manual`. In this case, perform a manual certificate installation. For further details see “Deploying Manual Certificate with Installation Key” on page 163.

6. **Prepare the Management Server**

   On the new management server proceed in the same way as for adding a new managed node, including granting the certificate request, assigning policies, and deploying configuration. For further details, see “Installing HTTPS Managed Nodes Manually” on page 131.

Certificate Backup and Recovery in HPOM

It is extremely important to be aware of the impacts of loosing a private key or when keys and certificate errors arise. The normal configuration upload and download does not include certificate and key data.

There is a utility on the HP Operations management server to back up and recover certificates plus the associated private keys and OvCoreIds:

`/opt/OV/bin/OpC/opcsvcertbackup/`

This utility has the following options:

- **`-remove`**

  Removes all certificates from an HP Operations management server, including:

  — Certificate Authority root certificate and its private key.

  — Server certificate and its private key.

  — Managed node certificate on the HP Operations management server.

  However, a backup is also created automatically before the removal takes place.

- **`-backup`**

  A tar archive is created at the following default address:

  `/tmp/opcsvcertbackup.<date_time>.tar`

  The *<date_time>* format is `YYMMDD_hhmmss`.

  The default storage location can be changed by using the **`-file`** option.

  The information recorded includes:

  — Certificate Authority root certificate, private key and ID

  — HP Operations management server certificate with key and OvCoreId

  — Managed node certificate with key and `OvCoreId`

  You must secure the data by using the **`-pass`** option with a password.

The tar archive contains a text file named:

`opcsvcertbackup.<date_time>.txt`

This information can be useful for archiving and includes OvCoreIds of the backed up certificates, hostname, and time stamp of the backup. This information is not used during a restore.

- **`-restore`**

  A tar archive as created using the `-backup` option can be restored using this command.

  The filename must be provided with the `-file` option. The password used at backup time must be entered with the `-pass` option.

  The restore cannot work, if any of the certificates or private keys for the Certificate Authority, HP Operations management server, or managed node already exists on the management server system but are not the same as the corresponding values stored in the backup archive.

  To avoid this, enforce the restore by using the **`-force`** option. `opcsvcertbackup` also returns with an error when the OvCoreIds of the certificates to be restored do not fit with those stored in the HPOM database. When the `-force` option is used, the OvCoreIds are replaced and confirmation is displayed.

When to Back Up Certificates

The following are the times when a backup using `opcsvcertbackup` is recommended:

- **Initial HPOM Installation**

  After a successful HP Operations management server installation, it is highly recommended to make a backup of the certificate data with the command:

  `opcsvcertbackup -backup`

  The resulting tar archive should be stored in a secure place.

- **HP Operations Management Server Re-installation on Alternative System**

  Perform a standard HP Operations management server installation on the alternative system. Install the backup from the original management server installation onto the newly installed system with the command:

  opcsvcertbackup -restore -file *<filename>* -pass *<password>* -force

NOTE

The `-force` option must be used because the server installation has automatically created a Certificate Authority, HP Operations management server, and managed node certificates. These certificates are unsuitable because the managed nodes are configured to use the existing ones from the first installation.

- **Recovery**

  If something is deleted accidentally, use the command:

  opcsvcertbackup -restore -file *<filename>* -pass *<password>*

  Carefully check any error output.

- **Recovery from Configuration Errors**

  If a normal recovery without force option id not successful, check the error messages from the `opcsvcertbackup` call. If this does not help, clean the certificate information stuff with the command:

  opcsvcertbackup -remove

  or directly overwrite the existing certificate configuration with the command:

  opcsvcertbackup -restore -file *<filename>* -pass *<password>* -force

- **Configuring a Certificate Trust for MoM Environments**

  After creating a certificate trust it is recommended that you make a new backup. This ensures that the additional root certificate(s) can be restored in case a recovery is needed.

- **Configuring a Shared Certificate Authority**

  When configuring a shared Certificate Authority, the following command can be useful for removing the unwanted certificates from a second HP Operations management server installation.

  ```
  opcsvcertbackup -remove
  ```

  For further details “Environments Hosting Several Certificate Servers” on page 63.

Other HTTPS Agent Problems

This section describes HTTPS agent problems that are not related to the HTTPS communication or certificates.

Action request queues after HTTPS agent restart.

After a restart of an HTTPS agent or of a node on which the agent is running, a queue of pending actions overloads the system.

Problem

Once the agent is restarted all the scheduled tasks that are backed up are initiated instantly. This leads to multiple identical tasks start running immediately trying to perform the same function.

Solution

To clean up the queue, restart the agent again with the following command:

```
opcagt -cleanstart
```

B Tracing HPOM

Quick Start to Tracing HPOM

To help you investigate the cause of problems, HPOM provides problem tracing. Trace logfiles can help you pinpoint when and where problems occur, for example, if processes or programs abort, performance is greatly reduced, or unexpected results appear.

The following tracing mechanisms can be used with HPOM:

- HP tracing is the mechanism for tracing the latest HP BTO Software products and will be incorporated into all future products. HP tracing can be used to help solve problems with HTTPS agents and the HP Operations management server.

  Tracing allows remote access using a proprietary format. SSL encryption is not used. By default, the communication port is 5053.

- HPOM-style tracing, using configuration settings, can also be used to problem solve HTTPS agents as well as the HP Operations management server. The configuration settings set with the `ovconfchg` command.

HPOM-Style Tracing Overview

The configuration settings which specify the HPOM tracing are set with the `ovconfchg` command.

Activate HPOM-Style Tracing on the Management Server

You can activate the HPOM trace facility for the management server processes by entering the following `ovconfchg` command:

To enable tracing on an HP Operations management server, enter the command:

```
ovconfchg -ovrg server -ns opc -set OPC_TRACE TRUE
```

This entry is always required and enables tracing for the areas `MSG` and `ACTN`.

It is not necessary to restart any processes. Doing so may also remove the cause of the problem you are investigating.

Activate HPOM-Style Tracing on Managed Nodes

You can activate the HPOM trace facility for the HTTPS agent processes by entering the following command:

```
ovconfchg -ns eaagt -set OPC_TRACE TRUE
```

This entry is always required and enables tracing for the`MSG` and `ACTN` areas.

The tracing settings are automatically read by the processes at runtime, as soon a trace configuration setting has changed.

De-activate HPOM-Style Tracing

To de-activate HPOM problem tracing, complete the following steps:

Mgmt Server To disable tracing, enter one of the following commands:

```
ovconfchg -ovrg server -ns opc -clear
OPC_TRACE
```

or

```
ovconfchg -ovrg server -ns opc -set OPC_TRACE
FALSE
```

To inform the processes about new configuration settings on the management server, enter the command:

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

HTTPS Agents Enter the command:

```
ovconfchg -ns eaagt -clear OPC_TRACE
```

or

```
ovconfchg -ns eaagt -set OPC_TRACE FALSE
```

Trace Output File Locations

Trace information is written to the `trace.bin` logfile:

- Management Server

  <OvDataDir>`/share/tmp/OpC/mgmt_sv/trace.bin`

  Default: `/var/opt/OV/share/tmp/OpC/mgmt_sv/trace.bin`

- Managed Nodes

  <OvDataDir>`/tmp/OpC/trace.bin`

  HP-UX default: `/var/opt/OV/tmp/OpC/trace.bin`

Configuring HPOM-Style Tracing of the Management Server and Managed Nodes

This reduces the amount of data that is entered into the trace output file and simplifies the interpretation of the trace logfile. You can activate tracing for specific functional areas by specifying one or more functional areas in the trace statement.

Functional Areas

You can select the most suitable functional areas from the following list to more precisely target the area of investigation. Functional areas are set using the `OPC_TRACE_AREA` statement.

NOTE Not all functional areas are available for all processes.

`ACTN`	Actions.
`ALIVE`	Agent-alive check.
`ALL`	All tracing areas (except `DEBUG` and `PERF`).
`API`	Configuration API.
`AUDIG`	Auditing.
`DB`	Database.
`DEBUG`	Debugging information. Use this option carefully, as it provides extensive and detailed information, but the trace logfile will also be correspondingly large.
`DIST`	Distribution.
`INIT`	Initialization.
`INST`	Installation.
`INT`	Internal.
`LIC`	Licensing.
`MISC`	Miscellaneous.

MSG	Message flow.
NAME	Name resolution.
NLS	Native language support.
NTPRF	NTPerfMon.
PERF	Performance.
SEC	Security.
SRVC	Service.

Customize Tracing

To configure tracing:

1. Specify **OPC_TRACE TRUE**

   This is always required and enables tracing for the areas MSG and ACTN.

2. To trace a specific functional areas, select the appropriate functional area or management server/agent process by entering statements of the following formats:

   OPC_TRACE_AREA *<area>*[,*<area>*]

   OPC_TRC_PROCS *<process>*[,*<process>*]

   OPC_DBG_PROCS *<process>[,<process>]*

<area>	HPOM area to be traced or debugged. By default, MSG and ACTN are enabled. For a list of all available areas, see “Functional Areas” on page 305.
<process>	HPOM process to be traced or debugged.

NOTE Spaces are not allowed between entries in the lists for each process or area.

The following examples illustrate how to enable tracing for the message/action flow and initialization and debug. Generate trace output only for `opcmsga` and `opcacta`. Enable debug output only for `opcmsga`.

Example B-1 Management Server Configuration Commands

```
ovconfchg -ovrg server -ns opc -set OPC_TRACE TRUE \
-set OP_TRACE_AREA MSG,ACTN,INIT,DEBUG \
-set OPC_TRC_PROCS opcacta,opcmsga \
-set OPCDBG_PROCS opcmsga
```

Example B-2 HTTPS Managed Node Configuration Commands

```
ovconfchg -ns eaagt -set OPC_TRACE TRUE \
-set OP_TRACE_AREA MSG,ACTN,INIT,DEBUG \
-set OPC_TRC_PROCS opcacta,opcmsga \
-set OPCDBG_PROCS opcmsga
```

If the granularity of the above tracing options is not sufficient, use the variable `OPC_RESTRICT_TO_PROCS` to enable tracing for a particular area of a HPOM process.

3. To receive verbose trace information output, enter the following command:

   Mgmt Server `ovconfchg -ovrg server -ns opc -set OPC_TRACE_TRUNC FALSE`

   HTTPS Agents `ovconfchg -ns eaagt -set OPC_TRACE_TRUNC FALSE`

   By default, `OPC_TRACE_TRUNC TRUE` is enabled.

   For more information on tracing configuration, see “Examples of Tracing” on page 308.

Examples of Tracing

This section contains some examples to show how tracing can be activated for different areas and processes.

Enter the appropriate command:

- **Default**

  Collect trace information for the trace areas `MSG` (message flow) and `ACTN` (actions).

  Mgmt Server `ovconfchg -ovrg server -ns opc -set OPC_TRACE TRUE`

  HTTPS Agents `ovconfchg -ns eaagt -set OPC_TRACE TRUE`

- **Tracing for Heartbeat Polling and Message Flow**

  Collect trace information for the trace area `ALIVE` (agent-alive check).

  Mgmt Server `ovconfchg -ovrg server -ns opc -set OPC_TRACE TRUE -set OPC_TRACE_AREA ALIVE`

  HTTPS Agents `ovconfchg -ns eaagt -set OPC_TRACE TRUE -set OPC_TRACE_AREA ALIVE`

- **Tracing for Specific Areas of Specific Processes**

  Collect trace information for the trace area API (application programming interface) of the Message Manager process `opcmsgm`.

  Mgmt Server `ovconfchg -ovrg server -ns opc -set OPC_TRACE TRUE -set OPC_TRACE_AREA API -set OPC_TRC_PROCS opcmsgm`

- **Tracing and Debugging**

  - Collect trace information for *all* trace areas (except `PERF`), as well as debug information for all debug areas. Debug areas are to be used by HP Support Personnel only.

    Mgmt Server `ovconfchg -ovrg server -ns opc -set OPC_TRACE TRUE -set OPC_TRACE_AREA ALL,DEBUG`

    HTTPS Agents `ovconfchg -ns eaagt -set OPC_TRACE TRUE -set OPC_TRACE_AREA ALL,DEBUG`

- Collect trace information for *all* trace areas (except PERF) for the process ovoareqsdr (request sender), as well as debug information for all debug areas of the process ovoareqsdr (request sender).

  Mgmt Server
  ```
  ovconfchg -ovrg server -ns opc -set
  OPC_TRACE TRUE -set OPC_TRACE_AREA
  ALL,DEBUG -set OPC_TRC_PROCS ovoareqsdr
  -set OPC_DBG_PROCS ovoareqsdr
  ```

  HTTPS Agents
  ```
  ovconfchg -ns eaagt -set OPC_TRACE TRUE
  -set OPC_TRACE_AREA ALL,DEBUG -set
  OPC_TRC_PROCS ovoareqsdr -set
  OPC_DBG_PROCS ovoareqsdr
  ```

❑ **Different Trace Areas for Different Processes**

Restricting tracing to a specified process must specify the process in the tracing command.

The areas to be traced are specified as usual.

The first configuration entry enables tracing for the trace areas INIT (initialization) and INT (internal) of the control agent process (opcctla). The second configuration entry enables tracing for the trace areas MSG (message flow) and ACTN (actions) of the message agent process (opcmsga).

Mgmt Server
```
ovconfchg -ovrg server -ns opc.opcctla
-set OPC_TRACE TRUE -set OPC_TRACE_AREA
INIT,INT

ovconfchg -ovrg server -ns opc.opcmsga
-set OPC_TRACE TRUE
```

HTTPS Agents
```
ovconfchg -ns eaagt.opcctla -set OPC_TRACE
TRUE -set OPC_TRACE_AREA INIT,INT

ovconfchg -ns eaagt.opcmsga -set OPC_TRACE
TRUE
```

Syntax for Trace Files

The general format of the trace information is as follows:

```
<mm/dd/yy> <hh:mm:ss> <process_name>(pid)[<area>...]:
<detailed_ information>
```

mm/dd/yy	Date.
hh:mm:ss	Time.
process_name	Process name.
pid	Process ID.
area	Functional area(s) as specified in the trace statement.
detailed_information	Detailed information about the process.

NOTE New trace information is appended to existing trace logfiles. For this reason, you should delete the file to prevent it from becoming too large.

HP-Style Tracing Overview

HP tracing implements a hierarchy of elements: `Applications`, `Components`, `Categories` and `Attributes`. By specifying a combination of these in the trace GUI or in a trace configuration file, the area of interest can be traced.

Table B-1 illustrates how these elements relate to HPOM components, processes, and areas.

Table B-1 Tracing Terminology

Name	HPOM-Style Name	Examples
Application	Process, `OPC_TRC_PROCS` and `OPC_DBG_PROCS`	`opcmsga`, `ovpolicy`
Component	n.a.	`opc`, `eaagt`
Subcomponent	Trace Areas, `OPC_TRACE_AREA`	`actn`, `msg`, `init`, `debug`
Category	`OPC_TRACE TRUE`	`Trace`
Attribute	n.a.	`Info`, `Warn`, `Error`, `Developer`, `Verbose`

There are two ways to trace HPOM using HP tracing:

- Configure Remote Tracing Using the Windows Tracing GUI.
- Configure Manual Tracing Using Trace Configuration Files.

These methods are described in the next sections.

Configure Remote Tracing Using the Windows Tracing GUI

The tracing GUI, available after installing the HTTPS agent on a Windows system, helps to simplify tracing configuration. It can be used to connect to the remote trace server to identify the application, component, and category names and to view the attributes. It requires that port 5053 is opened in firewalls between the system where the GUI is running and the system where the trace output is generated. Using the features provided within the Tracing GUI, the required configuration setting can be selected and a configuration file saved.

To configure HP tracing on HPOM processes with the Tracing GUI:

1. Identify the HPOM processes that you want to trace. The following example uses the `opcmsga` and `opcmsgm` processes.
2. Start the Tracing GUI on a Windows system. In a Windows Explorer window, go to the directory:

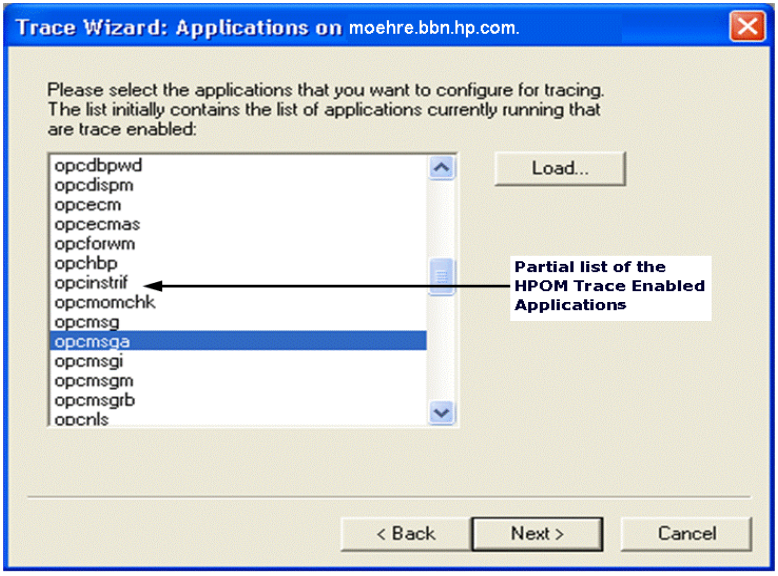
   `<OvInstallDir>\support\`

   Default location: `<ProgramFilesDir>\HP\HP BTO Software\support\`

3. Start the GUI by double-clicking the file:

   `ovtrcgui`

Figure B-1 TraceMon Applications Dialog for HPOM Applications



4. Select the `opcmsga` and `opcmsgm` applications.
5. Set all `opc` and `OvEaAgt` sub-components, except for the `DEBUG` to `Support`. This sets tracing attributes to the `Support` defaults of `Info`, `Warn`, and `Error` for all sub-components, with the `Verbose` attribute added to each component/sub-component combination entry.

   After you have selected the required configuration settings, save the configuration file.

Configure Manual Tracing Using Trace Configuration Files

In many cases, in particular on UNIX systems, the simplest way is to manually create the trace configuration files specifying the components to be traced and log the trace output into a file. Three management server and three agent example trace configuration files are provided at the following location on the management server system:

`/opt/OV/contrib/OpC/TraceConfig`

You must copy the appropriate file to the managed node system, if you want to use it to trace an agent.

NOTE You can also use the Tracing GUI to create a trace configuration file on a Windows system and then copy this to the system where you want to investigate a problem.

These files include trace configuration statements for all HPOM processes. refer to the lines beginning with `APP:`. If you want to trace specific processes, create a new trace configuration file and copy and paste the appropriate pieces from the example files and add the header line - the first line, beginning with `TCF`.

HP Tracing implements a hierarchy of elements starting with `Applications`, `Components`, `Categories` and `Attributes`. In HP Tracing terminology, the processes defined by `OPC_TRC_PROCS` and `OPC_DBG_PROCS` are referred to as `Applications`. The `TRACE AREAS` defined by the `OPC_TRACE_AREA` parameter are referred to as `subcomponents`.

Component = *<component name>*

Trace area = *<sub-component>*

Category = `Trace`

To configure the same type of trace configuration using HP Tracing, you create a Trace Configuration File (See Example B-3), enable tracing using the `ovtrccfg` tool, and monitor the trace messages using the `ovtrcmon` tool.

Example B-3 Trace Configuration File

```
TCF Version 3.2
APP: "opcmsga"
SINK: Socket "prodnode" "node=10.1.221.22;"
TRACE: "eaagt.actn" "Trace" Info Warn Error Developer
Verbose
TRACE: "eaagt.debug" "Trace" Info Warn Error Developer
Verbose
TRACE: "eaagt.init" "Trace" Info Warn Error Developer
Verbose
```

```
TRACE: "eaagt.msg" "Trace" Info Warn Error Developer Verbose
APP: "opcacta"
SINK: Socket "prodnode" "node=10.1.221.22;"
TRACE: "eaagt.actn" "Trace" Info Warn Error Developer
Verbose
TRACE: "eaagt.init" "Trace" Info Warn Error Developer
Verbose
TRACE: "eaagt.msg" "Trace" Info Warn Error Developer Verbose
```

Activating Tracing

To activate tracing into a local file, complete the following steps:

```
/opt/OV/support/ovtrcadm -a localhost
```

```
/opt/OV/support/ovtrccfg -server localhost \
<my_trace_config_file>
```

For example:

```
ovtrccfg -server localhost \
/opt/OV/contrib/OpC/TraceConfig/ServerAll.tcf
```

Viewing Trace Results

To view the trace output you need to use the formatting tool `ovtrcmon`:

```
/opt/OV/support/ovtrcmon -fromfile <binary_output> [ -tofile
<ascii-output> ]
```

You can specify output formats. Details are available from the `ovtrcmon` usage text:

```
/opt/OV/support/ovtrcmon -help
```

An alternative way to capture trace output, assuming you want to use one of the pre-configured trace configuration files from the directory on the management server:

`/opt/OV/contrib/OpC/TraceConfig/*.tcf`:

is as follows:

1. In your trace configuration file (file extension `.tcf`), replace the lines beginning with `SINK: File` with the string:

   ```
   SINK: Socket "localhost" "node=localhost;"
   ```

2. Load the trace configuration file using the command:

   ```
   /opt/OV/support/ovtrccfg <my_trace_config_file>
   ```

3. Start `ovtrcmon` to dump the output into a file:

   ```
   /opt/OV/ovtrcmon -server localhost >\
   <my_ascii_trace_output_file>
   ```

   See `ovtrcmon` usage message for output formatting options.

Disable Remote Tracing (No Ports Opened)

The ovtrcd process, by default, opens port 5053 for external access. You can switch off the opening of this externally visible port using one of the following methods:

- **On a Managed Node**

  1. Disable remote tracing using the following command:

     ovtrcadm -disableremotetracing

  2. Restart the trace daemon (ovtrcd) process using the following command:

     /opt/OV/support/ovtrcadm -srvshutdown

     /opt/OV/lbin/xpl/trc/ovtrcd

     Or use the OVTrcSrv boot script located in the platform-dependent boot directory, for example, on Solaris:

     /etc/init.d/OVTrcSrv

  3. After ovtrcd restarts, localhost:5053 is still used, but on local loopback only. Restart the applications that you want to trace. For example, the HTTPS agent.

- **On a Management Server**

  The bbc_inst_defaults file on the management server contains the configuration setting:

  eaagt:DISABLE_REMOTE_TRACE_AT_INSTALL

  If this setting is set to TRUE, all appropriate newly installed agents automatically execute the following steps, as required by the above method, before they are started.

  ovtrcadm -disableremotetracing

  /opt/OV/support/ovtrcadm -srvshutdown

  /opt/OV/lbin/xpl/trc/ovtrcd

  For more information on how to configure the bbc_inst_defaults file, refer to the section “Changing the Default Port” on page 92 or the example file at the following location:

  /etc/opt/OV/share/conf/OpC/mgmt_sv/bbc_inst_defaults.sampl

Switch Off Tracing

To switch of tracing, enter the command:

```
/opt/OV/support/ovtrccfg off
```

An Example of Tracing HPOM Processes

The following sample procedure provides an example of how to set up HP tracing on HPOM processes. The example makes the following configuration assumptions:

- The `opcmsga` and `opcmsgm` process running on a UNIX system must be traced.
- The `ovtrccfg` trace configuration client will be used to make configuration changes.
- The trace configuration file must be named: `$OV_CONF/OVOTrace.tcf`
- The `ovtrcmon` trace monitor client will be used to monitor the traces.
- The trace output must be written to a file named: `$OV_LOG/OVOTrace.trc`

To set up tracing on HPOM processes:

1. Identify the HPOM processes that you want to trace. (The following example uses the `opcmsga` and `opcmsgm` processes).
2. Create a trace configuration file named `OvoTrace.tcf`. Locate the file in the `$OV_CONF` directory.

   This sample trace configuration file (See Example B-4) enables tracing on the two HPOM applications: `opcmsga` and `opcmsgm`. The Sink is configured as a socket with the machine `supnode1` as the target server. The components selected are the `opc` and `eaagt`. All the associated sub-components are selected except for the `DEBUG` sub-components. This would correspond to selecting `All Areas except DEBUG`. The tracing attributes are set to the `Support` defaults of `Info`, `Warn`, and `Error` for all, with the `Verbose` attribute added to each component/sub-component combination entry.

Example B-4 Trace Configuration File $OV_CONF/OVOTrace.tcf

```
TCF Version 3.2
APP: "opcmsgm"
SINK: Socket "supnode1" "node=10.111.1.21;"
TRACE: "opc.actn" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.agtid" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.alive" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.api" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.audit" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.db" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.dist" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.fct" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.gui" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.init" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.inst" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.int" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.lic" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.mem" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.memerr" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.misc" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.mon" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.msg" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.name" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.nls" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.ntprf" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.ocomm" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.pdh" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.perf" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.pstate" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.sec" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.srvc" "Trace" Info Warn Error Developer Verbose
TRACE: "opc.wmi" "Trace" Info Warn Error Developer Verbose
APP: "opcmsga"
SINK: Socket "supnode1" "node=10.111.1.21;"
TRACE: "eaagt.actn" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.agtid" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.alive" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.api" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.audit" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.db" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.dist" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.fct" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.gui" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.init" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.inst" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.int" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.lic" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.mem" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.memerr" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.misc" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.mon" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.msg" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.name" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.nls" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.ntprf" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.ocomm" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.pdh" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.perf" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.pstate" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.sec" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.srvc" "Trace" Info Warn Error Developer Verbose
TRACE: "eaagt.wmi" "Trace" Info Warn Error Developer Verbose
```

If you have access to a Windows system with the `TraceMon` tool installed, it can be used to connect to the remote trace server to identify the application, component, and category names and to view the attributes. Refer to Figure B-2 and Figure B-3 for screen shots of associated dialogs from TraceMon GUI. Using the features provided within the TraceMon GUI tool, the required configuration setting can be selected and the configuration file saved.

Figure B-2 TraceMon Applications Dialog for HPOM Applications

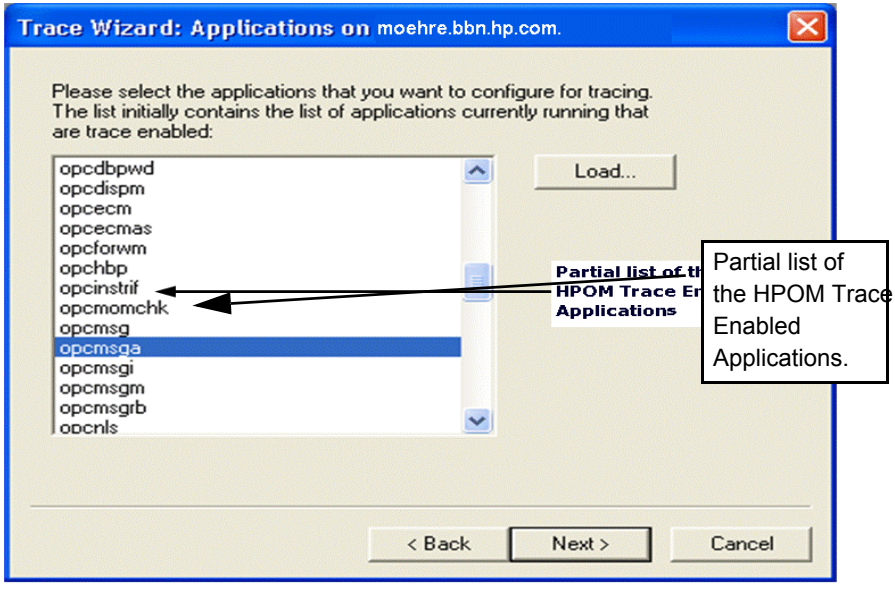
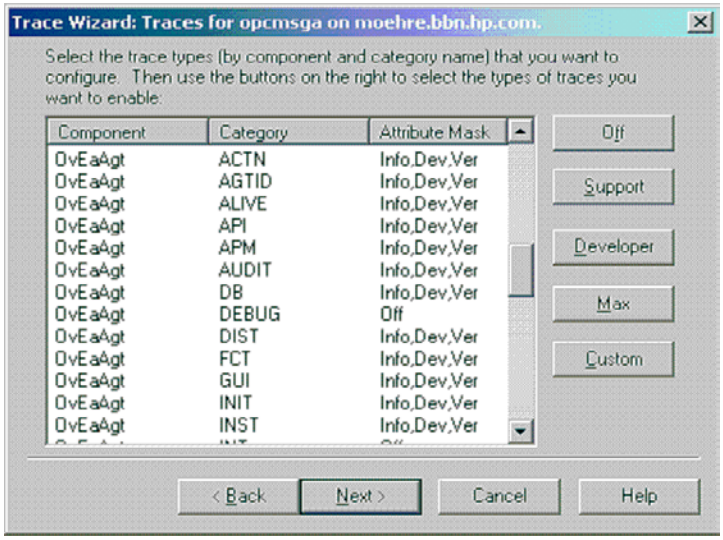


Figure B-3 TraceMon Trace Dialog for HPOM Applications



3. Verify that the trace server is running on the system by executing the command:

   `ps -ef | grep ovtrcd`

   If the process is running, the information returned should be of the following form:

   ```
   root 18750  1  0  Mar  5  ?0:00 /opt/OV/bin/ovtrcd
   ```

4. Verify that the applications being traced `opcmsgm`, are running on the system.

   To verify a process is running, execute commands of the following form:

   `ovc -status opcmsga opcmsgm`

   The information returned should be of the following form:

   ```
   opcmsgm OMU Message Manager SERVER,OPC (14038)  Running
   opcmsga OMU Message Agent   AGENT,EA   (5380)   Running
   ```

5. Use the `ovtrccfg` configuration client to set the tracing configuration, using the command:

   `$OV_BIN/ovtrccfg -server supnode1 $OV_CONF/OvoTrace.tcf`

6. Use the `ovtrcmon` monitor client to monitor the trace messages generated from the `opcmsga` and `opcmsgm` applications. To monitor the trace server running on the `supnode1` system and output the trace messages in binary format to the `$OV_LOG/OvoTrace.trc file`, enter the command:

   `$OV_BIN/ovtrcmon -server supnode1 -tofile $OV_LOG/OvoTrace.trc`

7. Provided that the processes to be traced are running (`opcmsga` and `opcmsgm` in our example), they should now be generating trace messages. Once enough trace information has been captured, stop the tracing. To Stop tracing, enter the command:

   `$OV_BIN/ovtrccfg off`

8. View the trace output using the `ovtrcmon` monitor client. The trace output can be read from the binary trace file created using the `ovtrcmon -fromfile` option. This option reads in a binary trace file and converts it to text. The converted trace messages can be sent directly to standard out or can be redirected to trace text file.

   To convert the binary trace file to text and send the output to standard out, enter the following command:

   `$OV_BIN/ovtrcmon -fromfile $OV_LOG/OvoTrace.trc`

   To redirect the converted trace messages to a text file, enter the following command:

   `$OV_BIN/ovtrcmon -fromfile $OV_LOG/OvoTrace.trc \`
   `> /tmp/trc.text`

   The binary `$OV_LOG/OvoTrace.trc` can be viewed from within the TraceMon Windows tool, where additional filtering can be done.

9. If analysis of the trace output is inconclusive, additional tracing can be done to capture more trace information. If needed, the trace configuration file can be modified to include or remove applications, components, categories or attributes.

HPOM Trace-Enabled Applications

All HPOM processes use HP Tracing. The HPOM Trace Enabled processes can be divided into three groups:

- The Server processes
- The Agent processes
- The processes that link with a lower level component which implemented XPL Tracing.

There are no pre-configuration steps required to enable tracing within HPOM. This is accomplished by either adding XPL Tracing into the HPOM code base or by incorporating core functionality from a foundation component and linking with the corresponding library. In the case where XPL Tracing was added to the HPOM code base, the existing tracing was converted to XPL Tracing. In cases where functionality from a foundation component was added, the XPL Tracing incorporated into these foundation components is pulled into HPOM.

Table B-2 HPOM Trace-enabled Applications on Management Server and Managed Nodes

Platform	Application Name		
UNIX/Linux	coda	ovas	ovconfget
	codautil	ovbbccb	ovcoreid
	ctrlconfupd	ovc	ovcreg
	logdump	ovcd	ovcs
	opc_getmsg	ovcert	ovdeploy
	opc_ip_addr	ovcm	ovpolicy
	opccrpt	ovconfchg	
	opcnls	ovconfd	

Table B-3 HPOM Trace-enabled Applications on Management Server

Platform	Application Name		
UNIX/Linux	opc	opcdbck	opcsvcm
	opc_dbinit	opcdbinst	opcsw
	opc_dflt_lang	opcdbmsgmv	opcttnsm
	opc_rexec	opcdbpwd	opcuiadm
	opcactm	opcdispm	opcuiopadm
	opcagtdbcfg	opcforwm	opcuiwww
	opcagtutil	opchbp	ovoareqsdr
	opcauddwn	opchistdwn	
	opcbbcdist	opcmsgm	
	opccfgupld	opcmsgrb	
	opccsacm	opcnode	
	opccsad	opcragt	
	ovcd	opcservice	

Table B-4 HPOM Trace-enabled Applications on Managed Nodes

Platform	Application Name		
UNIX/Linux	opcacta	opcmon	opcmsgi
	opceca	opcmona	opctrapi
	opcecaas	opcmsg	
	opcle	opcmsga	

Server and Agent Applications

HP BTO Software and HPOM Specific Components

There are many components and sub-components defined for each application. The most important are `eaagt` and `opc`. Table B-5 lists the Tracing Components which are defined for the server and agent processes.

Table B-5 HPOM Server and Agent Components

HPOM Component Name	Component Description
`eaagt`	Event Action Agent
`opc`	Management Server Control

Table B-6 lists the components defined for the shared components which have been incorporated into the product.

Table B-6 HP BTO Software Shared Components

Application with Component and Subcomponent Names	
Black Box Communication	
bbc.cb	bbc.http.output
bbc.fx	bbc.http.server
bbc.fx.client	bbc.messenger
bbc.fx.server	bbc.rpc
bbc.http	bbc.rpc.server
bbc.http.client	bbc.soap
bbc.http.dispatcher	
Control Component	

Table B-6 HP BTO Software Shared Components (Continued)

Application with Component and Subcomponent Names	
ctrl.action	ctrl.ovc
ctrl.autoshutdown	ctrl.process
ctrl.component	ctrl.rpcclient
ctrl.controller	ctrl.rpcserver
ctrl.main	ctrl.soap
ctrl.monitor	ctrl.xml
ctrl.monitorproxy	
Configuration Management Component	
conf.cluster	conf.ovconfd
conf.cluster.clioutputs	conf.ovpolicy
conf.config	conf.policy
conf.message	
Certificate Server Adapter	
CSA-CertRequestImpl	Csa-Main
CSA-CertReqContainer	csa.ovcmwrap
CSA-Database	Csa-RpcServer
Csa-Log	CSA-UpdateHandler
Security Core Component	
sec.cm.client	sec.core.base
sec.cm.server	sec.core.ssl
sec.core.auth	
Cross Platform Library	

Table B-6 HP BTO Software Shared Components (Continued)

Application with Component and Subcomponent Names	
xpl.cfgfile	xpl.net
xpl.config	xpl.runtime
xpl.io	xpl.thread
xpl.log	xpl.thread.mutex
xpl.msg	
Embedded Performance Agent	
coda	coda.mesa
coda.dataaccess	coda.mesainstances
coda.kmdatamatrix	coda_mesametricrdr
coda.localmesa	coda.mesarea
coda.logger	coda.prospector
Deployment Component	depl

HPOM Specific and XPL Standard Categories

HPOM trace areas are designated by HP BTO Software categories. In addition, a number of the standard categories are used by both HPOM processes and the lower level HP BTO Software components used by HPOM.

Table B-7 lists the tracing categories which are defined for the `eaagt` and `opc` components.

Table B-7 HPOM opc and eaagt Sub-components

Sub-Component Name	Sub-Component Description
HPOM Specific Tracing Categories	
actn	Actions
agtid	IP independence using AgentID
alive	Agent alive checking
api	Configuration API
apm	Cluster APM
audit	Auditing
db	Database (dblib)
debug	Debug
dist	Distribution
fct	Function (control flow)
init	Initialization (e.g. err init, conf init)
inst	Installation
int	Internal
lic	Licensing
memerr	Problems with Memory allocation
memory	Rest of memory allocation
misc	Miscellaneous
mon	Monitor
msg	Message flow

Table B-7 HPOM opc and eaagt Sub-components (Continued)

Sub-Component Name	Sub-Component Description
name	Name resolution
nls	National Language Support (character set conversion,...)
ntprf	NT Performance trace
pdh	Performance data helper
perf	Performance
pstate	Policy and Source state changes
sec	Security
srvc	Service
wmi	Conversion of LE-Templates to WMI-Templates
Generic XPL Tracing Categories	
Trace	Generic traces
Proc	Procedure traces
Operation	Operational traces
Init	Initialization
Cleanup	Cleanup operation
Event	Event
Parms	Parameters
ResMgmt	Resource Management

C Configuring HTTPS-Based Communication

Communication Configuration Parameters

HP applications may be customized for installation using configuration parameters. The communication broker configuration parameters are contained in the `bbc.ini` file located at:

`<OVDataDir>/conf/confpar/bbc.ini`

The parameters used for communication are described in "HTTPS Communication Configuration File" on page 334.

The Communication Broker uses the namespace `bbc.cb`. An additional namespace, `bbc.cb.ports`, has been defined to specify the Communication Broker port number for all managed nodes. This enables different Communication Brokers to have different port numbers. This configuration takes precedence over the `SERVER_PORT` parameter defined in the namespace `bbc.cb`.

NOTE

A namespace is a unique URL, for example:

`www.anyco.com` or `abc.xyz`

Namespaces provide a simple method for qualifying element and attribute names used in Extensible Markup Language documents by associating them with namespaces identified by URL references.

The name/value pairs in the `bbc.cb.ports` namespace define the port numbers for the Communication Brokers within the network. The syntax of the name/value pairs is:

`NAME=<host>:<port>` or `NAME=<domain>:<port>`

Multiple host/port or domain/port combinations may be defined per line. Each is separated by a comma or semicolon.

A domain takes the form `*.domainname`. All entries for this domain will use the specified port. More specific entries take precedence. The name of the name/value pair is ignored, although the names must be unique within this namespace. The following are entry examples:

- `HP=jago.sales.hp.com:1383, *.sales.hp.com:1384; *.hp.com:1385`

- `SUN= *.sun.com:1500`

In this example the Communication Broker running on the host `jago.sales.hp.com` will have the port number `1383`.

All other hosts within the domain `sales.hp.com` use the port number 1384. All other hosts within the domain `hp.com` use the port number 1385. Hosts in the domain `sun.com` use the port number 1500. All other hosts use the default port number 383.

Synchronization of Configuration Data from One HPOM Server to Another

To use HTTPS-based communication for the transfer, the following prerequisite must be met:

- ❏ The source HPOM management server must be set up as an action-allowed manager on the target HPOM server.

To allow synchronization of configuration data from one HPOM server to another by using HTTPS-based communication, you must perform the following steps:

1. Create the appropriate configuration download information by running the `opccfgdwnld` CLI on the source HPOM server.
2. Run the following commands on the source HPOM server:

```
#!/usr/bin/sh
PATH=$PATH:/opt/OV/bin/OpC/install
tar cvf - /var/opt/OV/share/tmp/OpC_appl/cfgdwn | gzip >
/tmp/cfgdwn.tar.gz
opcdeploy -deploy -file /tmp/cfgdwn.tar.gz -node mgmtsv2
-targetdir /tmp -trd absolute
opcdeploy -cmd "rm -rf
/var/opt/OV/share/tmp/OpC_appl/cfgdwn" -node mgmtsv2
opcdeploy -cmd "gunzip < /tmp/cfgdwn.tar.gz| tar xvf -
2>&1"  -node mgmtsv2
```

3. Upload the configuration on the target HPOM server by running the `opccfgupld` CLI at a convenient time (for example, the planned maintenance window of the targeted HPOM server).

HTTPS Communication Configuration File

bbc.ini(4)

NAME

bbc.ini – Configuration file for HTTPS communication.

DESCRIPTION

`bbc.ini` is the configuration file of an HP Operations managed node using HTTPS communication and is located at:

`/<OVDataDir>/conf/confpar`

It consists of sections headed by namespaces which contain the settings for each namespace. The `bbc.ini` file contains the namespaces listed below. Possible and default settings are described for each namespace.

bbc.cb

The Communication-Broker Namespace. You can use the following parameters:

`string CHROOT_PATH = <path>`

On UNIX systems only, the `chroot` path is used by the `ovbbccb` process. If this parameter is set, the `ovbbccb` process uses this path as the effective root thus restricting access to a limited part of the file system. Default is `<OvDataDir>`. This parameter is ignored on Windows systems. See the `chroot` man page for details on `chroot`.

`bool SSL_REQUIRED = false`

If this parameter is set to `true`, the communication broker requires SSL authentication for all administration connections to the communication broker. If this parameter is set to `false`, non-SSL connections are allowed to the communication broker.

`bool LOCAL_CONTROL_ONLY = false`

If this parameter is set to `true`, the communication broker only allows local connections to execute administrative commands such as `start` and `stop`.

`bool LOG_SERVER_ACCESS = false`

If this parameter is set to `true`, every access to the server is logged providing information about the sender's IP address, requested HTTP address, requested HTTP method, and response status.

`int SERVER_PORT = 383`

By default this port is set to `383`. This is the port used by the communication broker to listen for requests. If a port is set in the namespace `[bbc.cb.ports]`, it takes precedence over this parameter.

`string SERVER_BIND_ADDR = <address>`

Bind address for the server port. Default is `INADDR_ANY`.

bbc.cb.ports

The Communication-Broker-Port Namespace. This parameter defines the list of ports for all Communications Brokers in the network that may be contacted by applications on this host. The default port number for all communication brokers is 383. You can use the following parameters:

`string PORTS`

This configuration parameter must be the same on all managed nodes. To change the port number of a communication broker on a particular host, the hostname must be added to this parameter, e.g. `name.hp.com:8000`. You can use an asterisk "`*`" as a wild card to denote an entire network, e.g.; `*.hp.com:8001`. Note too, that either a comma "," or a semi-colon ";" should be used to separate entries in a list of hostnames, for example;

`name.hp.com:8000, *.hp.com:8001`.

In these examples, all hostnames ending in “hp.com” will configure their BBC Communication Broker to use port 8001 except host “name” which will use port 8000. All other hosts use the default port 383.

You can also use IP addresses and the asterisk wild card (*) to specify hosts. For example;

`15.0.0.1:8002, 15.*.*.*:8003`

bbc.http

The HTTP Namespace for managed node-specific configuration. For application-specific settings, see the section bbc.http.ext.*. Note that application-specific settings in `bbc.http.ext.*` override managed node-specific settings in `bbc.http`. You can use the following parameters:

`int SERVER_PORT = 0`

By default this port is set to `0`. If set to `0`, the operating system assigns the first available port number. This is the port used by the application *<appName>* to listen for requests. Note that it only really makes sense to explicitly set this parameter in the `bbc.http.ext.`*<appName>* namespace, as the parameter is application specific with any other value than the default value.

`string SERVER_BIND_ADDR = `*<address>*

Bind address for the server port. Default is `localhost`.

`string CLIENT_PORT` = 0

Bind port for client requests. This may also be a range of ports, for example 10000-10020. This is the bind port on the originating side of a request. Default is port `0`. The operating system will assign the first available port.

Note that MS Windows systems do not immediately release ports for reuse. Therefore on Windows systems, this parameter should be a large range.

`string CLIENT_BIND_ADDR = `*<address>*

Bind address for the client port. Default is `INADDR_ANY`.

`bool LOG_SERVER_ACCESS = false`

If this parameter is set to `true`, every access to the server is logged providing information about the sender's IP address, requested HTTP address, requested HTTP method, and response status.

`string PROXY`

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

Format:
`proxy:port +(a)-(b);proxy2:port2+(a)-(b); ...;`

a: list of hostnames separated by a comma or a semicolon, for which this proxy shall be used.

b: list of hostnames separated by a comma or a semicolon, for which the proxy shall *not* be used.

The first matching proxy is chosen.

It is also possible to use IP addresses instead of hostnames so `15.*.*.*` or `15:*:*:*:*:*:*:*` would be valid as well, but the correct number of dots or colons MUST be specified. IP version 6 support is not currently available but will be available in the future.

bbc.fx

BBC File-Transfer Namespace for managed node-specific configuration. For application-specific settings, see the section bbc.fx.ext.*. Note that application-specific settings in `bbc.fx.ext.*` override managed node-specific settings in `bbc.fx`. You can use the following parameters:

`int FX_MAX_RETRIES = 3`

Maximum number of retries to be attempted for the successful transfer of the object.

`string FX_BASE_DIRECTORY` = *<directory path>*

Base directory for which files may be uploaded or downloaded. Default directory is *<OvDataDir>*.

`string FX_TEMP_DIRECTORY = <directory path>`

Temporary directory where uploaded files are placed while upload is in progress. At completion of upload, the file will be moved to *<directory path>*. Default directory is *<OvDataDir>*/tmp/bbc/fx.

`string FX_UPLOAD_DIRECTORY = <directory path>`

Target directory for uploaded files. By default this is the base directory. The upload target directory may be overridden with this configuration parameter. Default directory is FX_BASE_DIRECTORY.

bbc.snf

BBC Store-and-Forward Namespace for managed node-specific configuration. For application-specific settings, see the section bbc.snf.ext.*. Note that application-specific settings in bbc.snf.ext.* override managed node-specific settings in bbc.snf. You can use the following parameters:

`string BUFFER_PATH = <path>`

Specifies the SNF path were the buffered requests are stored. Default is:

<OVDataDir>/datafiles/bbc/snf/*<appName>*

`int MAX_FILE_BUFFER_SIZE = 0`

Specifies the maximum amount of disk space that the buffer is allowed to consume on the hard disk.

0 = No limit

bbc.http.ext.*

HTTP External-Communication Namespaces: bbc.http.ext.*<compID>*.*<appName>* and bbc.http.ext.*<appName>*.

This is the Dynamic External-Communication Namespace for application-specific settings. Note that application-specific settings in bbc.http.ext.* override managed node-specific settings in bbc.http.

See the section bbc.http for a list of the parameters you can use in the bbc.http.ext.* namespace.

bbc.fx.ext.*

The Dynamic File-Transfer (fx) Namespace for external-component and application-specific settings. Note that application-specific settings in `bbc.fx.ext.*` override managed node-specific settings in `bbc.fx`.

File Transfer External Namespaces:
`bbc.fx.ext.<compID>.<appName>` and `bbc.fx.ext.<appName>`.

See the section `bbc.fx` for a list of the parameters you can use in the `bbc.fx.ext.*` namespace.

bbc.snf.ext.*

The Dynamic Store-and-Forward (snf) Namespace for external-component and application-specific settings. Note that application-specific settings in `bbc.snf.ext.*` override managed node-specific settings in `bbc.snf`.

Store and Forward External Namespace:
`bbc.snf.ext.<compID>.<appName>` and `bbc.snf.ext.<appName>`.

See the section `bbc.snf` for a list of the parameters you can use in the `bbc.snf.ext.*` namespace.

AUTHOR

`bbc.ini` was developed by Hewlett-Packard Company.

EXAMPLES

```
PROXY=web-proxy:8088-(*.hp.com)+(*.a.hp.com;*)
```

The proxy `web-proxy` is used with port `8088` for every server `(*)` except hosts that match `*.hp.com`, for example `www.hp.com`. If the hostname matches `*.a.hp.com`, for example, `merlin.a.hp.com` the proxy server will be used.

SEE ALSO

ovbbccb (1)

D HTTPS Communication Architecture

Communication (Broker) Architecture

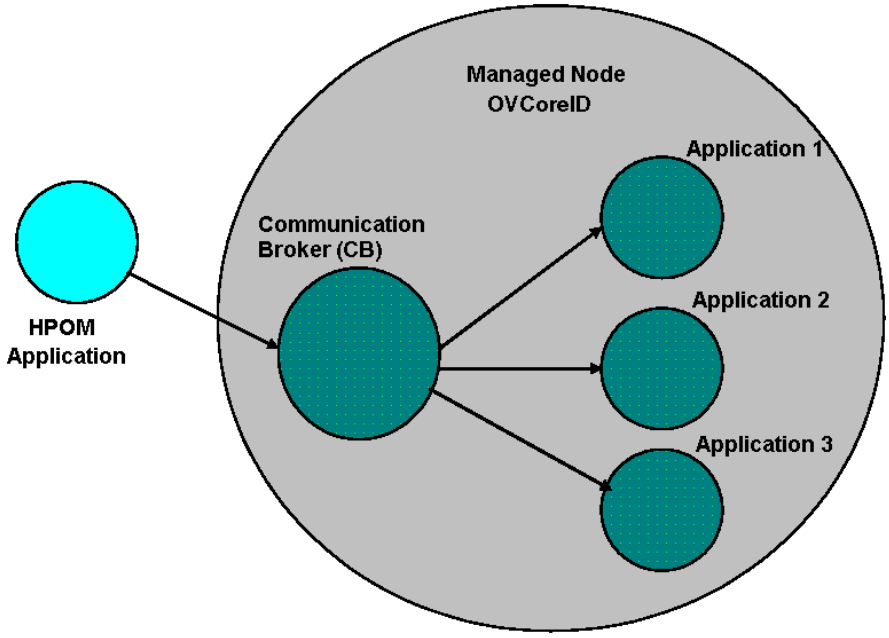
The Communication Broker acts as a proxy on the local managed node and provides a central point of entry to the managed node for all applications on that managed node. Applications that want to receive data register an address with the Communication Broker. The registration defines the port number, protocol, bind address, and base path the application wants to receive data on. Other applications, local or remote, either query the Communication Broker for the location of the application or use the Communication Broker as a proxy to forward the request to registered applications. The Communication Broker loads configuration data from the standard HP Operations Configuration File.

The Communication Broker has the following characteristics:

- The Communication Broker provides a single port solution for the managed node. Requests for all registered servers on this managed node can be directed through the Communication Broker. The Communication Broker transparently forwards the request to the registered server in the same way as an HTTP proxy forwards an HTTP request. The default port for the Communication Broker is 383 but can be changed.
- For higher security on UNIX systems, `chroot` can be used at start up of the Communication Broker. `chroot` restricts the part of the file system visible to the Communication Broker process by making the specified path act as the root directory, thus reducing exposure to hackers.
- The Communication Broker can be run as non-root on UNIX systems if its port number is greater than 1024.
- The Communication Broker can be configured to run as root-only on UNIX systems to open its port and then switch to a non-root user for all other operations.
- The Communication Broker can be:
  - — Started as a daemon on UNIX systems.
  - — Installed as a Windows NT Service on Windows systems.
- Control commands for the Communication Broker can be restricted to the local managed node only.

- The Communication Broker applies SSL encryption of data transmission over the network.
- The Communication Broker applies SSL authentication through guaranteed identity of senders and receivers.

Figure D-1 Communication Broker Architecture



A Communication Broker configures a minimum of one port for accepting incoming data to a managed node. The port is associated with an OVCoreID to identify the managed node. The Communication Broker can be configured to open multiple ports for high availability managed nodes. Each port can have a different identity associated with it. If SSL is enabled, the port is configured with X509 certificates. These certificates allow connecting applications to verify the identity of both message senders and receivers.

All applications on the current managed node that register with the Communication Broker are automatically registered for all active incoming ports opened by the Communication Broker. The port

associated with the default namespace, `bbc.cb`, is automatically activated on startup of the Communication Broker. Other ports can be activated or deactivated dynamically after startup. See the command line interface parameters for the Communication Broker for details.

E Firewalls and HTTPS Communication

Firewall Scenarios

Firewalls are used to protect a company's networked systems from external attack. They usually separate the Internet from a company's private intranet. It is also quite common to implement multiple levels of firewalls to restrict access to the more trusted environments from those of lower sensitivity. For example, the research and finance departments may be contained in the environment of highest security, while direct sales may need to be easily accessible from the outside. Systems on the intranet are allowed, under certain conditions, to cross the firewall to access systems on the internet, for example located in the DMZ. The firewall can also allow systems on the Internet to cross the firewall and access systems on the private intranet. For either of these situations, the firewall must be configured to allow that operation.

HP Operations HTTPS communication provides features that allow firewall administrators to configure HP Operations applications to communicate through firewalls.

Contacting an Application on the Internet from an Intranet Using an HTTP Proxy

An HP Operations HTTPS-based application on a private intranet wants to contact an application outside of the firewall on the public Internet or Demilitarized Zone (DMZ). The HP Operations application initiates the transaction and acts as a client contacting a server application on the Internet. The server application could be another HP Operations application acting as an HTTP server or any other HTTP server application. A common example of a client is a web browser on the private intranet wanting to contact a web server on the Internet. An HTTP proxy must be configured in the browser which forwards the request across the firewall and contacts the web server in the Internet. The firewall is configured to allow the HTTP proxy to cross the firewall. The firewall does not allow the web browser to directly cross the firewall. In the same way, HP Operations HTTPS communication applications can also be configured to use HTTP proxies to cross firewalls.

Contacting an Application on the Internet from an Intranet Without an HTTP Proxy

An HP Operations HTTPS-based application on a private intranet wants to contact an application outside of the firewall on the Internet without using an HTTP proxy. The firewall must be configured to allow the HP Operations application on the private intranet to cross the firewall. This is very similar to configuring a firewall to allow an HTTP proxy to cross the firewall. The firewall administrator may want to set source and target ports for the transaction to restrict communication across the firewall. The `CLIENT_PORT` configuration parameter specifying the source ports can be set from the HP Operations application when initiating the transaction. The target or destination port is defined in the URL (Uniform Resource Locator or Identifiers) address used to contact the HTTP server on the Intranet. This is the communication broker port on the target node.

Contacting an Application Within a Private Intranet from an HP Operations Application on the Internet

An HP Operations HTTPS-based application on the Internet wants to contact an application on a private intranet. This means that a firewall must be crossed from the outside and is usually only allowed by organizations under very restricted conditions set by the firewall administrator. The initiating or client application may do this using an HTTP proxy or go directly through the firewall. The HTTP proxy is outside the firewall and the firewall must be configured to allow the HTTP proxy to cross it. The HTTP proxy could either directly contact the server on the private intranet or go through another proxy, in a cascading proxies arrangement. In either case, the HP Operations HTTPS communication client application is configured in the same way. However, the HTTP proxies must be configured differently.

Contacting an Application Within a Private Intranet from an HP Operations Application on the Internet Without Using HTTP Proxies

An HP Operations HTTPS-based application on the Internet wants to contact an application on the private intranet, but there is no HTTP proxy. The firewall must be configured to allow the HP Operations client application to cross the firewall. The firewall administrators may want to

set the source and target ports for the transaction to restrict communication across the firewall. The `CLIENT_PORT` configuration parameter specifying the source port can be set from the HP Operations application when initiating the transaction. The target or destination port used to contact the HTTP server on the Intranet is defined in the URL address and is the Communication Broker port on the target node.

If the target server is registered with the Communication Broker, the target port will always have the port number of the Communication Broker. This makes it easier when configuring firewalls. It can greatly reduce the number of target ports an administrator must configure at the firewall.

For information on configuring HPOM with firewalls, refer to the *HPOM Firewall Configuration*.

Index

Index

Index

Index

Index

Index