HP Performance Agent

For AIX Operating System

Software Version: 5.00

Installation and Configuration Guide

Manufacturing Part Number: B7490-90009
Document Release Date: August 2009
Software Release Date: August 2009

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

Trademark Notices

UNIX® is a registered trademark of The Open Group.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

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

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

Documentation Updates

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

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

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

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

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

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

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

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

Support

Visit the HP Software Support web site at:

www.hp.com/go/hpsoftwaresupport

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

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

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

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

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

To find more information about access levels, go to:

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

Contents

1 Installing or Upgrading HP Performance Agent

HP Performance Agent captures performance, resource, and transaction data from your IBM AIX system. Using minimal system resources, the software continuously collects, summarizes, time stamps, and detects alarm conditions in current and historical resource data across your system. You can analyze the data using spreadsheet programs, Hewlett-Packard analysis products such as HP Performance Manager, or third-party analysis products. Also, Performance Agent provides data access to Performance Manager and sends alarm notifications to HP Network Node Manager (NNM) and HP Operations Manager.

The name Performance Manager refers to versions 4.00 and later. Performance Manager 3.xx refers to the product that was formerly known as PerfView.

Performance Agent supports monitoring data for virtualized environments like LPARs and WPARs, which is captured by the BYLS class of metrics.

For more information, see Performance Agent in a Virtualized Environment on page 20.

Performance Agent uses Data Source Integration (DSI) technology to receive, alarm on, and log data from external data sources such as applications, databases, networks, and other operating systems.

The comprehensive data logged and stored by Performance Agent allows you to:

- Characterize the workloads in the environment.
- Analyze resource usage and load balance.
- Perform trend analyses on historical data to isolate and identify bottlenecks.
- Respond to error conditions.
- Perform service-level management based on transaction response time.

- Perform capacity planning.
- Solve system management problems before they arise.

For a comprehensive description of Performance Agent, see the *HP Performance Agent for UNIX User's Manual*.

Before using HP Performance Agent, you must review and accept the license terms and conditions detailed in the readme file available in `/<directory>/<os>/readme.ovpa,` where <*directory*> is your optical media directory.

Installation Requirements

For Performance Agent to run properly, your system must meet the requirements described in this section.

Hardware

Performance Agent generally runs on hardware platforms supporting the operating system, including:

- IBM RS/6000 and pSeries systems
- IBM POWER5, POWER6 systems

Software

- Performance Agent 5.00 is supported on IBM AIX 5L V5.3 ML3 and later, and on AIX 6.1 TL2.
- The `libC.a` library is required for the Performance Agent to operate properly. The library is bundled within the `xlC.rte` package, available from your AIX OS DVD-ROM disk media
- The `libSpmi.a` library is a prerequisite on AIX 5L V5.3 and later for the memory metrics to be calculated accurately and also to collect cross-partition metrics for the BYLS class. The library is bundled within the `perfagent.tools` file set from your AIX OS DVD-ROM disk media and is installed in the `/usr/lib/` directory.
- BYLS class of metrics is supported on IBM AIX 5L V5.3 ML3 and later.

Daemons required for Virtualization metrics

- To collect and log cross-partition metrics, either `xmservd` or `xmtopas` daemon should be available. `xmtopas` is a part of `perfagent.tools` fileset and `xmservd` is a bundled software of the Performance Toolbox for AIX component which is a licensed software.

Supported Versions of Virtual I/O (VIO) Server

- Supports VIO Server 1.3, 1.4, 1.5, and 2.1 versions

Communication Protocols

- Performance Agent supports only the HTTP(S) 1.1 communication protocol.
- If you are installing Performance Agent on a system which has HP Software products such as HP Operations Agent, HP Operations Manager Unix Management Server, HP Performance Manager, HP Performance Insight, and OV Internet Service, restart them after the Performance Agent installation is completed.
- If you are adding new hardware or making any configuration changes, it is recommended to stop `scopeux` and restart it to make the changes to take effect.
- All the default OS daemons and services should be enabled and running for the IBM AIX system.

Disk Space

Performance Agent installs in the `/usr/lpp/perf/ and /usr/lpp/OV/` directories and creates its log and status files in the `/var/opt/OV/ and /var/opt/perf/` directories.

- For first time installation of Performance Agent, 70 MB of disk space is required in the `/usr/lpp/perf/ and /usr/lpp/OV/`directories.
- For Performance Agent databases and status files, allow for 60 MB of disk space in the `/var/opt/OV/ and /var/opt/perf/` directories.

If you do *not* have enough space in your `opt/perf` and/or `/var/opt/perf` directories, you should install Performance Agent on symbolic links. Refer to Installing Performance Agent on Symbolic Links on page 18.

For a description of how the `parm` file is used to limit and configure log file data storage, see the “parm File” section in Chapter 2 of the *HP Performance Agent for UNIX User’s Manual*.

Install or Upgrade Procedures

Performance Agent is on the DVD-ROM installation media in several file sets. The size of the product is approximately 70 MB.

If you had previously installed version of Performance Agent or GlancePlus on your system, stop any performance tools or process that may be running. For instructions, see Stop Active Performance Tools or Processes. For installation instructions, refer to the section, Install Performance Agent

Read Before Installation

Usage of Symbolic Links

Symbolic links are created to redirect the default product installation directory (base directory) to a directory of your choice. You need to read this section only if you are planning to use the base directory symbolic links. Otherwise, you can ignore this section and read the installation instructions explained in the subsequent sections.

AIX platform supports this feature of creating base directory symbolic links. These links are preserved only during the first time installation of the product and do not work when you upgrade to a new version of the product. This implies that whenever you upgrade to a new version, the installer program removes the symbolic links and again replaces the link to the default directory applicable to the product that is installed.

Example, the base directory for HP Performance Agent is `/var/opt/perf`, which can be redirected to a different directory using the symbolic links. See the Installing Performance Agent on Symbolic Links section for more information.

Apart from using symbolic links, you can also use directory mounts to redirect the base directories to other locations in the file system.

Usage of Directory Mounts

You can use directory mounts to redirect the base directories to other directories in the file system before the product installation. Perform the following steps to migrate an already existing installation with symbolic links to the usage of mount points:

You can find the following steps to redirect `InstallDir` and `DataDir` to a different file system.

1. Stop the OV software by typing the following command:

   `ovc -kill`

2. Remove the symbolic links.
3. Create mount points for `InstallDir` and `DataDir` to mount the directories of the installed software at the new mount points.

   a. **`mkdir /usr/lpp/OV`**

   b. **`mkdir /var/opt/OV`**

4. Add the mount points to `/etc/filesystems`
5. Edit `/etc/filesystems` and add entries for `InstallDir` and `DataDir` (file system type `namefs`)

Example

To redirect `InstallDir` to `/mgmt/install/OV` and `DataDir` to `mgmt/data/OV`:

1. Open the file using the following command:
   `vi /etc/filesystems`
2. Add the following entries

```
/usr/lpp/OV:

            dev             = /mgmt/install/OV
            vfs             = namefs
            mount           = true
            options         = rw
            account         = false
/var/lpp/OV:

            dev             = /mgmt/data/OV
            vfs             = namefs
            mount           = true
            options         = rw
            account         = false
```

3 Mount the file systems by typing the following commands:

   a **mount /usr/lpp/OV**

   b **mount /var/lpp/OV**

4 Type the following command to verify the setup:

   mount

   The base directories `InstallDir` is redirected to `/mgmt/install/OV` and `DataDir` is redirected to `mgmt/data/OV`.

Stop Active Performance Tools or Processes

1 Log in as user **root**.

2 Run `perfstat` to check for active performance tools by typing:

   /usr/lpp/perf/bin/perfstat

   If `perfstat` reports any active performance tools such as GlancePlus, stop them. (Make sure that users have exited these tools before doing so.)

   lsdaemon should be stopped prior to installation. Run `ps -ef | grep lsdaemon`, to make sure that no lsdaemon process is running.

3 If a previously installed version of Performance Agent is running, stop it by typing:

   /usr/lpp/perf/bin/mwa stop

Customized configuration files such as the `parm`, `alarmdef`, and `ttd.conf` as well as any customized log files are not overwritten by the new installation. The new configuration files are installed in the `/opt/perf/newconfig/usr/lpp/perf/newconfig` directory.

4 As a precaution, make sure you have backed up your customized configuration files such as the `parm, alarmdef`, and `ttd.conf` files, and any customized export template files.

If you stop `ttd`, you must also stop any ARM-instrumented applications that are running before you restart `ttd` and Performance Agent processes.

5 Run `perfstat` again to ensure that no performance tools or processes are active. When all tools or processes have been stopped, proceed with the installation.

Install Performance Agent

While installing Performance Agent and upgrading Performance Agent to the current version, the data communication protocol to be used is set to HTTP.

For a detailed description of `install.ovpa` options, see The install.ovpa Script on page 18.

If you are also running the GlancePlus product on your system, be sure to update GlancePlus to the same release version as Performance Agent. Both Performance Agent and GlancePlus must always be the same version.

If you have Operations Manager agent installed on your system, see Installing Performance Agent with Operations Manager Installed on Your System on page 17.

To install:

1. Make sure you are logged in as user **`root`**.
2. Insert your installation CD-ROM into the drive.
3. Mount the DVD-ROM to a file system (using `SMIT` or the `mount` command).
4. Change to the DVD-ROM directory by typing:

   `cd /`<*directory*>**`/AIX`**

   where <*directory*> is your DVD-ROM directory.
5. Type **`ls`** to verify that you are in the correct directory. You will see the `install.ovpa` script, the `readme.ovpa` file, and the `paperdocs` and `rpmtools` directory listed on the screen.

   The `install.ovpa` script automatically starts all Performance Agent. If you do *not* want Performance Agent to start after installation, run the install script with the option `-R`.

   In case you intend to install Performance Agent in the cluster environment, check if `/usr/opt` and `/var/opt` are shared among cluster nodes. If they represent shared file systems, you should perform the following steps before you run the installation script:

   a. Create the following directories:

   ```
   mkdir /usr/opt/perf
   mkdir /var/opt/perf
   ```

b Make content-dependent symbolic links (CDSL):

```
mkcdsl -a /usr/opt/perf
mkcdsl -a /var/opt/perf
```

6 Run the installation script.

To install using the HTTP communication protocol, type:

```
./install.ovpa
```

The installation script automatically starts all Performance Agent processes. If you do *not* want Performance Agent to start after installation, run the installation script with the option `-R`.

The Performance Agent processes are also started or stopped automatically if you restart or shutdown. See Chapter 2, Starting and Running HP Performance Agent.

7 Exit the DVD-ROM directory by typing:

```
cd /
```

8 You can unmount the CD-ROM using `SMIT` or the `umount` command. by typing:

```
eject
```

`Unmount the CD-ROM`.

Performance Agent installation is now complete. Go to Chapter 2, Starting and Running HP Performance Agent for details on other tasks you need to perform to get Performance Agent up and running.

For instructions to install HP Operations Agent, see the Installation Guide for HP Operations Agent available at the following URL:

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

If you are also running the Glance product on your system, be sure to update GlancePlus to the same release version as Performance Agent. Both Performance Agent and GlancePlus must always be the same version.

Installing Performance Agent on Symbolic Links

If you do not have enough space in the default Performance Agent installation directory `usr/lpp/perf`, you can select an alternate directory (or directories) of your choice and symbolically link the `/usr/lpp/perf` to the required directories.

Run the following command for redefining the installation directory using symbolic links:

```
ln -s /<dir>/usr/lpp/perf /usr/lpp/perf
```

where <*dir*> refers to the directory of your choice.

During the installation process, the `install.ovpa` script traces the symbolic link(s) and continues with the installation displaying the following on-screen message(s):

```
NOTE: Found symbolic link for /usr/lpp/perf -> /<dir>/usr/lpp/perf
Installation will continue on this symbolic link
```

Installing Performance Agent with Operations Manager Installed on Your System

The presence of Operations Manager 8.xx agent on your system does not affect the default installation behavior of Performance Agent. During first time installation of Performance Agent on systems that have Operations Manager 8.xx agent installed, Performance Agent is started in the HTTP mode. If you are upgrading, Performance Agent is started in HTTP mode. For more information on how Performance Agent is installed, see Install Performance Agent on page 15.

Deploying Performance Agent Using Operations Manager

If you are using HP Operations Manager for UNIX 8.x, HP Operations Manager for UNIX 9.0, or HP Operations Manager for Windows 8.10, you can deploy HP Performance Agent from the management server to an IBM AIX managed node.

For details on deploying Performance Agent from the HP Operations Manager for UNIX mangement server see *HP Performance Agent Deployables for the HP-UX 11i v3, Linux 2.6 (RHEL 5.3 x64) and Solaris Operating Systems for HP Operations Manager for UNIX 8.x and 9.0*.

For details on deploying Performance Agent from the HP Operations Manager for Windows mangement server see the HP Operations Manager for Windows *Online Help*.

The install.ovpa Script

To install Performance Agent, you must run the `install.ovpa` script. This section describes the installation script command line options, which can be used for more advanced installations. The syntax of the command is as follows:

`install.ovpa [-hR]`

The command line options have the following meaning:

`-h`	Display this message and exit..
`-n`	Do not install. Only display the installation parameters and exit.

Removing Performance Agent

If you need to remove Performance Agent from a system, use the `ovpa.remove` script that is in the `/usr/lpp/perf/bin/` directory. However, before removing Performance Agent, make sure you archive any log files that were created. These files contain performance data for that system and can be used to extract or view data at a later time.

To uninstall Performance Agent from a system, do the following:

1. Log in as user **root**.
2. Change the directory path by typing:

   `cd /usr/lpp/perf/bin/`
3. Type **`ls`** to verify that the `ovpa.remove` script is available in this directory.
4. Run the uninstall script. To uninstall, type:

   `./ovpa.remove`

   Type **`y`** when asked for a confirmation to remove Performance Agent.

   A message displays, as follows:

   ```
   "Do you want to remove the Perf Agent configuration & logfiles
   in the /var/opt/perf/datafiles directory? You should not
   remove the logfiles if you plan to re-install Perf Agent and
   have not backed up your logfile data.

   Enter y to remove Perf Agent logfiles:"
   ```

   You need to confirm if you want to remove the Performance Agent configuration and logfiles. Answer **`N`** (no) if you want to keep the configuration and log files at the original location.

Note that these files will *not* be overwritten by a new Performance Agent installation. The new configuration files are uploaded to the `/usr/lpp/perf/newconfig` directory.

Some product packages might remain installed on the system, if those packages are shared across other HP Software products and are required by other tools. They are removed only when the last tool requiring them is also removed.

Performance Agent in a Virtualized Environment

Performance Agent installed on the LPARs provides a CEC (Central Electronics Complex) wide view. Performance Agent uses the RSI (Remote Statistics Interface) interface to discover all the LPARs configured on a CEC and to collect performance data (BYLS metrics) from the LPARs. The list of LPARs discovered using RSI interface is controlled through configuration file `Rsi.hosts`. The RSI interface searches for the configuration file in following directories (in the listed order): `$HOME`, `/etc/perf`, and `/usr/lpp/perfmgr`.

BYLS is a class of metrics that collects LPARs (and WPARs data on AIX 6.1 TL2) and is supported on IBM AIX 5L V5.3 ML3 and later.

If any LPARs are restricted from responding through the configuration file `Rsi.hosts` then information about those LPARs will not be available. For information on `Rsi.hosts`, refer to the latest IBM documentation on Remote Statistics Interface Programming.

Performance Agent might not always discover all the LPARs configured on the current CEC.

If the configuration file `Rsi.hosts` is not available, then the RSI interface sends invitational broadcast messages to all the systems within the network. From the list of systems which respond to the message, Performance Agent discovers LPARs configured on the CEC.

Some LPARs may not be reported by Performance Agent if they are not responding to RSI calls within the `timeout period`. This `timeout period` cannot be configured from Performance Agent.

Shared WPAR

Performance Agent can be installed in Shared WPAR on AIX 6.1 TL2.

Installing Performance Agent in Shared WPAR

You can install Performance Agent in Shared WPAR in the following ways:

- Execute `install.ovpa` script from Shared WPAR
- Execute **`syncwpar`** from global partition
- Execute **`syncroot`** from Shared WPAR

Prerequisites

You need to install Performance Agent in the global partition before installing Performance Agent on Shared WPAR.

If you do not install Performance Agent in global partition first, `install.ovpa` will report an error and abort the installation. The error message displays as follows:

```
"ERROR:   Install First on Global Partition"
```

Execute `install.ovpa` script from Shared WPAR

This is the recommended method of installation as the script triggers the daemons to start functioning.

1. Install Performance Agent in the global partition. To install, type the following command:

   `./install.ovpa`

2. Login to Shared WPAR. To login, type the following command:

   `clogin` <*Shared WPAR name*>

3. Install Performance Agent in Shared WPAR. To install, type the following command:

   `./install.ovpa`

Execute **syncwpar** from global partition

1. Install Performance Agent in the global partition. To install, type the following command:

   ./install.ovpa

2. To install the package in Shared WPAR, type the following command:

   syncwpar <*Shared WPAR name*>

   If you want to update all Shared WPARs, type the following command:

   syncwpar -A

   This will install the package in Shared WPAR but the daemons do not start automatically. You need to start the daemons manually.

3. Login to Shared WPAR. To login, type the following command:

   clogin <*Shared WPAR name*>

4. To start the daemons, type the following command:

   ovpa start

Execute **syncroot** from Shared WPAR

1. Install Performance Agent in the global partition. To install, type the following command:

   ./install.ovpa

2. Login to Shared WPAR. To login, type the following command:

   clogin <*Shared WPAR name*>

3. To install the package in Shared WPAR, type the following command:

   syncroot

   This will install the package in Shared WPAR but the daemons do not start automatically. You need to start the daemons manually.

4. To start the daemons, type the following command:

   ovpa start

Removing Performance Agent in Shared WPAR

You can uninstall Performance Agent in Shared WPAR in following three ways.

- Uninstall using `ovpa.remove` script
- Uninstall using **`syncwpar`** command from global partition
- Uninstall using **`syncroot`** command from Shared WPAR

Uninstall using `ovpa.remove` script

This is the recommended way to uninstall Performance Agent from Shared WPAR.

1. Login to Shared WPAR. To login, type the following command:

   `clogin` <*Shared WPAR name*>

2. Uninstall Performance Agent from Shared WPAR. To uninstall, type the following command:

   `./ovpa.remove`

3. Uninstall Performance Agent from global partition. To uninstall, type the following command:

   `./ovpa.remove`

   This will remove Performance Agent from Shared WPAR and the global partition.

Uninstall using **`syncwpar`** command from global partition

1. Uninstall Performance Agent from global partition. To uninstall, type the following command:

   `./ovpa.remove`

2. To uninstall the package in Shared WPAR, type the following command:

   `syncwpar` <*Shared WPAR name*>

   If you want to uninstall from all Shared WPARs, type the following command:

   `syncwpar -A`

3 Login to Shared WPAR. To login, type the following command:

clogin <*Shared WPAR name*>

4 From root, change the directory path by typing:

cd /var/opt/perf

Delete all files in the directory. This will remove Performance Agent from the global partition and the Shared WPAR.

Uninstall using **syncroot** command from Shared WPAR

1 Uninstall Performance Agent from global partition. To uninstall, type the following command:

./ovpa.remove

2 Login to Shared WPAR. To login, type the following command:

clogin <*shared WPAR name*>

3 To uninstall the package in Shared WPAR, type the following command:

syncroot

You need to execute the command for all the Shared WPAR where Performance Agent is Installed.

4 From root, change the directory path by typing:

cd /var/opt/perf

Delete all files in the directory. This will remove Performance Agent from the global partition and Shared WPAR.

`ovtrc, ovcd,` and `coda` daemons are not killed when **syncroot** or **syncwpar** is used after uninstallation. You need to manually kill them.

To kill, type the following command:

kill -9 *<pid>*

2 Starting and Running HP Performance Agent

If you are planning to log data from other sources using data source integration (DSI), and have *not* yet done so, read the *HP Performance Agent for UNIX Data Source Integration Guide*.

Starting and Stopping Performance Agent

The `mwa` and `ovpa` scripts allow you to perform the following tasks

- Start all or some of the processes
- Stop or restart processes that are currently running

It is recommended that you use the `ovpa` script to start Performance Agent and enable the HTTP data communication protocol.

The following table lists the different services that are started for the http protocol.

Services started for HTTP protocol
`scopeux`
`coda`
`perfalarm`
`midaemon`
`ttd`

Services started for HTTP protocol
ovc
ovbbccb

Before you start Performance Agent, check to see if any processes are running by typing:

/usr/lpp/perf/bin/perfstat

Using the Performance Agent Script

1. Log in as user **root**.
2. Type: **/usr/lpp/perf/bin/ovpa start** for Performance Agent
   /usr/lpp/perf/bin/mwa start for mwa

   The `ovpa start` or `mwa start` script starts Performance Agent and all its processes, including the `scopeux` (data collector), `midaemon` (measurement interface daemon), `ttd` (transaction tracking daemon), `coda`, `ovc`, `ovbbccb` and the alarm generator. As the script executes, the status of the processes that are started is displayed on the screen.

You can stop Performance Agent processes while they are running and restart them using the `ovpa` or `mwa` script and appropriate options.

- `ovpa stop or mwa stop` stops all Performance Agent processes except `ttd` (the transaction tracking daemon), `ovc` and `ovbbccb`. These processes must always be left running. If Operations Manager agent is running on the system, `ovpa stop` does not stop the `coda` daemon.

If you must stop `ttd`, any ARM-instrumented applications that are running must also be stopped before you restart `ttd` and Performance Agent processes.

- The command `ovpa stop scope` stops `scope`, and it also stops `midaemon` if no other application is attached to `midaemon`.

Individual components can be re initialized as well with the `ovpa restart or mwa restart` option. Changes to configuration files will not take effect on your system unless the corresponding process is restarted.

- `ovpa restart server` or `mwa restart server` causes `coda` to stop and then start, temporarily disabling alarming and access for clients such as Performance Manager, and rereads the `datasources` file. It also stops and then restarts the `perfalarm` process and rereads the `alarmdef` file.
- `ovpa restart or mwa restart` causes `scopeux` and the server processes to temporarily stop and then start. It reads the `parm` file as well as forces the transaction daemon `ttd` to reread its configuration file `ttd.conf`.
- `ovpa restart alarm` or `mwa restart alarm` causes the `perfalarm` process to temporarily stop and then start and reread the `alarmdef` file, so that if you have made changes to the file, the new alarm definitions will take effect without restarting all Performance Agent processes. This action does *not* disrupt any other process.

Starting Performance Agent Automatically

The process of starting Performance Agent automatically whenever the system reboots and to stop when the system shuts down is controlled by the file `/etc/inittab`.

If you do *not* want Performance Agent to start automatically, remove the line that begins with `mwa` in the file `/etc/inittab` or set the variable `MWA_START =0` in the `/etc/default/ovpa` file.

The /etc/default/ovpa File

The `/etc/default/ovpa` file is available with Performance Agent. The file contains various environment variables that control the behavior of Performance Agent when starting it. The file is a source file for the following scripts:

- `/usr/lpp/perf/bin/ovpa` Performance Agent control script

- `/etc/rc.ovpa` Performance Agent auto-start script

The file is removed only when Performance Agent is removed from a system and is *not* overwritten when Performance Agent is updated. When Performance Agent is updated, a copy of the default `/etc/default/ovpa` file is left in the `/usr/lpp/perf/newconfig` directory under the name `ovpa.default` so that your customized copy does *not* get affected.

The environment and shell variables that can be modified to change the default behavior of Performance Agent are listed below.

- `MWA_START` controls the auto-start of Performance Agent whenever your system reboots. The variable can have one of the following values:

0 do *not* start Performance Agent at the system boot

1 start Performance Agent at the system boot

- The `MWA_START_COMMAND` contains a variable that is used to start Performance Agent whenever your system reboots. Normally, the variable is set to `/usr/lpp/perf/bin/mwa start`.

Status Checking

Several status files are created in the `/var/opt/perf/` and `/var/opt/OV/` directories when Performance Agent is started. You can check the status of all or some Performance Agent processes using the `perfstat` command.

The following status files contain diagnostic information you can use to troubleshoot problems that may arise with the Performance Agent processes.

```
/var/opt/perf/status.scope
/var/opt/perf/status.perfalarm
/var/opt/perf/status.ttd
/var/opt/perf/status.mi
/var/opt/perf/status.ls
/var/opt/OV/log/coda.txt
```

Every time the Performance Agent process writes a message to its status file, it checks to see if the file is larger than one MB. If it is, the file is renamed to `status.filename.old` and a new status file is created.

Examples Directory

The `/usr/lpp/perf/examples` directory contains examples of configuration files, syntax files, and sample program files that can be used to customize your HP Performance Tools. For example, the `/example/ovpaconfig/` subdirectory contains sample alarm definitions and examples of `parm` file application-specific parameters. For more information, see the `/usr/lpp/perf/examples/README` file.

Communicating Across a Firewall

A firewall can be defined as a method for filtering the flow of data between one network and another. Performance Agent supports HTTP 1.1-based communications interface for data access between clients such as Performance Manager and Reporter and server applications, in addition to the previously supported communication mechanism through a packet-filtering network firewall.

Performance Agent supports certificate-based secure (HTTPS) data communication only in the Operations Manager 8.xx environment. For more information, see Using Certificates on page 37.

The HTTP-based interface is flexible, because it can use proxies, requires fewer ports, and is firewall friendly.

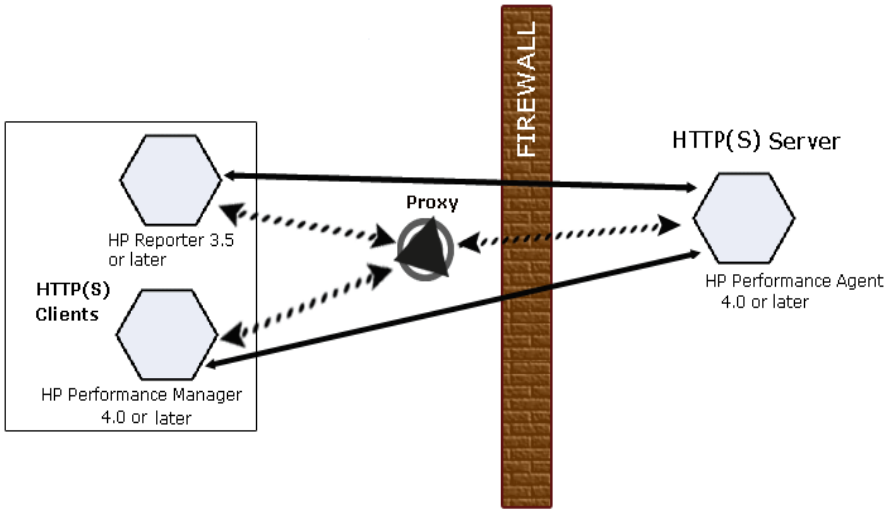
The following sections explain how to configure HTTP communication across a firewall.

The name Performance Manager 3.xx refers to the product that was formerly known as PerfView.

Communicating in the HTTP Environment

It is important to know which system initiates the communication (client) and which receives communication requests (server), so that the firewall rules can be set up. In a typical remote communication, a client, using the source port, connects to a server that is listening on the destination port on a remote system.

The following figure shows how Performance Agent communicates with Reporter (version 3.50 or later) and Performance Manager (version 4.00 or later) through a firewall. Performance Agent is an HTTP or HTTPS server. Reporter and Performance Manager 4.xx are HTTP clients. Performance Manager 5.00 can be an HTTP or HTTPS client. If an HTTP proxy is used, Reporter and Performance Manager communicate with Performance Agent through the proxy.



Configure Performance Agent Ports

You can configure Performance Agent ports in a firewall environment in following ways.

On a Performance Agent system using BBC5, by default, the BBC communication broker uses port 383, and `coda` uses a dynamically allocated port.

Configure Port Settings for the BBC Communication Broker

You can configure the port settings of the default port used by the BBC communication broker. Use the `ovconfchg` command to change the port settings on the Performance Agent system. You can use one of the following options:

— **`ovconfchg -ns bbc.cb -set SERVER_PORT <`***`port`***`>`**

Or

— **ovconfchg -ns bbc.cb.ports -set PORTS <*domain*>:<*port*>**

Example: **ovconfchg -ns bbc.cb.ports -set PORTS xyz.abc.com:50383**

The second option is the preferred way of changing ports.

Restart ovpa using the following command:

```
ovpa restart server
```

Configure Two-Port Communication

By default, the `coda` daemon uses a dynamically chosen second port, in addition to port 383 used by the BBC communication broker. You can configure the port settings of `coda` to listen at a well-known port of your choice using the `ovconfchg` command. Type the following commands:

```
ovconfchg -ns coda.comm -set SERVER_PORT <portnumber>

ovpa restart server
```

Using a dynamic port when connecting to Performance Agent remotely through a firewall can be difficult, because you may not know which firewall ports to open.

Configure Single-Port Communication

On the Performance Agent system, the BBC communication broker uses port 383, and `coda` uses a port that is dynamically allocated. You can configure the port settings for `coda` to share the same port used by the communication broker using the `ovconfchg` command. Type the following commands:

```
ovconfchg -ns coda.comm -set SERVER_BIND_ADDR localhost

ovpa restart server
```

To enable two-port communication from single-port communication, type the following command:

```
ovconfchg -ns coda.comm -set SERVER_BIND_ADDR
```

Verify Port Settings

To verify the port settings, type the following command:

```
perfstat -d
```

The output displays the following information:

- Port number of the port used by `Coda`
- Port number of the port used by `BBC communication broker`
- The port settings configured
- Whether secure communication is enabled
- Whether `coda` metric collection is enabled

For example:

```
Datacomm configuration :
------------------------
 Coda Port                          49552 (Dynamic)
                                    Two port Communication
 BBC communication broker port           383
 SSL security                            NONE
 Coda Metric Collection(Prospector)      Disabled
```

Configure HTTP Clients in a Firewall Environment

You can configure HTTP clients in a firewall environment in the following ways:

To access data from Performance Agent nodes, only one port needs to be opened on the HTTP server (Performance Agent) side.

Configuring HTTP Clients (Reporter/Performance Manager) with HTTP Proxy

It is recommended that you use HTTP proxies when communicating through a firewall. This simplifies the configuration by using proxies that are often already in use in your environment. The firewall must be open for exactly one port if proxies are to be used in both directions. To access data collected by Performance Agent, ports for the HTTP server (Performance Agent) and the HTTP client (Reporter and Performance Manager) must be opened.

It is recommended that you do not change the default 383 port.

When an HTTP proxy is used, Reporter and/or Performance Manager for Windows and UNIX need to be configured to specify the proxy to be used to contact Performance Agent.

To configure Performance Manager versions 5.00 and later, and Reporter 3.7x and later, type the following command:

ovconfchg -ns bbc.http -set PROXY proxy:port+(a)-(b)

The variables *a* and *b* are comma-separated lists of hostnames, networks, and IP addresses that apply to the proxy. Multiple proxies may be defined for one PROXY key using the "*;*" or "*,*" delimiter. "-" before the list indicates that those entities do not use this proxy, "+" before the list indicates that those entities do use this proxy. The first matching proxy is used.

To configure Reporter versions 3.60 and earlier, and Performance Manager 4.xx, edit the `/var/opt/OV/conf/BBC/default.txt` configuration file.

In the `[DEFAULT]` section of the `default.txt` file, locate the lines that relate to the `PROXY` and set the `PROXY` parameter as follows.

PROXY web-proxy.hp.com:8088-(localhost, *.hp.com) + (*)

In this example, the proxy `web-proxy` will be used with port 8088 for every server (*) except requests for the local machine (localhost) and requests internal to HP (matching *.hp.com, for example **www.hp.com**.

Configuring HTTP Clients (Reporter/Performance Manager) without HTTP Proxy

If HTTP proxies are not available, additional configuration settings are required on the HTTP clients (Reporter and Performance Manager system).

If Reporter and Performance Manager for Windows are installed on the same system and both access Performance Agent in parallel, you can specify a port range as described in this section. If they are running on different systems, you can specify a single-port for each. Depending on the versions of Performance Manager and Reporter you are using, select from the following options:

Configure Performance Manager 5.00 and later, and Reporter 3.7x by typing the following command:

ovconfchg -ns bbc.http -set CLIENT_PORT <*port range*>

In this instance <*port range*> is the range of ports you want to use. For example:

ovconfchg -ns bbc.http -set CLIENT_PORT 14000-14003

Configure Reporter versions 3.60 and earlier, and Performance Manager 4.xx by editing the `/var/opt/OV/conf/BBC/default.txt` file as follows.

1. Locate the lines that apply to `CLIENT_PORT` and uncomment the line `;CLIENT_PORT =`.
2. Specify the port range for the `CLIENT_PORT` parameter; for example:

   ```
   CLIENT_PORT = <port range>
   ```

   In this instance, *<port range>* is the range of ports you want to use; for example:

   ```
   CLIENT_PORT = 14000-14003
   ```

Verify Firewall Configuration

To verify your configuration, run the following command:

ovcodautil -ping -n <*system name***>**

This output of this command indicates the status of your communication settings.

Configuring Systems with Multiple IP Addresses

If your environment includes systems with multiple network interfaces and IP addresses, and you want to use a dedicated interface for the HTTP-based communication, you can use the parameters `CLIENT_BIND_ADDR` and `SERVER_BIND_ADDR` to specify the IP address that should be used.

- If you have multiple network interfaces and IP addresses on the Performance Agent (Server) system, specify the `SERVER_BIND_ADDR` parameter as follows:

  ovconfchg -ns bbc.http -set SERVER_BIND_ADDR <IP Address>

- If you have multiple network interfaces and IP addresses on the Performance Manager 5.00 (client) system, specify the `CLIENT_BIND_ADDR` parameter as follows:

  ovconfchg -ns bbc.http -set CLIENT_BIND_ADDR <IP Address>

- If you have multiple network interfaces and IP addresses on the Reporter/ Performance Manager 4.xx system, specify the `CLIENT_BIND_ADDR` parameter.

Edit the `/var/opt/OV/conf/BBC/default.txt` file as follows:

— Locate the lines that apply to `CLIENT_BIND_ADDR` and uncomment the line
`;CLIENT_BIND_ADDR =`

— Specify the IP address for the `CLIENT_BIND_ADDR` parameter.

Configuring Secure Communication

Performance Agent supports certificate-based secure communication and client authentication based communication.

Using Certificates

Performance Agent supports certificate-based secure data communication only in the Operations Manager 8.xx environment.

To configure secure communication on your Operations Manager setup, see the *HP Operations Manager for UNIX Firewall Concepts and Configuration Guide*. For more information on Operations Manager 8.xx HTTPS agent, see the *HP Operations Manager HTTPS Agent Concepts and Configuration Guide*.

If you have already configured HTTPS communication in the Operations Manager 8.xx environment, make the following changes to configure secure communication between Performance Agent and Performance Manager 5.00.

Reporter and Performance Manager 4.xx do not support certificate-based secure communication.

On the Performance Agent system, set `SSL_SECURITY` to `REMOTE` for `coda`. Type the following commands:

```
ovconfchg -ns coda -set SSL_SECURITY REMOTE
ovcodautil -config
```

Using Client Authentication

Performance Agent enables optional authentication of client connections from products such as, Performance Manager or Reporter (Service Reporter). The authentication capability allows you to specify, for a given Performance Agent instance, which hosts are allowed to make client connections to that instance.

The Client Authentication feature enables/disables connections from any version of the Performance Manager and Reporter clients. Your client software does *not* need to be updated for you to take advantage of this feature.

For authorized clients the authentication process is transparent, their client connection proceeds as it has with previous versions of Performance Agent. Unauthorized clients receive a message indicating denial of service, for example:

```
Could not connect to Performance Agent data source on host
<hostname>.
```

Enabling Authentication with the authip File

Authentication is enabled by the presence of a file called `authip`. On systems where HTTP communication is enabled, the `authip` file exists in the `/var/opt/OV/conf/perf/` directory.

- If the `authip` file exists in the default directory, its contents determine which hosts are permitted client connections. Clients running on the same host as the Performance Agent instance are automatically authenticated, which means the clients do *not* need an entry. A zero-length `authip` file dictates that only clients running on the Performance Agent host can connect.
- If the `authip` file does *not* exist in the default directory, no authentication is performed and any client will be allowed to connect, as was the case with prior Performance Agent versions.

The `authip` file is checked each time a client attempts to register for service with Performance Agent. Performance Agent does *not* need to be restarted for changes to the `authip` file to become effective.

An existing authorized client session can continue its current connection despite a subsequent change in the server's `authip` file, which would otherwise disqualify it, until the client takes an action that requires re-registration with Performance Agent. Thus, an authorized Performance Manager connection continues to be permitted, regardless of changes in the Performance Agent `authip` file, until the data source to the Performance Agent host has been closed. If there is then an attempt to reopen the data source, the `authip` file is reread and the connection is denied.

In the case of Performance Manager registration for alarms, a previously authorized client will continue to receive alarms until the data source has been removed (not just closed) by the client. To force removal of a client from the server's alarm generator database from the Performance Agent side, use the command:

`agsysdb -delpv <host>`

The Performance Agent client authentication capability requires that your network be able to resolve the client entries in the `authip` file. Depending on the nature of the entries, this may require name services such as those provided by DNS, NIS, or `/etc/hosts` files.

A good test is to ensure that you can successfully "ping" each `authip` entry from the Performance Agent host. Client authentication works through a firewall with the same proviso that the client entries in the `authip` file be pingable from the Performance Agent host.

Formatting the authip File

The `authip` file must conform to the following format:

- One client host may be listed per line.
- Client entries can be in any one of the following formats:
  - Fully qualified domain name
  - Alias
  - IP address (must be in IPv4 dotted quad format)
- Client entries can have no embedded spaces.
- A line containing a `#` in the first column is taken as a comment, and is ignored.
- Blank or zero-length lines are ignored.
- The IP address may *not* have a leading zero. For example, the IP address 23.10.10.10 cannot be represented as `023.10.10.10`.

  Thus, given the following `/etc/hosts` entry:

  ```
  123.456.789.1 testbox testbox.group1.thecompany.com
  ```

  any one of the following entries in the `authip` file would enable clients from the `testbox` host to connect:

  ```
  #============ Examples of authip file entries ==============
  #
  # Use of an IP address
  123.456.789.1
  ```

```
#
# Use of an alias
testbox

#
# Use of a fully qualified domain name
testbox.group1.thecompany.com

#============ End of examples of authip file entries ========
```

Configuring HP Performance Agent to Run on a Cluster Node

Performance Agent running in HTTP mode can run on a cluster node, that is on systems running HACMP for AIX software. To run on a cluster node Performance Agent has to have a fixed, always accessible IP address available.

- If on the cluster node, Operations Manager agent is installed and running, use the Operations Manager agent's IP alias (<*systemname*>_ito). For more information see the *HP Operations Manager for UNIX Administrator's Reference Volume II*. Proceed with Troubleshooting Hints on page 42.
- If an additional adapter (that is, network interface card) with a fixed IP address that is not used by HACMP (as a boot, service, or standby adapter) is available on a HACMP node, you can use this adapter's IP as the fixed, always accessible IP address used by Performance Agent. Proceed with Troubleshooting Hints on page 42.
- If none of the above is available on your cluster node you will have to assign each node an IP alias in the same network in which the boot and service IP addresses reside. In addition, you must configure the node in such a way that this IP alias address is assigned to the service adapter as an alias for the boot IP address. To set the IP alias proceed with the following section.

Naming Scheme for IP Addresses

Using a standard naming scheme in your cluster environment will help you avoid confusion with the following:

- IP Addresses

  Other IP addresses that may be set on the interface.

- Messages

  Messages in the message browser originating from addresses other than the service address of the system.

Use the following naming scheme in your cluster environment:

<*systemname*>_boot	Boot address of a system
<*systemname*>_svc	Service address of a system
<*systemname*>_stdby	Standby address of a system
<*systemname*>_mwa	IP alias of a system

In this naming scheme, <*systemname*> is the name of the system as defined in the cluster configuration.

To Set an IP Alias

Before running Performance Agent on a cluster node, you *must* set an IP alias on each system on which you wish to run the Performance Agent.

To set an IP alias, follow these steps:

1. Use the System Management Interface Tool (SMIT) menus.
2. In a shell, enter the following command:

   smit tcpip

3. Select the following from the menu bar:

   Further Configuration -> Network Interface Selection -> Configure Aliases -> Add an IPV4 Network Alias

4. Select the interface you want (for example, en0).
5. Enter values for the IP address and network mask.

Troubleshooting Hints

The following topics are described in this section:

- Possible problems

Problems you may encounter when running Performance Agent on a cluster node with workarounds.

- Fixing problems with IP aliases

  Useful information on how to fix problems with IP aliases if you are using HACMP for AIX software.

Possible Problems

After a cluster is switched on/off, Performance Agent servers cannot be restarted. The problem occurs in one of the following cases:

- If HTTP was started prior to running the cluster when the cluster was still inoperative.

  Workaround:

  a. Stop your cluster software. For information on how to do that, refer to your HACMP documentation.

  b. Stop the HTTP daemon.

  c. Run your cluster software. For information on how to do that, refer to your HACMP documentation.

  d. Start the HTTP daemon.

  e. Make sure there is no Performance Agent server running on your system, else you will have to stop them.

  f. Start the Performance Agent.

- If HTTP was started prior to stopping the cluster when the cluster was still active.

  Workaround:

  a. Start your cluster software. For information on how to do that, refer to your HACMP documentation.

  b. Stop the HTTP daemon.

  c. Stop your cluster software. For information on how to do this, refer to your HACMP cluster documentation.

  d. Start the HTTP daemon.

  e. Make sure there is no Performance Agent server running on your system, else you will have to stop them.

f Start Performance Agent.

Fixing Problems with IP Aliases

Once you set the IP alias for Performance Agent on AIX, HACMP no longer works correctly. This problem applies to *all* events that deal with IP addresses (for example, `acquire service address`, `acquire takeover address`, `swap adapter`, and so on). This problem results from a flaw in the AIX operating system.

To fix AIX problems with IP aliases and HACMP, follow these steps:

1 Download and install the appropriate fixes for the AIX operating system.

You can get the fixes with the IBM "FixDist" package or from the IBM website.

For systems where AIX operating system fixes have already been installed, refer to To Reset Events on HACMP 4.2.2 on page 45.

To get the fixed versions of related packages, use the following APAR:

`IX78397`

2 Reset IP aliases on the network interface card.

Once you have installed the fixes to the AIX operating system, all HACMP events work, and the IP alias is set on the interface. However, the IP alias address no longer works after the `ifconfig` command is used to change the main IP address on the interface. For this reason, you have to reset the IP alias on the interface after each change of the IP address. For instructions, see To Reset the IP Alias on the Network Interface Card.

You have to reset the IP alias on all cluster systems where Performance Agent is to be installed.

To Reset the IP Alias on the Network Interface Card

To reset the IP alias on the interface where the service or boot IP address is set, use the following shell script (from here on referred to as `set_alias` script):

```
#!/bin/sh
# Specify MWA alias IP address below
ALIAS_IP="0.0.0.0"
SERVICE_IP=`/usr/sbin/cluster/utilities/cllsif -cSi \
```

```
  $LOCALNODENAME | grep ":service:.*:ether" | cut -d: -f7 |\
uniq`
BOOT_IP=`/usr/sbin/cluster/utilities/cllsif -cSi \
$LOCALNODENAME |\
  grep ":boot:.*:ether" | cut -d: -f7 | uniq`
INTERFACE=`/usr/sbin/cluster/utilities/clgetif -a
$SERVICE_IP`
if [ $? -ne 0 ]; then
  INTERFACE=`/usr/sbin/cluster/utilities/clgetif -a $BOOT_IP`
fi
if [ "$INTERFACE" != "" ]; then
  #IP has changed, set IP alias again on interface with
SERVICE_IP
  /usr/sbin/ifconfig $INTERFACE $ALIAS_IP alias
fi
```

The *ALIAS_IP* variable should contain the same IP address you used to install the Performance Agent. If you copy the shell script to other systems in the cluster, make sure to change the *ALIAS_IP* variable. The shell script gets service and boot IP addresses for the local system, and sets the IP alias on the interface where either of the two was found.

In addition, you can use the `set_alias` script as the post-event script for the following HACMP events:

- Acquire service address
- Release service address
- Swap adapter

To Reset Events on HACMP 4.2.2

To reset events on HACMP 4.2.2, follow these steps:

1. Use the `SMIT` screens by entering the following command in a shell:

   `smit hacmp`

2. Select the following:

   Cluster Configuration -> **Cluster**

   Resources -> **Change/Show Cluster Events**

3. Select the appropriate option from the list, and fill in the `Post-event Command` field.

You can put the set_alias script in the following directory:

/usr/sbin/cluster/local

To Reset Events on HACMP 4.3.1

To reset events on HACMP 4.3.1, follow these steps:

1. Use the SMIT screens by entering the following command in a shell:

   smit hacmp

2. Go into the Cluster Events menu.
3. Select the following:

   Cluster Configuration -> Cluster Resources -> Cluster Events

4. Add the set_alias script to the Known Cluster Events list.
5. Select the following:

   Define Custom Cluster Events -> Add a Custom Cluster Event

6. Set the following:

   Cluster Event Name Set to set_alias

   Cluster Event Description Set to MWA set_alias

   Cluster Event Script Filename Set to /usr/sbin/cluster/local/set_alias

   Then click **[OK]**.

7. Assign it to all appropriate events.

   Press **Cancel** to go to the previous level. Then select **Change/Show Cluster Events**.

8. Select the appropriate option and enter **set_alias** in the Post-event Command field for each event:

   - acquire service address
   - release service address
   - swap adapter

Configuring Data Sources

Performance Agent uses the coda daemon to provide collected data to the alarm generator and the Performance Manager analysis product. The coda daemon uses the HTTP data communication mechanism. Each data source consists of a single log file set.

The data source list that coda accesses is maintained in the datasources configuration file that resides in the /var/opt/OV/conf/perf/ directory.

When you first start up Performance Agent after installation, a default data source named SCOPE is already configured and provides a scopeux log file set. If you want to add other data sources, you can configure them in the datasources file. Then, when you restart Performance Agent the coda daemon reads the datasources file and makes the data available over datacomm linkages to analysis tools for each data source it finds.

You can also remove the log file set if you no longer need the data. If you remove the log file set but do not remove the data source from datasources, coda will skip the data source.

You might also choose to stop logging DSI data to a log file set but keep the coda daemon open so you can view the historical data in Performance Manager. In this case, stop the dsilog process but do not delete the data source from the datasources file.

Datasources Configuration File Format

Each entry you place into the datasources configuration file represents a data source consisting of a single log file set. The entry specifies the data source name and location. Fields are case-insensitive except for the log file path name. The syntax is:

datasource=datasource_name logfile=logfile_set

- **datasource** is a keyword and it is case-insensitive. **datasource_name** is the name used to identify the data source. For example, the data source name used in alarm definitions or by analysis software. Data source names must be unique. They are translated into upper case. The maximum length for a data source name is 64 characters.

- **logfile** is a keyword. **logfile_set** is the fully-qualified name identifying the DSI log file (created by the `dsilog` process, ending in `.log`), and is case-sensitive.

Following are two examples of the `datasources` file's data source entries:

```
DATASOURCE=SCOPE LOGFILE=/var/opt/perf/datafiles/logglob
datasource=ASTEX logfile=/tmp/dsidemo/log/astex/ASTEX_SDL
```

After updating `datasources`, run the following command to make the new data sources available through `coda`:

```
/usr/lpp/perf/bin/ovpa restart server
```

Examine the contents of the `/var/opt/OV/log/coda.txt` file to check if the `coda` daemon was activated or for error messages.

For specific examples of configuring DSI data sources, see "Configuring Data Sources" in Chapter 4 of the *HP Performance Agent for UNIX Data Source Integration Guide*.

Parm File

The `parm` file is a text file that specifies configuration of the `scopeux` data collector including log file maximum sizes, interesting process threshold definitions, and application definitions. Comments in the file provide an overview of the various settings.

The `parm` file is provided with Performance Agent in the `/usr/lpp/perf/newconfig/` directory and is copied into the `/var/opt/perf/` directory during installation, if there is not an existing `/var/opt/perf/parm` file. For a complete description of the `parm` file and its parameters, see the "Parm File" section in Chapter 2 of the *HP Performance Agent for UNIX User's Manual*.

Defining Alarms

If you plan to use alarms to monitor performance, you need to specify the conditions that generate alarms in a set of alarm definitions in the Performance Agent `alarmdef` file which is a text file. When Performance Agent is first installed, the `alarmdef` file contains a set of default alarm definitions. You can use these default definitions or customize them to suit your needs.

For instructions on defining alarms, see Chapter "Performance Alarms," in your *HP Performance Agent for UNIX User's Manual*. This chapter also describes the alarm definition syntax, how alarms work, and how alarms can be used to monitor performance.

Performance Agent Documentation

Performance Agent software includes the following documents. You can view the Adobe Acrobat format (`*.pdf`) documents online and print them as needed. ASCII text (`*.txt`) documents are printable. You can view a text file on your screen using any UNIX text editor such as `vi`.

Document	File Name	Format
HP Performance Agent for IBM RS/6000 systems Installation & Configuration Guide	`ovpainst.pdf`	`/usr/lpp/perf/paperdocs/ovpa/C/`
HP Performance Agent for UNIX User's Guide	`ovpausers.pdf`	`/usr/lpp/perf/paperdocs/ovpa/C/`
HP Performance Agent for UNIX Data Source Integration Guide	`ovpadsi.pdf`	`/usr/lpp/perf/paperdocs/ovpa/C/`
HP Performance Agent & GlancePlus for UNIX Tracking Your Transactions	`tyt.pdf`	`/usr/lpp/perf/paperdocs/ovpa/C/`
Application Response Measurement (ARM) API Guide	`arm2api.pdf`	`/usr/lpp/perf/paperdocs/arm/C/`
HP Performance Agent AIX Metric Definitions	`metaix.txt`	`/usr/lpp/perf/paperdocs/ovpa/C/`
HP Performance Agent Metrics list by Data Class for all operating systems	`mettable.txt`	`/usr/lpp/perf/paperdocs/ovpa/C/`

ASCII Text Files

To print a `.txt` file, type:

`lp -dprintername` *filename*

For example,

`lp -dros1234 metaix.txt`

A Configuring Coda

Coda is a lightweight data collection agent for HP Operations Agent. It is a subset of Performance Agent and acts as a communication conduit for Performance Agent. All the configuration parameters are configured under the namespaces `coda` and `coda.comm` using the command `ovconfchg`.

Coda Namespace Configuration Parameters

Parameters in coda namespace	Description	Default Value
DISABLE_PROSPECTOR	Used to disable data collection from coda datasource in a coexistence environment of HP Operations Agent and Performance Agent	false

Parameters in coda namespace	Description	Default Value
ENABLE_PROSPECTOR	Used to enable data collection from coda datasource in a standalone environment of Performance Agent	false
SSL_SECURITY	Used to enable secure communication from coda	NONE
RESPONSE_SIZE_LIMIT	Used to specify the maximum amount of memory allocated by coda	104857600 (100 megabytes)

DISABLE_PROSPECTOR

Use this option to specify the data collection preferences through coda, when both the HP Operations Agent and Performance Agent are installed. The default value is `false`. The format is as follows:

`ovconfchg -namespace coda -set DISABLE_PROSPECTOR` <*value*>

- `true`: `coda` will not collect data for the Coda datasource
- `false`: `coda` will collect the data for the Coda datasource

ENABLE_PROSPECTOR

Use this option to specify the data collection preferences through coda, when only Performance Agent is installed. The default value is `false`. This parameter is ignored in a coexistence scenario. The format is as follows:

`ovconfchg -namespace coda -set ENABLE_PROSPECTOR` <*value*>

- `true`: `coda` will collect data for the Coda datasource
- `false`: `coda` will not collect data for the Coda datasource

To verify if coda prospector is enabled, type the following command:

ovcodautil -dumpds coda

SSL_SECURITY

Use this option to enable secure communication through coda. The default value is NONE. The format is as follows:

ovconfchg -namespace coda -set SSL_SECURITY <*value*>

- NONE: coda does not require SSL connections for either the local or remote clients
- REMOTE: coda requires all remote connections to use SSL
- ALL: coda requires all connections (both local and remote) to use SSL

Use this parameter only when certificates are present on the system. Certificates are installed only if HP Operations Agent 8.xx is present on the system.

RESPONSE_SIZE_LIMIT

Use this command to specify the maximum amount of memory allocated by the coda daemon for a query response. The default value is 104857600 (100megabytes). The format is as follows:

ovconfchg -namespace coda -set RESPONSE_SIZE_LIMIT <*value*>

If the specified limit is exceeded, the following error message appears:

```
Response exceeds memory limits, use several smaller requests
```

Coda Communication Namespace (coda.comm) Configuration Parameters

Parameters in coda.comm namespace	Description	Default Value
SERVER_PORT	Used to configure port settings	0
SERVER_BIND_ADDR	Used to specify bind address for the server port	INADDR_ANY
LOG_SERVER_ACCESS	If set to 'true', coda logs every access to the server providing the information about sender's IP address, requested HTTP address, requested HTTP method, and response status.	false

SERVER_PORT

You can configure the port settings of the default port used by coda. The default value for this port is `0`. If the port is set to `0`, the operating system assigns the first available port number. Use the `ovconfchg` tool to change the port settings on the Performance Agent system. Type the command:

`ovconfchg -namespace coda.comm -set SERVER_PORT` <*port no*>

SERVER_BIND_ADDR

Use this option to specify the bind address for the server port. When the value is set to localhost, all the communication to coda server takes place through `ovbbccb`. The format is as follows:

`ovconfchg -namespace coda.comm -set SERVER_BIND_ADDR` <*Bind address*>

LOG_SERVER_ACCESS

You can enable or disable the access to server using this option. If this option is set to `true`, coda records every access to the server, providing information about the sender's IP address, requested HTTP address, requested HTTP method, and response status. This value typically is not changed.

`ovconfchg -namespace coda.comm -set LOG_SERVER_ACCESS` <*value*>

Single-Port Communication

This is the default communication method with Performance Agent 4.70. Use the following options to enable single-port communication in coda:

ovconfchg -ns coda -set SSL_SECURITY REMOTE/ALL

ovconfchg -ns coda.comm -set SERVER_BIND_ADDR localhost

Multi-Port Communication

Use the following option to enable multi-port communication in coda:

ovconfchg -ns coda.comm -set SERVER_BIND_ADDR ""

There are two methods to find out single-port and multi-port communication in `coda`:

- You can use this option to verify if the port is used for single-port or multi-port communication from the local host machine:

  bbcutil -reg

  For single-port communication,

  ```
  BasePath=/Hewlett-Packard/OpenView/Coda/
  Protocol=HTTPS
  BindAddress=localhost
  Port=59814
  Authentication=NONE
  ```

  If the value returned is `local host` or `127.0.0.1`, then it is single-port communication.

  For multi-port communication,

  ```
  BasePath=/Hewlett-Packard/OpenView/Coda/
  Protocol=HTTPS
  BindAddress=ANY
  Port=381
  Authentication=NONE
  ```

  If the value returned is `any` other value other than `local host`, then it is multi-port communication.

bbcutil is present in the <*Install Dir*>/`bin` directory.

- Use this option to verify if the port used is for single-port or multi-port communication from a system other than local host:

  ovcodautil -n <*hostname*> **-ping**

  Here is an example,

  ovcodautil -n ovphpt4 -ping

  For single-port communication enter the following,

  Ping of '**OvBbcCb**' at: '`http://ovphpt4:383/Hewlett-Packard/OpenView/BBC/ping`' successful

  Ping of '**Coda**' at: '`http://ovphpt4:383/Hewlett-Packard/OpenView/Coda/`' successful

  For multi-port communication enter the following,

  ovcodautil -n ovphpt4 -ping

  Ping of '**OvBbcCb**' at: '`http://ovphpt4:383/Hewlett-Packard/OpenView/BBC/ping`' successful

  Ping of '**Coda**' at: '`http://ovphpt4:62581/Hewlett-Packard/OpenView/Coda/`' successful

  The port numbers are different in the two outputs.

For the Coda clients, all the parameters in the `coda.comm` namespace override the parameters defined in the `bbc.http` namespace.

Communication Broker Namespace (bbc.cb) Configuration Parameters

The following table lists the configuration parameters for the namespace bbc.cb:

Parameters in bbc.cb namespace	Description	Default Value
SERVER_PORT	Used to configure port settings	383
SERVER_BIND_ADDR	Used to specify bind address for the server port	INADDR_ANY

SERVER_PORT

You can configure the port settings of the default port used by the communication broker. The default value for this port is 383. Use the ovconfchg tool to change the port settings on the Performance Agent system. The format is as follows:

ovconfchg -namespace bbc.cb -set SERVER_PORT <*port no*>

If a port is already defined in the communication broker port namespace (bbc.cb.ports), the operating system assigns it as the default port and overrides the SERVER_PORT value.

SERVER_BIND_ADDR

Use this option to specify the bind address for the server port. The format is as follows:

ovconfchg -namespace bbc.cb -set SERVER_BIND_ADDR <*Bind address*>

Communication Broker Port Namespace (bbc.cb.ports) Configuration Parameters

The following table lists the configuration parameter for the namespace `bbc.cb.ports`:

Parameter in bbc.cb.ports namespace	Description	Default Value
PORTS	Used to define the list of ports for all the communication brokers in the network that may be contacted by the applications on this host. The client applications use this as target port to communicate with the communication broker in the network. If the host name matches with one of the entries in this port settings, then the local communication broker port will be set to the port specified here.	The value of ports is not set by default.

PORTS

This configuration parameter must be same on all the nodes. To change the port number of a communication broker on a particular host, the hostname must be added to the parameter; for example:

```
name.hp.com:8000
```

You can use an asterisk as a wild card to denote the entire network

```
*.hp.com:8001
```

You can use a comma or a semicolon to separate entries in a list of hostnames.

For example,

```
name.hp.com:8000, *.hp.com:8001
```

In this example, all the hostnames ending with hp.com will configure their BBC communication broker to use port 8001 except the host “name”, which will use port 8000. All the other ports use the default port 383.

You can also use the IP addresses and asterisk (*) to specify the hosts; for example:

```
15.0.0.1:8002, 15.*.*.*:8003
```

Run the following command to set ports:

ovconfchg -namespace bbc.cb.ports -set PORTS <*port no*>

HTTP Namespace (bbc.http) Configuration Parameters

Parameters in bbc.http namespace	Description	Default Value
RESPONSE_TIMEOUT	Used to specify the maximum number of seconds to wait for a response	300
CLIENT_PORT	Used to specify bind port for the client requests	0
PROXY	Used to specify the proxy and port to be used for the specified hostname	The value of proxy is not set by default.

RESPONSE_TIMEOUT

Use this option to specify the maximum number of seconds to wait for a response. The default value is `300`. The format is as follows:

`ovconfchg -namespace bbc.http -set RESPONSE_TIMEOUT` <*value*>

CLIENT_PORT

Use this option to specify the bind port for the client requests. The default value is `port 0`. The operating system assigns the first available port. This parameter is ignored for the requests to the localhost.

On a Windows system, this parameter should be defined on a large value because Windows system does not immediately release ports for reuse.

PROXY

Use this option to specify the proxy and port to be used for the specified hostname.

The format is as follows:

`proxy:port+(a)-(b);proxy2:port2+(a)-(b); ...;`

In this instance, the variables *a* and *b* are comma or semicolon separated lists of hostnames that apply to the proxy.

`a: for which the proxy shall be used`

`b: for which the proxy shall not be used`

The first matching proxy is chosen.

You can also use the IP addresses instead of hostnames. For example, 15.*.*.* is also valid, provided the correct number of dots and colons is specified.

Glossary

A

alarm

An indication of a period of time in which performance meets or exceeds user-specified alarm criteria. Alarm information can be sent to an analysis system (such as Performance Manager) and to Operations Manager. Alarms can be identified in historical data log files using the `utility` program.

alarm generator

Handles the communication of alarm information. It consists of `perfalarm` and the `agdb` database. The `agdb` database contains a list of Performance Manager analysis nodes (if any) to which alarms are communicated, and various on/off flags that you set to define when and where the alarm information is sent.

alarmdef file

The file containing the alarm definitions in which alarm conditions are specified.

application

A user-defined group of related processes or program files. Applications are defined so that performance software can collect performance metrics for and report on the combined activities of the processes and programs.

application log file

See **logappl**.

C

CEC

Central Electronics Complex. A CEC is a single HMC-attached pSeries server, which can be divided into LPARs.

coda daemon

A daemon that provides collected data to the alarm generator and analysis product data sources including `scopeux` log files or DSI log files. `coda` reads the data from the data sources listed in the `datasources` configuration file.

D

data source

Consists of one or more classes of data in a single `scopeux` or DSI log file set. For example, the Performance Agent SCOPE data source is a `scopeux` log file set consisting of global data. See also **datasources file**.

datasources file

A configuration file residing in the `/var/opt/OV/conf/perf/` directory. Each entry in the file represents a scopeux or DSI data source consisting of a single log file set. See also **coda** and **data source**.

data source integration (DSI)

The technology that enables Performance Agent to receive, log, and detect alarms on data from external sources such as applications, databases, networks, and other operating systems.

default.txt

A communications configuration file used to customize communication parameters for Operations Manager applications.

device

A device is an input and/or output device connected to a system. Common devices include disk drives, tape drives, DVD-ROM drives, printers, and user terminals.

device log file

See **logdev**.

DSI

See **data source integration**.

DSI log files

Log files containing self-describing data that are created by Performance Agent's DSI programs.

E

extract

The Performance Agent program that allows you to extract (copy) data from raw or previously extracted log files and write it to extracted log files. It also lets you export data for use by analysis programs.

extracted log file

A log file created by the `extract` program. It contains user-selected data ranges and types of data. An extracted log file is formatted for optimal access by the workstation analysis tool, Performance Manager. This file format is suitable for input to the `extract` and `utility` programs and is the preferred method for archiving performance data.

G

GlancePlus

GlancePlus (or Glance) is an online diagnostic tool that displays current performance data directly to a user terminal or workstation. It is designed to assist you in identifying and troubleshooting system performance problems as they occur.

global

A qualifier that implies the whole system.

global log file

See **logglob**.

I

interesting process

A process becomes interesting when it is first created, when it ends, and when it exceeds user-defined thresholds for cpu use, disk use, response time, and so on.

L

log file set

A collection of files that contain data collected from one source.

logappl

The raw log file that contains measurements of the processes in each user-defined application.

logdev

The raw log file that contains measurements of individual device (such as disk and `netif`) performance.

logglob

The raw log file that contains measurements of the system-wide, or global, workload.

logindx

The raw log file that contains additional information required for accessing data in the other log files.

logproc

The raw log file that contains measurements of selected “interesting” processes. A process becomes interesting when it is first created, when it ends, and when it exceeds user-defined thresholds for CPU use, disk use, response time, and so on.

logtran

The raw log file that contains measurements of transaction data.

M

midaemon

The Performance Agent program that translates trace data into Measurement Interface counter data using a memory based MI Performance Database to hold the counters. This database is accessed by collector programs such as `scopeux`.

mwa script

The Performance Agent script that has options for starting, stopping and restarting Performance Agent processes such as the `scopeux` data collector, `midaemon`, `ttd`, `coda`, `ovc`, `ovbbccb`, and the alarm generator. See also the `mwa` man page.

O

ovbbccb

The Operations Manager Communication Broker for HTTP(S) based communication controlled by `ovc`. See also **`coda`** and **`ovc`**.

ovc

The Operations Manager controlling and monitoring process. In a standalone Performance Agent installation, `ovc` monitors and controls `coda` and `ovbbccb`. If Performance Agent is installed on a system with Operations Manager for UNIX 8.x agent installed, `ovc` also monitors and controls Operations Manager for UNIX 8.x processes. See also **`coda`** and **`ovbbccb`**.

ovpa script

The Performance Agent script that has options for starting, stopping and restarting Performance Agent processes such as the `scopeux` data collector, alarm generator, `ttd`, `midaemon`, `ovc`, `ovbbccb`, and `coda`. See also the `ovpa` man page.

Performance Manager

Provides integrated performance management for multi-vendor distributed networks. It uses a single workstation to monitor environment performance on networks that range in size from tens to thousands of nodes.

P

parm file

The Performance Agent file containing the parameters used by `scopeux` to customize data collection.

perfstat

A program that displays the status of all performance processes in your system.

PerfView

See **Performance Manager**.

process

Execution of a program file. It can represent an interactive user (processes running at normal, nice, or real-time priorities) or an operating system processes.

process log file

See **logproc**.

R

raw log file

Summarized measurements of system data collected by `scopeux`. *See* **logappl**, **logproc**, **logdev**, **logtran**, and **logindx**.

real time

The actual time in which an event takes place.

resize

Changes the overall size of a log file using the `utility` program's `resize` command.

run file

Created by the `scopeux` collector to indicate that the `scopeux` process is running. Removing the `run` file causes `scopeux` to terminate.

S

scopeux

The Performance Agent data collector program that collects performance data and writes (logs) it to raw log files for later analysis or archiving. *See also* **raw log files**.

scopeux log files

See **raw log files**.

status.scope file

Created by the `scopeux` collector to record status, data inconsistencies, and errors.

system ID

The string of characters that identifies your system. The default is the host name as returned by `uname -n`.

T

transaction log file

See **logtran**.

transaction tracking

The technology used in Performance Agent that allows information technology (IT) resource managers to measure end-to-end response time of business application transactions.

ttd.conf

The transaction configuration file where you define each transaction and the information to be tracked, such as transaction name, performance distribution range, and service level objective.

U

utility

The Performance Agent program that allows you to open, resize, scan, and generate reports on raw and extracted log files. You can also use it to check

`parm` file and `alarmdef` file syntax, and obtain alarm information from historical log file data

Index

M

O

P

R

S

T

V

We appreciate your feedback!

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

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

Product name:

Document title:

Version number:

Feedback: