

HP Performance Agent

For the Windows® Operating System

Software Version: 4.70

Installation and Configuration Guide

Manufacturing Part Number: B7491-90089

Document Release Date: September 2007

Software Release Date: September 2007



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

© Copyright 1983-2007 Hewlett-Packard Development Company, L.P.

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.

All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

Support

You can visit the HP Software Support web site at:

www.hp.com/go/hpsoftwaresupport

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support 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 find more information about access levels, go to:

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

To register for an HP Passport ID, go to:

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

Contents

1	Installing or Upgrading HP Performance Agent	9
	Introduction	9
	Installation Requirements	11
	Hardware	11
	Supported Architecture and Operating Systems	12
	Communication Protocols	13
	Disk Space	13
	Network Considerations	15
	Installing Performance Agent using Terminal Services	16
	Installing Performance Agent from the Control Panel	16
	Installing Performance Agent from the Command Prompt	16
	Install or Upgrade Procedures	18
	Stopping Performance Agent	18
	Installing Performance Agent	18
	Attended Installation	18
	Unattended Installation	20
	Installation Results	20
	Directory Structure	21
	Deploying Performance Agent Using Operations Manager	21
	Performance Agent on a Virtual Machine	22
	Removing Performance Agent	23
	Attended Uninstallation	23
	Unattended Uninstallation	23
	Removing all Performance Agent Files	24
	Results of the Uninstallation	24
2	Starting and Running HP Performance Agent	25
	Introduction	25

Security Restrictions	27
Starting and Stopping Performance Agent Services	28
Starting and Stopping from the Windows GUI.	28
Starting and Stopping from Command Prompt	28
Checking the Status of Performance Agent Services	29
Automatic Startup at System Restart	29
Restarting Performance Agent.	29
Refreshing Performance Agent Services	30
Configuring Communication Mode for Performance Agent.	32
Status Checking	32
Examples Directory	33
Communicating Across Firewall	34
Communicating in the HTTP Environment	35
Configuring Systems with Multiple IP Addresses	40
Communicating in the RPC Environment	40
Tables for Configuring the Firewall.	42
Configuring Secure Communication	44
Using Certificates	44
Using Client Authentication	44
Enabling Authentication with the authip File	45
Configuring Data Sources	48
Configuring Data Sources for Performance Manager 3.x and Reporter	48
Configuration Options	49
Customized Data Collection.	50
Defining Alarms	51
Controlling Performance Agent Services from the Command Prompt	51
Backup Considerations	52
Unattended Backups	53
Viewing and Printing Documents	54
Viewing Documents on the Web.	55
Adobe Acrobat Files	55
A Configuring Coda	57
Introduction	57
Coda namespace	57
Coda Communication namespace (coda.comm).	60

Communication Broker namespace (bbc.cb)	64
Communication Broker Port namespace (bbc.cb.ports)	65
HTTP namespace (bbc.http)	67
Index	69

1 Installing or Upgrading HP Performance Agent

Introduction

HP Performance Agent software captures performance, resource, and transaction data from systems running Microsoft Windows. (See [Supported Architecture and Operating Systems](#) on page 12 for details on the supported Windows platform) Using minimal system resources, the software continuously collects, logs, summarizes, and time stamps data, and detects alarm conditions on current and historical data across your system. Using the Application Response Measurement (ARM) API standard, Performance Agent can log the end-to-end response times for instrumented business applications.

Performance Agent supports monitoring of virtual machines hosted on VMware ESX Server console 2.5.2 and later and 3.0.x. For more information, refer to the section titled [Performance Agent on a Virtual Machine](#).



Henceforth, in this document:

- Performance Agent for Windows will be used to refer to MeasureWare Agent (MWA) for Windows
- HP Performance Manager in this document refers only to versions 4.0 and later. The name Performance Manager 3.x is used throughout this document to refer to the product that was formerly known as PerfView
- HP Operations Manager will be used to refer to IT/Operations

The process names and software components will operationally remain as MeasureWare Agent (MWA).

Performance Agent includes the Extended Collection Builder and Manager, which allows access to Windows Registry performance counters. With the Extended Collection Builder and Manager, data available through the Windows registry can be collected and logged.

You can analyze the data using spreadsheet programs, Hewlett-Packard analysis products such as Performance Manager, or third-party analysis products. Also, Performance Agent provides data access to Performance Manager, HP Network Node Manager, and HP Operations Manager.

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 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 analysis on historical data to isolate and identify bottlenecks.
- Perform service-level management based on transaction response time.
- Facilitate capacity planning.
- Respond to alarm conditions.
- Solve system management problems before they arise.



If you have a factory integrated system, skip this chapter and go directly to [Chapter 2, Starting and Running HP Performance Agent](#).

Installation Requirements

Before installing Performance Agent make sure your system meets the requirements described in this section. These system and configuration prerequisites are necessary for Performance Agent to operate properly on your system.

Hardware

Performance Agent runs on Microsoft Windows systems satisfying one of the following requirements:

- Intel Pentium processor or equivalent
- Intel Itanium2
- AMD Opteron
- Intel Pentium with EM64T
- Intel Xeon with EM64T

Supported Architecture and Operating Systems

Table 1 Supported Architecture and operating system versions

Architecture	Operating System	Protocol
X86	<ul style="list-style-type: none">• Windows 2003 Standard Edition, Windows 2003 Enterprise Edition, Windows 2003 Datacenter Edition, Windows 2003 Web Edition, Windows 2003 R2 Enterprise Edition• Windows Vista Enterprise Edition, Windows Vista Business Edition• Windows XP Standard with Service Pack 1 or later	HTTP(S), RPC
X86_64, AMD 64, EM64T	<ul style="list-style-type: none">• Windows 2003 Server for x64 Editions• Windows XP Professional x64 Edition• Windows Vista Enterprise Edition	HTTP(S), RPC
IPF	Windows 2003 Server for Itanium-based Systems	RPC

See [Network Considerations](#) on page 15 for information on networking software requirements for Performance Agent.

- ▶ If you are installing Performance Agent for the first time in Vista/64-bit platform, it is recommended to disable User Access Control (UAC) in the **msconfig > tools > Disable UAC**.
- ▶ On IPF hardware running Windows operating system, Performance Agent 4.7 runs in 32-bit emulation mode. For Performance Agent 4.7 to function properly on IPF hardware running Windows OS, install Microsoft Visual C++ 2005 Redistributable Package (x86). Download Microsoft Visual C++ 2005 Redistributable Package (x86) from Microsoft site or contact HP Software Support.

Communication Protocols

Performance Agent supports the following communication protocols:

- HTTP(S) 1.1
- RPC
- ▶ • Performance Agent supports HTTP and RPC data communication on Microsoft Windows 64-bit platforms.
- ▶ If you are installing Performance Agent 4.70 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, it is recommended to restart them after Performance Agent 4.70 installation is completed.
- ▶
 - 1 If you are adding new hardware or making any configuration changes, it is recommended to stop `scopent` and restart it to make the changes to take effect.
 - 2 All the default OS daemons and services should be enabled and running.

Disk Space

Performance Agent uses disk space in the following areas—program files, Control Panel applet, data files, log files, and temporary files.

For Performance Agent applications, allow for at least 50 MB of free space on the drive you specify. For Performance Agent log files, allow for at least 60 MB of free space on the drive you specify.

- Program Files - Performance Agent requires approximately 10 MB of disk space for installation of program files that are stored in the Install directory path. Some additional space is required during installation (see “Temporary files” below).
- Control Panel Applet - Performance Agent services program and various DLLs require 2.5 MB disk space in the <\$windir\$>\system32 directory.



InstallDir is the directory where Performance Agent will be installed. All Performance Agent related binaries and shared libraries can be found at locations <InstallDir>\bin and <InstallDir>\lib respectively. The default path for InstallDir is <drive>:\Program Files\HP\HP BTO Software. DataDir is the default directory where the data files are stored. The default path for DataDir is <drive>:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\Data.



If you have already installed any HP Software Products, Performance Agent will be installed in the same directory.

- Configuration, Status, and Log Files - Configuration, status, and log files by default are stored separately from program files. Status and configuration files are stored in the <DataDir> directory and require about 1 MB of disk space for the installation. As the status files accumulate data, this number could increase to 10 MB.

Log files are stored in the <DataDir>\datafiles directory. The amount of disk space used for log files varies significantly depending on the system workload and the amount of performance data you collect. Using the default configuration settings, you can anticipate a 60 MB maximum size to be reached between two to six months. However, if you are *not* tracking transactions, the maximum size is 50 MB. See Chapter 3 of the *HP Performance Agent for Windows: User's Manual* for information on how to limit and configure the data storage requirements for Performance Agent log files.

- Archived Log Files - When the Performance Agent log files reach their maximum size, the oldest data is automatically rolled out to make room for more data. See Chapter 2 of the *HP Performance Agent for Windows User's Manual* for more information on Performance Agent automatic roll action and for strategies to effectively manage data collection.

- **Temporary Files** - The Performance Agent installation program uses about 10 MB of temporary storage in the <\$TEMP\$> directory, which is released when the installation is complete. Performance Agent also uses the <\$TEMP\$> directory during normal operation for storing temporary files during Scan, Analyze, and Status operations. The exact amount of free disk space required depends on the number and size of reports that are open at same time.

Network Considerations

Performance Agent cannot install unless TCP/IP network protocol is installed and running. You can check for this by looking for the TCP/IP Service in the Services program under Administrative Tools in the Windows Control Panel.

If you are not using a Domain Name System (DNS) name server, you must have a HOSTS file present on each system where Performance Agent is installed. A HOSTS file is a locally stored text file that maps host names to IP addresses. The HOSTS file should be stored in the <\$windir\$>\system32\drivers\etc directory and have the same format as the /etc/hosts file on a UNIX system. The HOSTS file should include the name of the Performance Agent system, as well as any Performance Manager and Operations Manager system you plan to connect to in the HOSTS file.

Installing Performance Agent using Terminal Services

Performance Agent can be installed in a terminal services session by either from Control Panel or command prompt.

Installing Performance Agent from the Control Panel

Performance Agent can be installed from Control Panel as follows:

- 1 Click **Start > Control Panel > Add or Remove Programs**.
- 2 Select **Add New Programs** and then click **CD or Floppy**.
- 3 Click **Browse** and select the **setup.exe** file.
- 4 Click **Finish** to install Performance Agent.

Installing Performance Agent from the Command Prompt

Performance Agent can be installed from the Windows command prompt as follows:

- 1 Click **Start > Run**.
- 2 Type **cmd** and click OK. The command prompt window is displayed.
- 3 Change the drive to the folder where Performance Agent **setup.exe** file is located.
- 4 Type the following command

```
change user /install
```

The following message is displayed:

```
User session is ready to install applications
```




Note: The following message will be displayed if terminal server is installed in remote administration mode.

Install mode does not apply to a Terminal server configured for a remote administration.

- 5 Enter **setup.exe** to complete the installation.

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 have previously installed version of Performance Agent or GlancePlus on the system, stop any performance tools or processes that may be running.

Stopping Performance Agent

Performance Agent can be stopped from the Windows command prompt or from a batch file using the `mwacmd` (`mwacmd.exe`) command as described below.

```
mwacmd stop or mwacmd stop all
```

stops all Performance Agent services from the command prompt



If you stop the `tttd`, any ARM-instrumented applications that are running *must* also be stopped before you can restart `tttd` and Performance Agent process.

Installing Performance Agent

Log on to your Windows system as Administrator or as any user that is part of the Administrators group. You can install Performance Agent using one of the following two modes:

- [Attended Installation](#)
- [Unattended Installation](#)

Attended Installation

Install Performance Agent by the following installation procedure. This procedure may take several minutes to complete.

- 1 If you already have Performance Agent installed and are updating to this version, close all Performance Agent windows and programs as well as other application windows in use, including the Windows Control Panel.

- 2 Place the Performance Agent DVD in the DVD-ROM drive. The Performance Agent files in the DVD is displayed.
- 3 Select the Win folder.
- 4 Follow the instructions as they appear.



- You cannot install Performance Agent on a network drive. Performance Agent must begin at startup time, before network drives are connected.
- If your system disk performance counters are turned off, you will see a message indicating that no disk metrics will be collected unless the disk performance counters are turned on. Run the command **diskperf -y** to turn on both logical and physical disk performance counters. Turning on disk performance counters takes effect only after you have rebooted your system.
- If you do not choose to start Performance Agent automatically whenever you restart your system, you must manually start Performance Agent as described in [Chapter 2, Starting and Running HP Performance Agent](#).
- If you have applications running on your system that have ARM technology, your system is prompted for a restart.
- The Performance Agent setup program starts the Remote Procedure Call (RPC) services and sets them to automatically start when you restart the system (if they are not already running.)

See the Performance Agent Release Notes for updates to Performance Agent. The Performance Agent Release Notes contain information not covered in the documentation set.

Unattended Installation

To carry out unattended installation run the command `setup.exe /s` from the Windows command prompt with command line options.

To start the Unattended Installation:

- 1 Open the Windows command prompt and change to the drive where the Performance Agent `setup.exe` file is located by typing:

`<drive>:`

where *drive* is the CD-ROM drive containing the Performance Agent files.

- 2 Follow the syntax format for the command and available options as explained below:

To activate unattended installation, enter:

```
setup.exe /s[/z"-p1 <Install directory path> -p2 <Data  
directory path> -s -v "]
```

Where,

- **-p1**: used to specify the input for the Install Directory path (the default directory path is `C:\Program Files\HP\HP BTO Software`).
- **-p2**: used to specify the input for the Data Directory path (the default directory path is `C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\data`).
- **-s**: used if you want to start Performance Agent services immediately after installation.
- **-v**: used if you want Performance Agent services start-up type to be set to "Manual" instead of "Automatic".
- **/s**: used to carry out installation in unattended mode.
- **/z**: used if you want to give inputs to the installation program. Inputs should be given in between " ".

Installation Results

After Performance Agent files are installed in the default or designated locations, the setup program performs the following activities:

- Performance Agent Control Panel applet is installed to control Performance Agent services. For a description of Performance Agent services, see [Chapter 2, Starting and Running HP Performance Agent](#).
- On Windows, the Performance Agent folder is added to the **Start > Programs** menu, with a submenu containing icons/commands for Performance Agent programs, online help, and the Release Notes.
- The system path variable is modified to include <InstallDir>\bin\.

Directory Structure

For upgraded installations, files are automatically placed in the same directories as those of the previously installed version.

Default file locations are as follows:

- Program and other files are stored in sub-directories of the <InstallDir>\bin\ directory.
- Data files (log files and other files containing data) are stored in subdirectories of the <DataDir>\ directory.

The environment variable *windir* is used to denote the Windows directory in your system. The environment variable `TEMP` is used to denote the temporary files directory stored on your Windows system.



Striped Disks - This option does not enable disk performance counters for physical drives in a striped disk set. If you want to collect data for striped disks, run **diskperf -YE** from the Windows command prompt.

Deploying Performance Agent Using Operations Manager


If you are using Operations Manager for UNIX 8.x, you can install HP Performance Agent from the management server to a Windows managed node.

For installation instructions from an Operations Manager for UNIX 8.x management server, please see the chapter, HP Performance Agent, in the *HP Operations Manager for UNIX Administrator's Reference*.

Performance Agent on a Virtual Machine

The Performance Agent version from 4.60 supports monitoring of Virtual Machines (VMs) hosted on VMWare ESX Server console 2.5.2 and later and 3.0.x. For installation procedures refer to the section, [Install or Upgrade Procedures](#).

- Install **VMWare Tools** on the VM. Performance Agent installed on a VM, hosted on VMWare ESX Server console 2.5.2 and later, requires VMWare tools to recognize the virtual machine as a Guest operating system.
- On VMs hosted on VMWare ESX Server console 3.0.x, enable the **VMware Guest API** on the VMs. To capture the Virtual Machine's utilization of physical resources of a system, Performance Agent uses the **VMWare Guest API**. For more information about **VMware Guest API**, refer to latest documentation available on **VMware Guest SDK** from VMWare.

 For complete list of metrics and descriptions, refer to the *Release Notes* and *Dictionary of Performance Metrics*.

Removing Performance Agent

Log on to your Windows system as Administrator or as any user that is part of the Administrators group. You can uninstall Performance Agent using one of the following two modes on your system:

- [Attended Uninstallation](#)
- [Unattended Uninstallation](#)

Attended Uninstallation

You can uninstall Performance Agent using the uninstall program as follows:

- 1 Log on to your Windows system as administrator or as a user with administrative privileges.
- 2 Close the Performance Agent program, the Performance Agent Services window, and the Windows Control Panel.
- 3 Go to **Control Panel > Add or Remove Programs**.
- 4 Select **HP Performance Agent Software**.
- 5 Click on **Change/Remove** to uninstall.

Unattended Uninstallation

To carry out unattended uninstallation, run `setup.exe /s /x` from the Windows command prompt with command line options.

To uninstall from the command prompt, enter:

```
setup.exe /s /x [/z"-r all"]
```

where,

- **-r all**: used to specify deletion of Performance Agent created log files.
- **/s**: used to carry out tasks in unattended mode.
- **/x**: used to carry out uninstallation.
- **/z**: used to give inputs to the installation program. Inputs should be given in between “ ”.

Removing all Performance Agent Files

By default, the uninstall program does not remove Performance Agent configuration, status, and log files. It also does not remove `<InstallDir>\bin\` from the system path variable. You can manually remove these items if you want to clean up your system. Do not remove additional files or change the path variable if any RPM Tools application (Performance Manager or Reporter, for example) is still installed on your system.

If Performance Agent is the last RPM Tools application to be removed during an attended uninstall, you are prompted as to whether you want to remove all files in the `<InstallDir>\bin\` and the `<DataDir>\` directories.

During an unattended uninstall, you can achieve the same result of removing all files within the `<InstallDir>\bin\` and the `<DataDir>\` directories by including the `-r` all option.



After uninstallation, the Performance Agent uninstall program may display a message stating that it was not able to remove some items. The uninstall program marks these files for deleting and removes them during the next system restart. If you get this message, restart your system before you try to reinstall Performance Agent.

Results of the Uninstallation

The uninstall program removes Performance Agent program files, except for `perfstat.exe`. However, if Performance Agent is the only RPM Tool installed on the system, `perfstat.exe` is also removed. The uninstall program also removes the Performance Agent services and Windows registry entries associated with Performance Agent.

2 Starting and Running HP Performance Agent

Introduction

This chapter explains the tasks involved in starting up and running Performance Agent after it has been installed on your Windows system.

The following topics are discussed:

- Starting and Stopping Performance Agent Services
- Configuring Communication Mode for Performance Agent
- Communicating Across Firewall
- Configuring Secure Communication
- Configuring Data Sources
- Configuration Options
- Defining Alarms
- Backup Considerations



If you are planning to log data from other sources using data source integration (DSI), read the *HP Performance Agent for Windows Data Source Integration Guide*.

Performance Agent supports the HTTP data communication mechanism, along with RPC mode on 32-bit and 64-bit Windows systems. If you are installing Performance Agent for the first time, the default data communication mode is HTTP.

If you are upgrading Performance Agent, the previously used data communication mode is used. If you want to move to HTTP/RPC mode of data communication, you can change the configuration after installation. For more

information, see the section [Communicating in the HTTP Environment](#) on page 35. Performance Agent supports secure data communication (HTTPS) only in an Operations Managers environment.

Security Restrictions

The following security-related restrictions are applicable in controlling Performance Agent Services:

- To start or stop Performance Agent Services, you must be a member of the Administrators or Power Users group.
- To refresh Performance Agent configuration files, you must be a member of the Administrators or Power Users group.
- To configure Performance Agent Services, you must be a member of the Administrators group.

Any user can view the status of Performance Agent Services from the Services program in the Windows Control Panel or the Services program under Administrative Tools in the Windows Control Panel.

Starting and Stopping Performance Agent Services

When installation is complete, you can start Performance Agent from the Windows GUI or command prompt.

Starting and Stopping from the Windows GUI

To start the Performance Agent from the Windows GUI, do the following:

- 1 To open Performance Agent, click **Start > Programs > HP > Performance Agent > HP Performance Agent Software**. Or Choose **Start/Stop** from the Agent menu on the Performance Agent main window. Or, from the Windows Control Panel, double-click **PA** to open the Performance Agent Start/Stop dialog box.
- 2 To start all Performance Agent services, click **Start Services**.
- 3 To stop all Performance Agent services, click **Stop Services**.

Starting and Stopping from Command Prompt

You can start and stop Performance Agent services from the Windows command prompt or from a batch file using the `ovpacmd` (`ovpacmd.exe`) command as follows:

- **`ovpacmd start` or `ovpacmd start all`**
starts all Performance Agent services from the command prompt.
- **`ovpacmd stop` or `ovpacmd stop all`**
stops all Performance Agent services from the command prompt.



The executable `mwacmd.exe` is still provided in this release for backward compatibility. The functionality is same as `ovpacmd.exe`.

Checking the Status of Performance Agent Services

To check the status of the Performance Agent Services:

- Select **HP > Performance Agent > Status** OR
- Click the **Agent Status** icon from the main window OR

To check the status of Performance Agent services, from the command prompt run:

```
perfstat
```

Automatic Startup at System Restart

If you have not selected the installation option to automatically start Performance Agent Services when your system is restarted, do the following.

- 1 Select **Services** from Administrative Tools in the Control Panel.
- 2 Select **PA Collector**, click **Startup** and choose **Automatic** for the Startup Type .
- 3 Repeat step 2 for Performance Agent, Performance Agent Transaction Manager, Performance Agent Extended Collector, and Performance Agent DSI Service.

Do not set the Performance Agent Measurement Interface to start automatically.

Restarting Performance Agent

To restart the Performance Agent, stop and start Performance Agent by following one of the steps explained in [Starting and Stopping Performance Agent Services](#) on page 28.

Refreshing Performance Agent Services

If you modify any of the Performance Agent configuration files (`parm.mwc`, `ttddconf.mwc`, `alarmdef.mwc`, `dsiconf.mwc`), you must refresh the corresponding service to reflect the changes made to the configuration files. To enable the **Refresh** button, select at least one Configuration Parameter from the Performance Agent Services dialog box.

Refreshing from the Windows GUI

- 1 From the Agent menu on the Performance Agent main window, choose **Start/Stop**. Or, from the Windows Control Panel, double-click **OVPA** to open the Performance Agent Start/Stop dialog box.
- 2 Select the Configuration Parameters you have changed.
- 3 Click the **Refresh** button. Select at least one Configuration Parameter in the Performance Agent Services dialog box to enable the button.

Refreshing from Command Prompt

Open the Windows command prompt and type:

```
ovpacmd refresh <config>
```

where *<config>* is:

- **COL** for `parm.mwc`
- **TRAN** for `ttddconf.mwc`
- **ALARM** for `alarmdef.mwc`
- **DSI** for `dsiconf.mwc`

Services Started with Different Data Communication Modes

RPC

HP OpenView Ctrl Service

Performance Agent Collector

Performance Agent Alarm Generator
(only if `perfalarm` is used for
alarming)

Performance Agent DSI Service

Performance Agent Extend Collector

Performance Agent Measurement
Interface

Performance Agent Transaction
Manager

Performance Agent (starts `alarmgen`
only if `perfalarm` is not present)

HTTP

HP OpenView Ctrl Service

Performance Agent Collector

Performance Agent Alarm Generator

Performance Agent DSI Service

Performance Agent Extend Collector

Performance Agent Measurement
Interface

Performance Agent Transaction
Manager

Configuring Communication Mode for Performance Agent

Performance Agent supports both HTTP and RPC mode of communication. To view the current mode, type `Ovpacmd getdatacomm`

To change the communication mode to RPC or HTTP, perform the following steps:

- 1 Stop Performance Agent.
- 2 Run `ovpacmd setdatacomm <mode>`, where *mode* is one of the following:
 - **HTTP** - HTTP mode of communication
 - **RPC** - RPC mode of communication
- 3 Start Performance Agent.

Status Checking

Several status files are created in the `DataDir` directory when Performance Agent is started.

You can check the status of all or some of the Performance Agent processes using the `perfstat` command.

The following status files contain diagnostic information that you can use to troubleshoot problems that may arise with the processes that generate the files:

```
<DataDir>\status.alarmgen  
<DataDir>\status.perflbd  
<DataDir>\status.rep_server  
<DataDir>\status.scope  
<DataDir>\status.perfalarm
```


<DataDir>\status.ttd
<DataDir>\status.mi
<DataDir>\log\coda.txt



Whenever the Performance Agent process writes a message to its 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 <InstallDir>\examples\ directory contains examples of configuration files, syntax files, and sample program files that you can use to customize your HP Performance Tools. For example, the <InstallDir>\example\config\ subdirectory contains sample alarm definitions and examples of parm file application-specific parameters. For more information, see the <InstallDir>\examples\README file.

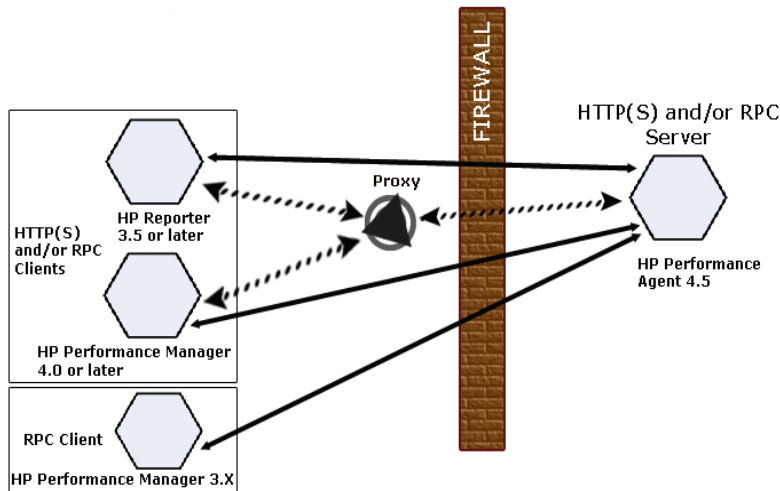
Communicating Across Firewall

In general, a firewall may be defined as a method for filtering the flow of data between two networks. Performance Agent now supports HTTP 1.1 based communications interface for data access between client and server applications, in addition to the previously supported communication mechanism through a packet-filtering network firewall. The HTTP based interface is flexible, since it can use proxies, requires fewer ports and is firewall friendly.

- ▶ Performance Agent supports certificate based, secure (HTTPS) data communication only in the Operations Manager environment. For more information, see [Using Certificates](#) on page 44.

If a network firewall exists between two system, Performance Manager and Reporter can get data from the Performance Agent system.

Figure 1 Communicating with Performance Agent in a Firewall Environment





The name Performance Manager 3.x is used throughout this document to refer to the product that is formally known as PerfView.

Communicating in the HTTP Environment

For firewall configuration 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 accordingly. 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. Understand your firewall environment including the client and server data flow. To configure communications with Performance Agent in a firewall environment, perform the following tasks:

- 1 [Configure Performance Agent Ports.](#)
- 2 [Configure HTTP Clients in a Firewall Environment.](#)
- 3 [Verify Firewall Configuration.](#)

[Figure 1](#) on page 34 shows how Performance Agent communicates with Reporter (version 3.5 or later) and Performance Manager (version 4.0 or later) through a firewall. Performance Agent is an HTTP or HTTPS server. Reporter and Performance Manager 4.x are HTTP clients. Performance Manager 5.0 can be an HTTP or HTTPS client. If an HTTP proxy is used, Reporter and Performance Manager communicate with Performance Agent through the proxy.

Performance Manager version 3.x uses the PerfView technology. PerfView does not use the HTTP datacomm components, but it connects to Performance Agent 4.5 when the DCE data communication mode is enabled.

Configure Performance Agent Ports

You can configure Performance Agent ports in a firewall environment in one of the two ways:

- [Configure Two-Port Communication](#)
- [Configure Single-Port Communication](#)
- [Verify Port Settings](#)

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. Type the following commands:

```
— 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 Performance Agent using the following command:

```
ovpa restart server
```

Configure Two-Port Communication

By default, `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
- indicates if secure communication is enabled
- indicates if 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

There are two ways to configure HTTP clients in a firewall environment:

- [Configuring HTTP Clients \(Reporter/Performance Manager\) with HTTP Proxy](#)
- [Configuring HTTP Clients \(Reporter/Performance Manager\) without HTTP Proxy](#)

In both cases, 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 5.0 and later, and Reporter 3.7: 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 3.6 and earlier, and Performance Manager 4.x:

Edit the `/var/opt/OV/conf/BBC/default.txt` configuration file.

For example, 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) + (*)
```

Here, 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 5.0 and later, and Reporter 3.7 as follows:

Type the following command,

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

Where *<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 3.6 and earlier, and Performance Manager 4.x as follows:

Edit 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>
```

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

```
CLIENT_PORT = 14000-14003
```

Verify Firewall Configuration

To verify your configuration, use the command:

```
ovcodautl -ping -n <system name>
```

The output of this command indicate 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, then 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 5.0 (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.x system, specify the `CLIENT_BIND_ADDR` parameter.

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

- a Locate the lines that apply to `CLIENT_BIND_ADDR` and uncomment the line

```
;CLIENT_BIND_ADDR =
```
- b Specify the IP address for the `CLIENT_BIND_ADDR` parameter.

Communicating in the RPC Environment

Performance Agent supports communication across a packet-filtering network firewall. This means that even if a network firewall exists between two systems, Performance Agent can send alarms to Performance Manager 3.x and Performance Manager 3.x can graph data from Performance Agent on a remote system. (To configure the Performance Manager 3.x for UNIX systems to use restricted port addresses see the *HP Performance Manager Installation Guide*).

To restrict UDP, TCP RPC ports on applications running on Windows system, do the following:

Create the following registry keys using `regedt32` as shown in the example below. The example shows configuration for restriction of port usage from 2200 through 2300.

New registry key:

`HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Internet`

Add the following values:

Type	Name	Value
REG_SZ	PortsInternetAvailable	"Y"
REG_SZ	UseInternetPorts	"Y"
REG_MULTI_SZ	Ports	2200-2300

For more information, refer to MSDN article "Configuring the Windows XP/2000/NT Registry for Port Allocations and Selective Binding".

Currently, Performance Agent cannot restrict UDP RPC ports running on Windows on a per application basis. If you are using a packet filtering firewall based on ports, you need to open all ports greater than 1023 to communicate across the firewall.

To permit Windows nodes to access your internal network based on IP addresses not ports, do the following:

- 1 Configure the Windows node outside your firewall to use the firewall IP address as a Gateway.
- 2 Add the firewall IP address to the local or SUBNET routing table in which the Windows node resides (see Table 2).
- 3 Configure your firewall to give the Windows node access to your internal network.

How you perform these steps depends on several factors including, the security policy of the SUBNET in which the Windows node resides, the default Gateway configuration of your Windows node, and the firewall configuration of your internal network. Consult your firewall administrator or network security officer before making any changes to your environment.

Tables for Configuring the Firewall

Determining the destination and source variables for the firewall will depend on which application resides within the firewall and which operating system the application is running on.

Table 1 Performance Manager 3.x and later (PV) for Windows, Reporter (OVR) for Windows, Performance Agent for Windows

Source	#Ports / Protocol	Destination	Ports / Protocol
PV, OVR	1024-65535/UDP	MS_RPC service	135, 1024-65535/UDP
PV, OVR	382/TCP	Performance Agent	382/TCP
PV, OVR	1024-65535/UDP	Performance Agent	1024-65535/UDP
Performance Agent	1024-65535/UDP	MS RPC service	135, 1024-65535/UDP
Performance Agent	1024-65535/UDP	Performance Manager	1024-65535/UDP

Table 2 Performance Manager 3.x and later on UNIX, Performance Agent for Windows

Source	#Ports/Protocol	Destination	Ports / Protocol
Performance Manager/ UNIX	OVPM_RANGE/ UDP	MS RPC service	135, 1024-65535/UDP
Performance Manager/ UNIX	382/TCP	Performance Agent/WIN	382/TCP
Performance Manager/ UNIX	OVPM_RANGE/ UDP	Performance Agent/WIN	1024-65535/UDP
Performance Agent/WIN	1024-65535/UDP	DCE daemon	135,OVPM_RANGE/ UDP
Performance Agent/WIN	1024-65535/UDP	Performance Manager/ UNIX	OVPM_RANGE/UDP

OVPM_RANGE is the range of ports that have been calculated for the Performance Manager.

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.x environment.

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

If you have already configured HTTPS communication in the Operations Manager 8.x environment, make the following changes to configure secure communication between Performance Agent and Performance Manager 5.0.



Performance Manager 4.x 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
ovcodautl -config
```

Using Client Authentication

Performance Agent enables optional authentication of client connections, for example by Performance Manager 3.x or 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 will work to enable or disable 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.

Enabling Authentication with the authip File

Authentication is enabled by the presence of a file called `authip`. For HTTP based communication, the `authip` file exists in the `<DataDir>\data\conf\perf` directory. For RPC based communication, the `authip` file exists in the `<disk drive>:\Program Files\HP\HP BTO Software\data\` directory. The `authip` file lists hosts from which client connections are to be permitted.

- 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, then 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 that would otherwise disqualify it, until the client takes an action that requires reregistration with Performance Agent. To ensure the `authip` changes are enforced, you may want to stop and restart all Performance Agent services. If there is then an attempt to reopen the data source, the `authip` file will be reread and the connection denied.

In the case of Performance Manager 3.x 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 add or delete entries into the `agdb` file use the `agsysdb` utility program. Refer to *HP Performance Agent for Windows User's Manual*. Additionally, you can also use Performance Manager 3.x to enable or disable alarms.

The Performance Agent client authentication capability requires that your network be able to resolve the client entries in the `authip` file. Depending upon the nature of the entries, this may require name services such as those provided by DNS, NIS, or `<%windir%>\system32\drivers\etc\hosts` files. A good test is to make sure that you can successfully "ping" each `authip` entry from the Performance Agent host. Client authentication will work 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 in IPv4 dotted quad format
- 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 leading zeros, that is, the IP address 23.10.10.10 cannot be represented as 023.10.10.10.
- Client entries may have spaces or tabs preceding them.
- Client entries on a line are terminated by spaces, tabs, new lines, or the # sign.

Thus, given an `<%windir%>\system32\drivers\etc\hosts` entry as follows: `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 =====
```



In order to use the authentication capability (aliases or hostnames in the authip file), the Domain Name System (DNS) on your local system has to be configured properly. For further information on how to configure your DNS, refer to the Microsoft Windows online help.

Configuring Data Sources

Performance Agent uses a set of repository servers that provides previously collected data to the alarm generator and the Performance Manager analysis product. There is a repository server for each specific data source such as scopeux log files or DSI log files. Each data source consists of a single log file set. The data source is configured in the `datasources` file that resides in the `<DataDir>\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 repository servers for other data sources, configure them in the `datasources` file. When you restart Performance Agent, the `perflbd` daemon looks for `perflbd.mwc` (the file that resides in `<DataDir>` directory is a link to `datasources` file), reads it, and starts a repository server for each data source it finds.

Configuring Data Sources for Performance Manager 3.x and Reporter

Performance Agent data is automatically configured for accessibility and alarm generation in Performance Manager 3.x and Reporter. You can configure additional data sources in the `datasources` file (or `perflbd.mwc` file) as described in Chapter 3 of the *HP Performance Agent for Windows: User's Manual* and the *HP Performance Agent for Windows: Data Source Integration Guide*. Additional data sources can include raw log files, extracted log files, or log files created with Performance Agent's Data Source Integration (DSI) technology or from data collections you create using the Extended Collection Builder and Manager.

IP Addresses

After you have configured the Performance Agent system as a data source for Performance Manager 3.x, avoid changing the IP address of either the Performance Agent system or the Performance Manager 3.x system.

However, if you must change the IP address of one or more systems, follow the procedure below to avoid problems.

To change the IP address of a Performance Agent system:

- 1 On the Performance Manager 3.x system, select **Manage** from the **Data Sources** menu on the Performance Manager 3.x dialog box.
- 2 Delete the Performance Agent system from the list of known systems.
- 3 Change the IP address of the Performance Agent system.
- 4 Add the Performance Agent system back as a data source to Performance Manager 3.x.

To change the IP address of a Performance Manager 3.x system, see Performance Manager 3.x documentation.

Configuration Options

Performance Agent includes default configuration files that allow you to quickly start monitoring the performance of systems across your organization. You can change the default settings to suit the conditions in your particular computing environment.

Collection Parameters File (`parm.mwc`)

By default, Performance Agent is set up to monitor global, process, application, transaction, and disk data with a maximum log file size of 60 MB (50 MB if you are *not* tracking transactions).

You use the `parm.mwc` file to customize various data collection parameters, such as specifying the types of data to monitor, setting up groups of processes to be monitored together as one application, and changing the maximum size of the log file. See Chapter 2 of the *HP Performance Agent for Windows User's Manual* for more information.

Transaction Configuration File (`ttdconf.mwc`)

You can monitor transaction data for applications that have been instrumented with Application Response Measurement (ARM) API calls. The `ttdconf.mwc` file allows you to define transaction and application names, performance distribution ranges, and the service level objectives to be met by each transaction. See the *HP Performance Agent for Windows: Tracking Your Transactions* manual for more information on transaction tracking.

Customized Data Collection

With the Extended Collection Builder and Manager, you can configure customized data collections of Windows registry counters. See the Extended Collection Builder and Manager Online Help for details on how to build and manage Windows registry counter collections. The Online Help is available by choosing **Extended Collections** from the Configure menu in the Performance Agent main window. Then click the **Help** button from the Extended Collection Builder and Manager dialog box.

Using Data Source Integration (DSI) technology, you have another means for customizing data collections. Once you have your data collection method implemented, you can feed data into Performance Agent using DSI. Refer to the *HP Performance Agent for Windows Data Source Integration Guide* for information about using DSI.

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. 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 detailed information about defining alarms, see Chapter 7, “Performance Alarms,” in the *HP Performance Agent for Windows User's Guide*. This chapter describes the alarm definitions syntax, how alarms work, and how alarms can be used to monitor performance.

Controlling Performance Agent Services from the Command Prompt

Performance Agent services can be started and stopped from the Windows command prompt or from a batch file using the `ovpacmd` (`ovpacmd.exe`) command as described below.

You must be a member of the Administrators or Power Users group to execute these commands.

- **`ovpacmd stop`**
stops the OV Performance Collector and Performance Agent services.
- **`ovpacmd start`**
starts the OV Performance Collector, Performance Agent, Transaction Manager, Extended Collection services.
- **`ovpacmd start dsi`**
starts the Data Source Integration service that allows for continual logging for data feeds configured in the `dsiconf.mwc` file.
- **`ovpacmd stop dsi`**
stops the Data Source Integration service that allows for continual logging for data feeds configured in the `dsiconf.mwc` file.

An example of using the command prompt would be to restart Performance Agent services from a batch file to refresh Performance Agent configuration files if you want to automatically shift to a different set of alarm definitions during off hours. Include a command in the batch file to copy an alternate `alarmdef.mwc` file into the `<DataDir>\data` directory.

Backup Considerations

You may want to keep the following items in mind when backing up a Windows system on which Performance Agent is installed and running.

- You need not stop Performance Agent services in order to back up the system.
- If Performance Agent services are running at the time of the backup, the files listed below are not included in the back up. Additional files may also be excluded in the back up if the Performance Agent program is open. If the backup program you use has the option to back up open files, you may want to set this option so that these files will be included in the backup.

```
<DataDir>\status.scope  
<DataDir>\status.mi  
<DataDir>\status.perflbd  
<DataDir>\status.ttd  
<DataDir>\status.rep_server  
<DataDir>\status.alarmgen  
<DataDir>\datafiles\logindx  
<DataDir>\datafiles\logglob  
<DataDir>\datafiles\logappl  
<DataDir>\datafiles\logproc  
<DataDir>\datafiles\logdev  
<DataDir>\datafiles\logtran  
<DataDir>\datafiles\agdb  
<DataDir>\datafiles\agdb.lk  
<DataDir>\datafiles\.perflbd.pid
```

- If Performance Agent log files are backed up while Performance Agent is running, each raw log file (logglob, logappl, logproc, logdev, and logtran) may contain a slightly different amount of data. This situation arises because each individual file is backed up at a slightly different time. This behavior may make the data more difficult to interpret if you ever have to restore the log files from the backup tape.
- If you want to stop Performance Agent services prior to backing up your system, you can do so by selecting **Start/Stop** from the Agent menu of the Performance Agent main window. (You can also use the Windows Control Panel, Windows command prompt, or a batch file to stop Performance Agent services as described earlier in this chapter).

- Restart the Performance Agent services after the backup is complete.



Stopping and starting Performance Agent services causes a gap in your log files for the period while data collection is stopped.

Unattended Backups

Control Performance Agent services from a batch file if you want to stop Performance Agent prior to an unattended backup. You can then restart it automatically when the backup is finished.

Viewing and Printing Documents

Performance Agent software includes the standard Performance Agent documentation set in viewable formats. You can view the Adobe Acrobat format (*.pdf) documents online and print as needed. The ASCII text (*.txt) documents are printable. However, you can view a text file on your screen using any text editor. The documents are listed in the following table along with their file names and online locations.

Table 3 Performance Agent Documentation Set

Document	File Name	Windows Location
<i>HP Performance Agent for Windows Installation & Configuration Guide</i>	ovpainst.pdf	<i>InstallDir</i> \paperdocs\ovpa\C
<i>HP Performance Agent for Windows User's Manual</i>	ovpausers.pdf	<i>InstallDir</i> \paperdocs\ovpa\C
<i>HP Performance Agent for Windows Data Source Integration Guide</i>	ovpadsi.pdf	<i>InstallDir</i> \paperdocs\ovpa\C
<i>HP Performance Agent for Windows: Tracking Your Transactions</i>	tytnt.pdf	<i>InstallDir</i> \paperdocs\ovpa\C
<i>Application Response Measurement (ARM) API Guide</i>	arm2api.pdf	<i>InstallDir</i> \paperdocs\arm\C
<i>HP Performance Agent for Windows Dictionary of Operating System of Performance Metrics</i>	metwin.txt	<i>InstallDir</i> \paperdocs\ovpa\C

Release Notes

See Performance Agent Release Notes for additional information that you may not find in the Performance Agent manuals and online help. The Release Notes offer a list of new features as well as explanations of fixes to previous problems and current known problems, and how to deal with them. You can read the Release Notes at the end of the installation. You can also access them after installation from the HP -> Performance Agent -> HP Performance Agent Software folder on the **Start -> Programs** menu.

Online Help

Refer to the Performance Agent Online Help, accessible from the HP Software program folder or from Performance Agent main window. Metrics Online Help is also available at the same location.

Viewing Documents on the Web

The listed documents can also be viewed on the HP Software Manuals web site at:

http://ovweb.external.hp.com/lpe/doc_serv

Select performance agent from the product list box, select the release version (which automatically selects the appropriate OS), and click **[Open]** to view the document online, or click **[Download]** to save the file to your computer.

Adobe Acrobat Files

The Adobe Acrobat files were created with Acrobat 7.0 and are viewed with the Adobe Acrobat Reader versions 4.0 and higher. If Acrobat Reader is not installed on your system, you can download it from Adobe's web site:

<http://www.adobe.com>

While viewing a document in the Acrobat Reader, you can print a single page, a group of pages, or the entire document.

Configuring Coda

Introduction

Coda is a light weight 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

The following table lists the configuration parameters for the namespace `coda`:

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
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 will be 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:

```
ovcodauti1 -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 will be installed only if HP Operations Agent 8.x 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)

The following table lists the configuration parameters for the namespace `coda.comm`:

Parameters in coda.comm namespace	Description	Default Value
<code>SERVER_PORT</code>	Used to configure port settings	0
<code>SERVER_BIND_ADDR</code>	Used to specify bind address for the server port	<code>INADDR_ANY</code>
<code>LOG_SERVER_ACCESS</code>	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 the coda. The default value for this port is 0. If the port is set to 0, the operating system will assign 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 happen 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 senders IP address, requested HTTP address, requested HTTP method, and response status. This value typically will not be 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:

- 1 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 will be present in the `<Install Dir>/bin` directory.

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

```
ovcodauti1 -n <hostname> -ping
```

For example,

```
ovcodauti1 -n ovphpt4 -ping
```

For single port communication,

```
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,

```
ovcodauti1 -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.com` namespace override the parameters defined in the `bbc.http` namespace.

Communication Broker namespace (bbc.cb)

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

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

`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)

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

Parameter in <code>bbc.cb.ports</code> namespace	Description	Default Value
<code>PORTS</code>	<p>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.</p> <p>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.</p>	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 uses 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)

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

Parameters in <code>bbc.http</code> namespace	Description	Default Value
<code>RESPONSE_TIMEOUT</code>	Used to specify the maximum number of seconds to wait for a response	300
<code>CLIENT_PORT</code>	Used to specify bind port for the client requests	0
<code>PROXY</code>	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 the Windows system, this parameter should be defined on a large value because Windows system does not immediately release ports for reuse.

PROXY

Used 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 correct number of dots and colons are specified.

Index

A

- authip file, 45
 - examples, 46
 - formatting, 46

B

- backup considerations, 52
- backups, unattended, 52
- batch file, 18, 28, 51, 52

C

- changing IP addresses, 48
- Client Authentication, 44
- collection parameters, 14, 49
- Collector service
 - starting, 51
 - stopping, 51
- command line control of services, 18, 28, 51
- Control Panel applet for Performance Agent, 14
- Control Panel applet for Performance Agent, 21
- customizing
 - data collection parameters, 49

D

- data collection parameters, 49

- data directory, 14
- data source integration
 - alarming on data in PerfView, 48
 - viewing data in PerfView, 48
- data sources, adding PerfView
 - adding data sources for, 48
- default
 - collection parameters, 49
- disk space requirements, 14
- DNS name server, 15
- documents
 - Performance Agent documentation set, 54
 - viewing on the web, 55
 - viewing PDF files from UNIX, 55
- Domain Name System name server, 15

E

- examples directory
 - README, 33
- external data logging, 48

F

- files
 - authip, 45
 - status.scope, 32

firewall
 communicating across, 34, 40
 overview of Performance Agent
 communications configuration, 35
 systems with multiple IP addresses, 40

H

hardware requirements, 11
HOSTS file
 required if not using DNS, 15

I

installation procedures, 18
installation requirements
 hardware, 11
 networking, 15
IP addresses
 changing, 48

L

log files
 disk space required for, 14
 gaps in, 53
 managing, 14, 49
 maximum size of, 14
 not removed with uninstall program, 24
logging external data, 48
logging performance data, 14
 default parameters, 49

M

metric definitions, printing, 54
Microsoft RPC service, starting, 19
monitoring
 transaction data, 49
mwacmd.exe utility, 18, 28, 51, 52

N

networking considerations, 15

P

Path variable, 24
 modified by Performance Agent, 21
Performance Agent
 command line interface, 18, 28, 51
 default collection parameters, 49
 disk space requirements, 14
 documentation set, 54
 monitoring transaction data, 49
 networking considerations, 15
 release notes, 55
 setup program, 19
 starting, 18, 28, 51
 startup, 25
 status files, 32
 stopping, 18, 28, 51
 uninstallation, 23
Performance Agent Collector service
 starting, 51
 stopping, 51
Performance Agent service
 starting, 51
Performance Agent Services
 command line control of, 18, 28, 51
 security restrictions on, 27
 starting, 18, 28, 51
 stopping, 18, 28, 51
Performance Agent Services window, 21
performance data
 collecting, 49
 storage requirements for, 14
printable files, 54
printing documents, 54

R

- release notes, 55
- Remote Procedure Call service, starting, 19
- RPC service, starting, 19
- RPM Tools folder on Start Programs menu, 21

S

- security requirements
 - for de-installation, 18, 23
 - for services, 27
- setup program, 19
- starting
 - Microsoft RPC service, 19
 - Performance Agent, 18, 25, 28, 51
 - Performance Agent Services, 18, 28, 51
- Start Programs menu, RPM Tools folder on, 21
- status files, 32
 - coda.txt, 33
 - status.alarmgen, 32
 - status.mi, 33
 - status.perfalarm, 32
 - status.perflbd, 32
 - status.rep_server, 32
 - status.scope, 32
 - status.ttd, 33
- stopping
 - Performance Agent, 18, 28, 51
 - Performance Agent Services, 18, 28, 51
 - processes prior to installation, 18
- striped disks, collecting data for, 21

T

- TCP/IP protocol
 - required for Performance Agent, 15

- temp directory, 21
 - use of, 15
- transaction tracking, 49

U

- unattended backups, 52

V

- viewing
 - documents on the web, 55
 - PDF documents from UNIX, 55

W

- Windows
 - installation directory, 21
 - Path variable, 21, 24
 - temporary directory, 15, 21

