HP OpenView Operations/Performance for Windows®

Installation Guide

Version: 7.20

Manufacturing Part Number: B7491-90029

July 2003

Legal Notices

Warranty

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

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

Restricted Rights Legend

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

Hewlett-Packard Company
United States of America

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

Copyright Notices

Trademark Notices

OpenView® and VantagePoint® are trademarks of Hewlett-Packard Development Company, L.P.

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

Microsoft®, Windows NT®, Windows 2000®, Windows®, and MS Windows® are U.S. registered trademarks of Microsoft Corporation.

Pentium® is a U.S. registered trademark of Intel Corporation.

UNIX® is a registered trademark of The Open Group.

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

Support

Please visit the HP OpenView website at:

http://openview.hp.com/

There you will find contact information and details about the products, services, and support that HP OpenView offers.

The support area of the HP OpenView website includes:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information

contents

1

HP OpenView Operations/ Performance for Windows

Overview

HP OpenView Operations/Performance for Windows is a powerful, service-driven solution. It provides a business-driven approach to achieve rapid control of your IT infrastructure and services on heterogeneous platforms, including Windows and UNIX systems.

It offers the ability to monitor, control, and report on the health of your entire IT infrastructure.

Products on the Media

This release of the HP OpenView Operations/Performance for Windows solution includes OVO for Windows (OVO), Smart Plug-ins (SPIs), and add-on products on the installation CDs. SPIs and add-on products provide additional documentation (not included in this guide) that you should read before installing these components.

This guide gives a brief description of each of these products and instructions for running the common installer. Product documentation, including file name and location on the installation media, is described in Chapter 8, Documentation.

The Power of SPIs

HP OpenView for Windows 7.20 Smart Plug-ins (SPIs) provide preconfigured, out-of-the-box functionality to simplify and enhance your ability to manage the services and environment that are critical to your business. By means of preconfigured policies, SPIs monitor and measure hundreds of key application availability and health indicators, report and display data in a single console, and offer corrective actions to resolve problems promptly.

All SPIs include report and graph templates, and many SPIs provide service views out-of-the-box so you can view business-critical services and infrastructure right away. SPIs included on the product media are described in further detail in the following pages.

HP OpenView Operations for Windows (OVO)

HP OpenView Operations for Windows is a distributed, client/server software solution designed to provide service-driven event and performance management of business-critical enterprise systems, applications, and services.

OVO enables management of distributed, heterogeneous e-business infrastructures and includes support for a broad range of Windows and UNIX systems and applications, including e-commerce, web and application servers, conferencing and email, databases, ERP software, and more.

OVO provides console and server functionality to centrally monitor performance and events using agents installed on nodes being managed. To install add-ons and Smart Plug-ins, you must first install OVO on a management server.

Components included as part of the OVO basic functionality include the following three core Smart Plug-ins (SPIs), which are included as part of the basic product and do not need to be separately purchased or installed. All other products included on the media and described in this documentation require additional license purchases.

Smart Plug-in for Windows Operating System

The Smart Plug-in for Windows Operating System (Windows OS SPI) provides preconfigured policies and tools for managing the operations and performance of your Windows nodes. This functionality is provided as part of the OVO product and includes system and basic application management, including policies to manage Exchange, SQL, and Active Directory (AD). Where preconfiguration is either not possible or not necessary, it can easily be customized to suit specific needs.

The Windows OS SPI integrates seamlessly with OVO and its related products. The integration provides policies, tools, user roles, and a powerful automatic service discovery feature to help you monitor and manage your local and distributed Windows-based file systems and processes.

Smart Plug-in for UNIX Operating System

The Smart Plug-in for UNIX Operating System (UNIX OS SPI) is designed to monitor the availability and performance of typical UNIX-based operating systems. The UNIX OS SPI provides preconfigured monitoring solutions for the most important UNIX platforms; where preconfiguration is either not possible or not necessary, it can easily be customized to suit specific needs.

The UNIX OS SPI integrates seamlessly with OVO and its related products. The integration provides policies, tools, user roles, and a powerful automatic service discovery feature to help you monitor and manage your local and distributed UNIX-based file systems and processes.

Smart Plug-in for Web Servers

The Smart Plug-in for Web Servers integrates with OVO and provides policies, tools, and other configuration information to manage web servers such as Apache, Microsoft IIS, Microsoft Proxy Server, Microsoft Site Server, and Microsoft Commercial Internet System on Windows 2000 systems. Management is mainly carried out through monitoring Windows Event Logs, Windows Services, Windows Processes, and Windows Performance Monitor.

Smart Plug-in for Microsoft Active Directory Server

The Smart Plug-in (SPI) for Active Directory adds master operations, replication, DNS, and DIT monitoring capabilities to OpenView Operations for Windows. The Active Directory SPI also includes a tool, the AD Topology Viewer, that generates a map, showing replication connections among Active Directory sites/domain controllers. In addition to the map, the AD Topology Viewer also provides a hierarchical rendering of Active Directory components.

By using the Active Directory SPI, you stay informed of Active Directory-related conditions as follows:

- Data is consistent across all domain controllers and replication is completing successfully in a timely manner.
- Systems are able to cope with outages.
- All role masters are running and domain controllers are not contending with overly utilized CPUs.
- Active Directory is not experiencing capacity and fault-tolerance issues.

Smart Plug-in for Microsoft Exchange Server

The Smart Plug-in (SPI) for Microsoft Exchange Server adds Exchange server-monitoring capabilities to OVO and supports Exchange versions 5.5 and 2000. After the Exchange SPI is installed, configured, and deployed, you can use the OVO console to receive Exchange-related messages/alarms, configure graphs that chart Exchange performance, increase Exchange availability and performance, and improve Exchange capacity management and planning. Additional features include:

- Process monitor (to monitor the amount of CPU time being used by core Exchange processes).
- Inactive Process Monitor (to monitor core Exchange processes for activity and status).
- Exchange Service Monitor (to monitor Exchange Server processes for activity).
- Data of message processes by Message Transfer Agent and SMTP.
- MTA Work Queue and SMTP Queues.
- IS Public Average Delivery Time

- IS Private Average Delivery Time

Smart Plug-in for Microsoft SQL Server

The Smart Plug-in for Microsoft SQL Server helps administrators efficiently manage SQL Server environments of any size, from a single SQL Server database managed with local tools to a distributed environment of hundreds of databases managed from a central, best-in-class console. Features include:

- More than 30 predefined threshold events and several logfile conditions.
- Space management, concurrency problems, and workload metrics.
- Interception of hundreds of error log messages such as corruptions and space shortages.

Smart Plug-in for Informix

The Smart Plug-in for Informix helps administrators manage Informix environments of any size, from a single Informix database managed with local tools to a distributed environment of hundreds of databases managed from a central, best-in-class console. Additional features include:

- More than 45 predefined threshold events and over 150 logfile conditions.
- Space management, transaction management, and memory metrics.
- Interception of error log messages such as panics, chunkdown, and lock table overflow.

Smart Plug-in for Oracle

The Smart Plug-in for Oracle helps administrators efficiently monitor distributed enterprise-wide Oracle environments from a central best-in-class console. Features include:

- More than 80 predefined threshold events and more than 90 logfile conditions.
- Space management, table/index performance, and rollback segments.
- Snapshot reports of database environments when alerts occur.

- Thresholds based on ratios and percentages rather than raw data.
- Continuous availability to monitor Oracle listener, a single point of failure.

Smart Plug-in for Sybase

The Smart Plug-in for Sybase helps administrators efficiently manage Sybase environments of any size, from a single database managed with local tools to a distributed environment of hundreds of databases managed from a central, best-in-class console. Features include:

- More than 65 predefined threshold events and more than 15 log file conditions.
- Replication, index tuning, and resource hogs.
- Interception of over 1,000 error log messages such as corruptions and space shortages.

Smart Plug-in for Microsoft Enterprise Servers

The Smart Plug-in for Microsoft Enterprise Servers provides preconfigured policies for managing the operations and performance of Microsoft enterprise servers on your Windows nodes and offers these features:

- Topology/Service Mapping
- Service Monitoring
- Measurement Threshold Monitoring
- Event Log Monitoring

The Smart Plug-in for Microsoft Enterprise Servers supports the following Microsoft Enterprise Servers:

- Application Center 2000
- BizTalk Server 2000/2002
- Commerce Server 2000/2002
- Content Management Server 2001/2002
- Host Integration Server 2000

- Internet Security and Acceleration Server 2000
- Mobile Information Server 2000
- SharePoint Portal Server 2001

Smart Plug-in for mySAP.com

The Smart Plug-in for mySAP.com is a software package linking mySAP.com to OVO. The union offers a complementary and consolidated view of mySAP.com performance information and overall resource characteristics.

The SPI for mySAP.com provides the following capabilities for managing your mySAP.com systems:

- Availability management
- Performance management
- Service reporting
- Combined availability and performance management

Smart Plug-in for BEA WebLogic Server

The HP OpenView BEA WebLogic SPI integrates BEA WebLogic Server into the rest of the IT environments managed by the HP OpenView family of products. The WebLogic SPI monitors the following areas:

- Server performance
- Transaction rates
- Servlet executing times, time-outs, request rates
- Enterprise Java Bean resource utilization
- JDBC connection status
- Java Message Service
- Java Virtual Machine heap utilization
- Web applications
- User-definable metrics to extend monitoring for the performance of any custom applications that expose MBean management data via JMX

Smart Plug-in for IBM WebSphere

The HP OpenView SPI for WebSphere offers centralized tools that help you monitor and manage systems using IBM WebSphere. The WebSphere SPI monitors the following areas:

- Server availability and performance and memory usage
- Transaction rates
- Servlet executing times, time-outs, request rates
- JDBC connection status
- Web application processing and exception counts of scheduled
- WebSphere actions
- Java message service processing cluster processing

HP OpenView Reporter 3.0

Reporter is a flexible management reporting solution for the distributed IT environment. It automatically converts data captured by OVO agents into web-formatted, management-ready reports.

HP OpenView Network Node Manager (NNM) 6.2

Network Node Manager provides an accurate, open, extensible, and easy-to-use network management solution, which can be used out-of-the-box or easily customized to meet your needs.

Included capabilities let you know when there is a problem, so you can resolve it before it escalates to a critical stage. You can also intelligently collect and report on key network information and plan for network improvements.

Network Node Manager (NNM) Adapter

The NNM Adapter is an integration component that allows the automatic discovery and display of NNM nodes as a group that can be viewed the same way you view all other node sources in OVO. You can select and add them as a group to OVO and autodeploy policies based on node type.

HP OpenView Problem Diagnosis

HP OpenView Problem Diagnosis (PD) is a powerful, automated IP network path analysis tool that presents end-to-end path information clearly and concisely. Problem Diagnosis lets you see detailed information from nodes and devices in a particular path, and can be launched from other OpenView products like Network Node Manager and OVO.

HP OpenView Problem Diagnosis gives Network Operations Center (NOC) and Service Desk operators and engineers tools for fast problem diagnosis and resolution in IP-based networks. In particular, Problem Diagnosis offers:

- NetPath: A probe-based tool that finds and monitors the paths between itself and any reachable node that it is configured to test. A NetPath probe collects data over time and generates statistical and usage data about the paths it monitors.
- ShowPath: A path finder that leverages Network Node Manager functionality and topology data to determine the active path between two nodes in the NNM discovery domain.
- Integration: Integrates with HP OpenView NNM and OVO. For integration with NNM, PD must be installed on the same server as NNM, as explained in the PD documentation.

HP OpenView Network Diagnosis Add-On Module (NDAOM)

The Network Diagnosis Add-On Module is an integration component that provides detailed information from the Problem Diagnosis tool on network performance and how this performance is affecting services in your OVO environment. New service views help to identify network failures in relation to OVO-monitored services that are relying on those network connections. Reporting on networking statistics, network status, and performance data is achieved in conjunction with HP OpenView Reporter.

HP OpenView Performance Agent

The HP OpenView Performance Agent collects, summarizes, time stamps, and detects alarm conditions on current and historical resource data across your system. It provides performance, resource, and end-to-end transaction response time measurements and supports network and database measurement information.

Data collected outside of the performance agent can be integrated using data source integration (DSI) capabilities. Network, database, and your own application data can be brought in through DSI. This data is treated like data collected by OV Performance Agent; it is logged and time-stamped and can be alarmed.

Although OVO includes a combined event/performance agent (OV Operations Agent, or OVOA), OVOA's performance component provides basic performance monitoring capability. In contrast, OVPA (also sometimes referred to as MeasureWare Agent, or MWA) is an advanced performance monitoring agent. OVOA's performance component provides a subset of the metrics collected and features provided by the OV Performance Agent. These additional OVPA features, such as support for Application Response Measurement (ARM), API data collection, configurable data collection intervals, and performance data storage and management functions, are more advanced and may only be required in certain situations. For environments where the advanced OV Performance Agent is required, co-existence of the two agents (OV Operations Agent with embedded performance and advanced OV Performance Agent) is supported. Both agents can be installed on the same managed node.

➤ OV Performance Agent requires OV Performance Manager to graph the advanced performance data that it collects and OV Reporter to report on the advanced performance data.

HP OpenView Performance Manager

Performance manager (OVPM), a web-based analysis and planning tool, provides graphs and drill-down data of near real-time system performance information. With this information, you can evaluate system performance, manage systems, look at usage trends, and make system performance comparisons. Performance Manager can display the following items:

- Graphs, such as line, bar, or area graphs.
- Tables for data such as process details
- Baseline graphs
- Dynamic graphs in Java format that allow you to turn off display of individual metrics or hover over a point on a graph and see the values displayed.

Performance Manager displays consolidated performance information for systems with any of these agents or data collection software installed:

- OpenView Reporter
- OpenView Performance Agent (OVPA)
- OpenView Internet Services (OVIS)
- OpenView Operations 7 Agent
- VantagePoint Windows 6 Agent: Measurement Data Collector (MDC)
- Assorted Smart Plug-ins (SPIs) that supply data to a supported agent.

Before You Install

Some of the components you will install have prerequisites and require you to take some action before proceeding with the installation. Prerequisites are described below. If you are upgrading from a previous installation of HP OpenView ManageX, HP OpenView Express, HP OpenView VantagePoint for Windows, or HP OpenView Operations/Performance for Windows, please read the upgrade information below before proceeding with any installation steps.

If You are Upgrading...

If you are upgrading from HP OpenView ManageX, HP OpenView VantagePoint for Windows, HP OpenView Express, or HP OpenView for Windows 6.0, you may need to perform certain steps before installing HP OpenView Operations for Windows. Depending on your current product, you may be required to save your data or save any custom policies you developed. Tools are provided in some instances to make this process easier.

If you are upgrading from HP OpenView for Windows 7.0 to 7.20, see the instructions to back up and restore the reporting components database. These are available in the *HP OpenView Operations/Performance for Windows Upgrade Guide Version 7.20* and in the help topic “Back up and restore the reporting component database.”

If you are upgrading from HP OpenView for Windows 7.10 to 7.20, refer to the upgrade guide for details.

⚠ Do not uninstall your current product before reading the upgrade guide that applies to your current installation. See either the *HP OpenView Operations/ Performance for Windows Upgrade Guide Version 7.20* or the *HP OpenView Guide for Upgrading from ManageX/OV Express to OpenView Operations 7.0 for Windows*. The uninstall procedure otherwise results in permanent loss of management server data.

Required Windows Services

Certain Windows services are required for OVO installation, operation, and uninstallation. See the list of minimum Windows services in Chapter 2, Requirements.

SQL Server 2000 Support

OVO supports SQL Server 2000 only. The OVO server installs an SQL Server 2000 Desktop Edition (MSDE) instance named ".\OVOPS". After OVO installation, this instance can be upgraded to SQL Server 2000 Enterprise or Standard Edition by running that product's installation program and selecting "Upgrade Instance." This is described in detail in the SQL Server 2000 Online Books.

Microsoft Desktop Edition (MSDE) in OVO

HP OpenView Operations for Windows 7.20 includes Microsoft's MSDE with Service Pack 3.

The Microsoft Desktop Edition supports the following:

- Up to two processors on NT and Windows 2000
- 2GB data storage
- Up to six users
- Up to 16 named instances of MSDE on a given computer

For more information, see the following Microsoft web sites:

http://msdn.microsoft.com/library/default.asp?URL=/library/backgrnd/html/msdeforvs.htm

http://msdn.microsoft.com/library/default.asp?url=library/en-us/distsql/distsql_84xl.asp

OpenView Performance Agent

The OpenView Operations Agent (OVOA) and the OpenView Performance Agent (OVPA) can coexist on the same managed node. If you plan to install the HP OpenView Performance Agent (formerly called HP OpenView MeasureWare Agent) on this system in future, be sure to install in a directory path with no spaces. This is not a requirement if the Performance Agent already exists on the system.

OVO for Windows and Internet Information Services (IIS)

During management server installation, OVO connects to and configures IIS. You should first ensure that IIS contains all security patches deemed necessary for your site; activating IIS can potentially make your site vulnerable to virus attacks. For this reason, you may want to install only those IIS basic web page services specified in Chapter 2, “Requirements.” OVO supports IIS version 5.0.

Consult your IIS documentation and relevant Microsoft web sites for information regarding available IIS patches.

OVO Installation and Terminal Services

OVO management server and remote console may be installed via a Windows 2000 Terminal Services session only when the following criteria are met:

- Windows 2000 Terminal Services is running in Remote Administration Mode.
- Setup.exe for either component is run from the local file system on the target server (not from CD).

Terminal Services Support

OVO for Windows supports local and remote consoles executed via Windows 2000 Terminal Services under these conditions:

- When troubleshooting an OVO for Windows console issue that may be related to Windows 2000 Terminal Services, please verify the matter without running Terminal Services prior to contacting to OVEC or CPE teams.
- Windows Terminal Services are supported for use with OpenView Operations for Windows 7.x on Windows 2000, SP1 or later. Windows 2003 is not supported.
- Windows 2000 Terminal Services are supported in administration mode, which limits users to two concurrent sessions with the following hardware:
    - Management Server: PC with dual/multi 800 MHz Intel Pentium III or compatible processor, 768 MB Ram, at least 20 GB disk space, CD-ROM drive, and a dedicated system that is not a domain controller.
- Operating the console on Windows 2000 Terminal Services in application mode (maximum eight concurrent sessions) is supported, but requires all OVO for Windows and SPI components to be installed prior to installing Terminal Services.
    - When you are operating the console in application mode, in addition to Terminal Services admin mode requirements, 48 MB physical and 64 MB virtual memory must be added for each connected terminal service user.
    - When you are operating the console in application mode, you have to temporarily switch back to Terminal Services admin mode in order to install additional SPIs or OVO for Windows patches.

➤ This statement of support for Windows Terminal Services is only valid for the original Windows Terminal Server shipped with Windows 2000 and does not include any Terminal Server derivatives such as Citrix Metaframe.

Windows 2000 Fully-Qualified Domain Name (FQDN)

On Windows 2000, if the FQDN is not set on the management server system before installing OVO, the server is installed and configured with only the short name. For example, if the system is named “ov_server.first.hp.com” and the system has no DNS suffix set, the server name is set to "ov_server" when the system call `gethostbyname` is made.

On NT 4, the actual FQDN is returned. This discrepancy can affect applications written to support both NT 4.0 and Windows 2000 with the same binary files.

To correct this problem, set the Primary DNS suffix for the Windows 2000 system, as explained below. After this is set and the system is rebooted, behavior is the same on NT 4.0 and Windows 2000. If your Primary DNS suffix is already set correctly, you do not need to follow these steps.

Additionally, installing the server with just the short name can result in name resolution problems in agent node communication, because the OVO agent will use this short name to reach the server. This can result in problems that are difficult to resolve.

Set the Primary DNS Suffix

If the management server is installed in a DNS environment which uses domain suffixes, follow these directions to set the Primary DNS suffix.

1. Right-click the **My Computer** icon on the Windows 2000 desktop and select **Properties**.
2. Select the **Network Identification** tab and click **Properties** to open the **Identification Changes** dialog box.
3. Click **More** to open the **DNS Suffix and NetBIOS Computer Name** dialog box.
4. Type in the domain suffix for your computer.
5. Click **OK** to close the dialog boxes and confirm your changes.
6. Reboot your computer.

Manual Agent Installation

You can manually install the OVO Agent on the following computers:

- Windows:
  - Windows 2000
  - Windows NT 4.0
  - Windows XP
  - Windows Server 2003
- UNIX
  - HP-UX
  - Linux (RedHat, Suse, Debian, or Turbo)
  - Solaris
  - HP Tru64
  - AIX

See the help topics “Agent installation on Windows computers” and “Agent installation on UNIX computers” for details on manually installing agents.

About this Book

This guide provides the following information:

- Software and hardware requirements for installing the OVO components.
- Security information needed to properly implement OVO for Windows.
- Steps for installing the management server and management console of OVO on Microsoft Windows 2000 computer systems.
- Steps for installing required software on Windows managed nodes and information on installing and activating UNIX managed nodes.
- Steps for uninstalling OVO.
- Steps for installing the Network Node Manager Adapter.
- Steps for installing the Problem Diagnosis Network Diagnosis Add-on Module (NDAOM).

- More information on using OVO.
- Available documentation, file name, and location.

➤ This guide is for experienced Windows 2000 administrators.

Finding Additional Information

Additional information about OVO is available from several sources. The help system, containing over 1900 topics, is the primary source of information on how to configure your environment, perform day to day administrative tasks, and monitor and resolve events using the messages and maps available in the console.

Overviews, concepts, and upgrade instructions are available from other sources shown in the table. The table provides guidelines, but is not a complete list. See Chapter 8, “Documentation,” for details of other documentation provided with OVO and the help system Table of Contents for complete details on Help contents.

Table 1 Documentation RoadMap

Documentation	Where to find it	Content Highlights
HP OpenView Operations / Performance ReadMe	• Documentation \ ReadMe files hp OpenView OV Operations 7.20 for Windows startup CD	• What's New in this release • Known problems • Corrections and workarounds
HP OpenView Operations / Performance for Windows Installation Guide	• Documentation \ OVO Guides \ OVOInstall.pdf hp OpenView OV Operations 7.20 for Windows startup CD	• Hardware and software requirements for supported platforms • Security concerns • Installation steps
Basic Training	• Appears automatically after installation • Help system Table of Contents: Basic Training	• Step by step tutorial on all basic configuration and setup tasks You are strongly encouraged to work through the tutorial.

Table 1 Documentation RoadMap (continued)

Documentation	Where to find it	Content Highlights
OVO Help System (all procedures and tasks)	• OVO console Help dropdown menu • Product shortcut menus • Help buttons in dialog boxes • Standalone by opening the file: <%OVinstalldir%>\Nls\1033\Help\console.chm on the management server	• Configuration tasks — Configure Nodes — Configure Services — Configure Tools — Configure User Roles — Configure Service Types • Policy Tasks — Create, edit, deploy, remove, save, enable, disable policies — Install and remove agents — Policies and policy groups • Configure policies — Configure sources — Command line programs — Policy Types • Smart Plug-ins provided — Windows OS SPI — UNIX OS SPI • Any other SPIs purchased

Table 1 Documentation RoadMap (continued)

Documentation	Where to find it	Content Highlights
HP OpenView Integrated Service Assurance for Windows featuring HP OpenView Operations/ Performance for Windows Concepts Guide	• http:// www.openview.hp.com/ demos/index.html Select the link "hp OpenView integrated service assurance for Windows."	• High-level view of product features and concepts and scenarios for their use.
Upgrade Only *HP OpenView Guide for Upgrading from ManageX/ OV Express to OpenView Operations 7.0 for Windows.*	• Documentation\ OVO Guides \ManageXUpgrade.pdf hp OpenView OV Operations 7.20 for Windows startup CD	• Preparations for upgrade • Instructions for upgrading to OVO from a previous installation of HP OpenView ManageX or HP OpenView Express
Upgrade Only *HP OpenView Operations/ Performance for Windows Upgrade Guide Version 7.20.*	• Documentation\ \OVO Guides \OVOWUpgrade.pdf hp OpenView OV Operations 7.20 for Windows startup CD	• Preparation for upgrade • Instructions for upgrading to OVO from a previous installation of HP OpenView VantagePoint for Windows or HP OpenView Operations/Performance for Windows

2

Requirements

HP OpenView Operations for Windows (OVO) does not support the following scenarios:

- Reporter 2.0 and OVO management server/console installed on the same system
- Remote, unattended installation of OVO on the management server/console
- Installing OVO on a network drive
- Encrypted file systems
- Management server configured to use DHCP without a fixed IP address (DHCP is supported for managed nodes.)
- Installing the management server or console on Windows NT
- The OVO management server and remote console are not supported on a domain controller.

Running the management server in a Microsoft Cluster High Availability (HA) environment is possible. You should note the following requirements and limitations when installing on a node in a cluster:

- Management server software runs only on that node.
- Management server software cannot be run as an HA package; it cannot switch to another cluster system.

- System the management server software runs on must have a fixed IP address.
- If the node fails, the management server application is lost until the node is restored.

Hardware Requirements

Listed below are the minimum hardware requirements for OVO.

➤ Multiprocessor systems are supported.

Management Console

- PC with 500 MHz Intel Pentium (or compatible) processor, 1GHz recommended
- CD-ROM drive required
- 256 MB Physical Memory, with at least 256 MB Virtual Memory (page file)
- Minimum 1 GB hard disk space, 150 MB required for installation
- Minimum: 17-inch monitor with 1024x768 resolution and at least 256 colors.

  Recommended: 19-inch monitor with 1280x1024 resolution and at least 256 colors

Management Console/Server Combined System

- PC with 500 MHz Intel Pentium III (or compatible) processor, 1 GHz recommended
- 512 MB Physical Memory, with at least 512 MB Virtual Memory (page file)
- Minimum 10 GB hard drive, 1.2 GB disk space required for installation (depending on selected product options)

- Recommended at least 4 GB free disk space for event and performance data bases, hard drive with at least 20 GB recommended
- CD-ROM drive required
- Minimum: 17-inch monitor with 1024x768 resolution and at least 256 colors.

  Recommended: 19-inch monitor with 1280x1024 resolution recommended (if used as console system) and at least 256 colors

Managed Node Windows

OVO supports Windows 2000, Windows NT 4.0, Windows XP Professional, and Windows Server 2003.

Before installing OVO, be sure the Windows 2000, Windows NT 4.0, Windows XP Professional, and Windows Server 2003 systems you select as managed nodes meet the following hardware requirements.

- Agent Processes

  15 MB memory for agent processes.
- Local Drive

  40 MB hard disk space required for installation. Up to 40MB may be required for the performance database, depending on the configured collections. The actual disk space used depends on which packages and policies are installed on the managed node and the amount of performance data collected.

Restrictions if the Default Local System Account is Not Used

Observe the following restrictions if you are installing to an NT 4.0 primary domain controller or Active Directory domain controllers:

Active Directory Domain Controllers

If you want to install agents on Active Directory domain controllers (DC) and if you cannot use the default Local System account (your agent is running as an HP ITO account) follow the sequence described:

The Active Directory DC with the Primary domain controller (PDC) emulator FSMO role has to be installed with the agent software before you attempt to install the agent on any additional DC. After the installation of the first DC, it may take some time for the account information to be published to the other DCs. The installation of the agent software will only succeed if the account information has been replicated.

NT 4.0 Nodes as Primary Domain Controllers

The NT 4.0 node acting as a primary domain controller (PDC) has to be installed with the agent software before attempting to install the agent on any NT 4.0 backup domain controller (BDC) node. Additionally, after the installation of the PDC, it may take some time for the account information to be published to the BDCs. The installation of the agent software will only succeed if the account information has been replicated from the PDC.

If your agent is running as a Local System account, you can disregard these instructions.

Managed Node HP-UX

OVO supports HP-UX 10.20, 11.00, 11.11, and 11.22.

Before installing OVO, make sure that the HP-UX 10.x/11.x systems you select as managed nodes meet the following hardware requirements:

- Disk Space

  28 MB (about 80 MB is required during the software installation)

- Additional swap space

  None

- Additional RAM

  None

Only PA-RISC version 1.1 or higher is supported on HP-UX 10.20 managed nodes.

For HP-UX 11.22, IA64 is supported in 32-bit native mode only.

Managed Node Sun Solaris

OVO supports Sun Solaris 2.6, 7, 8, and 9.

Before installing OVO, make sure that the Sun Solaris systems you select as managed nodes meet the following hardware requirements:

- Disk Space

  65 MB (plus 65 MB required during software installation) for a total of 130 MB

- Additional swap space

  None

- Additional RAM

  None

Managed Node IBM AIX

OVO supports IBM AIX 4.3.1, 4.3.2, 4.3.3, and 5.1.

Before installing OVO, make sure that the IBM AIX systems you select as managed nodes meet the following hardware requirements:

- Disk Space

  45 MB (plus 45 MB required during software installation) for a total of 90 MB

- Additional swap space

  None

- Additional RAM

  None

Managed Node HP Tru64 UNIX

OVO supports HP Tru64 UNIX 4.0F, 4.0G, 5.0A, 5.1, 5.1A and TruCluster 5.1 and 5.1A.

Before installing OVO, make sure that the HP Tru64 systems you select as managed nodes meet the following hardware requirements:

- Disk Space

  50 MB (plus 50 MB required during software installation) for a total of 100 MB

  NOTE: For TruCluster systems, this disk space is required on each node.

- Additional swap space

  None

- Additional RAM

  None

Managed Node Linux RedHat

OVO supports Linux RedHat 6.2, 7.0, 7.1, 7.2, 7.3 (6.1J, 6.2J, 7.0J, 7.1J, 7.2J, 7.3J) SuSE 6.4, 7.0, 7.1, 7.2, 7.3, and 8.0 on Intel x86, Debian 2.2, 3.0, and Turbo Linux (Japanese only) 6.1J, 6.2J, 6.5J, and 7.0J.

Before installing OVO, make sure that the Linux systems you select as managed nodes meet the following hardware requirements:

- Disk Space
  - OVO agent must be installed on a second extended (`ext2`) file system.
  - 70 MB (plus 70 MB required during software installation) for a total of 140 MB

- Additional swap space

  None

- Additional RAM

  20 MB

Software Requirements

The following section describes the software requirements for Windows and UNIX platforms.

Windows platforms include NT4.0, 2000, XP, and Windows Server 2003

UNIX platforms include HP-UX, Sun Solaris, Tru64, AIX, and Linux. See the individual sections for details.

Management Console/Server Combined System, Windows 2000 Only

- Windows 2000 Server Edition, or Advanced Server Edition, SP3 is required.
- Adobe Acrobat Reader 5.0. It is available on the installation media, or you can download it from the **www.adobe.com** web site.
- Internet Explorer 5.0 with SP2 or higher
- Internet Information Services (IIS) 5.0. See page 39 in this chapter for minimum requirements.
- If you are running OVO and want to use DNS discovery, you must configure the DNS server to allow this. The DNS server should be set to Allow Zone Transfers. If the DNS and ADS domain names are different you will also need to create a New Zone in the DNS server configuration to match the ADS domain name. You should also add secondary DNS servers to the name servers list so that they can be searched by OVO. It may take several hours for the data to be propagated throughout the domain and appear correctly in OVO discovery. Please consult your DNS Server documentation for details on how to configure these zones correctly.

Remote Management Console

OVO supports remote consoles on Windows 2000, XP, and 2003.

- Adobe Acrobat Reader 5.0 is required. It is available on the installation media, or you can download it from the **www.adobe.com** web site.

- Internet Explorer 5.0 with SP2 or higher.

➤ Remote Microsoft Management Consoles (MMC) consoles are only supported if the management server has been installed using the domain installation. Remote MMC consoles are not supported with a standalone installation of the management server.

OVO for Windows Web Console

In addition to the MMC console interface, OVO provides a web console, supported on the following platforms:

- Internet Explorer 4.0 on Windows NT 4.0 SP4 and later
- Internet Explorer 5.0 on Windows 2000 SP2 and later
- Internet Explorer 5.5 on Windows 2000 SP2 and later
- Internet Explorer 6.0 on Windows 2000 SP2 and later
- Internet Explorer 6.0 on Windows Server 2003
- Internet Explorer 6.0 on Windows XP
- Netscape 4.7 on Windows 2000 SP2 and later
- Netscape 4.7 on RedHat Linux 7.x
- Netscape 4.7 on HP-UX 10.20 and 11.x
- Netscape 4.7 on Solaris 2.x
- Netscape 6.1 on Windows 2000 SP2 and later
- Netscape 6.1 on RedHat Linux 7.x

Windows Managed Node Software Requirements

The following section contains requirements for Windows managed nodes Windows NT 4.0, 2000, XP, Windows Server 2003, and Novell NetWare.

➤ Running the management server in a Microsoft Cluster HA package is possible. See page 31 for requirements and limitations.

You can run without NetBIOS as part of your Windows 2000 and XP managed node networking environments as long as Active Directory Service (ADS) client software is installed.

Required Windows Services

Certain Windows services are required for the installation, operation, and uninstallation of OVO. Be sure that the necessary Windows services are running before you install OVO. Required services may vary slightly, depending on platform.

Internet Information Services

OVO supports Internet Information Services (IIS) version 5.0 and requires certain components in order to run. You may wish to install only the required basic web page services listed, to minimize your vulnerability to virus attacks.

- Common Files (must be selected for any IIS installation)
- World Wide Web (WWW) server
- Internet Information Services Snap-In (forced by WWW server selection)

All other IIS components are optional.

Services Required for Windows Agents

Windows NT 4.0, 2000, XP, and Windows Server 2003 agent requirements include basic services, services needed for installation, services required for certain policy types, and services required to launch tools. Required services vary slightly between the platforms.

Basic Services

The following basic services are required; they cannot be stopped.

- Event Log (Windows 2000, Windows NT 4.0)
- Plug & Play (Windows 2000)
- RPC Service (Windows 2000, Windows NT 4.0)
- Security Accounts Manager (Windows 2000)

Installation and Uninstallation

The same services required for installation are required if you uninstall OVO. Required services vary somewhat by platform. For Windows 2000, required services include the following examples. The stated purpose is an example of the use of the service, but may not be the only use of the service.

Table 2 Windows 2000 Required Services for OVO Installation

Service	Purpose
Net Logon	• Required for authentication
Remote Registry	• Checks whether the node is already managed
Server	• Maps C$ to copy the binaries to the machine
Workstation	• Required by the Net Logon service

Table 3 Windows NT 4.0 Required Services for OVO Installation

Service	Purpose
Net Logon	• Required for authentication
NT LM Security Support Provider	• Required for authentication

Table 3 Windows NT 4.0 Required Services for OVO Installation

Service	Purpose
Server	• Required to map shares
TCP/IP Net BIOS Helper	• Required by the Net Logon service
Workstation	• Required by the Net Logon service

Additional Services Required for Policy Types

The additional services required for policy types are the same on both Windows 2000 and Windows NT 4.0, as shown:

Table 4 Services Required for Policy Types on W2K, NT 4.0

Policy Type	Service
WMI	• Windows Management Instrumentation
Service Auto Discovery	• Windows Management Instrumentation
SNMP	• SNMP Trap Service
Measurement Threshold • Source type: MIB • Source type: WMI	• SNMP Service • Windows Management Instrumentation

In addition to the services listed above, additional services might be required by instrumentation binaries. This includes instrumentation shipped with OVO Windows and OVO Smart Plug-ins (SPIs).

Additional Services Required for Launching Actions and Tools

Additional services required after installation for launching actions and tools are the same on both Windows 2000 and Windows NT 4.0, as shown:

Table 5 Services Required for Launching Actions and Tools

Services	Purpose
Net Logon	• Required for authentication
NT LM Security Support Provider	• Required for authentication

SNMP Requirements for all Windows Managed Nodes

All Windows managed nodes must meet these SNMP requirements to collect SNMP events and discover node properties:

- SNMP service must be installed and running
- Must have at least READ ONLY access to the community name “public” (See “System Type, OS Type, and OS Version for Managed Nodes” on page 46 for further details.)
- Option “Accept SNMP packets from any host” enabled

Managed Node Windows 2000

- Windows 2000 Professional, Server Edition, Advanced Server Edition or Data Center Edition, Service Pack 1, 2, or 3. Windows 2000 without any service packs is not supported.
- Recommended: Windows 2000 SP3, which fixes a WMI problem in Service Pack 2.

Microsoft recommends that users accept all critical updates from Windows Update, available from the top of your Start menu. Click Windows Update to reach the Microsoft Windows Update web page, where you can scan for recent updates of critical and lesser severity. A list of critical updates is returned and you can select those you want to download. HP OpenView for Windows 7.20 was tested with Microsoft’s critical updates.

Managed Node Windows XP

Microsoft recommends that users accept all critical updates from Windows Update, available from the Admin dialog. Select All Programs →Windows Update to reach the Microsoft Windows Update web page, where you can scan for recent updates of critical and lesser severity. A list of critical updates is returned and you can select those you want to download. HP OpenView Operations for Windows 7.20 was tested with Microsoft's critical updates.

SNMP trap interception and MIB monitoring requires SP1 on Windows XP.

Managed Node Windows Server 2003

Must meet the requirements for the SNMP service for all Windows managed nodes, as described in this chapter on page 42.

Microsoft recommends that users accept all critical updates from Windows Update, available from the Admin dialog. Select All Programs →Windows Update to reach the Microsoft Windows Update web page, where you can scan for recent updates of critical and lesser severity. A list of critical updates is returned and you can select those you want to download. HP OpenView Operations for Windows 7.20 was tested with Microsoft's critical updates

Managed Node Windows NT 4.0

Before installing OVO, be sure the following software is installed on the Windows NT nodes you want to manage.

- Windows NT 4.0 Workstation, Server Edition, or Enterprise Edition, Service Pack 4 or higher.
- Recommended: Service Pack 6a (MS hotfix Q297534 is highly recommended).
- Recommended: WMI version 1085 core components. To verify that you have the correct version of WMI, select **Start Programs Administrative Tools WMI Config Manager**. In the **General** tab of the WMI Control Window, the WMI version should be 1085.0005. (Available on the OVO for Windows installation CD as `wmicore_1085.exe` under the directory`\Redist`.)

- Must meet the requirements for the SNMP service for all Windows managed nodes, as described in this chapter on page 42.

➤ You must reapply the Microsoft Service Pack after installing SNMP Services.

Managed Node Novell NetWare

HP OpenView Operations for Windows version 7.20 provides alerting, performance monitoring, and reporting for NetWare® machines through one or more Windows machines acting as SNMP proxies. The SNMP proxy machines will have an OpenView Operations for Windows agent installed and will forward messages and events obtained via SNMP from the NetWare nodes to the Operations for Windows server.

HP OpenView Operations for Windows 7.20 introduces support for Novell NetWare 6.0.

Novell NetWare 6.0 Hardware Requirements

NetWare will run on the minimum system requirements listed below. For optimal performance, the system should meet the recommended requirements. For further details on Novell NetWare 6, see the manual *Novell NetWare 6 Overview and Installation,* provided with your NetWare product.

Minimum System Requirements

- Server class PC with a Pentium* II or AMD* K7 processor
- 256 MB of RAM
- Super VGA display adapter
- A DOS partition of at least 200 MB and 200 MB available space
- 2 GB of available disk space outside the DOS partition for volume SYS:
- One network board
- A CD drive
- USB, PS/2*, or serial mouse (recommended but not required.)

Recommended System Requirements

- Server class PC with two-way Pentium III 700 MHz or higher processors. Note that NetWare 6 can run on as many as 32 processors.
- 512 MB of RAM
- Super VGA or higher resolution display adapter
- DOS partition with 1 GB of available space
- 4 GB of available disk space outside the DOS partition
- One or more network boards
- A bootable CD drive that supports the El Torito specification
- USB, PS/2*, or serial mouse

Novell NetWare Software and Other Requirements

Depending on the network configuration, you might need one or more of the following software and information.

- *NetWare 6 Operating System* CD
- *NetWare 6 License / Cryptography* diskette
- Supervisor right at the [Root] of the eDirectory tree
- Supervisor right to the container where the server will be installed
- Read right to the Security container object for the eDirectory™ tree
- DOS and CD drivers (required if the computer does not boot from CD)

  You can make a bootable floppy diskette using the MKFLOPPY.BAT program located in the INSTALL directory of the *NetWare 6 Operating System* CD.
- Client connection utilities (optional, for installing from a network):
  - Novell Client™ for DOS and Windows*3.1x (optional, for installing from a NetWare server running IPX™).
  - IP Server Connection Utility (optional, for installing from a NetWare sever running IP only).

    For instructions, see PRODUCTS\SERVERINST\IPCONN.TXT on the *Novell Client* CD.

- IP address and domain names (required for connecting to the Internet):
  - An IP address
  - An IP address of a domain name server
  - The name of your domain

    For IP addresses and domain names, contact your network administrator and Internet Service Provider.
- Network board and storage device properties, such as the interrupt and port address (required if not included in NetWare)

  For more information, contact your computer hardware manufacturer.

System Type, OS Type, and OS Version for Managed Nodes

This information is required in order to deploy policies to the managed node. For the system type, OS type, and OS version to be automatically determined when a node is put under management, an SNMP service/daemon should be running on the managed node. In addition, at least the management server needs to have access read permissions to “system” (the SNMP object on the managed node).

By default, the management server uses the “public” community name to access the “system” object. If, in your organization, a different community name is being used for SNMP read access to the systems, you can change this default as described in the help topic “System Types” in the section titled “Changing the SNMP community name for automatic discovery of a node's properties.”

Some operating systems (for example, Sun Solaris) allow limiting access to the “system” SNMP object (for example, localhost only), which can prevent the management server from determining the information. Please consult the SNMP manuals on how this is done on a specific operating system.

If system type, OS type, and OS version cannot be determined automatically, which is not always possible despite the fact that everything is configured correctly, you can specify them manually.

UNIX Managed Node Software Requirements

Listed below are the hardware and software requirements for UNIX managed nodes. Supported systems include HP-UX, Sun Solaris, IBM AIX, HP Tru64, and Linux, as shown in Table 6, which also lists Windows agents to provide a complete list of OVO managed nodes.

Refer to the following tables for details on:

- Supported operating system versions
- Kernel parameters for the UNIX managed nodes.

Table 6 OS Versions on Managed Nodes Supported by OVO for Windows

Operating System	Platform	Supported OS Versions
AIX	IBM RS/6000 BULL DPX/20	4.3.1, 4.3.2, 4.3.3, 5.1 4.3.1 HACMP 4.2.2 & 4.3.1 4.3.2 HACMP 4.2.2 & 4.3.1 4.3.3 HACMP 4.2.2 & 4.3.1 5L (5.1) HACMP 4.4.1
HP-UX	HP 9000 Technical Workstations	10.20, 11.00, 11.11, 11.22 (11.22 supports IA64 in 32-bit native mode only) 10.20 MCSG A.10.10 and up 11.00 MCSG A. 11.12 and up 11.11 MCSG A. 11.12 and up 11.22 MCSG not supported
	HP 9000 Enterprise Servers [b]	10.20, 11.00, 11.11, 11.22
Linux (RedHat)	Intel Pentium compatible only [c]	6.2, 7.0, 7.1, 7.2, 7.3 E & J

a Direct port access mode.

b OVO for Windows uses the same binaries as for HP 9000 Technical Workstations.

c See `http://hardware.redhat.com/hcl/`for a list of platforms that are compatible with Linux RedHat.

Table 6 OS Versions on Managed Nodes Supported by OVO for Windows

Operating System	Platform	Supported OS Versions
Linux (SuSE)	Intel Pentium compatible only	6.4, 7.0, 7.1, 7.2, 7.3, 8.0
Debian	Intel Pentium compatible only	2.2, 3.0
TurboLinux (Japanese only)	Intel Pentium compatible only	6.1J, 6.2J, 6.5J, 7.0J
Solaris	Sun SPARC Fujitsu-Siemens SPARC	2.6, 7, 8, 9 2.6 Veritas Cluster Server 1.3.0; 2.0, 3.5; Sun Cluster 2.2 7 Veritas Cluster Server 1.3.0, 2.0, 3.5; Sun Cluster 2.2 8 Veritas Cluster Server 1.3.0, 2.0, 3.5; Sun Cluster 3.0 9 Veritas Cluster Server 3.5; Sun Cluster 3.0
HP Tru64 UNIX	Compaq	4.0F, 4.0G, 5.0A, 5.1, 5.1A TruCluster 5.1, 5.1A
Novell NetWare (proxy solution only)	Intel 486 or higher	OVO for Windows 7.0 and 7.10: 4.1, 4.1 SFT III, 4.11, 4.11 SFT III,5.0, and 5.1 OVO for Windows 7.20, all platforms listed for 7.0 and 7.1, plus Novell NetWare 6.

[a] Direct port access mode.

[b] OVO for Windows uses the same binaries as for HP 9000 Technical Workstations.

[c] See `http://hardware.redhat.com/hcl/`for a list of platforms that are compatible with Linux RedHat.

Table 6 OS Versions on Managed Nodes Supported by OVO for Windows

Operating System	Platform	Supported OS Versions
Windows NT [a]	Intel 486 or higher	4.0 SP4, SP5 or SP6a (NT Server, Workstation, and Enterprise Edition) MS Cluster Service on NT Server & Enterprise Edition
Windows 2000	Intel Pentium and compatible.	5.0, SP1, SP2, SP3 (Professional, Server, Advanced Server, DataCenter Families) MS Cluster Service on Advanced Server & Data Center
Windows XP	Intel Pentium and compatible.	Windows XP Professional SP1
Windows Server 2003	Intel Pentium and compatible.	Windows Server 2003, Standard Edition Windows Server 2003, Enterprise Edition* (32-bit only) Windows Server 2003, Datacenter Edition* (32-bit only) Windows Server 2003, Web Edition

[a] Direct port access mode.
[b] OVO for Windows uses the same binaries as for HP 9000 Technical Workstations.
[c] See `http://hardware.redhat.com/hcl/`for a list of platforms that are compatible with Linux RedHat.

Table 7 gives values for kernel parameters on HP-UX managed nodes. Other UNIX-based agent platforms generally require similar values, which may have different names, depending on the operating system. Consult your operating system documentation for details.

Table 7 Important Kernel Parameters for Managed Nodes

Parameter	Description	Minimum Value
nfile	Maximum number of open files.	20 [a]
semmns	Required semaphores.	20
shmmax	Maximum shared memory.	None required.
msgmni	Message queues.	None required.
nflocks	File locks.	10

[a] This number depends upon several factors. Normally a value of 20 per process is sufficient. However, the more logfiles that are configured for the logfile encapsulator, the more file descriptors are needed. Normally, one logfile requires about one file descriptor. Any actions that result in processes being started on the managed node need additional file descriptors.

Managed Nodes, HP-UX

OVO for Windows 7.20 provides three sets of binary files for HP-UX managed nodes, located in the three separate directories shown below. HP-UX 11.00 supports both 11.00 and 11.11. There is no separate agent for 11.11.

- HPUX\10.20 (on PA-RISC)
- HPUX\11.00 (for both 11.00 and 11.11, also on PA-RISC)
- HPUX\11.22 (for 11.22, on Itanium, native, 32-bit mode).

A directory is named with that platform version which is the lowest one it is supporting. You can use agents from this directory up to the version where a new directory is created. For example, if there are two directories, one labeled 11.00 and another 11.22, then the one labeled 11.00 supports all OS versions 11.00 up to, but not including, 11.22. The directory labeled 11.22 supports all OS versions 11.22 and above.

Managed Node HP-UX 10.20

Before installing the OVO agent, be sure the following software is installed on the HP-UX 10.20 managed nodes you want to manage.

- Operating System

  See Table 6 for details.

- Recommended Operating System Patches

XSW700GR1020	s700:HP-UX General Release Patches, September 2001, B.10.20.54.1
XSW800GR1020	s800: HP-UX General Release Patches, September 2001, version B.10.20.54.1

- Patches listed in the following table are required.

Table 8 Required Patches for HP-UX Managed Nodes

OS Version	Patch ID	Description
HP-UX 10.20	PHCO_25640	libc cumulative patch (supersedes PHCO_23684)
	PHSS_17225	dld.sl(5) cumulative patch
	PHSS_22354	HP aC++-AA runtime libraries (aCC A.01.30)
	No dependencies.	

Table 8 Required Patches for HP-UX Managed Nodes (continued)

OS Version	Patch ID	Description
HP-UX 11.0	PHCO_25707	libc cumulative patch (supersedes PHCO_24148)
	PHSS_24627	HP aC++_AA runtme libraries (aCC A.03.33) (supersedes PHSS_22543)
	PHSS_26262	ld(1) and linker tools cumulative patch (supersedes PHSS_23440)
	QPK1100	Quality Pack for HP-UX 11.0, September 2001 version B.11.00.54.7
	PHNE_22814	s700_800 11.00 patch for EISA 100VG-AnyLAN product
	Required Dependencies	
	PHCO_23651	ifsck_vxfs(1M) cumulative patch
	PHCO_23963	libc cumulative header file patch
	PHKL_18543	PM/VM/UFS/async/scsi/io/DMAPI/JFS/perf patch
	PHKL_22677	fix of getdirentries, MVFS, rcp, mmap & IDS
	PHKL_24027	VxFS 3.1 cumulative patch
	PHKL_25906	Probe,IDDS, PM, VM, PA-8700, asyncio, T600, FS
	PHKL_26059	syscall, signal, umask cumulative patch
HP-UX 11.11	PHCO-24402	libc cumulative header file patch (supersedes PHCO_23094)
	PHCO_26124	libc cumulative patch (supersedes PHCO_23427)
	PHNE_25625	ONC/NFS General Release/Performance Patch (supersedes PHNE_24910)
	PHSS_24638	HP aC++_AA runtime libraries (aCC A.03.33) supersedes PHSS_22898)

Table 8 Required Patches for HP-UX Managed Nodes (continued)

OS Version	Patch ID	Description
11.11	PHSS_26263	ld(1) and linker tools cumulative patch (supersedes PHSS_23441)
	GOLDBASE11i:	GoldBase Patches for HP-UX 11.11, June 2001; version B.11.11.0106.9
	PHSS_22898	HP aC++ -AA runtime libraries (aCC A.03.30)
	PHSS_23441	s700_800 11.11 ld(1) and linker tools cumulative patch
	PHNE_24910	ONC/NFS General Release/Performance Patch.
	PHNE_27063	Cumulative ARPA Transport patch
	Required dependencies	
	PHCO_24777	mountall cumulative patch
11.22	PHKL_28465	Processes not reactivated for a long time.
	PHKL_28670	Memory pressure with JFS3.3
	PHSS_27285	A.05.38 C++ library patch
	PHSS_27289	Improved performance/accuracy of libm.
	PHSS_27661	linker + fdp cumulative patch
	PHSS_28976	libunwind Library Cumulative Patch

Ensure that patch PHNE_24211 is not installed. It causes the embedded performance component to eventually core dump.

- System Parameters

  See Table 7, Important Kernel Parameters for Managed Nodes for details. You can verify and change the system parameters using the SAM tool.

- DCE RPC

  DCE RPC version 1.2.1 or higher on HP-UX 10.20

  SD package: DCE-Core.DCE-CORE-RUN

- Internet Services

  SD package: `InternetSrvcs.INETSVCS-RUN`

- LAN/9000

  SD-package: `Networking.NET-RUN`

- SNMP Agent for MIB Monitoring

  SD package for HP-UX 10.20 and lower: `NetworkingSnmpAgent`

- Native Language Support (NLS) Package

  SD-package: `OS-Core.NLS-AUX`

Managed Node HP-UX 11.x

Before installing OVO, be sure the following software is installed on the HP-UX 11.x managed nodes you want to manage.

- Operating System

  See Table 6, OS Versions on Managed Nodes Supported by OVO, for details.

- Operating System Patches: See Table 8 for required patches.

- System Parameters

  See Table 7 for details. You can verify and change the system parameters using the `SAM` tool.

  If monitoring performance metrics with the embedded performance component, increase the value of the kernel parameter `max_thread_proc` to at least (Number_of_Policies *2).

- DCE RPC

  DCE RPC version 1.7 or higher.

  SD package: `DCE-Core.DCE-CORE-RUN`

  OVO supports DCE versions supplied with the HP-UX 11.x operating system. Although the HP-UX operating system includes DCE, you must install DCE separately as an optional product.

- DCE/9000 Kernel Thread Support

SD package for HP-UX 11.0 DCE-KT-Tools

➤ Required for HP-UX 11.0 and HP-UX 11.11.

DCE-KT-Tools, which is available on the HP-UX Application Software CD-ROMs, contains a runtime library for kernel threads that OVO requires in order to run. For HP-UX 11.11, DCE-KT-Tools is included with the base installation. For HP-UX 11.00, you must install DCE-KT-Tools separately.

To install DCE-KT-Tools, start the swinstall GUI of SD-UX, change the software view to `Start with Products`, and choose `DCE-KT-Tools`. DCE-KT-Tools is licensed with the HP-UX OS.

- Internet Services

  SD package: `InternetSrvcs.INETSRVCS-RUN`
- LAN/9000

  SD package: `Networking.NET-RUN`
- SNMP Agent for MIB Monitoring

  SD Package for HP-UX 11.x and higher: `OVSNMPAgent`
- Native Language Support (NLS) Package

  SD package: `OS-Core.NLS-AUX`

Managed Node Sun Solaris

OVO supports Sun Solaris 2.6, 7, 8, and 9 on SPARC.

Before installing OVO, make sure that the following software is installed on the Sun Solaris managed nodes you want to manage.

- Operating System

  See Table 6, OS Versions on Managed Nodes Supported by OVO, for details.

- Required Patches for Sun Solaris Managed Nodes

  The following patches are required for the OVO Sun Solaris managed nodes. They are available from the `www.sunsolve.sun.com` web site.

➤ The Sun Microsystems download site may contain more recent patches than those listed in Table 9. Patches with higher version numbers than those listed should be usable, but they have not been tested with OVO. Note that Sun only allows downloading of their latest version

Also see the section "Problems Caused by Missing OS Patches for Sun Solaris" on page 58.

Table 9 Required Patches for Sun Solaris Managed Nodes

OS Version	Patch ID	Description
Solaris 2.6	107733-09	SunOS 5.6: Linker patch
Solaris 2.6	105591-11	SunOS 5.6: Shared library patch for C++
Solaris 2.6	106429-02	SunOS 5.6: /kernel/drv/mm patch
Solaris 2.6	105181-29	SunOS 5.6: Kernel update patch
Solaris 2.6	105210-38	SunOS 5.6: libaio, libc & watchmalloc patch
Solaris 2.6	105568-23	SunOS 5.6: /usr/lib/libthread.so.1 patch
Solaris 2.6	105633-59	OpenWindows 3.6: Xsun patch
Solaris 2.6	106841-01	OpenWindows 3.6: Keytables patch
Solaris 2.6	106842-09	SunOS 5.6: Feature patch for Euro currency support in Solaris 2.6
Solaris 7	106950-15	SunOS 5.7: Linker patch
Solaris 7	106327-10	SunOS 5.7: 32-Bit Shared library patch for C++
Solaris 7	107544-03	SunOS 5.7: /usr/lib/fs/ufs/fsck patch
Solaris 7	106541-17	SunOS 5.7: Kernel update patch
Solaris 7	106980-17	SunOS 5.7: libthread patch

Table 9 Required Patches for Sun Solaris Managed Nodes

OS Version	Patch ID	Description
Solaris 8	109147-09	SunOS 5.8: Linker patch
Solaris 8	108434-03	SunOS 5.8: Shared library patch for C++
Solaris 8	108827-11	SunOS 5.8: libthread patch

- Kernel Parameters: Set the following parameters shown in Table 10.

Table 10 Recommended Kernel Parameters for Sun Solaris Managed Nodes

Parameter	Description	Minimum Value
semmap	Number of entries in semaphore map	15 or greater
semmni	Number of semaphore identifiers	30
semmns	Number of semaphores in system	200 or greater
semms1	Maximum number of semaphores per ID	100

You can check and change the kernel parameters by editing the `/etc/system` file.

➤ In Table 7, the minimum value of 20 for nfile depends upon several factors. Normally a value of 20 per process is sufficient. However, the more logfiles that are configured for the logfile encapsulator, the more file descriptors are needed. Normally, one logfile requires about one file descriptor. Any actions that result in processes being started on the managed node need additional file descriptors.

- Communication Software

OVO supports the DCE RPC communication type. If none of the supported DCE packages is installed (or running) on the managed node, then the `HPlwdce` (HP Lightweight DCE runtime version 1.1) is installed and configured during agent installation. See Table 11 for details regarding supported DCE packages.

Table 11 Supported DCE Packages

OS	DCE
Solaris 2.6	TransArc DCE 2.0, HPlwdce, DASCOM DCE 1.1
Solaris 7	IBM DCE 3.1, HPlwdce, DASCOM DCE 1.1
Solaris 8	IBM DCE 3.1, HPlwdce, DASCOM DCE 1.1
Solaris 9	IBM DCE 3.1, HPlwdce, DASCOM DCE 1.1

- ARPA/Berkeley Services
- MIB

  The MIB monitoring functionality of OVO requires the snmpd of the HP OpenView platform, or SNMP-based, MIB-I (RFC 1156) or MIB-II (RFC1158) compliant agent software.

Problems Caused by Missing OS Patches for Sun Solaris

If the operating system patches for Sun Solaris are missing, the following problems occur:

- Patch Versions

  If version -04 or -05 of patch 101327 is installed, the OVO installation fails on Sun Solaris managed nodes with the following message:

  ```
  tar xof...core dump
  ```

  To solve this problem, do one of the following:

  — Install patch version -06 (or later).

  — De-install the old patch.

  To check which patches are currently installed on Sun Solaris systems, enter:

```
showrev -p
```

- Multi-processor Patch

  Be sure you have the following patches installed. The monitor agent process (opcmona) may hang on a multi-processor Solaris managed node if the following patches are not installed.

  For Solaris 2.6, use the following recommended patches:

  105568-23

  105210-38

  For Solaris 7, use the following recommended patches:

  106980-16

  106541-17

  107544-03

  For Solaris 8, use the following recommended patches:

  108827-11

Managed Node IBM AIX

OVO supports IBM AIX 4.3.1, 4.3.2, 4.3.3, and 5.1

Before installing OVO, be sure the following software is installed on the IBM AIX managed nodes you want to manage:

- Operating System

  See Table 6 on page 47 for details.

- Operating System Patches

  To resolve Monitor Agent (opcmona) crashes in mbstowcs () subroutine, at least the following revisions of OS patches should be installed on the system:

bos.rte.libc	4.3.3.89 (AIX 4.3)
box.rte.libpthreads	4.3.3.80 (AIX 4.3)

Maintenance Level 5100-03	5.x (AIX 5L)

- Runtime Operating System Library

  These libraries are prerequisites for the installation of the AIX agent. They can be downloaded from IBM's AIX Fix Distribution Service at:

  http://techsupport.services.ibm.com/rs6k/fixdb.html

xlC.rte	4.0.2.0
xlC.aix43.rte	4.0.2.1

  For AIX 5.1, corresponding libraries are installed from the OS CD default installation.

- System Parameters

  See Table 7, Important Kernel Parameters for Managed Nodes. You can verify and change system parameters with the System Management Interface Tool (SMIT) tool.

- Communication Software

  OVO supports the DCE RPC communication type.

- ARPA/Berkeley Services
- MIB-I or MIB II

  The MIB monitoring functionality of OVO requires SNMP-based, MIB-I (RFC 1156) or MIB-II (RFC 1158) compliant agent software.

Requirements for DCE RPC on AIX Managed Nodes

The DCE RPC communication type requires that you must install the following software:

- DCE on AIX

  DCE is supplied with the AIX operating system up to version 4.3.3. Nevertheless, you must install DCE separately.

- Filesets on AIX 4.3

On AIX 4.3 DCE RPC, you must install *one* of the following filesets:

dce.client.core.rte 2.1

dce.client.rte 2.1

dce.client.core.rte.admin 2.1

Managed Node Linux RedHat

OVO supports Linux RedHat 6.2, 7.0, 7.l, 7.2, 7.3, and SuSe 6.4, 7.0, 7.1, 7.2, 8.0 on Intel x86, and Debian 2.2 and 3.0.

The following software must be installed on Linux managed nodes:

- Operating System and Parameters

Supported operating system and kernel versions are listed in Table 12 on page 63.

The following kernel features must be enabled:

- CONFIG_NET

  Networking support
- CONFIG_BINFMT_ELF

  Kernel support for ELF binaries
- CONFIG_SYSVIPC

  System V IPC
- CONFIG_INET

  TCP/IP networking
- CONFIG_NETDEVICES

  Network devices support
- `CONFIG_EXT2_FS` or `CONFIG_REISERFS_FS`

  Second extended file system support or Reiser file system support
- CONFIG_PROC_FS

  Proc file system support

- Packages

  The following packages must be installed:

- bash
- gawk

In addition, the following packages must be installed for RedHat 7.x and SuSE 7.x:

- RedHat 7.x

  compat-libstdc++
- SuSE 7.x

  compat
- DCE RPC

  Delivered with the OVO agent packages.
- RedHat Package Manager (RPM)

  Must be installed.
- SNMP Daemon (optional)

To provide the management server with sufficient information to automatically determine the node type of the Linux managed node, the SNMP daemon (`snmpd`) should be running when you install the software remotely from the OVO management server. After you finish the installation, the daemon must be running if you want to use MIB variable monitoring.

Table 12 Supported Operating System and Kernel Versions

Language	Operating System and Version	Kernel	glibc, or libc6, or shlibs
English	RedHat 6.2	2.2.x x can be ≥ 14	2.1.3
	RedHat 7.0	2.2.x x can be ≥ 16	2.1.92
	RedHat 7.1	2.4.x x can be ≥ 2	2.2.2
	RedHat 7.2	Linux 2.4.x | x>=7	2.2.4
	RedHat 7.3	Linux 2.4.x | x>=18	2.2.5
	SuSE 6.4	2.2.x x can be ≥ 14	2.1.3
	SuSE 7.0	2.2.x x can be ≥ 16	2.1.3
	SuSE 7.1	2.2.x x can be ≥ 18 2.4.x x can be ≥ 0	2.2
	SuSE 7.2	2.4.x x can be ≥ 4	2.2.2

Table 12 **Supported Operating System and Kernel Versions**

Language	Operating System and Version	Kernel	glibc, or libc6, or shlibs
	SuSE 7.3	2.4.x x can be ≥ 10	2.2.4
	SuSE 8.0	2.4.x x can be ≥ 18	2.2.5
	Debian 2.2	2.2.x x can be ≥ 17	2.1.3
	Debian 3.0	2.4.x x can be ≥ 18	2.2.5
Japanese	RedHat 6.2J	2.2.x x can be ≥ 14	2.1.3
	RedHat 7.0.1J	2.2.x x can be ≥ 16	2.1.95
	RedHat 7.1J	2.4.x x can be ≥ 2	2.2.2
	RedHat 7.2J	Linux 2.4.x | x>=7	2.2.4
	RedHat 7.3J	Linux 2.4.x | x>=7	2.2.5
	TurboLinux 6.1J	2.2.x x can be ≥ 15	2.1.3
	TurboLinux 6.5J	2.2.x x can be ≥ 18	2.1.3
	TurboLinux 7.0J	2.4.x x can be ≥ 5	2.2.3

Table 13 Required Packages for Different Operating Systems and Versions

Language	Operating System and Version	Packages
English	RedHat 6.2	libstdc++ ldconfig glibc
	RedHat 7.0	compat-libstdc++ glibc
	RedHat 7.1	
	RedHat 7.2	
	RedHat 7.3	
	SuSE 6.4	compat shlibs
	SuSE 7.0	
	SuSE 7.1	compat glibc
	SuSE 7.2	
	SuSE 7.3	
	SuSE 8.0	
	Debian 2.2	libstdc++2.9glibc2.1 ldso libc6
	Debian 3.0	libstdc++2.9-glibc2.1 libc6

Language	Operating System and Version	Packages	
Japanese	RedHat 6.2J		
	RedHat 7.0.1J	compat-libstdc++	
	RedHat 7.1J		
	RedHat 7.2J		
	RedHat 7.3J		
	TurboLinux 6.1J Server		
	TurboLinux 6.5J Server		
	TurboLinux 7.0J Workstation	libstdc++-compat glibc	

Managed Node, HP Tru64

Please note that a directory is named with that platform version which is the lowest one it is supporting. You can use agents from this directory up to the version where a new directory is created. For example, if there are two directories, one labeled 4.0F and another 5.1A, then the one labeled 4.0F will support all OS versions 4.0F up to, but not including, 5.1A. The directory labeled 5.1A will support all OS versions 5.1A and above.

OVO supports HP Tru64 UNIX 4.0f, 4.0G, 5.0A, 5.1, 5.1A, and TruCluster 5.1 and 5.1A

Before you install the OVO agent software package, you must first uninstall any of the previous agent software packages installed on the managed nodes and remove the directories `/usr/opt/OV` and `/var/op/OV`.

Before installing OVO, be sure the following software is installed on the HP Tru64 UNIX managed node you want to manage:

- Operating System

  See Table 6 for details.

- Required Patches for the HP Tru64 UNIX Managed Nodes

  — The CXXREDIST632V11.tar patch is required for the HP Tru64 UNIX managed nodes except for Tru64 5.1A.

    Check if the installed libcxx is earlier than V60300001:

```
nm /usr/lib/cmplrs/cxx/libcxx.so | grep libcxx_V
```

```
_libcxx_V60200002   | 0004396996916008 | G | 0000000000000000
_libcxx_V60200003   | 0004396996916016 | G | 0000000000000000
_libcxx_V60300001   | 0004396996918728  | G | 0000000000000000
```

    If the symbol _libcxx_V60300001 exists in the image on your system, then you do *not* need to install this patch.

    You can download the latest version from the following web page:

    http://www.tru64unix.compaq.com/cplus

  — On a TruCluster, the following patch must be installed in order for clu_add_member to propagate the OOV agents properly when adding a TruCluster member. You can download the latest version from the following web pages:

    TruCluster 5.1:

    http://ftp1.support.compaq.com/patches/public/unix/v5.1/
    tcv51b20-c003710 1-18805-e-20030605 README

    TruCluster 5.1A:

    http://www.zk3.dec.com/dupatchwww/v50pats.html. Using the dupatch utility, install patach number TCRPAT00024600520 (00246-00).

- Kernel Parameters

  See Table 7 on page 50 for details.You can verify and change the kernel parameters using the setup tool.

  If monitoring performance metrics with the embedded performance component, and agent runs as non-root user, increase the value of the kernel parameter max_threads_user to: default + (Number_of_Templates * 2.)

- Basic Networking Services

  OSFCLINET4xx Basic Networking Services

- DCE Runtime Kit

  See the following table:

Table 14 DCE Runtime Versions

DCE Runtime Kit	Tru64 UNIX System	OS Version
DCERTS 310 DCE Runtime Services V3.1	single system only	V4.0D, V4.0E, V4.0F
DCERTS 320 DCE Runtime Services V3.2	single system only	V4.0G
DCERTS 400 DCE Runtime Services V4.0	single system	V5.0, V5.0A
DCERTS 410 DCE Runtime Services V4.1	TruCluster or single system	V5.1
DCERTS 420 DCE Runtime Services V4.2	TruCluster or single system	V5.1A

➤ OVO supports DCE versions supplied with the HP Tru64 UNIX operating system. However, although the HP Tru64 UNIX operating system includes DCE on the layered product CD up to version 5.0A, DCE has to be installed separately as an optional product.

For a TruCluster system, you must configure DCE on each TruCluster member individually.

- Japanese Base System

  `IOSJPBASE4xx` Japanese Base System. This system is only for managed nodes running HP Tru64 UNIX in a Japanese environment.

- Package: OSFINCLUDE440

  OSFINCLUDE440 Standard Header Files package is required for building executables on HP Tru64 UNIX nodes.

- Additional Prerequisite Packages

Install the following packages from the Associated Products Volume 1 CD, supplied with your HP Tru64 operating system.

-IOSWWBASE<version_id>
-IOSWWUCSBASE<version_id>, where version_id is:

- -440 for 4.0 F
- -445 for 4.0 G
- -520 for 5.1 A

Files are located here:

```
<cdrom_mount_point>Worldwide_Language_Support/kit
```

and can be installed with this command:

```
cd <cdrom_mount_point>/Worldwide_Language_Support/kit
setld -1 ‘pwd’ <package>
```

Reporter Versions and OVO

A new reporting component has been added to OVO. Reporter 2.0 with the OVO management server is not a supported configuration. Installing OVO on a machine where Reporter 2.0 is installed produces this message:

> The product Reporter has been detected on this system. Components of the Reporter product have been updated. Please install the newer version of the Reporter product to match the component version.

You must either uninstall Reporter 2.0 (and use the reporting component in OVO) or purchase and install Reporter 3.0 for full functionality and compatibility with OVO.

You can also install Reporter 3.5 with OVO for Windows 7.20 on the same system and no patches will be required.

Network Protocols

The following network protocols are used in OVO:

- OVO uses TCP and/or UDP.

- DCE RPC is used for connections between the management server and UNIX managed nodes.
- MS RPC is used for some communication between the management server and Windows managed nodes.
- DCOM is used for communication between the server and the consoles. DCE is used for some communication with Windows managed nodes. For the remote installation of the Windows agent, DCOM is still used.
- HTTP is used for some management server and agent combinations.
- Novell NetWare 6 can process Internet Protocol (IP) network packets and traditional Internetwork Packet Exchange (IPX) packets. The IPX protocol is required for the OVO Smart Plug-in for Windows Operating System. For further details, see the manual *Novell NetWare 6 Overview and Installation*, provided with your NetWare product.

Cluster Awareness in OVO

OVO supports cluster awareness for a number of platforms and for some Smart Plug-ins. Please see the help topic “Cluster support in OVO” for details on supported platforms.

3

Security

Review this section carefully before installing HP OpenView Operations for Windows. It contains information on how to set up and maintain security in OVO.

Before implementing OVO security, carefully consider your current environment and security needs in planning how to incorporate these security features.

Users who are establishing security for OVO should be:

- Experienced Windows 2000 administrators who understand Windows 2000 security concepts and terminology.
- Experienced with the Windows NT/2000 domain environment.

Security Groups and Accounts

Before installing and using OVO, you need to understand the following OVO security groups and accounts:

- Accounts Used for User Roles
  - HP-OVE-ADMINS group
  - HP-OVE-OPERATORS group
- Accounts Used for Remote Deployment

- HP-OVE-GROUP
- HP-OVE-User

- Account Used on the Managed Node
    - Local System account
    - HP ITO Account and opc_op account
    - root

Accounts Used for User Roles

- HP OpenView Enterprise Administrators (HP-OVE-ADMINS) group
- HP OpenView Enterprise Operators (HP-OVE-OPERATORS) group

OVO creates the HP-OVE-ADMINS and HP-OVE-OPERATORS groups locally on the management server when it is installed. The groups are initially empty (do not contain any members). However, all users who are members of the local Administrators group on the management server are treated as members of the HP-OVE-ADMINS group by default.

The purpose of these groups is to allow you to extend default accessibility to users who are not Windows 2000 administrators on the management server (using Windows 2000's User Manager tool). For example, you can add Rosa Galvez, who is not a Windows administrator, to the HP-OVE-ADMINS group so she can perform OVO administrator tasks, or add Sean Payne, another OVO user who is not a Windows administrator, to the HP-OVE-OPERATORS group.

Tasks Permitted by Group

Group membership confers certain privileges and rights, as described below.

➤ No user should be part of both groups. An OVO administrator should not be added to the HP-OVE-OPERATORS group. This also applied to Windows administrators on the management server, because they are automatically treated as OVO Admins.

HP-OVE-ADMINS Tasks

Users classified as HP-OVE-ADMINS can perform OVO Administrator functions. For example, they can add managed nodes, configure managed nodes, deploy policies, create and modify policies, tools, services, and user roles, and create automatic and operator-initiated commands. They can also expand and navigate Policy Management in the console tree, create and modify policies, and perform all operator tasks.

HP-OVE-OPERATORS Tasks

Users classified as HP-OVE-OPERATORS can perform all OVO tasks except those listed under HP-OVE-ADMINS tasks. For example, they can own and acknowledge messages, create and use message filters, add annotations, and send messages to the acknowledged messages browser. They can also execute tools if they have authority, view service maps, and draw performance graphs.

As an administrator, after adding a user to the HP-OVE-OPERATORS group, you can further define the rights of that user with the User Roles Editor, described in the online help in the “Creating User Roles” section.

Accounts Used for Remote Deployment

The following Windows accounts are used by OVO to control security:

- HP-OVE-GROUP account
- HP-OVE-User account

Installation types, described in the following section, define which Windows group or groups will be created during OVO installation.

Specifying an Installation Type

User and group accounts in Windows can be either local or domain accounts. When you specify these account names during installation, you need to decide whether you are going to use local or domain accounts. This decision is partially determined by whether you are going to do a domain or standalone installation.

Scenario 1: Domain Installation (Typical Installation)

This installation assumes the OVO management server to be a member of a Windows domain. This method creates (or uses existing) domain accounts and groups (default HP-OVE-User and HP-OVE-Group).

These domain accounts allow the OVO server to automatically manage a Windows node and install the agent software to this node.

The Windows node has to be either in the same domain as the OVO management server or must have a trust relationship in place with the domain of the management server. To add the HP-OVE-Group to a managed node successfully, the user running the OVO console has to have administrative permission on that Windows node (direct, or indirect via (for example) the Domain Admins group).

Scenario 2: Standalone Installation

This installation does not require any Windows domain accounts or groups and is not embedded in Windows security. The OVO management server can be either a member of a Workgroup (=standalone) or a member of a Windows domain. This installation method has the following limitations:

- Automatic agent software installation of Windows managed nodes is not possible (except the agent on the management server itself). All remote Windows managed nodes have to be installed using the Windows manual Agent installation.
- Agent functionality packages which are used by some SPI products cannot be auto-deployed and require manual installation on the Windows managed node (please refer to the installation instructions for each SPI).
- Remote MMC consoles are not supported with a standalone installation of the management server. Remote MMC consoles are only supported with the Domain installation option. However, you can use terminal services.
- If you perform a standalone installation on a production machine, you cannot later change this to a domain installation.

➤ Management server to agent communication, such as events, policy and instrumentation deployment, drawing graphs, and so on, is not affected by a domain vs. standalone installation.

UNIX managed nodes are not affected by a domain vs. standalone installation; they always require a manual installation process.

HP-OVE-GROUP Account

When the OVO management server is installed, you are asked to supply the name of a Windows group that can be used by several OVO services and processes to control their security rights. The information you supply here should reflect your standard Windows security policies and the way you intend to use OVO.

If you are doing a Domain Installation, you must provide the name of a Windows global group.

When adding nodes, this (HP-OVE-Group) Domain group will be added to the local administrators group on a Windows managed node and allows the management server to automatically install software (agent, packages) to this node.

If you are doing a Standalone Installation, you can only provide a name of a Windows group local to the machine you are installing on.

The installation checks to see if the group exists and if not it will try to create it. If it cannot create the group, enter another name or cancel out of the installation and find a valid name.

In order to create a domain account, the installing user has to have domain administrative privileges. If this is not possible, or desired, ensure that the accounts which are intended for use for OVO are already created and the password of the HP-OVE-User is available to the user installing the management server.

In order to create a local account, the installing user has to have local administrative privileges.

⚠ The account name that you supply during installation for HP-OVE-GROUP **cannot be changed**! If you do decide to change it, you must uninstall the product and then install it again.

This account is intended solely for the use of the OVO product. As such, the OVO product assumes that it owns this account and can safely manipulate it as needed to meet the needs of the product. Selecting an account that is used for other purposes may cause problems in your environment. Choose an account name that will not be used by anyone else in your organization.

HP-OVE-User Account

When the OVO management server is installed, you are asked to supply the name of a Windows user account that can be used by several OVO services and processes to control their security rights. The information you supply here should reflect your standard Windows security policies and the way you intend to use OVO.

This account is a member of the HP-OVE-Group. The management server processes are run in the context of this user account, which grants these processes access to managed nodes configured with the HP-OVE-Group.

If the user does not already exist and you are doing a domain installation, you must be a domain administrator for the domain in which you are creating the user.

‼ If you choose to grant the HP-OVE-User domain administrator capabilities, understand that this grants any OVO administrator administrative access to all nodes in the domain.

This account is intended solely for the use of the OVO product. As such, the OVO product assumes that it owns this account and can safely manipulate it as needed to meet the needs of the product. Specifying an account that is used for other purposes may cause problems in your environment. Choose an account name that will not be used by anyone else in your organization.

The account name that you supply during installation for HP OVO-User can be changed if necessary following installation using the `ovchgpass.exe` command. Use the command to change the user name, password, or both. This command changes the password everywhere that the OVO system uses this account, to ensure that OVO services do not fail. See online help for information about changing the password for this account.

Accounts Used on the Managed Node

- Local System account
- HP ITO Account and opc_op account
- root

Local System Account

In OVO for Windows 7.20, the OVO for Windows agent package is installed by default as a Local System account; the HP ITO Account and opc_op account that were used in previous versions of OVO are no longer created on Windows nodes.

If, in a previous version of OVO for Windows, you configured actions, tools, and scheduled tasks to run as an HP ITO Account, these tools, scheduled tasks, and actions will continue to run because they are mapped to the Local System account. The installation program does not force you to use the Local System account; if you are upgrading you can keep any user that you previously configured. See the *HP OpenView Operations/Performance for Windows Upgrade Guide Version 7.20* manual for further details on upgrades.

Additionally, if a tool or policy is configured to run as Local System, it will run on all agents because Local System is mapped to the HP ITO Account on agents where the agent runs as HP ITO Account.

However, if in a previous installation you have configured tools or policies to run as opc_op user, these tools and policies are not automatically mapped to the Local System account. You must either create the opc_op account manually or reconfigure such tools and policies to specify another user, such as Local System.

See the documentation for individual SPIs to determine how specific policies might be affected by this change.

Benefits of Default Local System Account

HP strongly recommends using the default Local System account, which offers several advantages:

- Adds no additional accounts on managed nodes (HP ITO Account and opc_op are not created.)
- Eliminates problems with agent installation in Active Directory environments when HP ITO Account cannot be created.
- Does not conflict with password policies.
- Does not conflict with domain policies that do not allow local accounts.
- Does not conflict with domain policies that remove necessary privileges or user rights.

- Takes advantage of improvements to certain Smart-Plug-ins, such as the Smart Plug-in for Exchange Server. Refer to specific SPI documentation for details.

Restrictions of the Local System Account

- The Local System account cannot be used when using message synchronization between this and another OVO for Windows server. In this case, both agents that run on the management server systems have to use the HP ITO Account. Agents on other systems can run using the Local System account. See the online help for details."

HP ITO Account and opc_op Account

In previous releases, the two local user accounts (HP ITO Account and opc_op account) were created on every Windows node and random passwords were generated. In OVO for Windows 7.20, the HP ITO Account and opc_op are no longer created on the node. Instead, the Local System account is used as the default.

If you are upgrading from a previous release that used the HP ITO Account, you can continue to use this account. Upgrades keep the existing user on the node. In the following situations, you must continue to use the HP ITO Account and opc_op:

- SPI for mySAP.com is not supported with the Local System account.
- Default tools supplied with OVO for Windows are migrated to use the $AGENT_USER account. If you are upgrading from a previous release, custom tools that were previously configured to run as opc_op user must be manually changed to use the $AGENT_USER account. If you do not change your custom tools, then you have to continue to use your old accounts if you want these tools to run.

Table 15 Differences between Operating Accounts

	opc_op	**HP ITO Account**	**Local System account**
When created?	During Operations agent package installation (OVO 7.10 and earlier.)	During Operations agent package installation (OVO 7.10 and earlier)	Created by Windows Operating System. Always present.
Member of Administrator's Group?	No	Yes: added during Operations agent installation	Yes: by default
Member of user's group?	Yes	Yes	N/A
Password aging: expires and has to be changed	Switched off by default. Can be turned on.	Switched off by default. Can be turned on. Should not be turned on for domain controllers.	No. System account does not have a password.
Typically used for	Tools and programs that run under a normal user account.	All agent processes Tools/programs that run with administrator privileges.	Most Windows services.

HP ITO Account

The HP ITO Account is no longer automatically created when OVO for Windows is installed. (Upgrade installations that used the HP ITO Account can continue to use this account.)

The HP ITO Account user has administrative privileges and is automatically added to the local Administrators group when created. The password is different on every machine, and you may experience difficulties if you must change the password.

OVO does not recommend changing the password of the HP ITO Account. If the password for this account is changed, you must manually reconfigure the Windows service that starts the ITO agent. To do this, use **Control Panel** → **Administrative Services** → **HP ITO Agent** → **Properties** → **LogOn** and change the password here as well. If this is not done, the ITO agent cannot start up after it has been stopped or the system has been rebooted.

OVO does not support changing the password of the HP ITO Account on domain controllers. The agent installation on domain controllers requires that the password must not be changed. If this is a problem, use the Local System account to run the agent.

If you are installing the OVO Agent software on a Windows NT 4.0 PDC or BDC, this user is automatically set up as a domain administrator. Windows NT PDC and Windows 2000 DC do not have local accounts.

On domain controllers, password aging should not be turned on and the password should not be changed because all domain controllers share the same domain-user account and password. Passwords can only be changed when all necessary agents are installed on the domain controllers. To install any new agents on domain controllers, you must first delete all existing agents on the domain controllers and reinstall them again.

opc_op Account

Beginning with this 7.20 release, the opc_op account is no longer provided by default with the OVO for Windows installation and its use is not recommended. (The opc_op account is still created on UNIX managed nodes.)

Default tools and policies included with OVO for Windows do not use the opc_op account. If you have customized tools or policies from an earlier installation that require the opc_op account, you must take one of the following steps so that these tools and policies will continue to function:

- Create the opc_op user manually using Microsoft administrative tools so that this account is available for the tools or policies that require it.
- Change the user account for these tools or policies to use another account which exists on the node.
- Use the new variable $AGENT_USER, which means that the tool or policy will be executed using the account the agent currently uses (this could be Local System or HP ITO Account). In this case the tool or policy has administrative privileges.

The `opc_op` account is a domain user on Domain Controllers and a local user on all other systems. This account is a member of the Users Group and does not have any special privileges.

This user can be used as a valid user for tools. However, to use tools, the opc_op user must have the correct access on the NTFS partition that will be accessed by the tool. The password is different on every machine.

UNIX Systems Root Agent Account

On UNIX systems, root is used as an agent account. The installation also creates an opc_op user account, which you can use to execute tools.

Access Requirements for NTFS Partitions

For NTFS partitions, note the following:

- The local groups named Administrators, HP-OVE-ADMINS, and HP-OVE-OPERATORS must have at least Execute access to all of the executable files in the %OVOINSTALLDIR%\bin directory and the Windows %SYSTEMROOT%\system32 directory on the management server. These accounts should also have Execute access to all subdirectories of these directories and all of the executable files in those subdirectories. In addition, these groups must either be given the Bypass Traverse Checking privilege or they must also have Execute access to all of the parent directories of these directories. By default, Windows NT/2000 installations give this type of access to “Everyone,” so you should only need to make changes like this if you modified your file system security from the default settings.
- Accounts used for running tools must have the correct access on any NTFS partitions that will be accessed by the tool.

- On FAT file systems or partitions, there is no security to set.

Security Requirements for Using OVO

Security is involved in many of the OVO tasks performed by administrators and operators, such as installing the management server, adding managed nodes, and using OVO from a console, management server, or managed node. The information below explains how these tasks relate to security.

Installing the Management Server

To install a management server, you must be a member of the domain Administrators group. At installation, the HP-OVE-ADMINS and HP-OVE-OPERATORS groups are created. You are prompted for the domain, group, user, and user password of the accounts you want OVO to use for its security. See “Installing the Management Server and Console” in Chapter 4 for installation procedures. For domain installations you must be logged on as a domain administrator (not a local administrator).

Installing the RemoteConsole

To install the remote console, you must be a member of the local Administrators group. See “Installing the Management Server and Console” in Chapter 4 for installation procedures.

To use the remote console, the user must be a memeber of at least the types of groups described in Chapter 3, Security.

Adding Managed Nodes

To add a managed node, you must be a Windows administrator on the management server or a member of the HP-OVE-ADMINS group on the management server. For installing agent software to Windows nodes from the console, the user you are logged in as on the console also must be a member of the local Administrators group(s) on the managed node(s) you are adding. The following table shows the three available options for installing managed nodes:

Table 16 Options for Adding Managed Nodes

Configuration	Result
• Domain installation: the managed node is in same domain or has a trust relationship with the domain, and • Current user (OVO Administrator) has administrative privileges on the node to be added.	The group HP-OVE-Group can be added automatically to the Local Administrators group on the node to be managed. The Windows agent can be automatically installed.
• Domain installation: the managed node is not in the same domain and no trust relationship exists, or • Installing user (OVO administrator) has no administrative privileges.	The node can be added. Agent installation must always be done manually.
• Standalone installation:	The node can be added. Agent installation must always be done manually.

The system you are adding as a managed node must be up and running.

When you click the **OK** or **APPLY** button in the Configure Managed Nodes dialog box, the Configure Nodes dialog box appears. OVO attempts to configure security for nodes you are adding as Windows NT/2000/XP, or Windows Server 2003 managed nodes (or nodes you are updating to the Windows NT/2000/XP/2003 type) as follows:

1 Based on the user you are logged in as, the utility attempts to do some security setup and reports the results. Specifically, it checks to see if the HP-OVE-GROUP account is part of the local Windows Administrators group on the managed node, and if it is not, OVO adds the account to the group. It also makes sure that this group has the “Logon as a batch job” and “Logon as a service” privileges.

2. If the security configuration attempt fails (for example, if the node is not up and running), you are notified but OVO makes no further attempt to configure security for the node. In this case, you must correct the problem and then configure security manually on any nodes for which configuration failed, using the Node Configuration tool. If the HP-OVE-GROUP account is already an Administrator account on the node and the account has the correct privileges, you can ignore the failure.

You can

If you add the Windows NT Primary Domain Controller (PDC) or Windows 2000 Domain Controller (DC) as a managed node, you allow tools and scheduled commands to be defined to run without a password. This means that any administrator who configures tools in this environment can configure a tool to run as any user (including domain administrator) in that domain without a password.

You can close this security concern by setting the /auth /on switch in the SetMgmtServer tool. This sets the server to require authentication. Tools and scheduled task policies have to be configured with a password. See the help topic “Set the management server and other options in the Operations agent package.”

Configuring a Windows NT BDC as a Managed Node

If you are using the HP ITO Account, you can configure a BDC (Backup Domain Controller) as a managed node, but first you must do the following:

- Add the PDC as a managed node.
- Deploy the OpenView Operations agent package to the PDC node.
- Synchronize your BDCs.

These steps apply only if you are using the HP ITO account. This sequence does not have to be followed if the Local System account is used. HP recommends that you use the Local System account on domain controllers..

For OVO to work correctly, you should designate that all or none of the domain controllers in the domain be managed nodes.

Adding Managed Nodes from Other Domains and Across Domains

Managed nodes can be added from other domains in two ways:

- Automatic agent and deployment package installation: This requires the domain of the managed node to trust the domain of the HP-OVE-User and the console user.
- Manual agent installation: This approach does not use Windows security; it is possible to manage nodes across different domains without any Windows domain trust relationship. With this approach, you must install the Windows agent manually.

Configuring Tools

As an OVO administrator, you can specify the account a tool runs under when it executes, according to the following requirements. Requirements may vary depending on the target location.

Target: OVO Management Console

If the target location for the tool is the OVO management console, the tool runs as the user logged on to that console.

- User name: cannot specify
- Password: cannot specify

Target: OVO Management Server, Managed Node, or Node List

If the target location for the tool is the management server, a managed node, or the node list, you can:

- Specify both the user name and password.
- Specify a user name and leave the password blank.
  - This uses a security authentication module, deployed as part of the OVO agent package, to authenticate the login for the tool. This form of authentication is useful; because no password was required, you do not have to update the configuration of tools using the specified account if the password changes.

  - If you are using a local account that has a different password on each node, a single tool definition works for all of them. If you launch a tool and specify only the user, OVO does not ask for a password or check for one.
  - Supplying the user name but not a password allows an administrator to set up a tool to run under a special account without needing to know the account's actual password. For example, an administrator can create an account (opc_op), but if opc_op changes its password, the administrator might not know the new password. In this case, OVO allows the administrator to launch the tool as opc_op using the security authentication module (opcauth.dll).

    However, the administrator would not be able to interactively login using this account. The administrator can start the tool using the opcauth.dll, but he cannot log on to the system as opc_op, because this would require a password which he does not know.

    If the tool uses domain users, then the domain controllers of the target node's domain have to be configured as managed nodes (See "Adding Managed Nodes" on page 82.) and the agent package has to be deployed to the domain controllers. Because the execution of a tool without a password will fail if the Windows authentication subsystem contacts a domain controller where the subauthentication library is not installed, the agent has to be installed on all domain controllers.

    This happens when the OVO agent package is deployed to the domain controllers. Leaving the name and password blank can be limiting because the account the tool runs as does not have network credentials.

- Leave both the user name and password blank.

➤ All limitations mentioned above for an empty password also apply when both the user name and password are blank.

  - If you leave the user name blank, you must also leave the password blank. On Windows nodes, the tool runs as the user logged in to the console. The user you are logged in as must be a domain user.

- The machine on which you want to run the tool must recognize the account name. This takes place if the machine you're logged in on is in the same domain as the target node. If not, the domain of the target node must trust the domain of the user account used when executing the tool.
- On UNIX nodes, the tool runs as opc_op, because the Windows user account of the console user cannot be used on UNIX systems.

➤ Automatic and operator-initiated commands execute on the managed node as the agent user (either Local System or HP ITO Account, as configured).

About the Security Authentication Module

Even though the security authentication module is installed by default, you can disable it using the SetMgmtServer tool described in online help. You can also manually remove `opcauth.dll`, located in the %SYSTEMROOT% directory (for example `C:\WINNT\SYSTEM32\opcauth.dll`) on the node where the tool user is authenticated. If you remove this DLL, then a password will always be required to run a tool under this account. If you remove this DLL on all DCs, you cannot do a switch user without a password for domain accounts.

If you choose to use the subauthentication library, then it must be deployed to one of the following two locations, depending on the name you supply.

Domain Account Name

The security authentication module must be deployed to the domain controller that authenticates the user. There might be several DCs in a domain, and depending on the availability of these DCs, the Windows authentication system will contact different DCs; for this reason the security authentication module must be deployed to all DCs of that domain. The security authentication module on the domain controllers authenticates the login for any machine when the tool is launched. However, in this case, the account that the tool runs as does not have network credentials.

➤ You cannot run tools using domain accounts without passwords if none of the domain controllers are available.

Local Account Name

The security authentication module must be deployed to each machine on which you want to run the tool. This deployment is automatic, because the security authorization module is deployed with the OVO agent package, which is also required in order to execute tools on the managed node.

4

Installing HP OpenView Operations for Windows

This chapter contains the following instructions:

- Installing OVO on the management server and console
- Uninstalling policies and packages from Windows managed nodes
- Uninstalling OVO
- Installing, uninstalling, and activating agents on UNIX nodes

This section assumes you are an experienced Windows NT/2000 administrator and that you understand Windows NT/2000 security concepts and terminology.

If this is your first time installing OVO, we recommend installing it on one or more test systems so that you can become familiar with OVO before using it in your business environment.

➤ If you have a version of HP OpenView Operations 6.0 (VantagePoint for Windows), HP OpenView ManageX, HP OpenView Express, or HP OVO 7.0 or 7.10 already installed and need to upgrade to a new version, see the appropriate upgrade guide for your current installation. Upgrade guides are available on the installation media in .pdf format and provide instructions on preserving your data before upgrading, agent upgrades, and policy upgrades. Upgrade guides are also available in printed format if you ordered manuals.

Installing the Management Server and Console

The information below explains how to install the OVO management server and console on Windows 2000 systems.

You can install both the server and console or the management console alone. While it is possible to install SQL Server 2000 before installing the OVO management server, you must do so manually. If you choose to use full SQL 2000, you need to upgrade your MSDE instance after installing OVO, as explained in Chapter 1, “SQL Server 2000 Support.”

To install a remote console, the installing user must have local administrative rights. To connect from a remote console to an OVO server, the domain user running the remote console must be any one of the following (via direct or indirect group membership).

1. Local administrator on the OVO for Windows server
2. Member of the local group OVE-ADMINS
3. Member of the local group OVE-OPERATORS

For items 1 and 2, the domain user on the remote console is considered to be an OVO for Windows Administrator. For item 3, the user is considered to be an OVO for Windows Operator.

OVO does not support installing the management server or console on a domain controller. See the beginning of the Requirements chapter for other scenarios that are not supported.

Prior to Installation

- Ensure that all system requirements are met.
- Review the security information in Chapter 3 of this manual.

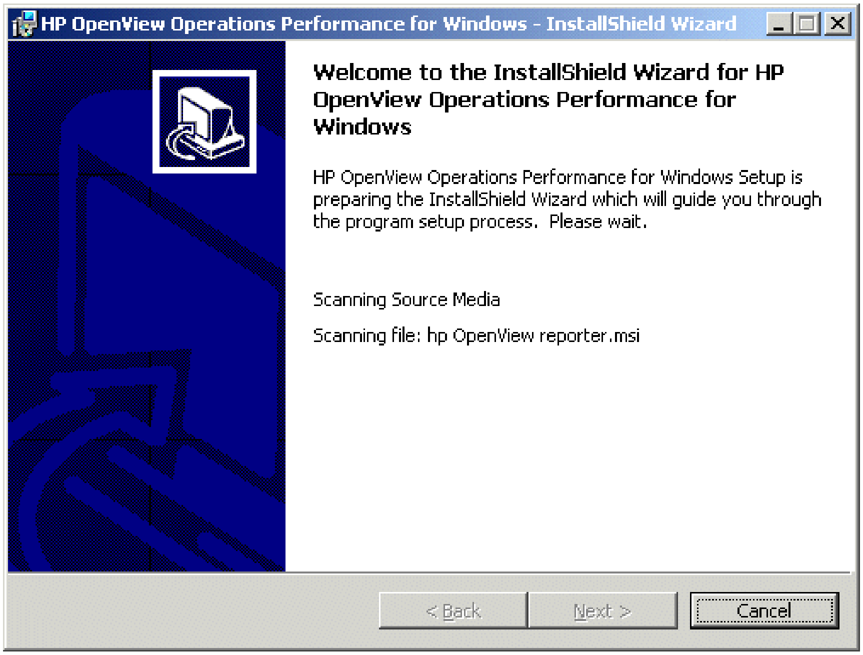
License Information

OVO comes with a 60-day trial license that allows you to use the product for 60 days after you install it. When you first start the OVO console you are prompted to request a permanent license password. A permanent password can be obtained at this time or deferred. Upon reaching the 61st day, the product is disabled until a permanent license is obtained. See “Entering License Information” on page 109.

Installing OVO

You can install other products (such as Smart Plug-ins or add-ons) as available on the installation media. However, OVO must be installed first or already be on the system in order to install the SPIs or add-ons.

1 Insert the *OV Operations 7.2 for Windows* disk into the CD drive of the system you will use as the management server and console or, for a console-only installation, the system you will use as the console. You will see the following Welcome screen. Click **Next** in the Welcome screen to open the main installation menu, shown on the following page.



HP OpenView Operations Performance for Windows - InstallShield Wizard

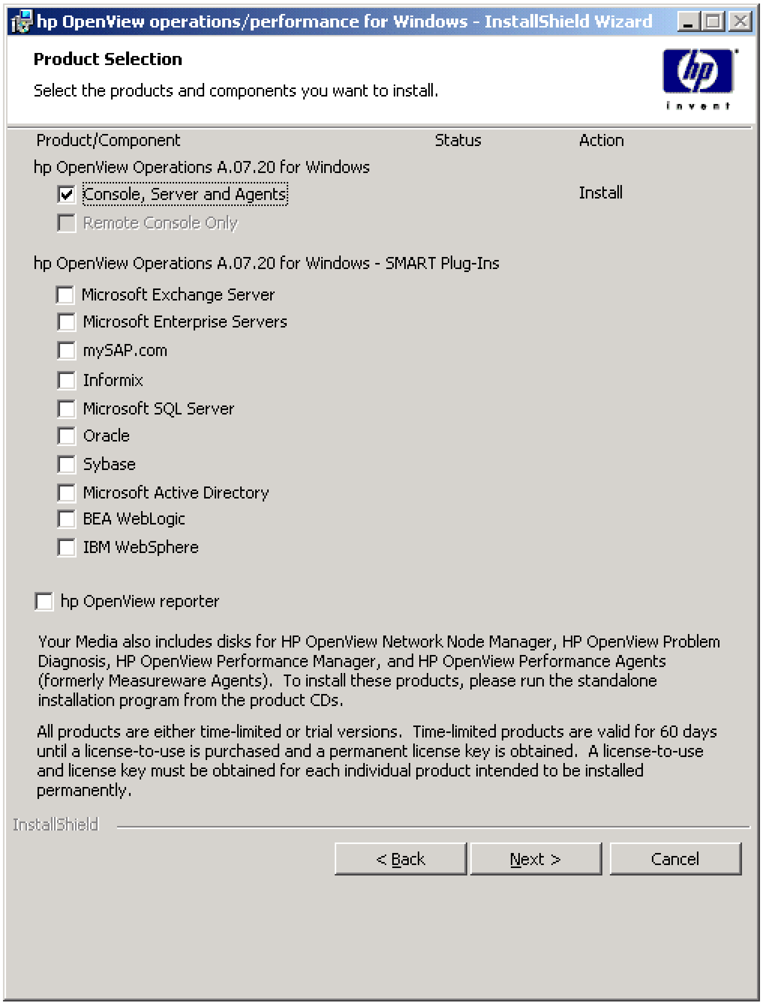
Welcome to the InstallShield Wizard for HP OpenView Operations Performance for Windows

HP OpenView Operations Performance for Windows Setup is preparing the InstallShield Wizard which will guide you through the program setup process. Please wait.

Scanning Source Media

Scanning file: hp OpenView reporter.msi

2 Select the products and components you want to install from the main installation menu, as shown. You must make the "Server and Console" selection first, before selecting any of the Smart Plug-ins or add-on products. If the installation process detects the presence of the server and console from a previous installation, then you can select Smart Plug-ins and add-ons without reinstalling the server and console. After making your selections, click **Next** to open the **Requirements Summary** screen. If your DNS primary suffix is not set, you will see a warning message.



hp OpenView operations/performance for Windows - InstallShield Wizard

Product Selection

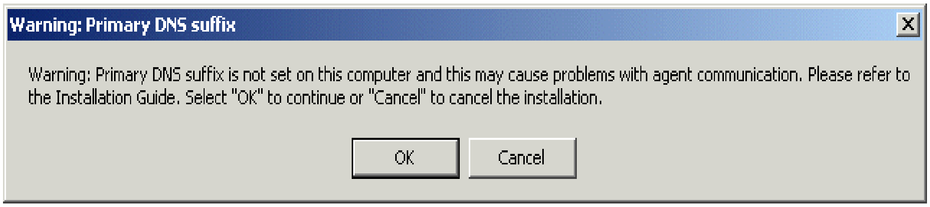
Select the products and components you want to install.

Product/Component	Status	Action
hp OpenView Operations A.07.20 for Windows		
☑ Console, Server and Agents		Install
□ Remote Console Only		
hp OpenView Operations A.07.20 for Windows - SMART Plug-Ins		
□ Microsoft Exchange Server		
□ Microsoft Enterprise Servers		
□ mySAP.com		
□ Informix		
□ Microsoft SQL Server		
□ Oracle		
□ Sybase		
□ Microsoft Active Directory		
□ BEA WebLogic		
□ IBM WebSphere		
□ hp OpenView reporter		

Your Media also includes disks for HP OpenView Network Node Manager, HP OpenView Problem Diagnosis, HP OpenView Performance Manager, and HP OpenView Performance Agents (formerly Measureware Agents). To install these products, please run the standalone installation program from the product CDs.

All products are either time-limited or trial versions. Time-limited products are valid for 60 days until a license-to-use is purchased and a permanent license key is obtained. A license-to-use and license key must be obtained for each individual product intended to be installed permanently.

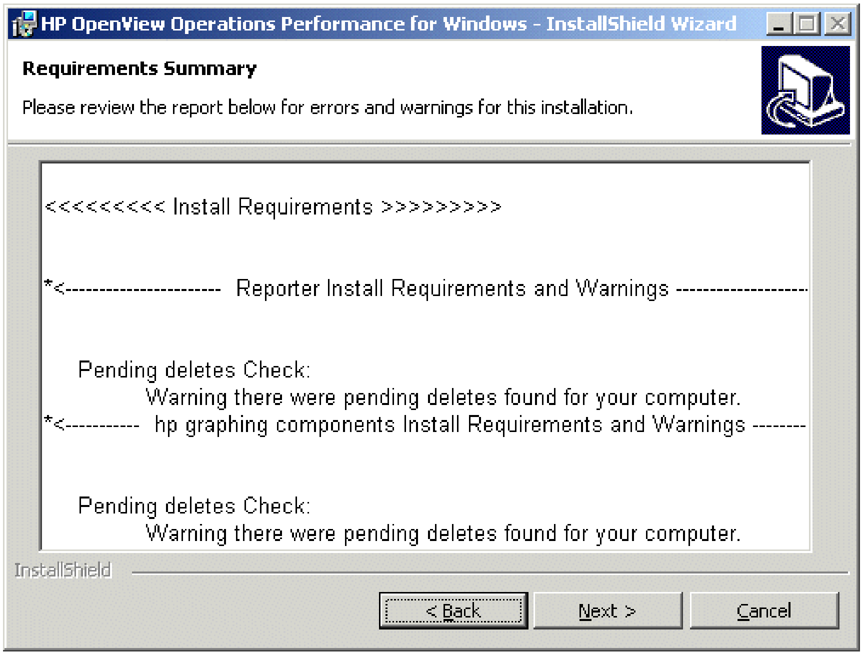
If you have not set the Primary DNS suffix on your computer, you will see this warning. See your Microsoft Windows documentation for instructions on how to set the Primary DNS suffix.



Warning: Primary DNS suffix

Warning: Primary DNS suffix is not set on this computer and this may cause problems with agent communication. Please refer to the Installation Guide. Select "OK" to continue or "Cancel" to cancel the installation.

3 The Requirements Summary screen displays the results of requirement checks performed on the products you selected for installation.



HP OpenView Operations Performance for Windows - InstallShield Wizard

Requirements Summary

Please review the report below for errors and warnings for this installation.

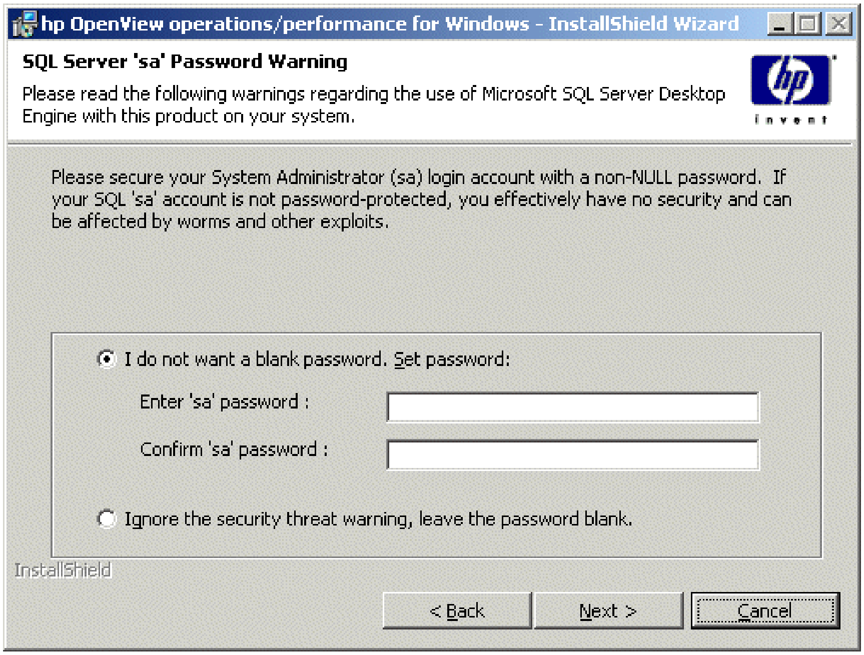
```
<<<<<<<<< Install Requirements >>>>>>>>>


*<----------------------  Reporter Install Requirements and Warnings -------------------


    Pending deletes Check:
            Warning there were pending deletes found for your computer.
*<-----------  hp graphing components Install Requirements and Warnings --------


    Pending deletes Check:
            Warning there were pending deletes found for your computer.
```

4 Click **Next** to open the **MSDE 'sa' Password Warning** dialog box, where you are strongly encouraged to supply a System Administrator (SA) password to protect your system from worms and other types of intrusions. The following screen appears the first time you install OVO.



hp OpenView operations/performance for Windows - InstallShield Wizard

SQL Server 'sa' Password Warning

Please read the following warnings regarding the use of Microsoft SQL Server Desktop Engine with this product on your system.

Please secure your System Administrator (sa) login account with a non-NULL password. If your SQL 'sa' account is not password-protected, you effectively have no security and can be affected by worms and other exploits.

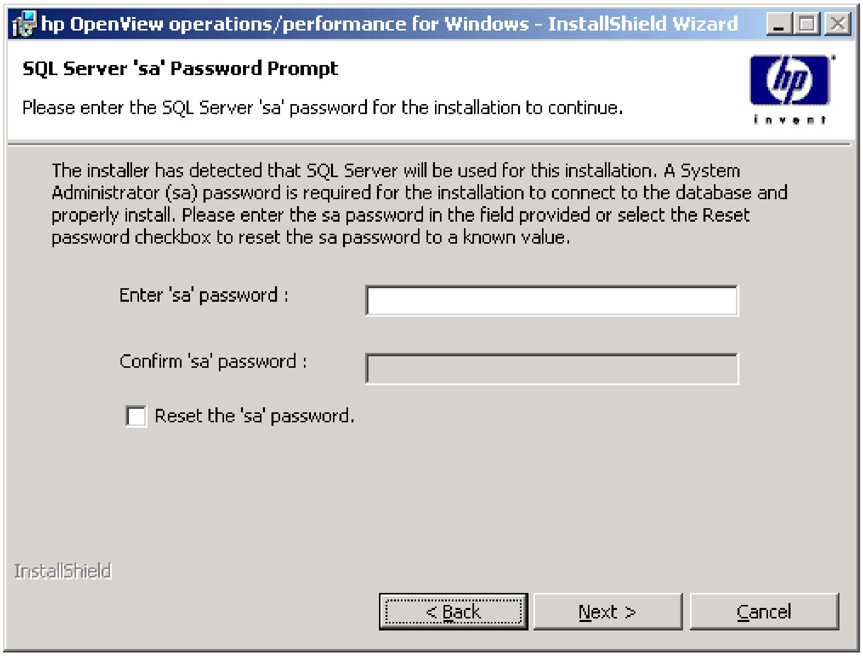
● I do not want a blank password. Set password:

Enter 'sa' password :

Confirm 'sa' password :

○ Ignore the security threat warning, leave the password blank.

If this is a subsequent installation, performed for example to add SPIs or add-on products, a slightly different screen appears. Because you have already set the 'sa' password during your initial installation, you are asked to supply that password for the additional installation you want to perform, as shown in the following dialog box.



hp OpenView operations/performance for Windows - InstallShield Wizard

SQL Server 'sa' Password Prompt

Please enter the SQL Server 'sa' password for the installation to continue.

The installer has detected that SQL Server will be used for this installation. A System Administrator (sa) password is required for the installation to connect to the database and properly install. Please enter the sa password in the field provided or select the Reset password checkbox to reset the sa password to a known value.

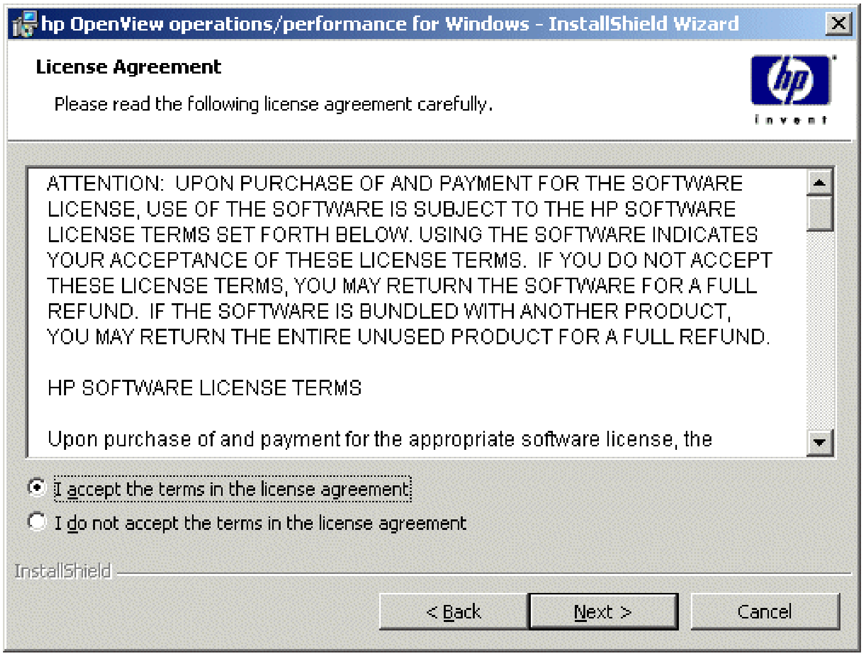
Enter 'sa' password :

Confirm 'sa' password :

□ Reset the 'sa' password.

Click **Next** to open the **License Agreement** screen.

5 In the **License Agreement** screen, accept the license agreement and click **Next** to continue with the installation. If you decline, the installation is cancelled.



hp OpenView operations/performance for Windows - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

ATTENTION: UPON PURCHASE OF AND PAYMENT FOR THE SOFTWARE LICENSE, USE OF THE SOFTWARE IS SUBJECT TO THE HP SOFTWARE LICENSE TERMS SET FORTH BELOW. USING THE SOFTWARE INDICATES YOUR ACCEPTANCE OF THESE LICENSE TERMS. IF YOU DO NOT ACCEPT THESE LICENSE TERMS, YOU MAY RETURN THE SOFTWARE FOR A FULL REFUND. IF THE SOFTWARE IS BUNDLED WITH ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE UNUSED PRODUCT FOR A FULL REFUND.

HP SOFTWARE LICENSE TERMS

Upon purchase of and payment for the appropriate software license, the

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

See details on obtaining a permanent license on page 109.

6 In the **Destination Folders** screen you can use the default destination directory or select a destination directory where you want to install OVO. The destination location you select here will be used as the default directory for other OpenView products you are installing from this CD and cannot be changed for subsequent installs.

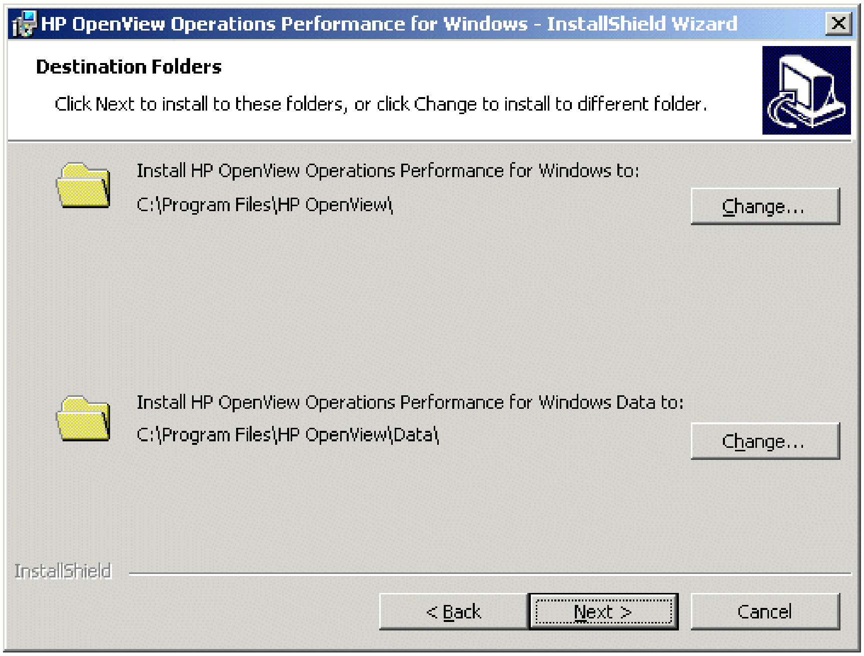
The default installation directory is:

```
C:\Program Files\HP OpenView\
```

The **Change** buttons in the **Destination Folders** dialog box are only available for the first OVO installation (OVO, Reporter, or OVIS). After the first installation, the **Change** buttons are disabled and the **Change Current Destination Folder** shown in step 7 does not appear.

If you want to install to a destination other than the default directory, click the appropriate **Change** button. The **Change Current Destination Folder** dialog box shown in step 7 displays.

To install to the default destination directory, click **Next**.



HP OpenView Operations Performance for Windows - InstallShield Wizard

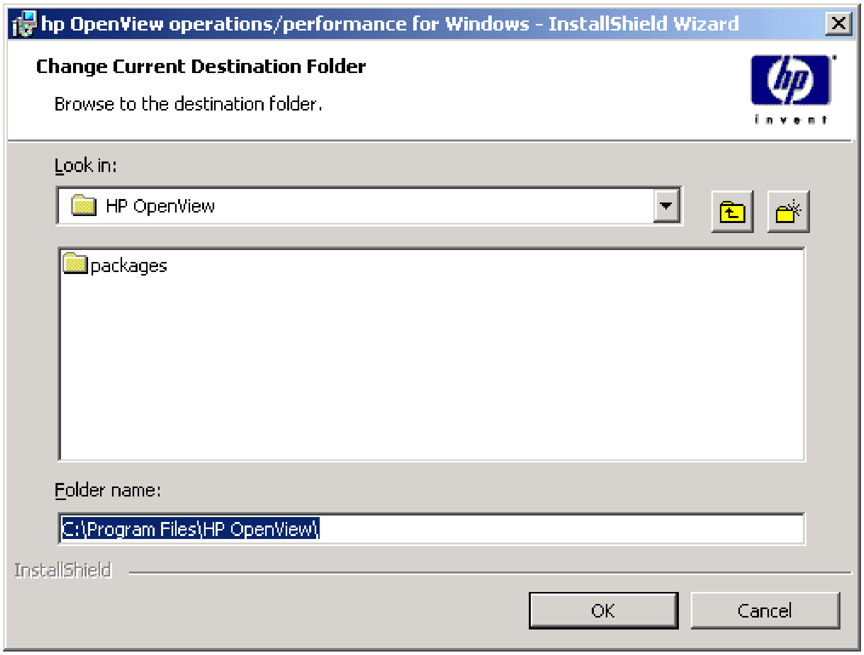
Destination Folders

Click Next to install to these folders, or click Change to install to different folder.

Install HP OpenView Operations Performance for Windows to:
C:\Program Files\HP OpenView\

Install HP OpenView Operations Performance for Windows Data to:
C:\Program Files\HP OpenView\Data\

7 This **Change Current Destination Folder** screen only appears for the first OVO installation (OVO, Reporter, or OVIS). If you have insufficient disk space, you see a message here when you click **OK**. When you close the message dialog, you return to the install menu.



hp OpenView operations/performance for Windows - InstallShield Wizard

Change Current Destination Folder

Browse to the destination folder.

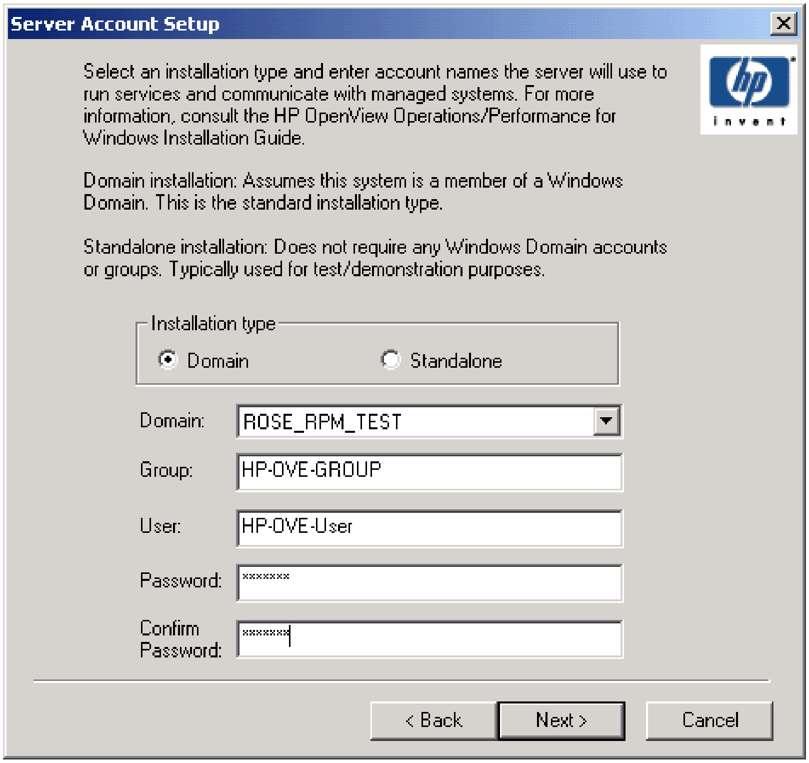
Look in: HP OpenView

packages

Folder name: C:\Program Files\HP OpenView\

8 In the **Server Account Setup** dialog box, you specify an account name and password and choose the installation type you prefer.

⚠ The HP-OVE-GROUP name that you specify during installation cannot be changed without completely uninstalling the product and then reinstalling it. Carefully read the information in Chapter 3, Security, before specifying an account name.



Server Account Setup

Select an installation type and enter account names the server will use to run services and communicate with managed systems. For more information, consult the HP OpenView Operations/Performance for Windows Installation Guide.

Domain installation: Assumes this system is a member of a Windows Domain. This is the standard installation type.

Standalone installation: Does not require any Windows Domain accounts or groups. Typically used for test/demonstration purposes.

Installation type

● Domain ○ Standalone

Domain: ROSE_RPM_TEST

Group: HP-OVE-GROUP

User: HP-OVE-User

Password: xxxxxxx

Confirm Password: xxxxxxx

In the **Server Account Setup** dialog box, choose the installation type you prefer.

Domain installation: This installation assumes the OVO management server to be a member of a Windows domain. This method creates (or uses existing) domain accounts and groups (default HP-OVE_User and

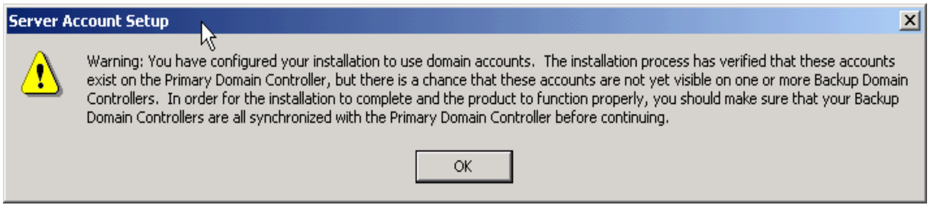
HP-OVE-Group).This domain group allows the OVO server to automatically manage a Windows node and install the agent software to this node.

This is only possible if a Windows node is in the same domain as the management server or has a trust relationship in place with the domain of the management server. To add the HP-OVE-Group successfully to a Windows node, the user running the OVO console must have administrative permission on that Windows node (direct or indirect via the Domain Admins group).

Standalone installation: This installation does not require any Windows domain accounts or groups. The management server can be either a member of a Workgroup (=standalone) or member of a Windows domain. This installation method has the following limitations:

- Automatic agent software installation of Windows managed nodes is not possible, except for the agent on the management server itself. All remote managed Windows nodes have to be installed using the Windows Manual Agent package.
- Agent functionality packages which are used by some SPI products cannot be auto-deployed and require manual installation on the Windows managed node (please refer to the installation instructions for each SPI).
- Remote MMC consoles are not supported with a standalone installation of the management server. Remote MMC consoles are only supported with the Domain installation option. However, you can use terminal services.
- If you perform a standalone installation on a production machine, you cannot later change this to a domain account.
- For management server to agent communication, events, policies, deployment, drawing graphs, and so on are not affected by the standalone installation.
- UNIX managed nodes are not affected by the domain versus standalone setup and always require a manual install process.

  If you select Domain in the **Server Account Setup** dialog box, you will see a warning message about synchronizing your Primary and Backup Domain Controllers before continuing with the installation. Click **OK** to continue with the installation in the **Server Account Setup** dialog box.



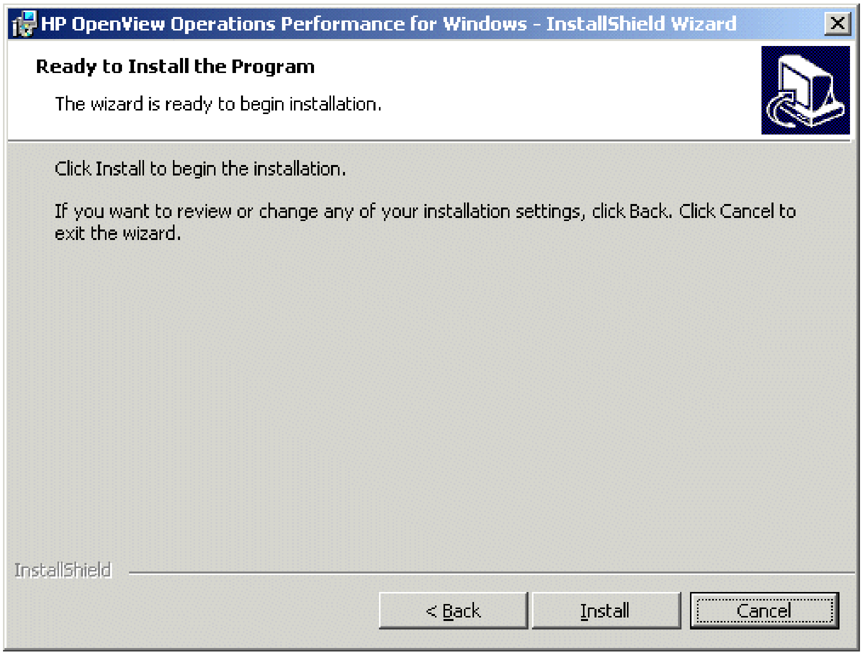
Warning: You have configured your installation to use domain accounts. The installation process has verified that these accounts exist on the Primary Domain Controller, but there is a chance that these accounts are not yet visible on one or more Backup Domain Controllers. In order for the installation to complete and the product to function properly, you should make sure that your Backup Domain Controllers are all synchronized with the Primary Domain Controller before continuing.

Once established, this account information is used by other products you install from the installation media. (for remote console installation only, this screen does not appear). Enter the security information for the type of install selected as follows.

- The domain to use for the security accounts (needed only for a domain installation)
- The group name for the HP-OVE-GROUP account
- The user name and password for the HP-OVE-User account

Click **Next** to go to the **Ready to Install the Program** screen.

9 Click **Install** to begin the installation.



HP OpenView Operations Performance for Windows - InstallShield Wizard

Ready to Install the Program

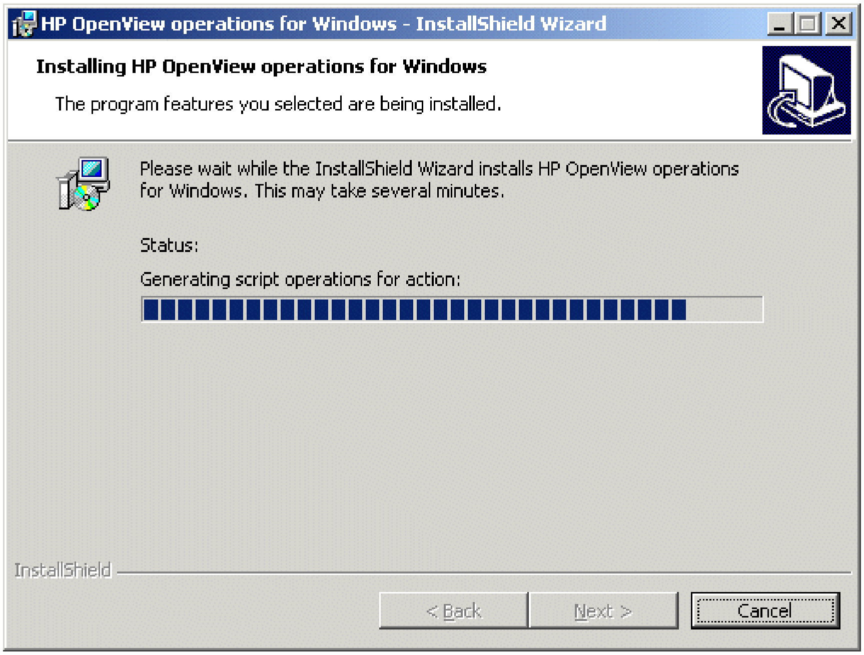
The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

10 You will see various status dialogs, like the example below, as the install program proceeds. Each installation component displays individual status dialog boxes as the install progresses. For example, you will see status dialogs for various components such as the licensing component, the reporting component, the graphing component, and others, and for the three SPIs that are included with the product and are installed by default.

Depending on the speed of your system and the components selected for installation, this process could take from several minutes to over an hour.



HP OpenView operations for Windows - InstallShield Wizard

Installing HP OpenView operations for Windows

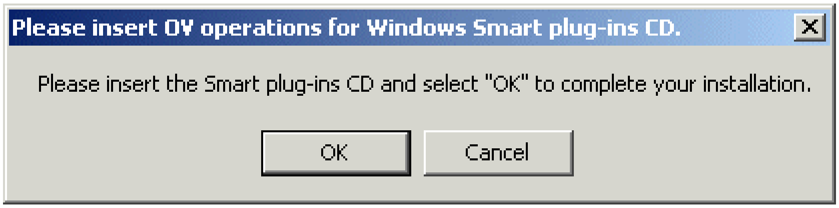
The program features you selected are being installed.

Please wait while the InstallShield Wizard installs HP OpenView operations for Windows. This may take several minutes.

Status:

Generating script operations for action:

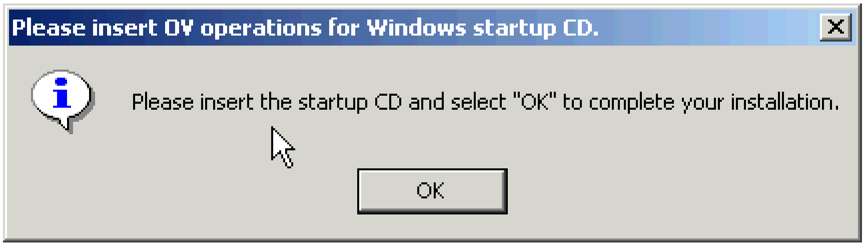
11 During the installation process, you are asked to remove the installation disk and insert the HP OpenView Operations/Performance for Windows Disk 2 CD. Click **OK** to begin the installation of the three Smart Plug-ins that are included with the product and are installed by default.



Please insert OV operations for Windows Smart plug-ins CD.

Please insert the Smart plug-ins CD and select "OK" to complete your installation.

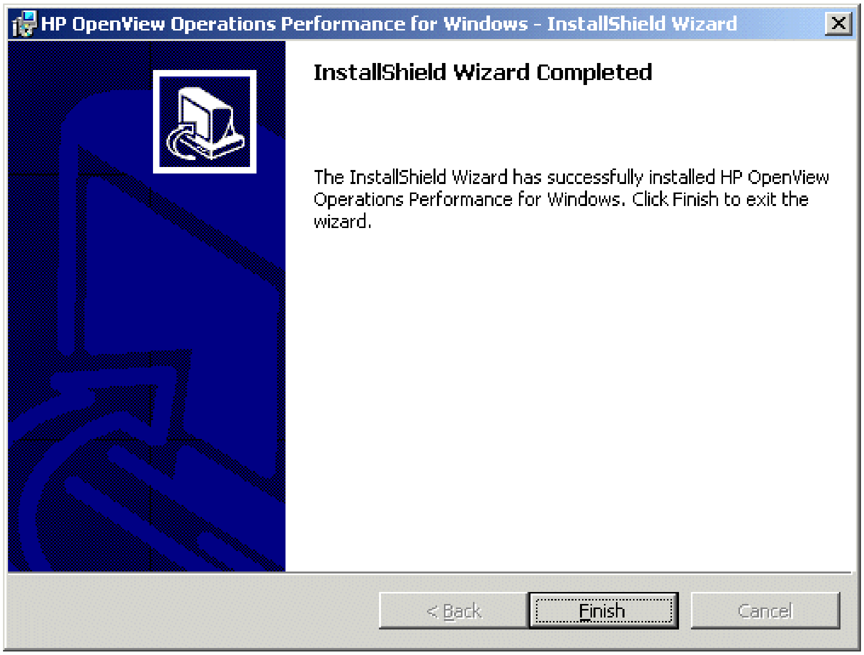
12 When Smart Plug-in installation completes, you are asked to remove Disk 2 and insert the HP OpenView Operations/Performance for Windows Disk 1 CD. Click **OK** in the message screen to complete the installation process.



Please insert OV operations for Windows startup CD.

Please insert the startup CD and select "OK" to complete your installation.

13 The installation is finished when the completion screen displays. Click **Finish** to conclude the installation.

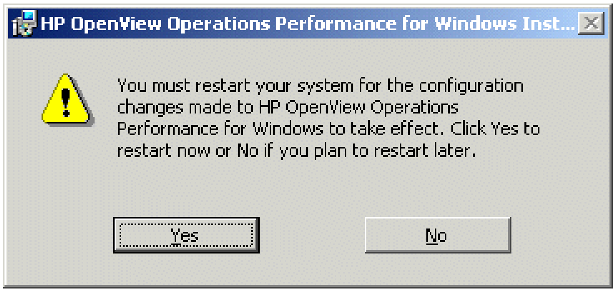


HP OpenView Operations Performance for Windows - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed HP OpenView Operations Performance for Windows. Click Finish to exit the wizard.

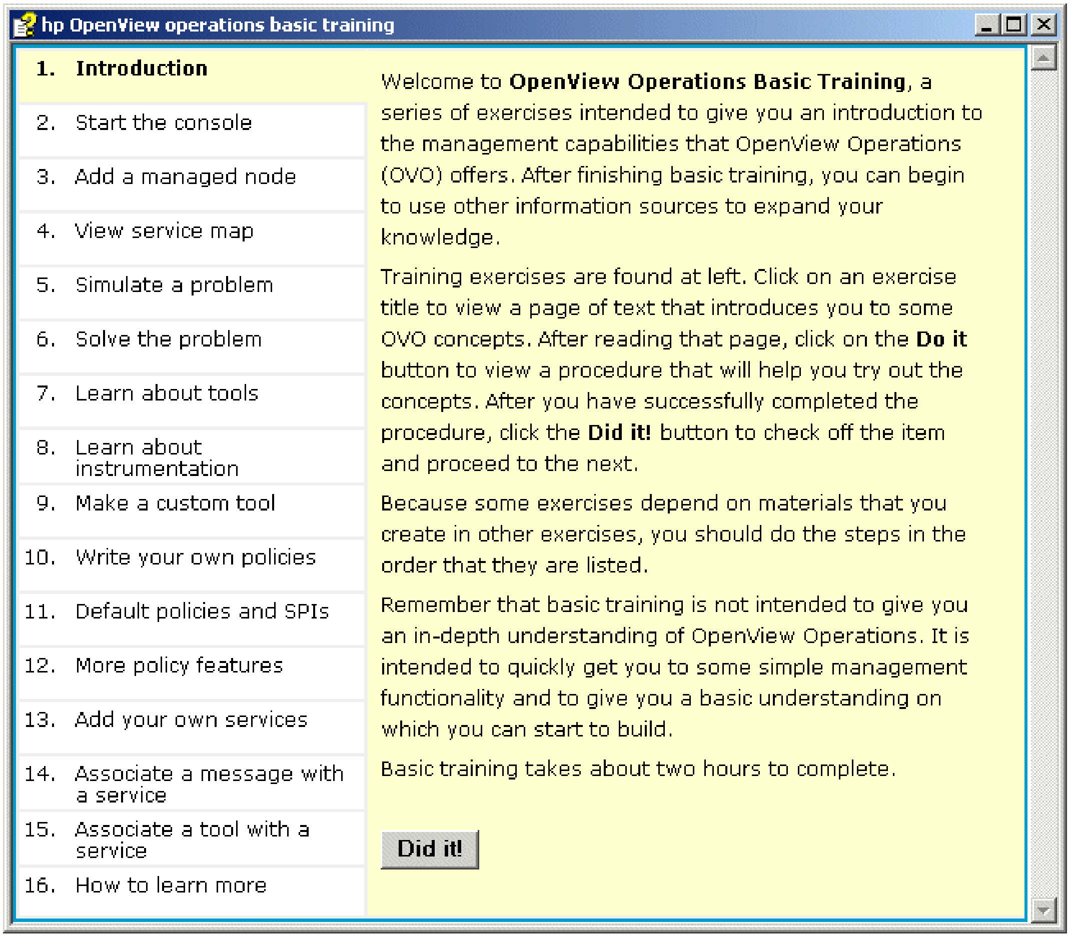
14 After all installation tasks are completed, you are prompted to reboot, if necessary. You can perform the reboot at a later time, but postponing the reboot produces a warning when running the console that some functionality will not work until the system reboots.



HP OpenView Operations Performance for Windows Inst...

You must restart your system for the configuration changes made to HP OpenView Operations Performance for Windows to take effect. Click Yes to restart now or No if you plan to restart later.

15 You are encouraged to view the basic training tutorial presented at the conclusion of the install program when the console is started for the first time. The tutorial introduces you to OVO features, provides a product overview, and details configuration and deployment steps you need to perform before you can begin working in OVO. View the tutorial now or return to it at a later time by selecting Basic Training from the Help Table of Contents. Use the introductory page, shown below, as a brief checklist of necessary tasks to be accomplished.



hp OpenView operations basic training

1. **Introduction**
2. Start the console
3. Add a managed node
4. View service map
5. Simulate a problem
6. Solve the problem
7. Learn about tools
8. Learn about instrumentation
9. Make a custom tool
10. Write your own policies
11. Default policies and SPIs
12. More policy features
13. Add your own services
14. Associate a message with a service
15. Associate a tool with a service
16. How to learn more

Welcome to **OpenView Operations Basic Training**, a series of exercises intended to give you an introduction to the management capabilities that OpenView Operations (OVO) offers. After finishing basic training, you can begin to use other information sources to expand your knowledge.

Training exercises are found at left. Click on an exercise title to view a page of text that introduces you to some OVO concepts. After reading that page, click on the **Do it** button to view a procedure that will help you try out the concepts. After you have successfully completed the procedure, click the **Did it!** button to check off the item and proceed to the next.

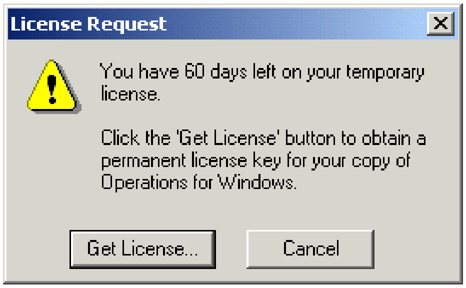
Because some exercises depend on materials that you create in other exercises, you should do the steps in the order that they are listed.

Remember that basic training is not intended to give you an in-depth understanding of OpenView Operations. It is intended to quickly get you to some simple management functionality and to give you a basic understanding on which you can start to build.

Basic training takes about two hours to complete.

Entering License Information

When you start the OVO console, the **License Request** dialog box is displayed.

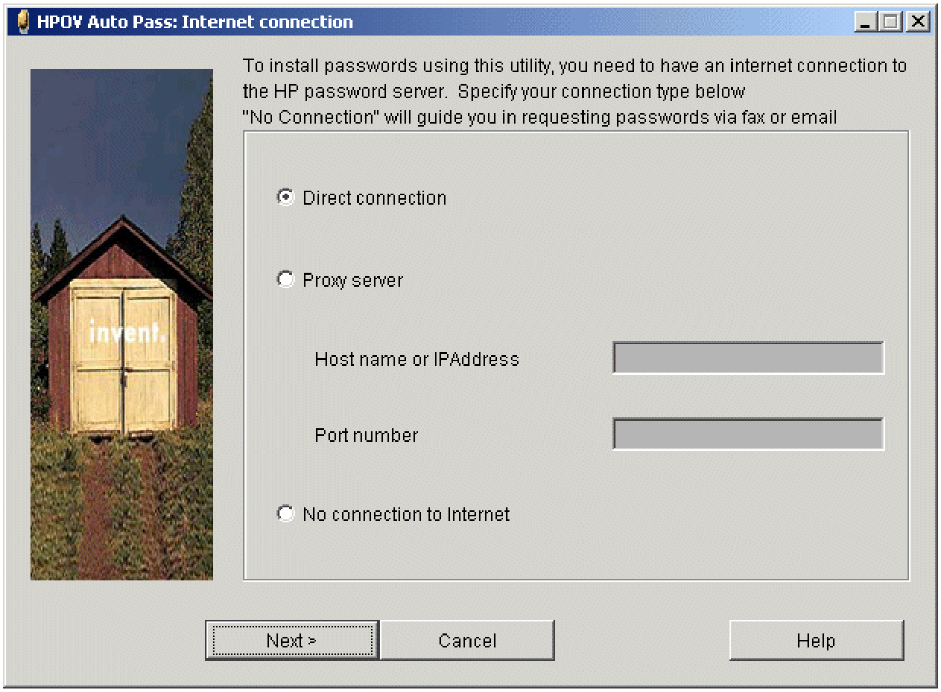


License Request

You have 60 days left on your temporary license.

Click the 'Get License' button to obtain a permanent license key for your copy of Operations for Windows.

To obtain your permanent license key, select **Get License** to open the AutoPass licensing program and follow the instructions on the screens.



HPOV Auto Pass: Internet connection

To install passwords using this utility, you need to have an internet connection to the HP password server. Specify your connection type below "No Connection" will guide you in requesting passwords via fax or email

● Direct connection

○ Proxy server

Host name or IPAddress

Port number

○ No connection to Internet

If you prefer, you can postpone licensing by launching the licensing program at a later time, as follows:

1. From the OVO management server, select the **Tools** folder from the console tree.
2. Select **Tools** → **OpenView Tools** → **Licensing** to display a list of tools.
3. Select **Obtain License**, which allows you to request permanent license passwords for the management server, agents, or Smart Plug-ins. Right-click to open the shortcut menu.
4. Select **All Tasks** → **Launch Tool** to open the **Obtain License** dialog box.
5. Select the Management Server product from the list and click **OK**.

Refer to the OVO online help topic “License HP OpenView Operations for Windows” for more information. Refer to the *HPOV Auto Pass User Guide* (`AutoPass_guide.pdf`) on the installation media for details on using the licensing program.

In the OVO console, under **Tools** → **OpenView** → **Licensing** you can also select the License Report tool, which gives you information on the passwords in use.

See the OVO online help topics “License HP OpenView for Windows” and “SPI License Report” for more information.

Requesting a Permanent License

To request a permanent license password, you need the following:

- Your HP Order Number
- IP Address of the Server
- Your Company information

To obtain a license, you must provide the number of the HP Purchase Order number you received from your HP OpenView authorized reseller when you bought the product that you want to license. If you have not yet purchased the product, call 1-877-686-9637 (in the United States and Canada) or visit **www.hp.com** to locate an HP OpenView authorized reseller.

Results of the Installation

After completing the installation of OVO, you can access the following:

- A folder is added to the Start Menu to allow you to open the console: **Start** → **Programs** → **HP OpenView** → **Console**
- OVO documentation (in Adobe Acrobat.PDF format) is available in the subdirectory `<%InstallDir%\Documentation\1033\OVO Guides` on the first installation CD . See Chapter 8, “Documentation,” for a complete list of available documentation.

Installation Log Files

After installation, several log files are created and placed in the Data directory, the location chosen for data files, under the *log* subdirectory:

%OVINSTALLDIR%/\data\HPOVInstall

Installing/Activating Agents on UNIX Nodes

For managing UNIX nodes, OVO includes agents for HP-UX, Sun Solaris, IBM AIX, HP Tru64, and Linux, and the OpenView Performance Agent (formerly MeasureWare Agent) for HP-UX, Sun Solaris, AIX, Tru64 and Linux.

If the UNIX nodes do not already have these agents installed, you can install the appropriate OpenView Operations and OpenView Performance Agents to those nodes. For information about installing to these nodes, see the OVO online help. Look in the Help Table of Contents under **Administering Your Environment → Policy Management and Deployment →Deployment Related Tasks\Agent Installation on UNIX Computers** for steps to install each of these agents.

If the UNIX node already has an OpenView Operations agent installed, you may need to make some changes for interoperability with OVO for Windows.. The 5.34 or higher version of the OpenView Operations for UNIX agent integrates with OVO for Windows. Version 5.33 or lower does not interoperate with OVO for Windows.

For information on moving from managing a UNIX node with OVO for UNIX to managing the node with OVO for Windows, see the OVO online help.

Upgrading OVO

If you already have a previous OVO 6.0 (formerly VantagePoint for Windows) version installed, such as A.06.01 or A.06.10, and want to upgrade to OVO, see the *HP OpenView Guide for Upgrading to OpenView Operations for Windows* Version 7.20 (OVOWUpgrade.pdf) on the installation media.

The upgrade guide contains important instructions about saving data and upgrading policies before installing OVO.

Uninstalling Policies and Packages from a Windows Managed Node

Follow these steps to completely uninstall policies and packages from Microsoft Windows managed nodes. You may want to do this when you no longer want to manage a node or in preparation for completely removing OVO and all related products. (See "Completely Removing OVO and Smart Plug-ins or Add-on Products" on page 117.)

⚠ Do not remove policies and packages from a managed node if you are upgrading from one version of OVO to another. Instead, follow the instructions in "Upgrading OVO" on page 112.

1 Open the OVO console.

2 Open the Nodes view and select the managed node from which you want to remove all packages and policies. Right-click the node and select **View** → **Package Inventory**.

3 Right-click on the packages that you want to remove.

Whenever you remove a package, all policies that require this package are removed automatically with it.

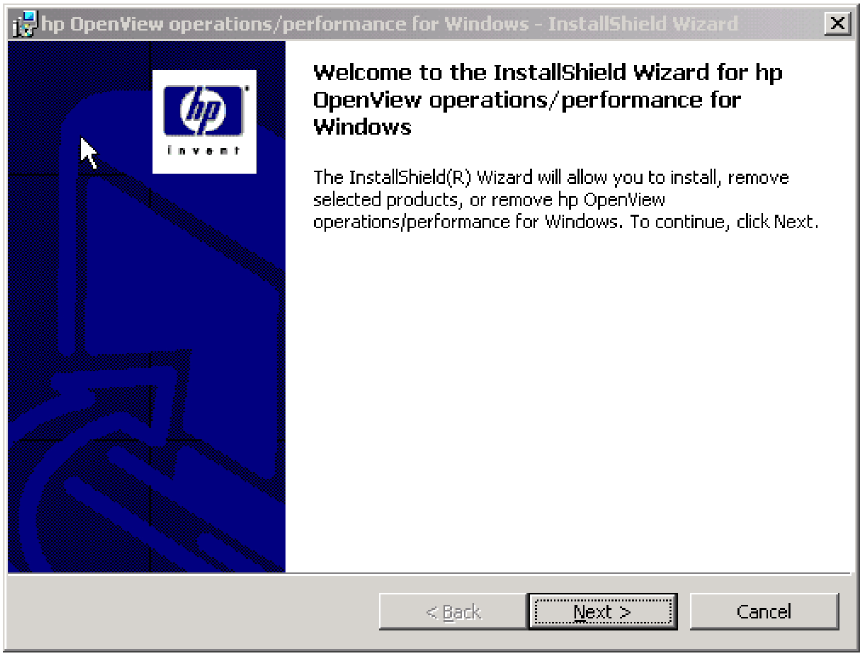
4 Select **All Tasks**→**Remove from node**. Ensure that ALL Policies and Packages are removed. To check, right-click the node name in the console tree and select **View** → **Policy Inventory** to display a list of deployed policies for that node. Select **View** → **Packages** from the context menu to display a list of deployed packages.

5 Repeat for other managed nodes as needed. Close the console.

➤ After the uninstall, some directories and the shared registry key are left behind. If you have no other OpenView products that require these files, you may manually remove them.

Uninstalling OVO and SPI or Add-On Products

You can choose to remove selected individual products or to completely remove OVO and any Smart Plug-ins or Add-on products. This process will differ depending on what you wish to remove. To remove individual products, you must use the product CDs. To remove all products, including SPIs and Add-ons, use Add/Remove programs, as described in the following sections. When you begin the uninstall process, you will see the following welcome screen. Click Next to continue.



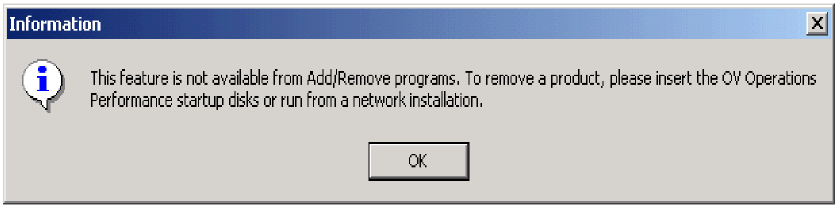
hp OpenView operations/performance for Windows - InstallShield Wizard

Welcome to the InstallShield Wizard for hp OpenView operations/performance for Windows

The InstallShield(R) Wizard will allow you to install, remove selected products, or remove hp OpenView operations/performance for Windows. To continue, click Next.

Removing Individual Products

To remove individual products selected from the **Product Selection Uninstall** dialog box, you must use the product CDs or network installation. You cannot remove individual products through Add/Remove Programs. If you try to use Add/Remove Programs for this purpose, you will see the following message:



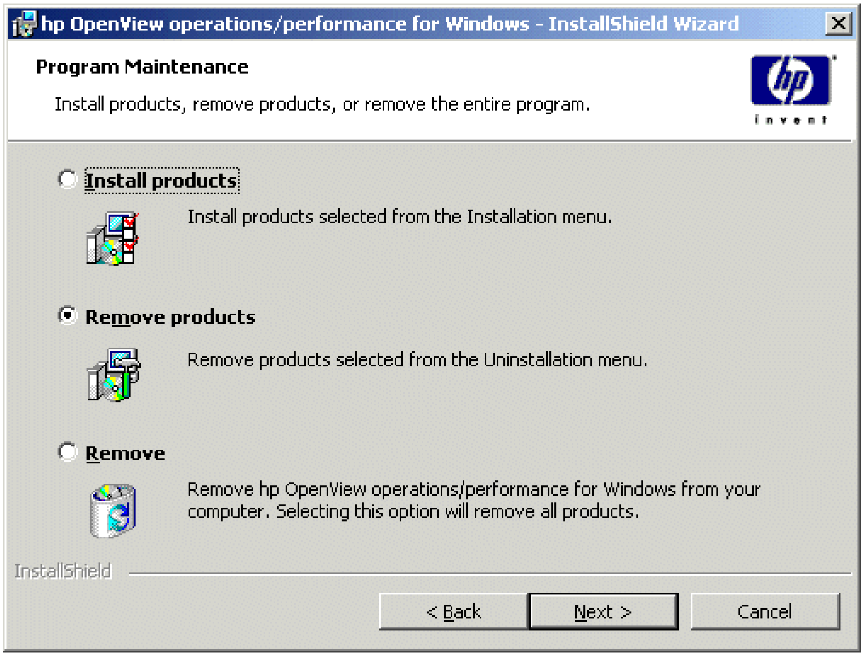
Information

This feature is not available from Add/Remove programs. To remove a product, please insert the OV Operations Performance startup disks or run from a network installation.

To remove products using the CDs, follow these steps:

1 Insert the HP OpenView OV Operations 7.20 for Windows startup CD in the disk drive.

2 From the **Program Maintenance** dialog box, select **Remove products,** as shown**.**



hp OpenView operations/performance for Windows - InstallShield Wizard

Program Maintenance

Install products, remove products, or remove the entire program.

○ Install products

Install products selected from the Installation menu.

● Remove products

Remove products selected from the Uninstallation menu.

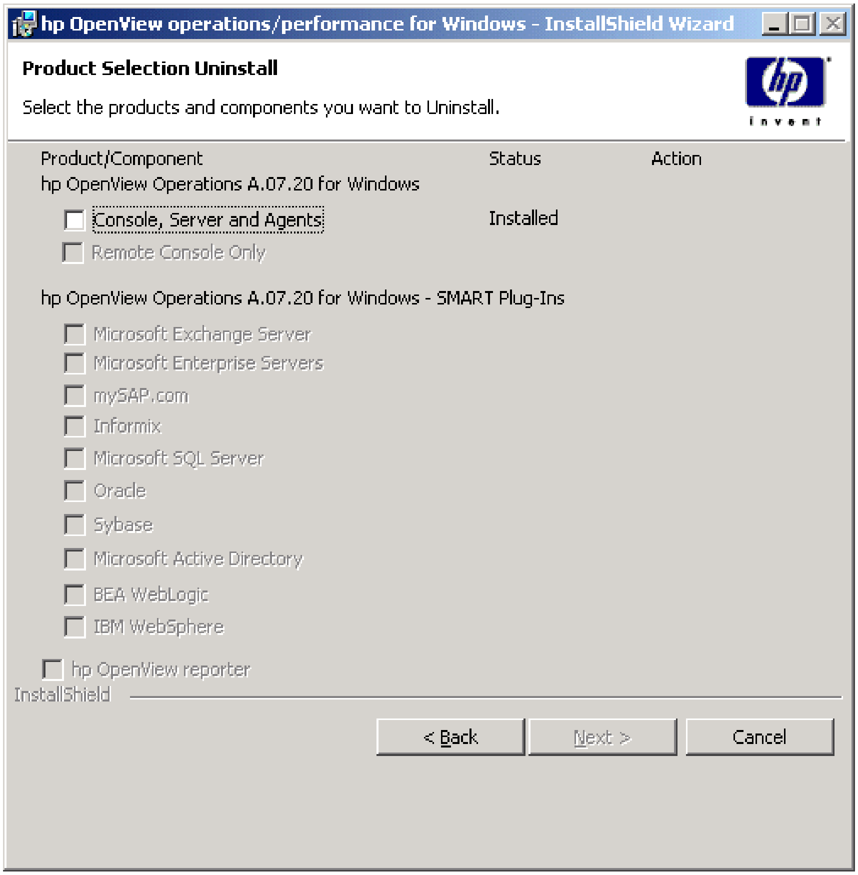
○ Remove

Remove hp OpenView operations/performance for Windows from your computer. Selecting this option will remove all products.

3 Click **Next** to open the **Product Selection Uninstall** dialog box and select the products you want to remove.

➤ All Smart Plug-ins previously installed must be selected to be removed before the **Console, Server, and Agents** option can be selected.

You must also select the **Console, Server, and Agents** option to be removed before you can select the Reporter option for removal.



hp OpenView operations/performance for Windows - InstallShield Wizard

Product Selection Uninstall

Select the products and components you want to Uninstall.

Product/Component	Status	Action
hp OpenView Operations A.07.20 for Windows		
□ Console, Server and Agents	Installed	
□ Remote Console Only		
hp OpenView Operations A.07.20 for Windows - SMART Plug-Ins		
□ Microsoft Exchange Server		
□ Microsoft Enterprise Servers		
□ mySAP.com		
□ Informix		
□ Microsoft SQL Server		
□ Oracle		
□ Sybase		
□ Microsoft Active Directory		
□ BEA WebLogic		
□ IBM WebSphere		
□ hp OpenView reporter		

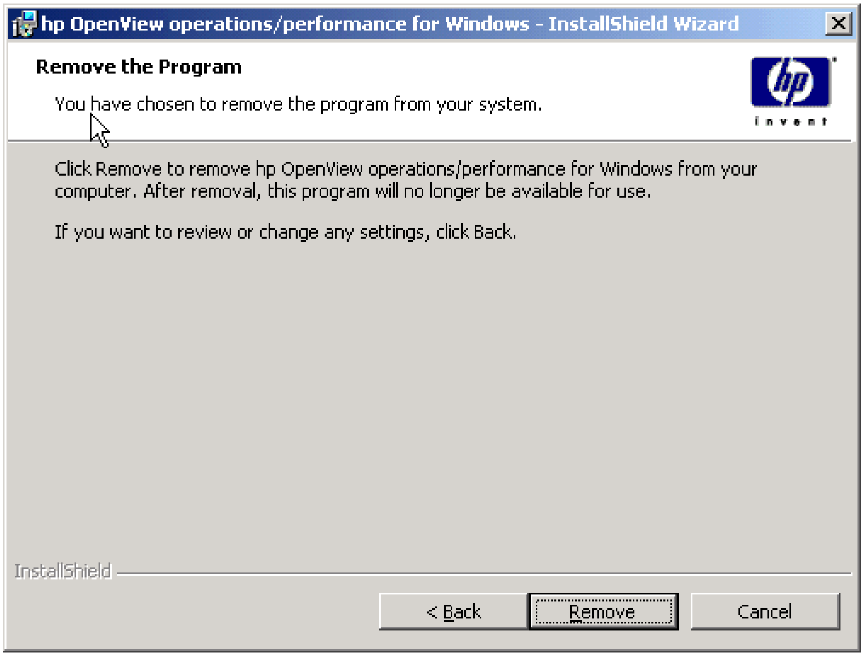
After selecting the products you want to remove, click **Next** and follow the instructions on the screen.

Completely Removing OVO and Smart Plug-ins or Add-on Products

To completely remove OVO and any dependent SPI and Add-on products that you installed from **hp OpenView operations/performance for Windows,** follow these steps.

➤ If other products (such as OVPM, OV Reporter, or OVIS) are installed on the same server, they may share common components with OVO for Windows. However, when OVO for Windows is removed, these products will not be affected, because any shared components will be removed only when no other OpenView product exists that requires them.

1. Exit any open management console sessions.
2. Select **Start** → **Settings** → **Control Panel** → **Add/Remove Programs.**
3. Select **hp OpenView operations/performance for Windows**.
4. Select **Change**.
5. From the **Program Maintenance** dialog box shown previously, select **Remove**.
6. From the **Remove the Program** dialog box, select **Remove**.



hp OpenView operations/performance for Windows - InstallShield Wizard

Remove the Program

You have chosen to remove the program from your system.

Click Remove to remove hp OpenView operations/performance for Windows from your computer. After removal, this program will no longer be available for use.

If you want to review or change any settings, click Back.

InstallShield
< Back
Remove
Cancel

Uninstalling UNIX Agents

For the steps to uninstall agents on UNIX managed nodes see the OVO online help. Look in the Table of Contents under **Administering Your Environment** → **Policy Management and Deployment** → **Deployment Related Tasks**.

Reinstalling OVO for Windows

Reinstallation of OVO for Windows management servers and remote consoles is essentially an uninstallation operation followed by a second install. For management servers, you have the option of either reusing data or performing a fresh install, during which the server database, policies, and so forth are newly created.

Reinstall the Management Server

OVO offers two options for reinstalling OVO for Windows 7.20 servers. Both options must be preceded by uninstalling the existing server, including SPIs (which happens automatically) and the NNM Adapter. Server uninstallation also automatically removes the server’s agent and any collected performance data.

Option1: Reuse Data

By default, data files are preserved during installation and can be reused in a subsequent server install by doing the following:

1 In the install wizard “Destination Directories” dialog box, select the same program and data directories that were used by the previous installation.

⚠ Failure to do this results in the data being ignored.

The installation process automatically reconnects to the existing database, reuses policy information, and so forth. Managed nodes will reconnect to the server after installation is complete.

2 Be sure that you reselect any needed SPIs during installation. You can also include additional SPIs.

Option 2: Do Not Reuse Data

If you choose this option, you will lose all OVO for Windows server data. This includes messages, managed node inventories, service maps, and custom tools and policies.

⚠ Use this option only if you do not want to preserve your management server data, including the database.

1 Delete the following directories before running the next install.

a All contents of the data directory (data destination directory chosen during installation

b. The Policies and MSSQL$OVOPS subdirectories under the program directory (program destination directory chosen during installation)

Use this option only if no other OpenView products are installed that share these program and data directories. This includes OpenView Reporter, OpenView Internet Services, and OpenView Performance Manager.

c. If you plan to install to a different program directory, then use **Add/ Remove Programs** to also uninstall the product “Java 2 Runtime Environment Standard Edition” that resides in the grapherjre directory. The subsequent installation will reinstall it in the new location automatically.

Reinstall Remote Consoles

To reinstall an OVO for Windows 7.20 remote console, follow these steps:

1. Uninstall the existing console using **Add/Remove Programs**.
2. Undeploy an OVO for Windows agent, if present.
3. Perform a second install.

   If you plan to install to a different program directory, then use **Add/ Remove Programs** to also uninstall the product “Java 2 Runtime Environment Standard Edition” that resides in the grapherjre directory. The subsequent installation will reinstall it in the new location automatically.

5

Install the Network Node Manager (NNM) Adapter

Install the Network Node Manager (NNM) Adapter after the OVO installation is complete. Before installing the NNM Adapter, be sure the following prerequisites are met.

Requirements

- HP OpenView Network Node Manager for Windows, Version B.06.20, is installed and configured on a Windows NT or 2000 system, including the installation of the NNM Web Interface.
- HP OpenView Operations for Windows Version 7.20 is installed and configured on a Windows 2000 server.
- The interactive user (the person who installs the NNM Adapter) must have administrative privileges on OVO and NNM servers.
- You must have a Windows account for running NNM Adapter components. The account must have administrative rights on the OVO server. You may use the same account that was used for the OVO installation.
- The NNM Adapter fully supports only configurations where the OVO server, NNM server, and managed nodes belong to the same DNS domain. If a node belongs to a different DNS domain than the OVO and NNM

servers, it might not be recognized as an NNM node and would not be added to the NNM Managed Nodes node group. If such a node is added using NNM discovery, this problem does not arise, even if the node belongs to a different DNS domain.

- Installation of both the NNM Adapter and OVO for Windows on the same machine is supported, but not recommended.
- 20 MB disk space on the HP OpenView Operations for Windows management server to install components necessary for the integration.
- 20 MB disk space on the HP OpenView Network Node Manager server to install components necessary for the integration.

➤ The NNM Adapter is not supported with Network Node Manager running on a backup domain controller (BDC). The adapter attempts to add a user, which is not possible on a BDC.

HP OpenView Operations for Windows NNM Adapter Features

Installing the NNM Adapter adds these features to OVO:

- Adds the <NNMSERVER> (NNM Server) on the node group root if the NNM server is not a managed node in OVO.
- Creates these three services:
  - Network Node Manager (under Services\Applications)
  - NNM Adapter (under Services\Applications)
  - Network Infrastructure (under Services)
- Creates the tool group NNM Web Tools, which contains NNM web tools. These tools are associated with the NNM Managed Nodes node group. All nodes that are discovered as NNM nodes are automatically associated with these tools indirectly through the NNM Managed Nodes group. (The tools are inherited from the NNM Managed Nodes node group.) All services hosted on nodes discovered as NNM nodes are associated with these tools.

- Creates the policy group NNM Policies, which contains the following four policies. These allow messages and events to be sent between OVO and NNM:
  - **NNM Adapter**: This policy is deployed on the management server during NNM Adapter installation and is used internally by the NNM Adapter.
  - **NNMAdap-FwdAllLogEntries**: This event log policy is deployed on the HP OpenView Network Node Manager server and the OVO management server during NNM Adapter installation. The policy forwards all NNM Adapter events logs to the OVO console.
  - **NNM-SNMP-NonNorm**: This SNMP policy is deployed on the NNM server during NNM Adapter installation. It forwards NNM events with severities other than “Normal” and normal correlated NNM events to the OVO for Windows console.
  - **NNM-SNMP-All policy**: This SNMP policy forwards all NNM events to the OVO for Windows console. It is provided as a template. While you could deploy the NNM-SNMP-All policy directly to the NNM server, it is not recommended because this policy forwards all NNM events, including normal messages, to the OVO for Windows console. This would produce large numbers of messages in the console.

➤ When you want to deploy a new SNMP policy, either NNM-SNMP-All or a policy you have created from this template, you should first remove the old policy NNM-SNMP-NonNorm to prevent duplicate messages from appearing in the browser.

Install and Configure the Web Server on the NNM for Windows System

Several of the NNM features are web-based, and require a web browser to be installed on the same system where NNM is installed. You can use any of these browsers:

- Netscape Navigator (Version 4.6 or later).
- Microsoft Internet Explorer (Version 5.0 or later) with Java/JavaScript options enabled. (Internet Explorer is required for NNM Web Tools.)

- Microsoft Internet Explorer 6.0 does not provide Java support but does offer a download option. If an NNM web tool that requires the Java Virtual Machine (VM) is started and the VM is not installed on the system, the user is given the option of downloading the Java VM. The Java VM can also be downloaded from the Microsoft web site.

To install the browser, follow the instructions that came with it. Be sure to configure any web proxies according to the browser's instructions.

To verify that a web server is installed on Windows 2000

You will need your Windows 2000 operating system CD.

1. From the **Start** menu, select **Settings** → **Control Panel**.
2. In the Control Panel, double-click the **Add/Remove Programs** applet.
3. In the **Add/Remove Programs** dialog box, select the **Add/Remove Windows Components** button, which displays the **Windows Components** wizard.
4. Scroll to **Internet Information Services**. If this box is already selected, then the web server is installed. If the web server is not listed, follow these steps:
   a. Select the **Internet Information Services** (IIS) check box.
   b. Click **Next** and wait while the wizard configures components.
   c. When prompted, insert the Windows 2000 operating system CD and click **OK**.
   d. In the **Windows Components** wizard, click **Finish** and remove the CD.
   e. In the **Add/Remove Programs** dialog box, click **Close**.

To verify that a web server is installed on Windows NT

1. On the Start menu, select **Settings** → **Control Panel**.
2. In the **Control Panel**, double-click the **Services** icon.
3. Look in the list for a service named:

   World Wide Web Publishing Service
4. If found, then the web server is already installed.
5. If not found, refer to the documentation accompanying your browser.

To verify that the web server is configured

1. From the browser, try to open an NNM for Windows Web GUI URL such as:

   http://<server name>/OVCgi/nnmRptPresenter.exe

2. If the URL opens without error messages, the web browser is configured correctly.

For further information on web browser installation and configuration on the NNM for Windows system, refer to the NNM documentation.

Installation

The HP OpenView Operations for Windows NNM Adapter is installed using an installation wizard that guides you through the procedure and prompts for information you must enter.

Components of the NNM Adapter are installed on both the OVO server and the Network Node Manager server.

Terminal Services

The NNM Adapter can be installed on top of Terminal Server when Terminal Server is in the "Remote administration mode." It fails in Application mode.

NNM Adapter on the OVO Computer

The NNM Adapter default destination directory on the OVO computer is:

C:\Program Files\HP OpenView\NnmAdapter

The following subdirectory structure is created:

• bin	Executable and library files
• log	Log files

NnmUtils	Remotely accessible executable files
Template	Template files for NNM tools
Uninstall	Files that are needed by Uninstall

NNM Adapter on the NNM Computer

The NNM Adapter default destination directory on the HP OpenView Network Node Manager computer is:

```
C:\Program Files\HP OpenView\Installed
Packages\{c9322d6f-d88c-11d3-98e3-080009ef5c3b}
```

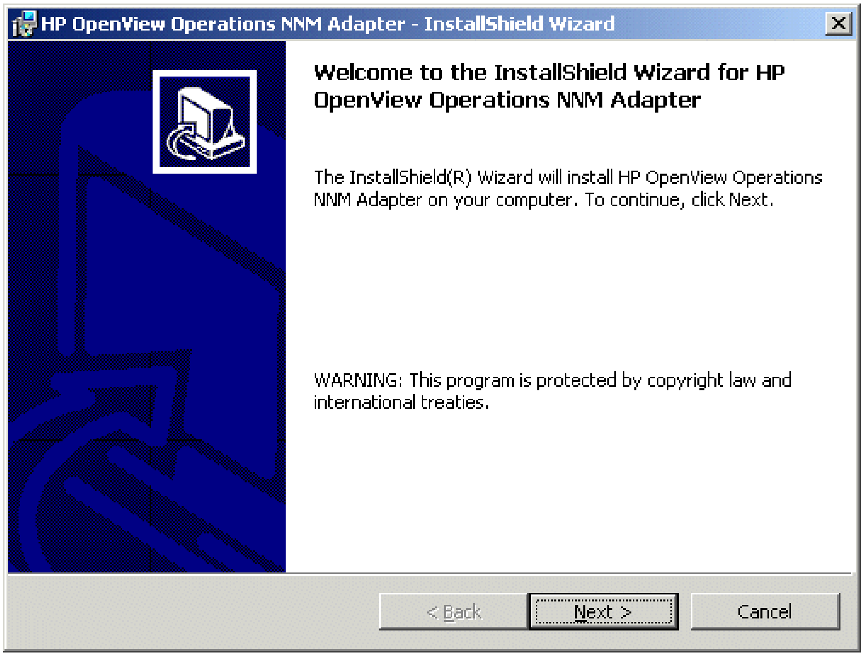
The following subdirectory structure is created:

bin	Executable and library files
data	Configuration and other files
log	Log files
temp	Temporary files

Running the Installation Wizard

To install the NNM Adapter, complete the following steps. Read the instructions before you begin so that you are familiar with the information you must supply during installation.

1 To start the installation process, click **Start** → **Programs** → **HP OpenView** → **Install NNM Adapter** to open the **Welcome** screen.



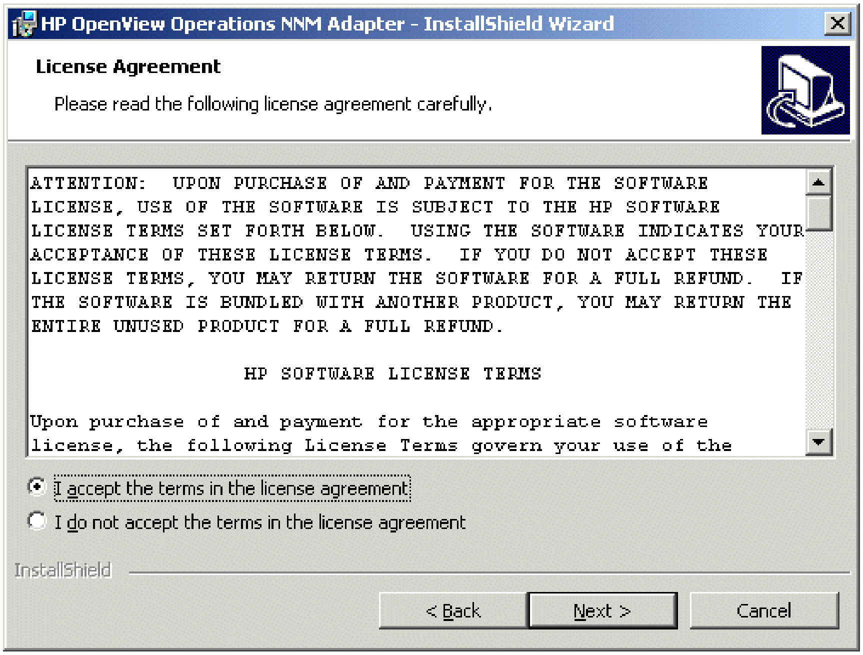
Welcome to the InstallShield Wizard for HP OpenView Operations NNM Adapter

The InstallShield(R) Wizard will install HP OpenView Operations NNM Adapter on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

The installation wizard leads you through the complete installation and configuration process. Follow the displayed instructions, taking particular note of the following steps.

2 Accept the Software License Agreement, shown in the following dialog box.



HP OpenView Operations NNM Adapter - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

```
ATTENTION:  UPON PURCHASE OF AND PAYMENT FOR THE SOFTWARE
LICENSE, USE OF THE SOFTWARE IS SUBJECT TO THE HP SOFTWARE
LICENSE TERMS SET FORTH BELOW.  USING THE SOFTWARE INDICATES YOUR
ACCEPTANCE OF THESE LICENSE TERMS.  IF YOU DO NOT ACCEPT THESE
LICENSE TERMS, YOU MAY RETURN THE SOFTWARE FOR A FULL REFUND.  IF
THE SOFTWARE IS BUNDLED WITH ANOTHER PRODUCT, YOU MAY RETURN THE
ENTIRE UNUSED PRODUCT FOR A FULL REFUND.

                  HP SOFTWARE LICENSE TERMS

Upon purchase of and payment for the appropriate software
license, the following License Terms govern your use of the
```

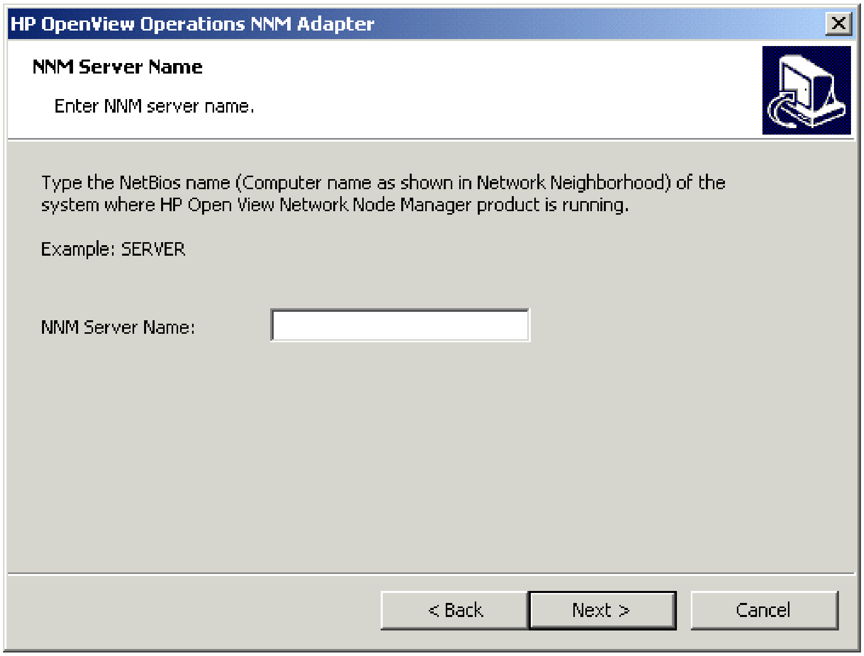
● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

Read the license agreement statement and select “I accept the terms in the license agreement” option if you agree to the terms. If you do not accept the agreement, you cannot proceed with the installation.

3 Specify the NNM Server Name.

Enter the NetBios name of the system where HP OpenView Network Node Manager for Windows is installed. This is the name that Windows uses for system names in Network Neighborhood.When this dialog box first appears, NNM Server Name is automatically filled with the local NetBios name if Network Node Manager is detected on the system.



NNM Server Name

Enter NNM server name.

Type the NetBios name (Computer name as shown in Network Neighborhood) of the system where HP Open View Network Node Manager product is running.

Example: SERVER

NNM Server Name:

Click **Next** to go to the next screen. Before you are taken to the next screen, the installation verifies access to the specified NNM for Windows server. When verification is successful and access to the NNM for Windows server is possible, the next screen is displayed. If access verification fails, one of the following error message may appear:

— Computer is not found - you are not allowed to continue.

— The user under which setup is run does not have administrative rights on computer <...> - you are not allowed to continue.

— Access to computer is denied - you can leave the wizard with **Abort**, try to change the name of computer with **Retry**, or select **Ignore** and continue to the next screen.

Verification may fail for a number of reasons:

- The computer is currently not available
- It is the wrong type of computer
- You do not have administrative rights on the specified computer

Please check for and correct the cause of the failure and retry.

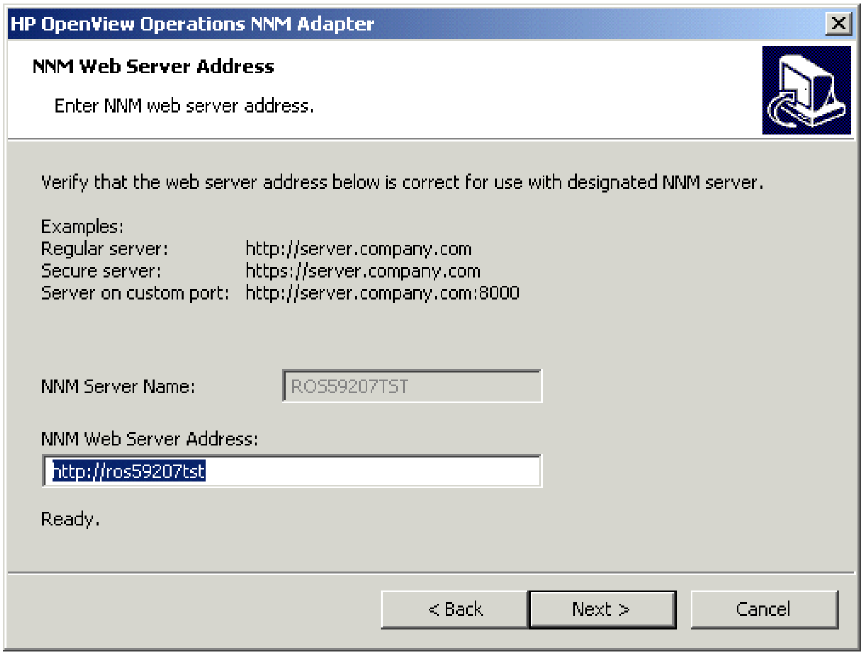
4 Specify the NNM Web Server Address.

Specify the address of the NNM Web Server. The web server name usually takes one of the following forms:

Regular server: http://server.company.com

Secure server: https://server.company.com

Server on custom port: http://server.company.com:8000



HP OpenView Operations NNM Adapter

NNM Web Server Address

Enter NNM web server address.

Verify that the web server address below is correct for use with designated NNM server.

Examples:

Regular server:	http://server.company.com
Secure server:	https://server.company.com
Server on custom port:	http://server.company.com:8000

NNM Server Name: ROS59207TST

NNM Web Server Address: http://ros59207tst

Ready.

Click **Next** to go to the next screen.

Access to the web server is tested when you press **Next**, but is not essential for the next step to be started.

If the web server is not found at the required location, a warning message appears and you can leave the wizard with **Abort**, try to change the name with **Retry**, or select **Ignore** and continue to the next screen.

5 Specify the NNM Adapter User.

Specify the Windows user account and password for the account to be used to run the NNM Adapter components on the OVO server. You need the domain name and the user name. All entries on this screen are required and must be valid.

When this dialog first appears, default values are displayed as follows:

Domain scenario:

Domain = the same domain that was specified during OVO installation.

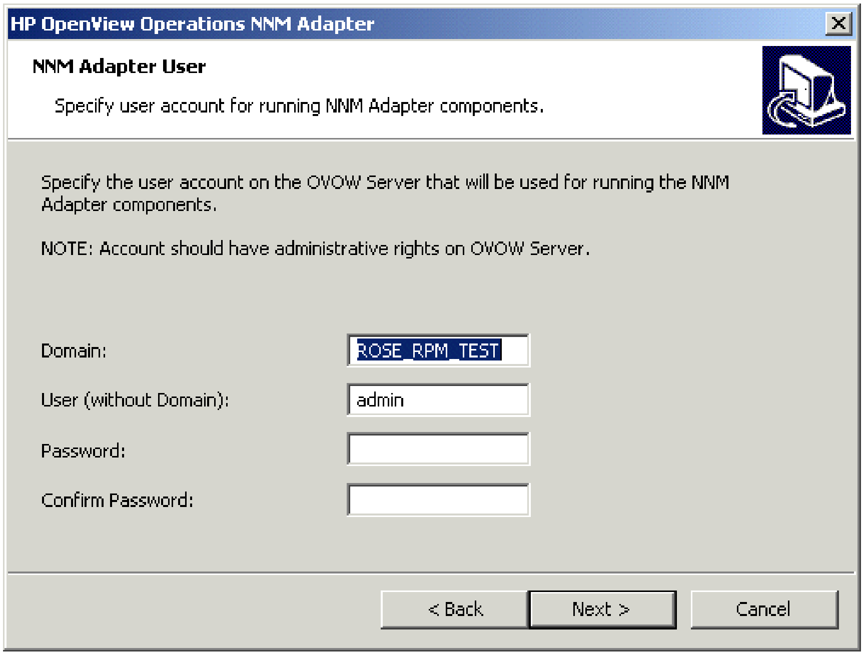
User = the same user that was specified during OVO installation.

Standalone scenario:

Domain = local computer NetBios name.

User = the same user that was specified during OVO installation.

The specified user account must have at least local administrator privileges on the system where OVO is installed. Use a domain user account. If you do not use the HP-OVE-User user, be sure that the chosen user has access rights to the NNM for Windows server and the OVO server. The user rights `Logon as a Service` must be set for the specified user on the OVO server.



HP OpenView Operations NNM Adapter

NNM Adapter User

Specify user account for running NNM Adapter components.

Specify the user account on the OVOW Server that will be used for running the NNM Adapter components.

NOTE: Account should have administrative rights on OVOW Server.

Domain: ROSE_RPM_TEST

User (without Domain): admin

Password:

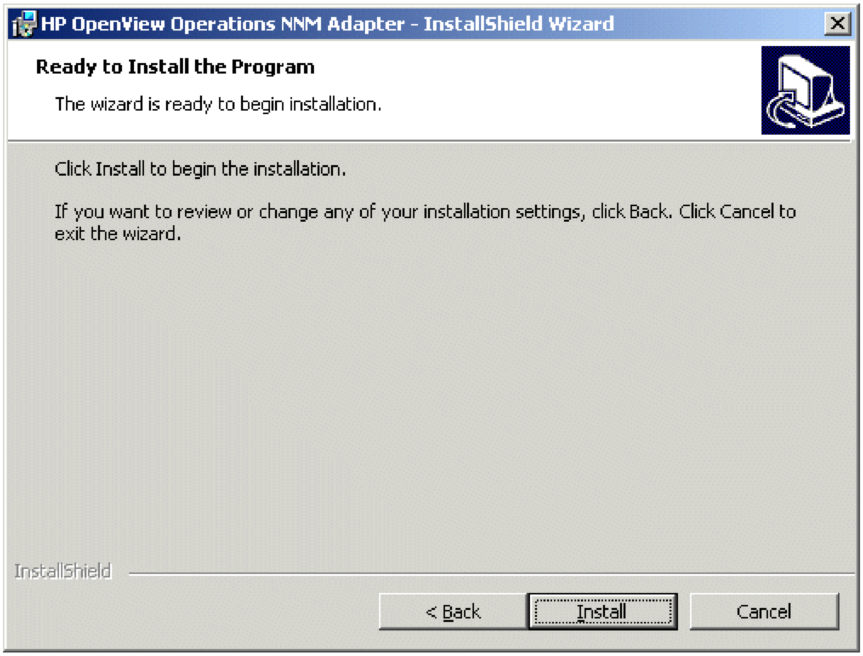
Confirm Password:

If OVO was installed with the Standalone option selected:

Specify the same account that OVO was installed with. In the Domain box, enter the local computer NetBios name.

Before continuing with the installation, create a local user account on the NNM server that is identical to the account OVO was installed with (same user name and password) and add it to the local Administrators group on the NNM server.

Click **Next** to view the **Ready to Install the Program** dialog box.



Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

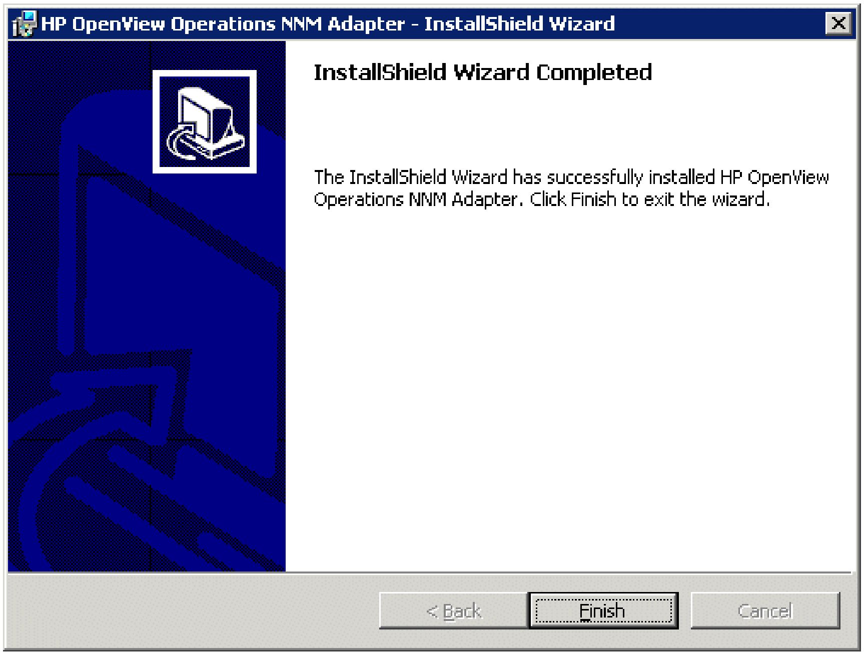
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Click **Install** to enter the final installation phase.

6 Installation completes. All required information has been entered and the installation begins its final phase. During the installation of the NNM Adapter component on the NNM server system, the installation checks to see if a valid installation is present, and if not, displays a message and aborts the installation.

This phase may take up to one hour for large environments and cannot be cancelled once started.

All OVO nodes that are also found in NNM are associated with NNM Web Tools.



InstallShield Wizard Completed

The InstallShield Wizard has successfully installed HP OpenView Operations NNM Adapter. Click Finish to exit the wizard.

Uninstallation tasks

Uninstallation removes components from both the NNM server and the OVO server. You can uninstall Network Node Manager Adapter using the Windows Add/Remove programs dialog box:

1. From the Windows Control Panel, open Add/Remove Programs.
2. Select the entry for “HP OpenView Operations NNM Adapter.”
3. Click **Remove**.
4. Select **Yes** in the message box that asks you to confirm the removal and to launch the uninstall process.

HP OpenView Network Node Manager Server

Uninstallation performs the following tasks on the NNM server:

- NNM deployment package is removed from the NNM server:
  - Registry keys are deleted.
  - Self-registering files are unregistered (COM components).
  - Additional files (COM components, configuration files) are uninstalled.
- SNMP policy is removed from the NNM server.
- Event log policy is removed from the NNM server.

HP OpenView Operations for Windows Server

Uninstallation performs the following tasks on the OVO server:

- The NNM Managed Nodes node group is cleared and associations between managed nodes and the NNM Web Tools are removed. Associations between services hosted on nodes contained in the NNM Managed Nodes group and NNM Web Tools are removed.
- Three services are deleted:
  - Network Node Manager (under Services\Applications)
  - NNM Adapter (under Services\Applications)
  - Network Infrastructure (under Services)
- OpenMessage policy is removed from the OVO management server.
- Event log policy is removed from the OVO management server.
- Self-registering files are unregistered.
- Additional server files are deleted.
- NNM Adapter registry entries are removed.

Post-uninstallation Tasks

To fully clean up the OVO and NNM management server systems, complete the following tasks after uninstalling the NNM Adapter.

- Restart both systems.
- Remove log files on NNM and OVO management server systems.

6

Installing NDAOM

Install the Network Diagnosis Add-On Module (NDAOM) after the OVO for Windows installation is complete. Before installing NDAOM, be sure the following prerequisites are met.

OVO Console Prerequisites

The console can be installed on the same system as the management server or on another suitable system in the network.

One of the following (or later) web browsers with a Java Plug-in is required:

- Netscape Navigator 4.72
- Microsoft Internet Explorer 4.0

OVO Management Server Prerequisites

- HP OpenView Operations for Windows, version A.07.00 through A.07.20 must be installed and configured on a Windows 2000 server system.

- HP OpenView Problem Diagnosis (PD), version A.01.00 or A.01.10 must be installed on the HP OpenView Operations management server system. The installation of HP OpenView Problem Diagnosis must at least include the OVO Problem Diagnosis Probe (selected via Customized installation during the installation of Problem Diagnosis).
- If HP OpenView Network Node Manager is being used, this must also be installed on the same system as the HP OpenView Operations management server. The supported versions of HP OpenView Network Node Manager are A.06.20 or higher.
- 25 MB disk space is required on the HP OpenView Operations management server system to install the integration components.

Managed Node Systems Prerequisites

- A performance agent is installed and configured. NDAOM works with either the OVO embedded performance component or the OpenView Performance Agent (formerly MeasureWare agent).

  On OVO managed nodes running under Sun Solaris operating systems (Solaris 2.6, 7, 8) the Sun Workshop Compilers Bundled libC installation package `SUNWlibC` must be installed so that the library `libCstd.so.1` is in the standard library path.
- All managed nodes must meet the prerequisites of the Problem Diagnosis Probe.
- Be sure that a Java Virtual Machine (JVM) version 1.2.2.06 or higher is installed on every target managed node.

➤ On UNIX nodes, it is possible that the Java executable file is not found by the subagent installation process. This is because the path to the Java executable is not contained in the PATH environment variable of this process.

To avoid this problem, set a link from the Java executable to `/usr/bin/` with the following command:

```
ln -s<path to Java executable file> /usr/bin/java
```

- Be sure that the Problem Diagnosis server is running before you start the NDAOM subagent deployment installation. If it is not running, start it with one of the following commands:
  - UNIX /opt/OV/pd/app_server/bin/ovpdstart
  - Windows Start →Programs → HP OpenView → Problem Diagnosis → PD Server-Start

  If the Problem Diagnosis server is not running during the NDAOM subagent deployment /installation, the newly installed Netpath Probe may not be able to register at the Problem Diagnosis server and so the Problem Diagnosis server may not know this Netpath Probe.
- 10 MB disk space on the managed node is required for the NDAOM software installation.
- In addition to the embedded performance component of the OVO Agent, OV Performance Agent can also be used to collect performance metrics.

The Problem Diagnosis Probe and the NDAOM program are available for the platforms shown in the table.

Table 17 Supported OVO Managed Node Software

Platform	Operating System
HP-UX	11.00, 11.11
Solaris	2.6, 7, 8
Windows	NT4.0 SP5 Windows 2000 SP1, SP2, SP3

Reporting

NDAOM can generate reports through HP OpenView Reporter, version 3.0, based on Crystal Reports 8.5. Be sure that HP OpenView Reporter and the supplied InstallShield package containing the NDAOM reports is installed on a dedicated Windows system.

Data from the following databases can be used to generate reports.

- SQL format data such as Microsoft SQL Server and Oracle

- Performance Agent DSI
- Embedded Performance Component of the OVO Agent.

Table 18 Product Support Matrix

Product Name	Product Version	NDAOM B.01.50
Embedded Performance Component	A.01.00	4
OV Performance	All releases	4
Problem Diagnosis	A.01.00	4
Problem Diagnosis	A.01.10	4
OV Performance Manager	A.02.00	4
PerfView (only in combination with OVP)	All releases	4
OV Reporter (in combination with the Embedded Performance Component or OVP)	A.03.00	4

NDAOM on the OVO Management Server

Installing the HP OpenView Network Diagnosis Add-On Module on the OVO management server system is handled via Microsoft Installer. Steps are detailed in "Installing NDAOM on the OVO Management Server " on page 143.

Please follow the instructions in this chapter to install NDAOM on a system where OVO is already installed.

NDAOM Features

Installation of the HP OpenView Network Diagnosis Add-On Module adds the following features to HP OpenView Operations for Windows.

- A virtual node, `NDAOM Infrastructure`: all network link related messages generated by the NDAOM policies are assigned to this node.

- A node group, `NDAOM`: all nodes on which the NDAOM subagent is to be deployed must be added to this node group.
- A tool group, `NDAOM-Admin`, is created that contains tools added by NDAOM used to administer the add-on module itself.
- A user role `NDAOM-Admin-Profile`.
- A user role `NDAOM-Operator-Profile`.
- A policy group, `NDAOM`, is created that contains the NDAOM policies. These policies should be deployed to each node that is to supervise a network connection relevant to a service to forward events to the OVO message browser.

NDAOM Files Installed

The following files are installed on the HP OpenView Operations for Windows management server and the managed nodes.

OVO Management Server

The NDAOM files are placed in these directories:

```
<OVO Installation Directory>
```

\bin	Batch and script files
\Installed Packages	Message Catalog file (ndaom.cat) for \{790C06B4-844E-11D2-972B NDAOM executable files-080009EF8C2A}\nls\<locale>
\ndaom	Management server tuple database (nwlmdb_sv)
\ndaom\bin	Binary files
\ndaom\conf	Configuration files
\ndaom\log	Log and trace files
\install\ndaom\gui	Nodes, tools, and user roles

• \install\ndaom\policies	Policies
• \instrumentation\<OS name>\<OS version>\NDAOM_INSTALL	Instrumentation files to install the NDAOM subagent
• \instrumentation\<OS name>\<OS version>\NDAOM_REMOVE	Instrumentation files to remove the NDAOM subagent

HP-UX and Solaris Managed Nodes

The NDAOM files are placed in the following directories:

• /opt/OV/subagent/ndaom	Deployed subagent files
• /opt/OV/ndaom/bin	Binary files
• /opt/OV/lib/nls/<locale>	Message Catalog file (ndaom.cat) for NDAOM executable files
• /etc/opt/OV/ndaom/ddf	Configuration and specification files for Dynamic Data Feed
• /etc/opt/OV/ndaom/conf	Configuration files
• /var/opt/OV/ndaom	Managed node tuple database (nwlmdb_agt)
• /var/opt/OV/ndaom/log	Log and trace files
• /var/opt/OV/ndaom/tmp	Temporary files
• /var/opt/OV/ndaom/ddf	Log files for OVPM and OVR integration via the Embedded Performance Component

Directories used by NDAOM via the OVO agent mechanisms are:

- /var/opt/OV/bin/OpC/vpwin/monitor
- /var/opt/OV/bin/OpC/vpwin/cmds
- /var/opt/OV/bin/OpC/vpwin/actions

Microsoft Windows Managed Nodes

Default directories used by the Add-On Module are within the directory:

```
<OVO Installation Directory>\Installed Packages\
{790C06B4-844E-11D2-972B-080009EF8C2A}
```

\ndaom	Managed node tuple database (nwlmdb_agt)
\ndaom\bin	Binary files
\ndaom\conf	Configuration files
\ndaom\ddf	Files used for OVPM and OVR integration
\ndaom\log	Log and trace files
\ndaom\tmp	Temporary files
\subagent\ndaom	Deployed subagent files
\nls\<locale>\<locale>	Message catalog file (ndaom.cat)

Directories used by NDAOM via the OVO agent mechanisms are:

```
<OVO Installation Directory>\Installed Packages\
{790C06B4-844E-11D2-972B-080009EF8C2A}
```

- \bin\OpC\vpwin\monitor
- \bin\OpC\vpwin\cmds
- \bin\OpC\vpwin\actions

Installing NDAOM on the OVO Management Server

Installation of the HP OpenView Network Diagnosis Add-On Module for HP OpenView Operations is divided into three parts:

- Install the Problem Diagnosis software.
- Install the NDAOM software on the management server.
- Install the NDAOM components on the managed node.

Installing the PD Server on the OVO for Windows Management Server

Installing the Problem Diagnosis software on the HP OpenView Operations for Windows management server system requires that you complete these steps:

- Install the Problem Diagnosis Server.
- Install the Problem Diagnosis Probe.

Installing the Problem Diagnosis Server

Install the Problem Diagnosis server on a system of your choice. The easiest option is to use the OVO Management server system.

➤ You may choose not to install the Problem Diagnosis server at all. NDAOM can work without the Problem Diagnosis server, provided that the OVO Problem Diagnosis Probes are installed. However, without the Problem Diagnosis server, the graphical user interface of HP OpenView Problem Diagnosis with which NDAOM integrates will not be available to you.

1. Be sure that the prerequisites for the Problem Diagnosis product have been fulfilled. Please refer to the installation documentation provided with the Problem Diagnosis product.
2. Start the installation of the Problem Diagnosis software.
3. When requested for the type of installation to make, select **Customize**.
4. Mark the following software components for installation:
   - Problem Diagnosis Server
   - OVO Problem Diagnosis Probe
5. Complete the installation.

6 Be sure that the Problem Diagnosis server is running. If not, start it with the appropriate command on the host system:

• UNIX	opt/OV/pd/app_server/bin/ovpdstart
• Windows	Start → Programs → HP OpenView → ProblemDiagnosis →PD Server-Start

Installing the OVO PD Probe on the OVO Management Server

If you have installed the Problem Diagnosis server on a system other than the OVO Management server system, or if you have chosen not to install the HP OpenView Problem Diagnosis server at all, perform the following additional installation tasks on the OVO Management server system.

1 Start the installation of Problem Diagnosis software on the OVO management server system.

When requested for the type of installation to make, select **Customize**.

2 Mark only the following software component for installation:

OVO Problem Diagnosis Probe

3 Complete the installation.

4 If during the installation of the OVO Problem Diagnosis Probe you have selected an alternative installation location from that suggested by the installer, manually set the value for the registry key on the OVO management server:

```
HKEY_LOCAL_MACHINE\SOFTWARE\HEWLETT-PACKARD\Op
enView\PD\Server\Pathname
```

to the location of the OVO Problem Diagnosis Probe installation.

➤ You may have to create new keys and a new Pathname string value and then enter the required location path.

Installing NDAOM on the OVO Management Server

To install NDAOM on the management server, follow these steps:

1. Insert the disk “hp OpenView Operations 7.20 for Windows” and start the installation package **NDAOM.msi** from the NDAOM directory. The NDAOM.msi file is located on Disk 2 in the NDAOM Reporter directory.

2. As setup type, choose the “Complete” installation and continue. The installation continues without further interaction.

3. Configure NDAOM by modifying the `ndaom.cfg` file as follows and adapt the entries for all variables to fit your environment. (BROWSER, PD_SERVER, PD_SERVER_IP, PD_SERVER_PORT, PERFMGR_SERVER). See “NDAOM Configuration File ndaom.cfg” for a full description of the variables.

   Open the file:

   ```
   <OVO Installation Directory>\ndaom\conf\ndaom.cfg
   ```

   and edit it so that it reflects the following requirements:

   — An entry is required which defines the name of the OVO management server system where the Problem Diagnosis server is installed. For example:

   PD_SERVER=bug.London.mycom.com

   The default value is the name of the management server.

   — An entry is required which defines the IP address of the OVO management server system where the Problem Diagnosis server is installed. For example:

   PD_SERVER_IP=16.216.111.55

   The default value is the IP address of the management server.

   — An entry is required which defines the port number that has been assigned to the Problem Diagnosis server. For example:

   PD_SERVER_PORT=9085

   The default value is 9085.

   — An entry is required which defines on which network node the OV Performance Manager installation resides. For example:

   PERFMGR_SERVER=bug.London.mycom.com

The default value is the name of the management server.

- An entry is required which defines the command to start your web browser. For example:

  BROWSER=iexplorer.exe

4. NDAOM installs two user profiles in the user profile bank: `NDAOM-Admin-Profile and NDAOM-Operator-Profile`. Be sure that you assign one of them to the current user.

5. Start the following command on the OVO management server system:

   ```
   cscript <OVO Installation Directory>\bin\update_templates.vbs
   ```

   This VBS script updates the NDAOM templates and tools that are necessary for the Problem Diagnosis Server integration and uploads them again to the OVO management server.

Installing NDAOM on the Managed Node Systems

Installing NDAOM on managed nodes requires the following steps:

- Adding nodes to the NDAOM node group
- Deploying instrumentation
- Deploying NDAOM policies
- Deploying the NDAOM subagent

Adding Nodes to the NDAOM Node Group

To enable `ovnwlinkmon` to deploy to a managed node, the node must be included in the `NDAOM` node group. To add nodes to this group, complete the following steps:

1. Select a node or node group.
2. Select **Action** → **Configure** → **Nodes**.
3. Right-click the node displayed in the right half of the **Configure Managed Nodes** dialog box and select **Copy**.
4. Right-click the `NDAOM` node group and select **Paste Shortcut**.

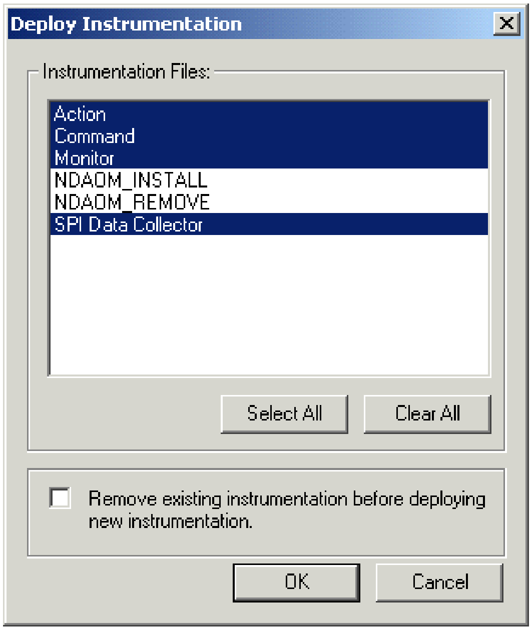
   Repeat steps 3 and 4 for all nodes on which NDAOM needs to be installed.

5 Click **OK**.

Deploying the Instrumentation

Deploying instrumentation deploys the tools to the managed nodes which are needed by the NDAOM policies and the NDAOM subagent. To deploy instrumentation, follow these steps:

1 Right-click the NDAOM node group and select **All Tasks** → **Deploy Instrumentation** to open the **Deploy Instrumentation** dialog box**.**



Deploy Instrumentation

Instrumentation Files:

- Action
- Command
- Monitor
- NDAOM_INSTALL
- NDAOM_REMOVE
- SPI Data Collector

□ Remove existing instrumentation before deploying new instrumentation.

2 Select Action, Command, Monitor, and SPI Data Collector, as shown.

3 Click **OK**.

Deploying the NDAOM Policies

Policies are deployed from the OVO management server system using the standard HP OpenView Operations for Windows mechanisms. To make this deployment easier, the NDAOM policies are assigned to the `NDAOM` node group. Follow these steps to deploy policies:

1. Select the policy that you want to deploy from the `NDAOM` policy group.
2. Right-click the policy name and Select **All Tasks** → **Deploy On** from the context menu to open the **Deploy Package on** dialog box.
3. Select the node to which the policies are to be deployed.
4. Click **OK**.

Alternatively, you can drag and drop the desired policy onto a target node.

Deploying the NDAOM Subagent

The NDAOM subagent consists of the Problem Diagnosis Probe, `ovnwmonitor`, and `ovnwpdc`. It is deployed from the OVO management server system using `ovnwlinkmon`.

Be sure that the Problem Diagnosis server is running. If not, start it with the appropriate command on the host system:

• UNIX	/opt/OV/pd/app_server/bin/ovpdstart
• Windows	Start -> Programs -> HP OpenView -> Problem Diagnosis -> PD Server-Start

If the Problem Diagnosis server is not running during the NDAOM subagent deployment/installation, the newly installed Netpath Probe may not be able to register at the Problem Diagnosis server and so the Problem Diagnosis server may not know this Netpath Probe.

1. Use the `ovnwlinkmon` program with the `-add` option to add the network connections to be monitored to the global tuple database.

   `ovnwlinkmon.exe` is located in:

   ```
   <OVO Installation Directory>\ndaom\bin
   ```

For more details, see `ovnwlinkmon -add [-NoNewObject]` on page 67 in the NDAOM documentation.

2 View the network connections in the global tuple database using the command:

```
ovnwlinkmon -list
```

3 Deploy the NDAOM subagent to the managed nodes that are listed as `Source` nodes in the global tuple database using the command:

```
ovnwlinkmon -deploy
```

4 Deployment of the NDAOM subagents via `ovnwlinkmon -deploy` usually takes a few minutes. After the NDAOM subagent packages are deployed to the managed nodes, the `checkinstall` script checks the configuration of the managed nodes. A background process then starts the subagent installation and registers the NDAOM agent executable files with the OVO agent. Please wait until you receive an `Installation Success` message in the OVO message browser on the management server.

If the NDAOM subagent installation fails, check the installation log file on the manage node system

• UNIX	/tmp/install_nwagt.log
• Windows	<drive>: \TEMP\install_nwagt.log

Installing the NDAOM Report Package

The NDAOM report package includes a component that must be installed on the Windows system where Reporter is installed. This component establishes the connection between Reporter and OVO.

To install the NDAOM report package on the system that hosts Reporter, follow these steps:

1 Insert the HP OpenView Operations 7.20 for Windows Standalone Agents disk, part number B7490-13081/15081 English (B7490-13086/15086 Japanese), from the OVO for Windows CD set in the CD-ROM drive of the Reporter host system.

2 Run the **ServiceReportsFor NDAOM.msi** program to install the report package.

3. Check the Reporter status pane to note the changes to the Reporter configuration which includes uploading the NDAOM policies.

   NDAOM reports are automatically assigned to ALL groups in the Reporter main window. See "Reports and Integrating NDAOM into HP OpenView Reporter on page 97 of the NDAOM documentation for details of OVO reports.

4. Add group and single system reports by assigning reports as desired.

Uninstalling NDAOM from Managed Node Systems

To uninstall the NDAOM software from a managed node, use one of these methods.

- Use the Remove `NDAOM Subagent (NT)` or `(UNIX)` tool from the tool group `NDAOM-Admin` on the management server
- Use the command line call `ovnwlinkmon -remove_sa`
- Call the `remove_nwagt` script from the command line directly on the managed node:
  - UNIX `/tmp/install_nwagt.log`
  - Windows <drive>: \TEMP\install_nwagt.log

7

After You Install

This chapter contains information about the following actions you can begin after you have installed HP OpenView Operations for Windows (OVO).

- Learn how OVO works.
- Begin to configure OVO.

Learn How OVO Works

- For information about key concepts that explain OVO strategy, basic architecture, and operation, see the multi-media *HP OpenView Integrated Assurance for Windows featuring HP OpenView Operations/Performance for Windows Concepts Guide*. You can access this guide from the following web site:

  http://www.openview.hp.com/seetrybuy/see/index.asp

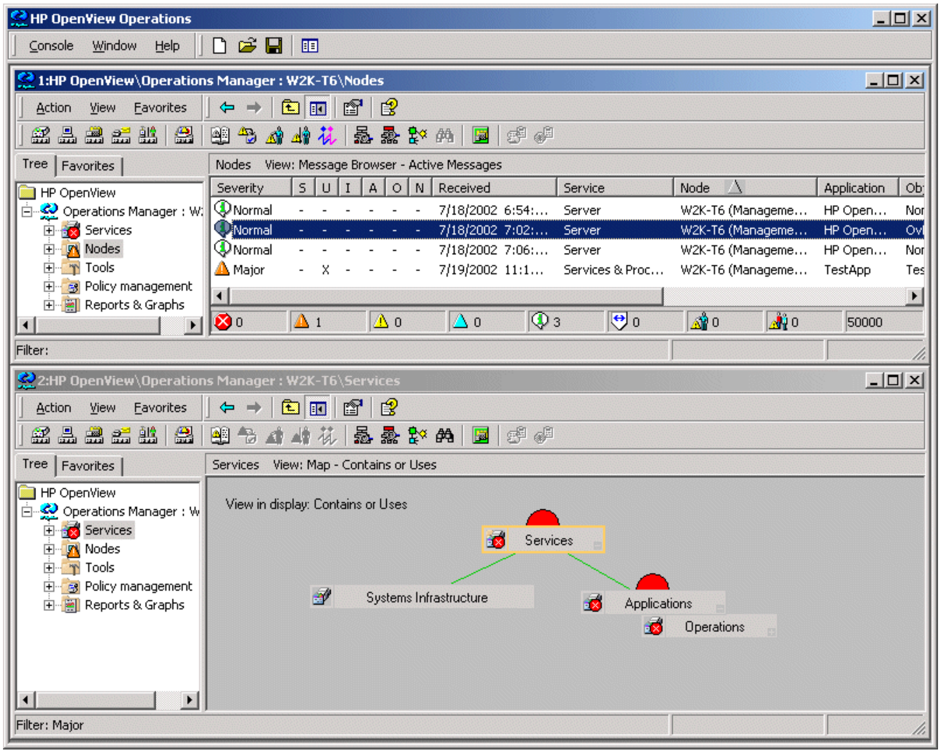
  Select the link “hp OpenView integrated service assurance for Windows.”
- For an interactive tutorial that combines an overview of essential tasks with hands-on procedures and examples, see the basic training information, available from within help and from the installation media. The option to view the basic training tutorial appears when installation is complete and the console is first opened. You can use the first page of the tutorial as a convenient checklist of administrative tasks to be performed.

- For information on administrator tasks such as node, tool, services, policy, and user roles configuration, policy deployment, and database maintenance, see the help system.

Overview of the Console

Open the OVO console. From the **Start** menu, select **Programs** → **HP OpenView** → **Console** to bring up the OVO management console**.** In the console tree, click on Operations Manager. Experiment by navigating within the console tree; expand and collapse the contents of the tree by clicking on the plus signs beside entries. Explore the options available by viewing messages and maps. A brief description follows; for more detailed information, see the online help.

The following illustration shows the default console view that opens when you launch the product. Two windows appear. One contains a map view of the systems infrastructure. The other displays the message browser. The console tree appears in the left side of each window and the details pane in the right, as shown.



Severity	S	U	I	A	O	N	Received	Service	Node	Application	Ob
Normal	-	-	-	-	-	-	7/18/2002 6:54:...	Server	W2K-T6 (Manageme...	HP Open...	Nor
Normal	-	-	-	-	-	-	7/18/2002 7:02:...	Server	W2K-T6 (Manageme...	HP Open...	Ov
Normal	-	-	-	-	-	-	7/18/2002 7:06:...	Server	W2K-T6 (Manageme...	HP Open...	Nor
Major	-	X	-	-	-	-	7/19/2002 11:1...	Services & Proc...	W2K-T6 (Manageme...	TestApp	Tes

Microsoft Management Console (MMC) and Menu

The Microsoft Management Console (MMC) menu bar is the topmost menu bar in the previous illustration. Menus include Console, Window, and Help. The MMC provides a software framework for administration tools such as OVO. From the MMC menu bar, you can perform a range of tasks, from manipulating the console windows to creating a new console. For more information on MMC, see online help on the MMC menu or the Microsoft web site at www.microsoft.com.

Web Console Interface

The HP OpenView Web Console provides a quick and convenient way to view and respond to messages that result from events that occur on your managed nodes. From any location, use your Internet Explorer or Netscape browser to instantly see the severity of a message and act to correct the problem that caused it. See Chapter 2 for supported browser versions.

See the help topic "Browse messages with the web console" in the OVO help system for information on accessing the web console. A separate help system is provided with the web console that explains its features and functionality.

OVO Menu

Use the OVO menu bar, directly under the MMC menu bar, to perform OVO tasks. Shortcut menus, which appear after you select an item and right-click the mouse, also are frequently used to perform tasks in OVO.

Details Pane

The details pane (the right side of the window) hosts the list, message browser, and map views. You can tile these views to see multiple windows.

Console Tree

The console tree (on the left side of the window) displays, in a list view, folders representing the key OVO components:

- **Services**: These are customer-based, user-oriented, or infrastructure capabilities provided by one or more hardware or software components within a computing environment (such as e-mail, network bandwidth, and application access). Policies help assure that appropriate service levels are provided to designated consumers of the service.
- **Nodes**: A node is a computer system or intelligent device that can be managed from the OVO management server. OVO can manage both Windows and UNIX nodes.

- **Tools**: In OVO, tools are software programs or commands used to perform tasks. For example, you can configure a URL, an executable, or a Visual Basic script to be run on a remote managed node.
- **Policies (shown in the console tree under Policy Management)**: Policies are specifications and/or rules that help automate network and service administration. OVO administrators deploy policies to managed nodes to provide consistent, automated administration across the enterprise. Policies can be thought of as templates that indicate which information is monitored and logged on managed nodes and which events and messages the management server passes to the console.
  - UNIX policies and tools are provided and can be deployed to UNIX nodes.
  - Two sets of policies are installed automatically when you install the management server:
    - Preconfigured policies for Microsoft Windows, which can be deployed on managed nodes to monitor the Windows operating system on those managed nodes.
    - Self Manager, which manages the OVO server and agents and can be deployed to the management server and managed nodes.
- **Smart Plug-ins (SPIs)**: SPIs are prepackaged software for managing specific types of business applications and databases, such asthe Exchange database. SPIs install into an MMC Snap-in and contain the necessary data sources, policies, diagnostic rules, and corrective actions to enable operational management of a computer system. SPIs also contain help systems and can provide other types of documentation as well.

Set or Change a System Administrator Password

When the database is first created at installation of HP OpenView Operations for Windows, a default user, sa, is created with no password. You were encouraged to provide a password for this user during OVO for Windows installation. If you did not do so then, it is recommended that you set a password for this system administrator at this time. You can also use this command to change the password at a later date.

Use the command:

```
osql -S.\OVOPS -U sa -P -Q"sp_password NULL, ’<new sa password>’"
```

What You Can Configure

As an administrator, you configure certain specific elements of the software. The list below gives you a high-level view of configuration tasks.

For instructions on how to configure OVO, see the basic training tutorial and the extensive online help provided from the console. Most administrative tasks are reserved for administrators, but a few are available to all users, and any of them can be assigned to user roles that control the functions that operators perform.

- **Add users:** (OVO Administrators and Operators) to appropriate security groups.
- **Configure nodes:** You configure nodes (systems) so that you can manage them. Configuration includes selecting systems (nodes) to be managed and selecting which tools are available for nodes, services, and user roles. As soon as a node is configured, it becomes a managed node. The management server is automatically added as a managed node at installation.
- **Configure services:** To relate your business services to OVO features, you define how services in the service hierarchy are dependent on each other, and define rules that evaluate the severity based on the state of the contributing services. To start, you can use the default values for status propagation and status calculation rules.
- **Configure tools:** You specify the tools that operators can apply to managed nodes and services. By applying the available tools, operators resolve problems reported in the message browsers that have critical business impact, or use tools to report on information about their managed environment. These tools can be associated with services, managed nodes, and user roles. Tools can also be configured to run on a predefined list of nodes.
- **Configure user roles:** As an administrator, you can configure an operator's view of the environment to focus on specific assigned tasks and responsibilities. By defining roles for specified users, you control the operator's view of your enterprise and the range of activities which that user has permission to perform. By assigning users to well-defined, specific roles, you can distribute monitoring and maintenance tasks across a group of individuals with their own particular areas of expertise and experience and customize each operator's console view.

- **Configure service types:** You can specify properties for service types, used when an instance of a service is created. Service type is similar to a template; you associate a service type with specific reports, graphs, tools, and deployment packages. That service type is then used when an instance of the associated service is created. Any tools, reports, graphs, and deployment packages associated with the service type are associated with every instance of that service that has been or will be created. The service type assures that these properties are applied globally to all services of that type.
- **Create or edit policies:** In addition to using the preconfigured default policies, you can configure user-defined policies, either by copying and then modifying a version of one or more default policies, or by creating a new policy from one of the policy types. You can also create automatic and operator-initiated commands designed to solve problems associated with messages received in the message browsers.
- **Configure message filters:** (operator or administrator). Messages that appear in the message browser are received from the nodes managed by the management server, as configured by the administrator. By setting filters, operators can further customize the way messages display to show only messages that match specific criteria.
- **Collect performance data on managed nodes:** The HP OpenView Operations for Windows Agent is deployed to all Windows managed nodes on which data will be collected.
- **Draw performance graphs:** You can use collected performance data to draw graphs for use in diagnosing performance problems and detecting trends. You can customize default graphs and also create your own.
- **Manage Microsoft Windows services:** Use preconfigured default policies until, based on events that display in the message browsers, you decide how to modify them to suit your exact needs.
- **Manage UNIX nodes:** Agents for managing UNIX nodes are provided as part of OVO. You can install and activate these agents and deploy preconfigured default policies and tools for managing your UNIX systems.
- **Manage OVO services using the Self Manager:** The Self Manager manages OVO services and agents. It is automatically deployed to the management server. You deploy the Self Manager policies to managed nodes to manage the agents.

8

Documentation

Extensive product documentation is provided on the HP OpenView Operations for Windows installation media. Each OVO component also provides a help system.

Manuals are in Adobe Acrobat PDF format and are located in the `\Documentation` directory on the product CDs, which also contain documentation for Smart Plug-ins. PDF files relating to the OVO for Windows foundation are also installed on the management server in this directory:

```
<%OVInstallDir%>\Nls\1033\Manuals\
```

The following documentation is available.

HP OpenView Operations for Windows

Document	File and Location	Purpose
OpenView Operations / Performance Installation Guide	`OVOInstall.pdf` OV operations 7.20 for Windows disk	Provides installation requirements, instructions, and security information.
HP OpenView Integrated Service Assurance for Windows featuring HP OpenView Operations / Performance for Windows	http://www.openview.hp.com/demos/index.html	Explains components and their inter-relationships.
HP OpenView Operations / Performance Upgrade Guide Version 7.20	`OVOWUpgrade.pdf` OV operations 7.20 for Windows disk	Explains the upgrade process for moving from previous versions to the 7.20 version of HP OpenView Operations/ Performance for Windows.
HP OpenView Guide for Upgrading from ManageX / OV Express to OpenView Operations 7.0 for Windows.	`ManageXUpgrade.pdf` OV operations 7.20 for Windows disk	Explains upgrade process for moving from previous products to HP OpenView Operations/ Performance for Windows.
OVOReadMe	`OVOReadMe.txt` OV operations 7.20 for Windows disk	Includes information on the HP OpenView Operations for Windows release.
HPOV Auto Pass User's Guide	`AutoPass_guide.pdf` OV operations 7.20 for Windows disk	Explains the licensing process and how to obtain permanent license passwords.

Smart Plug-in for Windows Operating System

Document	File or Location	Purpose
WinOSReadMe	`WinOSReadMe.txt` OV operations 7.20 for Windows Smart Plug-ins disk	Includes information on the HP OpenView Operations for Windows release.

Smart Plug-in for UNIX Operating System

Document	File or Location	Purpose
HP OpenView Smart Plug-in for UNIX Operating Systems Administrator's Guide	`SPI_UNIX Online Help.pdf` OV operations 7.20 for Windows Smart Plug-ins disk	Includes information on the HP OpenView Operations for UNIX release.

Smart Plug-in for Microsoft Active Directory Server

Document	File or Location	Purpose
HP OpenView Operations for Windows Smart Plug-in for Microsoft Active Directory Server Configuration Guide	`ADSPIi_Config.pdf` OV operations 7.20 for Windows Smart Plug-ins disk	Includes instructions and information about configuring the SPI for use with HP OpenView Operations for Windows.

Smart Plug-in for Microsoft Enterprise Servers

Document	File or Location	Purpose
ReadMe	`SPI_EnterpriseServersReadMe.txt`	Includes information on the HP OpenView Operations for Windows Smart Plug-in for Microsoft Enterprise Servers

Smart Plug-in for Microsoft Exchange Server

Document	File or Location	Purpose
HP OpenView Operations for Windows Smart Plug-in for Microsoft Exchange Server Configuration Guide	`ExchangeSPIConfig.pdf` OV operations 7.20 for Windows Smart Plug-ins disk	Includes instructions and information about configuring the SPI for use with HP OpenView Operations for Windows.
SPI ExchangeReadMe	`SPI_ExchangeReadMe.txt` OV operations 7.20 for Windows Smart Plug-ins disk	Includes information on the HP OpenView Operations for Windows Smart Plug-in for Exchange Servers.

Smart Plug-in for Oracle Database

Document	File or Location	Purpose
HP OpenView Operations for Windows Smart Plug-in for Databases Configuration Guide	`DBSPIConfig.pdf` OV operations 7.20 for Windows Smart Plug-ins disk	Includes instructions and information about configuring the SPI for use with HP OpenView Operations for Windows.
*DBReadM*e	`DBReadMe.txt` OV operations 7.20 for Windows Smart Plug-ins disk	Includes information on the HP OpenView Operations for Windows Smart Plug-in for Databases.

Smart Plug-in for Sybase Database

Document	File or Location	Purpose
HP OpenView Operations for Windows Smart Plug-in for Databases Configuration Guide	`DBSPIConfig.pdf` OV operations 7.20 for Windows Smart Plug-ins disk	Includes instructions and information about configuring the SPI for use with HP OpenView Operations for Windows.
DBReadMe	`SPI_dbReadMe.txt` OV operations 7.20 for Windows Smart Plug-ins disk	Includes information on the HP OpenView Operations for Windows Smart Plug-in for Databases.

Smart Plug-in for Informix Database

Document	File or Location	Purpose
HP OpenView Operations for Windows Smart Plug-in for Databases Configuration Guide	`DBSPIConfig.pdf` OV operations 7.10 for Windows Smart Plug-ins disk	Includes instructions and information about configuring the SPI for use with HP OpenView Operations for Windows.
DBReadMe	`SPI_dbReadMe.txt` OV operations 7.20 for Windows Smart Plug-ins disk	Includes information on the HP OpenView Operations for Windows Smart Plug-in for Databases.

Smart Plug-in for Microsoft SQL Server Database

Document	File or Location	Purpose
HP OpenView Operations for Windows Smart Plug-in for Databases Configuration Guide	`DBSPIConfig.pdf` OV operations 7.20 for Windows Smart Plug-ins disk	Includes instructions and information about configuring the SPI for use with HP OpenView Operations for Windows.
DBReadMe	`SPI_dbReadMe.txt` OV operations 7.20 for Windows Smart Plug-ins disk	Includes information on the HP OpenView Operations for Windows Smart Plug-in for Databases.

Smart Plug-in for mySAP.com

Document	File or Location	Purpose
HP OpenView Operations for Windows Smart Plug-in for mySAP.com Configuration Guide	`SAPSPIConfig.pdf` OV operations 7.20 for Windows Smart Plug-ins disk	Includes instructions and information about configuring the SPI for use with HP OpenView Operations for Windows.
SAPReadMe	`SPI_SAPReadMe.txt` OV operations 7.20 for Windows Smart Plug-ins disk	Includes information on the HP OpenView Operations for Windows Smart Plug-in for mySAP.com.

Smart Plug-in for Web Servers

Document	File or Location	Purpose
Web Servers ReadMe	`SPI_webserversReadMe.txt` OV operations 7.20 for Windows Smart Plug-ins disk	Includes information on the HP OpenView Operations for Windows Smart Plug-in for Web Servers.

Smart Plug-in for BEA WebLogic Server

Document	File or Location	Purpose
HP OpenView Smart Plug-in for BEA WebLogic Server Configuration Guide	`wlsspi_config.pdf` OV operations 7.20 for Windows Smart Plug-ins disk	Provides configuration instructions.

Smart Plug-in for IBM WebSphere

Document	File or Location	Purpose
Smart Plug-in for WebSphere Configuration Guide	`wbsspi_config.pdf` OV operations 7.20 for Windows Smart Plug-ins disk	Provides configuration instructions.

Network Node Manager 6.2

Document	File or Location	Purpose
Windows NT/2000 Installation Guide	`Installation_Guide.pdf` Network Node Manager disk	Provides installation requirements and instructions.
Managing Your Network with HP OpenView Network Node Manager	`Managing_Your_Network.pdf` Network Node Manager disk	Describes using NNM 6.2 for network management.
A Guide to Scalability and Distribution for HP OpenView Network Node Manager	`Scalability_and_Distribution.pdf` Network Node Manager disk	Includes information on the HP OpenView Network Node Manager 6.2 release.

Performance Agent

Document	File or Location	Purpose
Performance Agent Installation and Configuration Guide	`mwainst.pdf` Performance Agent disk	Installation and configuration procedures.
Performance Agent User's Guide	`mwausers.pdf` Performance Agent disk	Includes an overview and information about using the HP OpenView Performance Agent for UNIX product.
Performance Agent DSI Guide	`mwadsi.pdf` Performance Agent disk	Includes overview, information, and examples on using Data Source Integration (DSI) with the HP OpenView Performance Agent.
Performance Agent Dictionary of OS Performance Metrics	`metrics.pdf` Performance Agent disk	Reference manual for available operating system metrics.
Release Notes	`mwa` Performance Agent disk	Includes information on the HP OpenView Performance Agent release.

Performance Manager

Document	File or Location	Purpose
Concepts Guide	`OVPM_concepts_guide.pdf` hp OpenView Performance Manager disk	Product overview and features
Administrator's Guide	`OVPM_admin_guide.pdf` hp OpenView Performance Manager disk	Describes administrative task such as configuration, security, and troubleshooting.
Read Before Installing	hp OpenView Performance Manager disk	Lists items to consider before installing HP OpenView Performance Manager 4.0.
OVPM ReleaseNotes	`OVPMReleaseNotes.htm` hp OpenView Performance Manager disk	Provides information about changes from previous release.

Problem Diagnosis

Document	File or Location	Purpose
Concepts Guide	`ConceptsGuide_en.pdf` Problem Diagnosis disk	This guide is a subset of the online help information.
Release Notes	`ReleaseNotes_en.html` Problem Diagnosis disk	Includes installation information and information on the HP OpenView Problem Diagnosis release.

Reporter 3.0

Document	File or Location	Purpose
Concepts Guide	`ConceptsGuide.pdf` Reporter disk	Product overview and features
Installation and Special Configurations Guide	`InstallConfig.pdf` Reporter disk	Installation instructions.
ReadMeFirst	`ReadMeFirst.htm`	Guide to first steps.
Reporter Release Notes	`reporterreleasenotes.htm` Reporter disk	Includes information on the HP OpenView Reporter 3.0 release.

index