HP OpenView Operations

OVO DCE Agent Concepts and Configuration Guide

Software Version: A.08.10

UNIX

Manufacturing Part Number: None

October 2004

Legal Notices

Warranty.

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

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

Restricted Rights Legend.

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

Hewlett-Packard Company
United States of America

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

Copyright Notices.

Trademark Notices.

Adobe® is a trademark of Adobe Systems Incorporated.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Intel386, Intel80386, Intel486, and Intel80486 are U.S. trademarks of Intel Corporation.

1. About AIX Managed Nodes

2. About HP-UX Managed Nodes

3. About Linux Managed Nodes

4. About MPE/iX Managed Nodes

5. About Novell NetWare Managed Nodes

6. About Sequent DYNIX Managed Nodes

7. About SGI IRIX Managed Nodes

8. About SINIX RM/Reliant Managed Nodes

9. About Sun Solaris Managed Nodes

10. About Tru64 UNIX Managed Nodes

11. About Windows NT/2000 Managed Nodes

Printing History

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

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

First Edition:	September 1999
Second Edition:	June 2000
Third Edition:	January 2002
Fourth Edition:	June 2004
Fifth Edition:	October 2004

Conventions

The following typographical conventions are used in this manual.

Table 1 Typographical Conventions

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

Table 1 Typographical Conventions (Continued)

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

OVO Documentation Map

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

Electronic Versions of the Manuals

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

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

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

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

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

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

Watch this website regularly for the latest edition of the OVO Software Release Notes, which gets updated every 2-3 months with the latest news such as additionally supported OS versions, latest patches and so on.

OVO Manuals

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

Table 2 OVO Manuals

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

Table 2 OVO Manuals (Continued)

Manual	Description	Media
OVO Java GUI Operator's Guide	Provides you with a detailed description of the OVO Java-based operator GUI and the Service Navigator. This manual contains detailed information about general OVO and Service Navigator concepts and tasks for OVO operators, as well as reference and troubleshooting information.	PDF only
Service Navigator Concepts and Configuration Guide	Provides information for administrators who are responsible for installing, configuring, maintaining, and troubleshooting the HP OpenView Service Navigator. This manual also contains a high-level overview of the concepts behind service management.	Hardcopy PDF
OVO Software Release Notes	Describes new features and helps you: • Compare features of the current software with features of previous versions. • Determine system and software compatibility. • Solve known problems.	PDF only
OVO Supplementary Guide to MPE/iX Templates	Describes the message source templates that are available for the MPE/iX managed nodes. This guide is not available for OVO on Solaris.	PDF only
Managing Your Network with HP OpenView Network Node Manager	Designed for administrators and operators. This manual describes the basic functionality of the HP OpenView Network Node Manager, which is an embedded part of OVO.	Hardcopy PDF
OVO Database Tuning	This ASCII file is located on the OVO management server at the following location: `/opt/OV/ReleaseNotes/opc_db.tuning`	ASCII

Additional OVO-related Products

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

Table 3 Additional OVO-related Manuals

Manual	Description	Media
HP OpenView Operations for UNIX Developer's Toolkit If you purchase the HP OpenView Operations for UNIX Developer's Toolkit, you receive the full OVO documentation set, as well as the following manuals:		
OVO Application Integration Guide	Suggests several ways in which external applications can be integrated into OVO.	Hardcopy PDF
OVO Developer's Reference	Provides an overview of all the available application programming interfaces (APIs).	Hardcopy PDF
HP OpenView Event Correlation Designer for NNM and OVO If you purchase HP OpenView Event Correlation Designer for NNM and OVO, you receive the following additional documentation. Note that HP OpenView Event Correlation Composer is an integral part of NNM and OVO. OV Composer usage in the OVO context is described in the OS-SPI documentation.		
HP OpenView ECS Configuring Circuits for NNM and OVO	Explains how to use the ECS Designer product in the NNM and OVO environments.	Hardcopy PDF

OVO Online Information

The following information is available online.

Table 4 OVO Online Information

Online Information	Description
HP OpenView Operations Administrator's Guide to Online Information	Context-sensitive help system contains detailed help for each window of the OVO administrator Motif GUI, as well as step-by-step instructions for performing administrative tasks.
HP OpenView Operations Operator's Guide to Online Information	Context-sensitive help system contains detailed help for each window of the OVO operator Motif GUI, as well as step-by-step instructions for operator tasks.
HP OpenView Operations Java GUI Online Information	HTML-based help system for the OVO Java-based operator GUI and Service Navigator. This help system contains detailed information about general OVO and Service Navigator concepts and tasks for OVO operators, as well as reference and troubleshooting information.
HP OpenView Operations Man Pages	Manual pages available online for OVO. These manual pages are also available in HTML format. To access these pages, go to the following location (URL) with your web browser: `http://<management_server>:3443/ITO_MAN` In this URL, the variable <*management_server*> is the fully-qualified hostname of your management server. Note that the man pages for the OVO HTTPS-agent are installed on each managed node.

About OVO Online Help

This preface describes online documentation for the HP OpenView Operations (OVO) Motif and the Java operator graphical user interfaces (GUIs).

Online Help for the Motif GUI

Online information for the HP OpenView Operations (OVO) Motif graphical user interface (GUI) consists of two separate volumes, one for operators and one for administrators. In the operator's volume you will find the HP OpenView OVO Quick Start, describing the main operator windows.

Types of Online Help

The operator and administrator volumes include the following types of online help:

- **Task Information**

  Information you need to perform tasks, whether you are an operator or an administrator.

- **Icon Information**

  Popup menus and reference information about OVO icons. You access this information with a right-click of your mouse button.

- **Error Information**

  Information about errors displayed in the `OVO Error Information` window. You can access context-sensitive help when an error occurs. Or you can use the number provided in an error message to perform a keyword search within the help system.

- **Search Utility**

  Index search utility that takes you directly to topics by name.

- **Glossary**

  Glossary of OVO terminology.

- **Help Instructions**

Instructions about the online help system itself for new users.

- **Printing Facility**

  Printing facility, which enables you to print any or all topics in the help system. (An HP LaserJet printer or a compatible printer device is required to print graphics.)

To Access Online Help

You can access the help system in any of the following ways:

- **F1 Key**

  Press **F1** while the cursor is in any active text field or on any active button.

- **Help Button**

  Click `[Help]` at the bottom of any window.

- **Help Menu**

  Open the drop-down `Help` menu from the menu bar.

- **Right Mouse Click**

  Click a symbol, then right-click the mouse button to access the `Help` menu.

You can then select task lists, which are arranged by activity, or window and field lists. You can access any topic in the help volume from every help screen. Hyperlinks provide related information on other help topics.

You can also access context-sensitive help in the `Message Browser` and `Message Source Templates` window. After selecting `Help: On Context` from the menu, the cursor changes into a question mark, which you can then position over the area about which you want help. When you click the mouse button, the corresponding help page is displayed in its help window.

Online Help for the Java GUI and Service Navigator

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

Types of Online Help

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

- **Tasks**

  Step-by-step instructions.

- **Concepts**

  Introduction to the key concepts and features.

- **References**

  Detailed information about the product.

- **Troubleshooting**

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

- **Index**

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

Viewing a Topic

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

Accessing the Online Help

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

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

1 About AIX Managed Nodes

In this Chapter

This chapter explains how to install and configure HP OpenView Operations (OVO) on IBM AIX managed nodes.

Installation Requirements

This section explains OVO hardware and software requirements for AIX managed nodes.

Hardware Requirements

Before installing OVO, make sure the AIX managed nodes meet the following hardware requirements:

- **Disk Space**

  60 MB (about 120 MB is required during software installation)

- **Additional Swap Space**

  None

- **Additional RAM**

  None

Software Requirements

Before installing OVO, make sure the following software is installed on AIX managed nodes:

- **Operating System**

  For the supported operating system versions, see the *OVO Installation Guide for the Management Server*.

- **System Parameters**

  For a list of kernel parameters, see the *OVO Administrator's Reference*. You can verify and change system parameters with the System Management Interface Tool (`SMIT`) tool.

- **Communication Software**

  OVO supports the NCS RPC and DCE RPC communication types. For details, see "Requirements for NCS RPC on AIX Managed Nodes" on page 36 and "Requirements for DCE RPC on AIX Managed Nodes" on page 36.

- **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.

- **Additional Packages**

  The following packages are required in addition to the basic operating system package (`bos.rte`):

  - *All versions of AIX*

    `xlC.rte` version 4.0.2.0 or higher

    C Set ++ for AIX Application Runtime.

  - *Additional filesets*

    `bos.perf.libperfstat`

    Performance Statistics Library Interface

    version 4.3.3.4 for AIX 4.3.3

    version 5.1.0.52 for AIX 5.1

    version 5.2.0.12 for AIX 5.2

    `bos.perf.perfstat`

    Performance Statistics Interface

    version 4.3.3.1 for AIX 4.3.3

    version 5.1.0.51 for AIX 5.1

    version 5.2.0.12 for AIX 5.2

  - *AIX version 4.3.x only*

    `xlC.aix43.rte` version 4.0.2.1 or higher

    C Set ++ for AIX Application Runtime. Lowest version required on all 4.3.x versions.

  - *For Monitor Agent terminations*

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

- bos.rte.libc version 4.3.1.0

  COMMITTED libc Library

- bos.rte.libpthreads version 4.3.1.0

  COMMITTED pthreads Library

- ML-03 (for AIX 5.x)

  Maintenance level 03

The packages can be downloaded from IBM's Fix Central at http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp:

To download, first, select a Server ("pSeries, RS/6000") on the Fix Central main page, then select a Product or fix type ("AIX OS, Java, compilers"), select an Option ("Specific fixes"), and OS level (version of AIX). Then click Continue. On the Select fixes page, select "Fileset or PTF number" from the Search by drop-down list, and enter a search string (3 characters minimum) in the Search string field. Click Go.

❑ **Required Patches**

The following patches are required for AIX 4.3.1 managed nodes:

- bos.up version 4.3.1.1

  Base Operating System Uniprocessor Runtime

  PTF: U455996

- bos.mp version 4.3.1.1

  Base Operating System Multiprocessor Runtime

  PTF: U453884

The patches can be downloaded from IBM's AIX Fix Distribution Service at http://techsupport.services.ibm.com/rs6k/fixdb.html. (Select the PTF number (4 character minimum) search option.)

Requirements for NCS RPC on AIX Managed Nodes

If you choose NCS RPC as the default communication type, you must install the NCS Runtime package `bos.net.ncs`.

You can verify and install NCS with the following commands:

`lslpp -l <`*`package`*`>`

`installp -s <`*`package`*`>`

Requirements for DCE RPC on AIX Managed Nodes

If you choose DCE RPC as the default communication type, you must install the following software:

- **DCE on AIX**

  DCE is supplied with the AIX operating system up to version 4.2.x. With the version 4.3 or newer, DCE is a standalone product and has to be purchased 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
  ```

Installing and De-installing Agents

This section describes how to install and de-install AIX managed nodes.

Methods for Installing Agents

After you have configured and set up DCE, you can install the AIX agent automatically or manually:

- **Automatically**

  See “Installing Agents Automatically” on page 42.

- **Manually**

  See “Installing Agents Manually” on page 42.

Tips for Installing Agents

NOTE For installation tips for AIX managed nodes running HACMP, see “Installing Agents in HACMP” on page 46.

When installing AIX managed nodes, follow these guidelines:

- **Management Server**

  The name of the management server must be known to the managed node. That is, the name of the management server must be registered on the name server or in the local host table:

  `/etc/hosts`

  You can verify this registration with the `nslookup` command.

- **Secure TCP/IP**

  If `securetcpip` is enabled, verify that at least `rshd` or `ftpd` is available.

- **Security Limits**

  Verify that the security limits match your requirements:

  `/etc/security/limits`

  The `default`, `root`, and `opc_op` entries are especially important in this regard.

- **OVO Agent Software**

  The OVO agent software is installed on the following file tree:

  `/usr/lpp`

  If the file system that hosts the file tree is too small to install OVO agents, create a symbolic link before installing OVO.

  For example, if `/bigdisk` is a local file system with enough free space to install the OVO agents, enter the following:

  ```
  mkdir -p /bigdisk/OV
  ```

  ```
  ln -s /bigdisk/OV /usr/lpp/OV
  ```

  Or mount a dedicated volume.

  For example, enter the following:

  ```
  mount /dev/hd4 /usr/lpp/OV
  ```

  In a cluster environment, verify that the local file system is also accessible from all cluster clients, and that it is mounted from all client nodes. For example, the local file system `/bigdisk` on the cluster client must be mounted to the exported file system `/bigdisk` on the cluster server.

- **AIX Diskless Nodes**

  You may initially create AIX diskless nodes so the root password is not required. You can log into these systems remotely, but you cannot execute commands with `remsh` because `.rhosts` is initially not present on the diskless client. Also, you cannot FTP to this type of node because the root password is empty. As a result, you cannot install OVO automatically on a diskless node before you set up the root password or set up the `.rhosts` file properly.

NOTE

Initially, the `/etc/hosts` file on the diskless node does not include the OVO management server.

❑ **Installation on NIS Clients**

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

Configuring DCE

You can configure a minimal or full DCE environment.

To Configure a Minimal DCE Environment

A *minimal* DCE environment does not have DCE cells or a DCE security server.

To configure a minimal DCE environment for the OVO agents, enter the following:

```
mkdce -o local -n ito rpc
```

To Configure a Full DCE Environment (RPC Only)

A *full* DCE environment has DCE cells and a DCE security server.

To configure a DCE client, you must have configured the Master Security server and CDS server beforehand. For more details on how to configure a full DCE environment, refer to:

`http://www-3.ibm.com/software/network/dce/library/\`
`publications/`

To configure a DCE client on the OVO agents, follow these steps:

1. Open a terminal window on the AIX managed node and enter the following:

   `smit dce`

   and

   Select `Configure DCE/DFS: Configure DCE/DCS Clients -> full configuration for this machine` in the SMIT window.

2. Enter the following information in the corresponding text entry fields:

   `CELL name` Enter the name of the cell in which the server was configured (for example, **`ito`**).

   `CLIENTS to configure` Use the `[List]` button to select the clients that you want to configure. The exact client list depends on whether a CDS or DTS server is used.

   `MASTER SECURITY Server` Enter the name of the system that is configured as the master security server.

`CDS Server` Enter the name of the system that is configured as the initial CDS server (if not in the same network).

`Cell ADMINISTRATOR's account` Enter the name of the privileged user, specified during the initial configuration of the DCE server (for example, **`cell_admin`**).

`LAN profile` Enter the name of the LAN (for example, **`/.../ito/lan-profile`**).

`Machine's DCE HOSTNAME` Enter the hostname of system where configuration is to be performed.

3. Click `[OK]`.

   This command configures the managed nodes as DCE clients and starts the DCE daemon `dced`.

To Remove an Existing DCE Configuration

To remove an existing DCE configuration, use the `Unconfigure DCE/DFS` option from the `SMIT` window.

Tips for Configuring DCE on AIX

When installing DCE on AIX managed node, follow these guidelines:

- **Starting DCED Daemon**

  Even though the `rpcd` daemon does not exist on AIX 4.x, the System Management Interface Tool (`SMIT`) utility erroneously tries to run it in the option `Restart RPC Daemons in the local machine`.

  Start the `dced` daemon instead, using the script `/etc/rc.dce` or the `SMIT` option `Restart the DCE/DFS Daemons`.

Installing Agents Automatically

To find out how to install the AIX agent automatically, see the *OVO Administrator's Reference*.

If errors occur during the installation, check the local installation logfile:

```
/tmp/installp.log
```

Installing Agents Manually

In some situations, you may want to install the AIX agent software without using the management server. If you install the AIX agent software manually, you can prepare the system to become an OVO managed node when it is later connected to the network. This preparation is useful if you are preparing many systems in a central location, or if you want to avoid the root connection over the network that is necessary for a standard agent installation.

To Install the AIX Agent on the Managed Node

To install the OVO AIX agent on an AIX system that will become an OVO managed node, follow these steps:

1. **Copy the OVO agent packages and installation script to a temporary directory on the managed node.**

   On the management server, these are the following files:

   - `opc_pkg.Z`
   - `comm_pkg.Z`
   - `perf_pkg.Z`
   - `opc_inst`

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

   ```
   /var/opt/OV/share/databases/OpC/mgd_node/vendor/ibm/\
   rs6000/aix/A.08.10/RPC_[NCS|DCE_[TCP|UDP]]/
   ```

2. **Install the Agent.**

   a. Change the permissions of the agent installation script to ensure that it can be executed:

      ```
      chmod +x /tmp/opc_inst
      ```

b. Start the agent installation script by entering:

```
/tmp/opc_inst
```

To Activate the AIX Managed Node from the Command Line

To activate the agent on the AIX managed node from the command line, follow these steps:

1. Add the pre-installed nodes to the `OVO Node Bank` window.

   Use the menu sequence `Actions:Node->Add`.

2. Add the node to an OVO node group.

   Drag and drop the node onto a node group in the `OVO Node Group Bank` window.

3. Install the agent on the AIX managed node manually.

   For instructions, see “Installing Agents Manually” on page 42.

4. Enter the following:

   ```
   /usr/lpp/OV/bin/OpC/install/opcactivate -s\
   <OVO_mgt_server> -cs <server_codeset> -cn <agent_codeset>
   ```

   This command activates the agent, which then attempts to send messages to the management server.

   - Specifying the `-s` option with the `opcactivate` command is optional. This option starts the `/opt/OV/bin/OpC/install/upd_res.sh` script which integrates the OVO agent into the system startup and shutdown scripts, for example the `/etc/init.d` file.
   - `-cs <server_codeset>` is the character set for the OVO management server.
     `-cn <agent codeset>` is the character set for this agent.

     For more information about codesets, see the *OVO Administrator’s Reference* and the man page *opcactivate(1M)*.

NOTE

Use the `opcactivate` command with the `-mode` option to activate `hacmp` for OVO agents on AIX HACMP systems. For more information about AIX HACMP, see “Installation Requirements for AIX HACMP Agents” on page 48, as well as the man page *opcactivate(1m)*.

5. After the node is connected to the network, enter the following command on the management server:

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

   This command updates the database and starts heartbeat polling for the node. You must still install the templates, monitors, commands, and actions from the OVO administrator GUI.

To Activate the AIX Managed Node from the OVO GUI

After you have connected the AIX managed node with the pre-installed agent to the network, you can activate and register the managed node.

To activate the AIX managed node from the OVO GUI, follow these steps:

1. Add the pre-installed nodes to the `OVO Node Bank` window.

   Use the menu sequence `Actions:Node->Add...`.

2. Add the node to an OVO node group.

   Drag and drop the node onto a node group in the `OVO Node Group Bank` window.

3. Distribute the OVO configuration to the node:

   a. From the menu bar of the `OVO Node Bank` window, select `Actions:Agents->Install`.

      The `Install /Update OVO Software and Configuration` window opens.

   b. Select all components and click `[OK]`.

CAUTION

Do not check `[Force Update]`. If you check this option, the management server re-installs the agent.

If the agent is pre-installed on the node, the management server activates the node and installs the selected components.

NOTE

If the agent software is *not* pre-installed, the management server installs the agent.

4. To verify that the Control, Message, and Action Agents are all running on the managed node, enter the following:

   `/usr/lpp/OV/bin/OpC/opcragt -status <node>`

Installing Agents in HACMP

This section includes important information about installing OVO agents on nodes running HACMP.

TIP For general installation tips for AIX managed nodes, see “Tips for Installing Agents” on page 37.

About OVO Agents in HACMP

Each node in an HACMP cluster has its own OVO agent. And each node must be accessible on a fixed IP address, which represents the node in the `OVO Node Bank`. This IP address is always bound to the same node. As a result, IP addresses that are subject to change cannot be used to install and run an OVO agent running on HACMP system.

About IP Aliases in HACMP

If an additional adapter (that is, a network interface card) with a fixed IP address that is *not* used by HACMP (as a boot, service, or standby adapter) is available on an HACMP node, you can use this adapter for OVO agent installation. Communication with the OVO server *must* be possible through this additional adapter. If you use the adapter for OVO installation, you do not need to set up IP aliases or modify shell scripts. Equally important, you can skip all pre-installation tasks. Nevertheless, you may not change the IP address on this adapter.

If no such adapter is available, you should assign each node an IP alias in the same network in which the boot and service IP addresses reside. In addition, you must configure the node in such a way that this IP alias address is assigned to the service adapter as an alias for the boot IP address. Once a fixed IP address or an IP alias is available on a node, that address must be used to install the OVO agent on the node.

After successful installation of the OVO agent, the IP alias is present in the in the field `OPC_IP_ADDRESS` of the following file:

```
/var/lpp/OV/conf/OpC/nodeinfo
```

Naming Scheme for IP Addresses in HACMP

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

- **IP Addresses**

  Other IP addresses that may be set on the interface.

- **Messages**

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

Use the following naming scheme in your HACMP environment:

`<nodename>_boot`

Boot address of a node

`<nodename>_svc`

Service address of a node

`<nodename>_stdby`

Standby address of a node

`<nodename>_ito`

IP alias of a node

In this naming scheme, *<nodename>* is the name of the node as defined in the HACMP configuration.

NOTE The status icon for the node in `Node Bank` window does not change color immediately if the node in the HACMP cluster goes down. The icon changes color only after OVO has determined that it cannot contact the control agent on that node.

Installation Requirements for AIX HACMP Agents

OVO supports the following software versions for AIX HACMP agents:

- ❏ AIX 4.3 (for NCS and DCE agents)
- ❏ HACMP 4.2.2, 4.3.1, 4.4.1, 4.5 and 5.1

NOTE

HACMP version 4.5 supports "persistent adapters".This feature enables you to avoid the configuration of IP alias, therefore the following sections can be safely ignored when using HACMP version 4.5:

- “To Set an IP Alias for AIX HACMP Agents on AIX” on page 48.
- “Fixing Problems with IP Aliases on AIX” on page 49.
- “To Reset the IP Alias on the network interface card” on page 50.
- “To Reset Events on HACMP 4.2.2” on page 51.
- “To Reset Events on HACMP 4.3.1 and 4.4.1” on page 51.

To Set an IP Alias for AIX HACMP Agents on AIX

Before installing AIX HACMP agents, you *must* set an IP alias used by the OVO agents during and after installation on each node on which you want to run the OVO agent.

To set an IP alias for AIX HACMP agents on AIX, follow these steps:

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

   `smit tcpip`

3. Select the following from the menu bar:

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

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

Fixing Problems with IP Aliases on AIX

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

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

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

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

NOTE

For managed nodes where AIX operating system fixes have already been installed, refer to "To Reset Events on HACMP 4.2.2" on page 51.

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

`IX78397`

2. **Reset IP aliases on the network interface card.**

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

   For instructions, see "To Reset the IP Alias on the network interface card" on page 50.

NOTE

You have to reset the IP alias on all cluster nodes where the OVO agent is to be installed.

To Reset the IP Alias on the network interface card

To reset the IP alias on the interface where the service or boot IP address is set, use the following shell script:

```
#!/bin/sh
# Specify ito alias IP address below
ALIAS_IP="0.0.0.0"
SERVICE_IP=`/usr/sbin/cluster/utilities/cllsif -cSi \
  $LOCALNODENAME | grep ":service:.*:ether" | cut -d: -f7 |\
uniq`
BOOT_IP=`/usr/sbin/cluster/utilities/cllsif -cSi \
$LOCALNODENAME |\
  grep ":boot:.*:ether" | cut -d: -f7 | uniq`
INTERFACE=`/usr/sbin/cluster/utilities/clgetif -a
$SERVICE_IP`
if [ $? -ne 0 ]; then
  INTERFACE=`/usr/sbin/cluster/utilities/clgetif -a
$BOOT_IP`
fi
if [ "$INTERFACE" != "" ]; then
  #IP has changed, set IP alias again on interface with
SERVICE_IP
  /usr/sbin/ifconfig $INTERFACE $ALIAS_IP alias
fi
```

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

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

- ❏ Acquire service address
- ❏ Release service address
- ❏ Swap adapter

To Reset Events on HACMP 4.2.2

To reset events on HACMP 4.2.2, follow these steps:

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

   smit hacmp

2. Select the following:

   Cluster Configuration -> Cluster

   Resources -> Change/Show Cluster Events

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

   You can put the shell script in the following directory:

   /usr/sbin/cluster/local

To Reset Events on HACMP 4.3.1 and 4.4.1

To reset events on HACMP 4.3.1 and 4.4.1, follow these steps:

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

   smit hacmp

2. Go into the Cluster Events menu by selecting the following:

   Cluster Configuration -> Cluster Resources -> Cluster Events

3. Add the set_alias script to the Known Cluster Events list by:

   a. Selecting the following:

      Define Custom Cluster Events -> Add a Custom Cluster Event

   b. Setting the following:

      Cluster Event Name Set to set_alias

      Cluster Event Description Set to OVO set_alias

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

   c. Then click [OK].

4. Assign it to events.

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

5. Select an option and enter `set_alias` in the `Post-event Command` field for each event:

   - `acquire service address`
   - `release service address`
   - `swap adapter`

To Install AIX HACMP Agents

To install AIX HACMP agents, follow the procedure in "To Install the AIX Agent on the Managed Node" on page 42, with the following exceptions:

❑ **IP Alias Address**

You must use the IP alias address as the IP address for the host on which you want to install the OVO agent.

❑ **IP Address**

If the IP address used for the OVO installation is tied to the boot, service, or standby interfaces, the installation script issues a warning. The installation continues nonetheless.

❑ **OVO Agent Startup**

If you select automatic startup for OVO agents, the file `/etc/inittab` is also updated so the `clinit` entry remains the last item, as required by HACMP.

❑ **NCS Communication Type**

If you want to use the NCS communication type, you must start the `llbd` and OVO agents at boot time, when boot IP address is still available. First start the `llbd` process, and then the OVO agent, using the order in the file `/etc/inittab`. If agent is to be restarted, RPC registration will fail, due to a flaw in `llbd`.

- **Node Information**

  After you have successfully installed the OVO agent, the IP alias is added to the `OPC_IP_ADDRESS` field of the following file:

  `/var/lpp/OV/conf/OpC/nodeinfo`

- **Hostname**

  The following line is added to the `opcinfo` file during the installation process:

  `OPC_NAMESRV_LOCAL_NAME <hostname>`

  In this instance, *<hostname>* is the name of the host configured with the IP address you used to install the OVO agent. If this IP address changes, change this line of the `opcinfo` file accordingly.

De-installing Agents

This section describes how to de-install AIX managed nodes.

De-installing Agents Automatically

For general de-installation instructions, see the *OVO Administrator's Reference*. There is no special de-installation logfile available for AIX managed nodes.

To De-install OVO Manually

To manually de-install OVO software from AIX managed nodes, following these steps:

1. Stop all OVO agents running on the managed node.
2. To de-install the OVO agent software from AIX managed nodes, enter the following:

   ```
   installp -ug OPC OPCCOMM OPCPERF
   ```

NOTE If you are de-installing an older version of the agent, use: `installp -ug OPC`.

To Remove Older Agents

If you no longer need older OVO agent packages, and if the agent packages are not installed on any managed node, you can remove them.

To remove older OVO agent software, enter the following:

```
/opt/OV/bin/OpC/install/rm_opc.sh ibm/rs6000/aix \
<OVO_version>
```

In this command, *<OVO_version>* is the version of OVO that supports this agent platform (for example, `A.08.10`).

About Preconfigured Elements

This section describes preconfigured templates, template groups, and applications used by OVO on AIX managed nodes.

NOTE Default message templates and logfile templates can be installed with OS-SPI.

Support for SNMP Event Interception

OVO supports the SNMP event interceptor on the following version of AIX:

- ❏ AIX 4.3 (direct port access mode)

NOTE Local event interception is supported only with Network Node Manager (NNM) version 6.2.

Types of Default Applications

For a list of default applications available for UNIX managed nodes, see the *OVO Administrator's Reference*.

Starting the SMIT User Interface

You can use OVO to start the System Management Interface Tool (`SMIT`) user interface on AIX systems:

Command issued:	`smit`
Default user:	`root`
Default password:	None required. The application is started through the OVO action agent.

NOTE If the default user has been changed by the operator, you must supply a password.

Distributing Scripts and Programs

For AIX managed nodes, the platform selector and architecture identifier is the following:

```
ibm/rs6000/aix
```

Location of User Scripts and Programs

Table 1-1 shows the location of user scripts and programs provided on the management server.

Table 1-1 Location of User Scripts and Programs on the Management Server

Script/Program	Location
Automatic actions, operator-initiated actions, and scheduled actions	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /ibm/rs6000/aix/actions/*`
Monitoring scripts and programs used by the monitoring agent and logfile encapsulator	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /ibm/rs6000/aix/monitor/*`
Scripts and programs called through command broadcast or started from the Application Desktop	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /ibm/rs6000/aix/cmds/*`

About Temporary Directories

Table 1-2 shows the temporary directories for distributed scripts and programs on the managed nodes.

Table 1-2 Temporary Directories for Distributed Scripts and Programs on the Managed Nodes

Managed Node	Operating System	Temporary Directory

IBM RS/6000, Bull DPX/20	AIX	`/var/lpp/OV/tmp/OpC/bin/actions`
		`/var/lpp/OV/tmp/OpC/bin/cmds`
		`/var/lpp/OV/tmp/OpC/bin/monitor`

About Target Directories

Table 1-3 shows the target directories for distributed scripts and programs on the managed nodes.

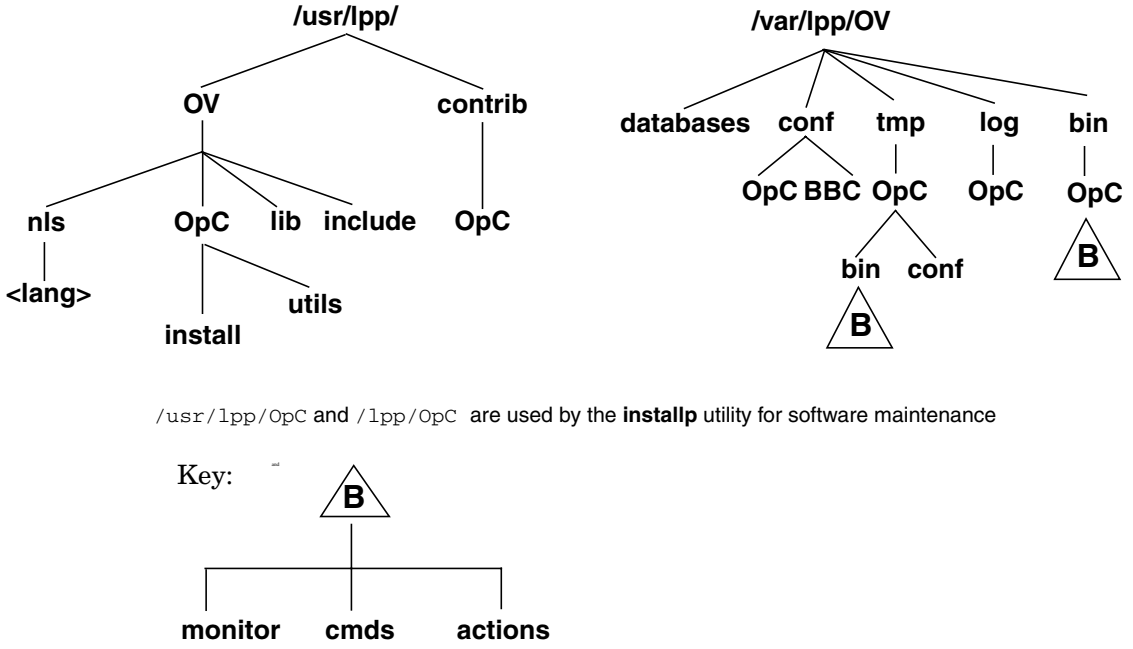
Table 1-3 Target Directories for Distributed Scripts and Programs on the Managed Nodes

Managed Node	Operating System	Target Directory	Access Rights
IBM RS/6000, Bull DPX/20	AIX	`/var/lpp/OV/OpC/actions`	`rwxr-xr-x` (owner: root)
		`/var/lpp/OV/OpC/cmds`	`rwxr-xr-x` (owner: root)
		`/var/lpp/OV/OpC/monitor`	`rwxr-xr-x` (owner: root)

Organization of Managed Nodes

Figure 1-1 shows how OVO software is organized on AIX managed nodes.

Figure 1-1 OVO Software on AIX Managed Nodes



Location of Files

On AIX managed nodes, files are located as follows:

- **Process-related Files**

  `/var/lpp/OV/tmp/OpC`

- **Agent Configuration Files**

  `/var/lpp/OV/conf/OpC`

About the Default OVO Operator

The default OVO operator, `opc_op`, owns `/home/opc_op` as home directory. By default, the operators use the Korn Shell (`/bin/ksh`) and are not allowed to log into the system directly (that is, enter * in `/etc/passwd`).

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

About System Resources

OVO applies changes in the following system resource files:

`/etc/passwd`
`/etc/security/passwd` Default OVO operator.

`/etc/group`
`/etc/security/group` Default OVO operator group.

`/etc/inittab`	OVO agent startup. Used only if the `Automatic Update of System Resource Files` option has been set.
`/etc/rc.opc`	OVO startup. Called by `/etc/inittab`.

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

Types of Libraries

Table 1-4 describes the managed node libraries for OVO A.05.xx, A.06.xx, and A.07.xx.

Table 1-4 Libraries for the OVO Managed Nodes

	Item	OVO A.05.xx	OVO A.06.xx	OVO A.07.xx
DCE	Library	**libopc_r.a**	**libopc_r.a**	**libopc_r.a**
	Libraries linked to the OVO library.	/usr/lpp/OV/lib/libnsp.a /usr/lib/libdce.a /usr/lib/libiconv.a	/usr/lpp/OV/lib/libnsp.a /usr/lpp/OV/lib/libopcas.a /usr/lib/libdce.a /usr/lib/libiconv.a	/usr/lpp/OV/lib/libnsp.a /usr/lpp/OV/lib/libopcas.a /usr/lib/libdce.a /usr/lib/libiconv.a /usr/lib/libdl.a /usr/lib/libc.a or /usr/ccs/lib/libc.a /usr/lib/libdcelibc_r.a /usr/lib/libdcepthreads.a /usr/lib/libpthreads_compat.a
	Link and compile options	-D_CMA_NOWRAPPERS_ -lopc_r -lpthreads -lc_r	-D_CMA_NOWRAPPERS_ -lopc_r -lpthreads -lc_r	-D_CMA_NOWRAPPERS_ -lopc_r -lpthreads -lc_r
	Description	Version 3.2 is obsolete with OVO A.05.x. **Note:** Only OVO A.04.xx integrations built on AIX 4.x with above options can be run on OVO A.05.xx.	N/A	N/A

Table 1-4 Libraries for the OVO Managed Nodes (Continued)

	Item	OVO A.05.xx	OVO A.06.xx	OVO A.07.xx
NCS	Library	**libopc.a**	**libopc.a**	**libopc.a**
	Libraries linked to the OVO library.	/usr/lpp/OV/lib/libnsp.a /usr/lib/libnck.a /usr/lib/iconv.a	/usr/lpp/OV/lib/libnsp.a /usr/lpp/OV/lib/libopcas.a /usr/lib/libnck.a /usr/lib/iconv.a	/usr/lpp/OV/lib/libnsp.a /usr/lpp/OV/lib/libopcas.a /usr/lib/libdl.a /usr/lib/libiconv.a /usr/lib/libc.a **or** /usr/ccs/lib/libc.a
	Link and compile options	-lopc	-lopc	-lopc
	Description	N/A	N/A	N/A

About the Include File

On IBM RS600 or Bull DPX/20 with AIX, the managed nodes use the following include file:

/usr/lpp/OV/include/opcapi.h

About the Makefile

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

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

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

- `Makef.aix`
- `Makef.aixncs`

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

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

About the Supplied Perl Interpreter

The managed node software includes a custom binary Perl 5.6.1 distribution.

The Perl is embedded in the Perl interpreter and the monitoring agent, and is designed to be used internally by OVO. Some OVO policies deployed by OpenView Operations for Windows management servers include Perl scripts (for example, some schedules and measurement threshold policies). Perl scripts are also used by some HP-supplied Smart Plug-ins (SPIs).

The Perl interpreter and other binaries are automatically installed into the `$OV_CONTRIB/perl` directory. A basic set of modules is installed in the /opt/OV/nonOV/perl/a/lib/5.6.1/File/ directory. Pre-existing Perl installations are not altered as a result of installing a managed node.

If you want to use the Perl distribution for additional purposes beyond its internal use within OVO, you should first check which modules are included by listing the `.pl` and `.pm` files within the `/opt/OV/nonOV/perl/a/lib/5.6.1/` directory.

For further information about Perl or if you need to add additional modules, go to the following web site:

`http://www.perl.com`

NOTE

Perl is supplied "as is" with no warranties whether express or implied according to the Perl artistic license agreement. Hewlett-Packard is not responsible for errors in Perl, which is public domain software and not produced by HP. Hewlett-Packard does not support any modifications to the provided Perl distribution. This software is licensed, not sold, and your use of the software is subject to the license terms contained in the license agreement."

2 About HP-UX Managed Nodes

In this Chapter

This chapter explains how to install and configure HP OpenView Operations (OVO) on HP-UX managed nodes.

Installation Requirements

This section explains OVO hardware and software requirements for HP-UX 11.x managed nodes.

Hardware Requirements for HP-UX 11.x

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

- **Disk Space**

  28 MB for HP-UX 11.0 and 11.11
  (about 56 MB is required during the software installation).

  47 MB for HP-UX 11.22
  (about 94 MB is required during the software installation).

- **Additional Swap Space**

  None

- **Additional RAM**

  None

NOTE Only IA64 managed nodes are supported for HP-UX 11.22.

Supported Agent Platforms

OVO supports the following platforms and operating systems on the managed nodes:

Table 2-1 OS Versions on HP-UX Managed Nodes Supported by OVO

Operating System	Platform	Supported OS Versions	Supported Communication Type [a]	Embedded Performance Component	SNMP Event Interception	Event Correlation 3.1	Manual Installation	SSH Installation Method
HP-UX	HP 9000 Technical Workstations	11.0, 11.11	DCE	✔	✔	3.1	✔	✔
	HP 9000 Enterprise Servers [b]	11.0, 11.11	DCE	✔	✔	3.1	✔	✔
	HP IA64 Workstations	11.22, 11.23	DCE	✔	✔	3.2	✔	✔
	HP IA64 Servers	11.22, 11.23	DCE	✔	✔	3.2	✔	✔

a. DCE is not included with the operating system for the following agent platforms:
Linux (supplied with the OVO agent software)
SINIX/Reliant (to be purchased separately at additional cost)
Solaris (supplied with the OVO agent software)
DCE is included with the operating system for all other platforms that support DCE (but may have to be installed separately as an optional product). Note that DCE is not included with AIX 4.3.3 and Tru64 UNIX 5.0A and has to be purchased separately.

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

Table 2-2 HP-UX OS Versions on Managed Nodes Supported by HP OpenView Performance Agent

Operating System	Platform	Supported OS Versions	Supported Communication Type [a]
HP-UX [b]	HP 9000 Technical Workstations	11.0, 11.11	DCE
	HP 9000 Enterprise Servers	11.0, 11.11	DCE
	HP IA64 Workstations	11.22	DCE
	HP IA64 Servers	11.22	DCE

a. For communications between HP OpenView Reporter or HP OpenView Performance Manager with HP HP OpenView Performance Agent.
b. Software is bundled with the OVO management server software.

Software Requirements for HP-UX 11.0 and 11.11

Before installing OVO, make sure the following software is installed on HP-UX 11.0 and 11.11 managed nodes:

❏ **Operating System**

For a list of operating system versions supported by OVO, see the *OVO Installation Guide for the Management Server*.

❏ **Operating System Patches**

- *HP-UX 11.0 Managed Nodes*

  QPK1100 . Quality Pack for HP-UX 11.0, September 2001, version B.11.00.54.7

- *HP-UX 11.11 Managed Nodes*

  GOLDBASE11i . Gold Base Patches for HP-UX 11.i, June 2003, version B.11.11.0306.4

  PHSS_26946. HP aC++ -AA runtime libraries (aCC A.03.37)

  PHSS_26560. ld(1) and linker tools cumulative patch

  PHSS_28568 s700_800 11.11 ONC/NFS General Release/Performance Patch

❏ **System Parameters**

For a list of kernel parameters, see the *OVO Administrator's Reference*. You can verify and change the system parameters using the `SAM` tool.

NOTE

If monitoring performance metrics with the embedded performance component, increase the value of the kernel parameter `max_thread_proc` to: min + (Number_of_Templates * 2).

- **DCE RPC**

  DCE RPC version 1.7 or higher.

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

NOTE

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

NOTE

Required for HP-UX 11.0 only.

DCE-KT-Tools, which is available on the HP-UX Application Software CD-ROMs, contains a runtime library for kernel threads that OVO requires to run. To install the product, 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`

Software Requirements for HP-UX 11.22

Before installing OVO, make sure the following software is installed on HP-UX 11.22 managed nodes:

- **Operating System**

  For a list of operating system versions supported by OVO, see the *OVO Installation Guide for the Management Server*.

- **System Parameters**

  For a list of kernel parameters, see the *OVO Administrator's Reference*. You can verify and change the system parameters using the `SAM` tool.

NOTE

If monitoring performance metrics with the embedded performance component, increase the value of the kernel parameter `max_thread_proc` to: min + (Number_of_Templates * 2).

- **DCE RPC**

  DCE RPC version 1.7 or higher, part of in HPUXBaseOS.DCE-CORE.DCE-CORE-RUN

- **Internet Services**

  SD package: `InternetSrvcs.INETSRVCS-RUN`

- **LAN/9000**

  SD package: `Networking.NET-RUN`

- **Native Language Support (NLS) Package**

  SD package: OS-Core.NLS-AUX

OVO File Tree on the Management Server

The layout of the 11.x file system conforms to the standard structure of UNIX System V Release 4 (SVR4).

The major OVO directories contain the following:

`/opt/OV`.	All OVO binaries
`/etc/opt/OV`.	Configuration data
`/var/opt/OV`.	Run-time data

NOTE The file tree may include additional subdirectories if OVO agent software or other HP OpenView software is installed.

Figure 2-1 File Tree on the Management Server (/opt/OV Branch)

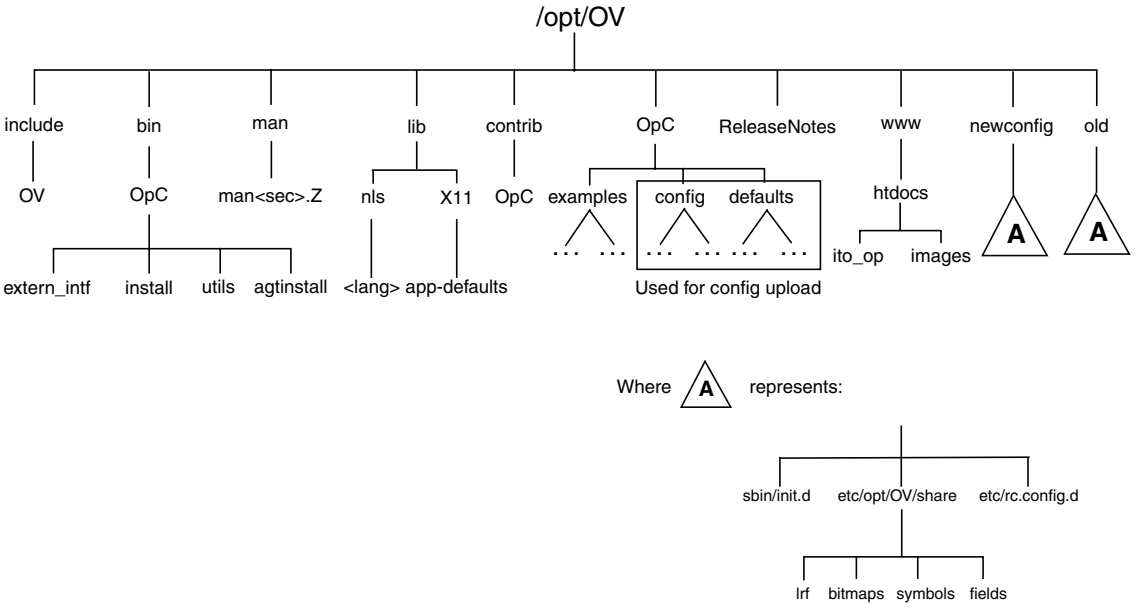


Figure 2-2 File Tree on the Management Server (/var/opt/OV Branch)

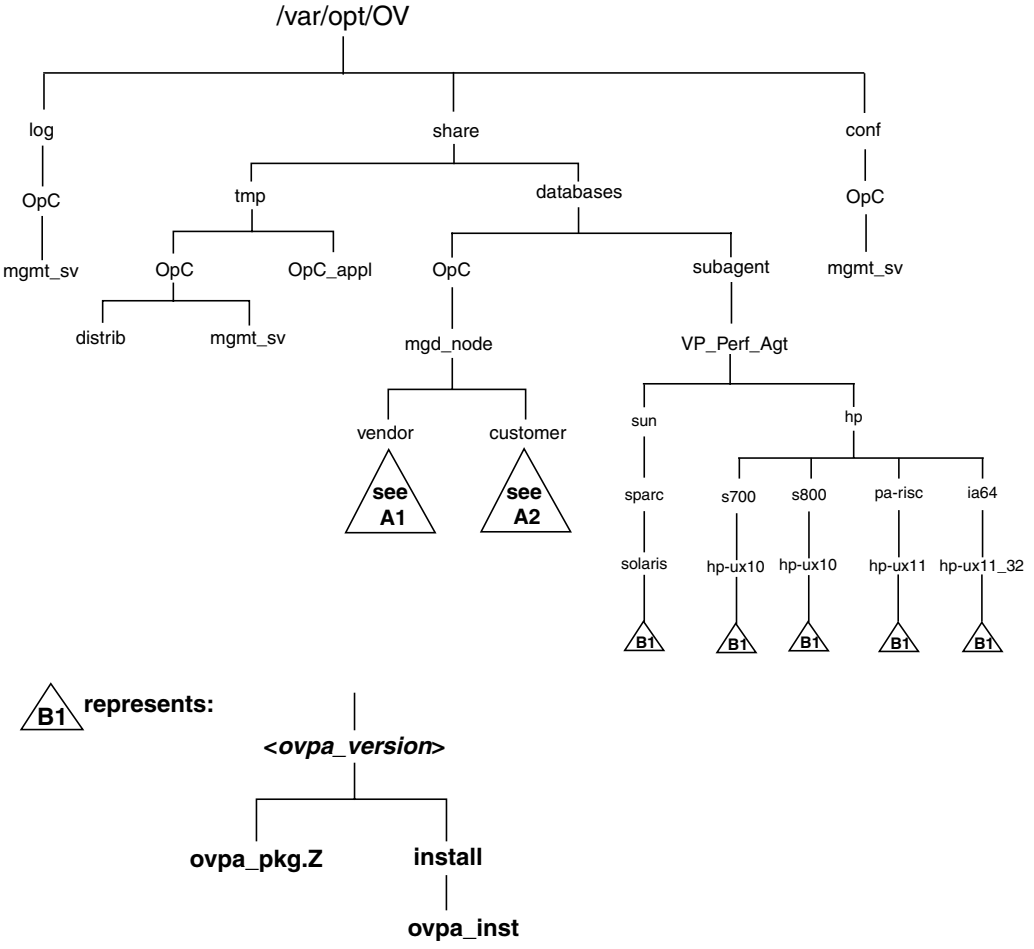
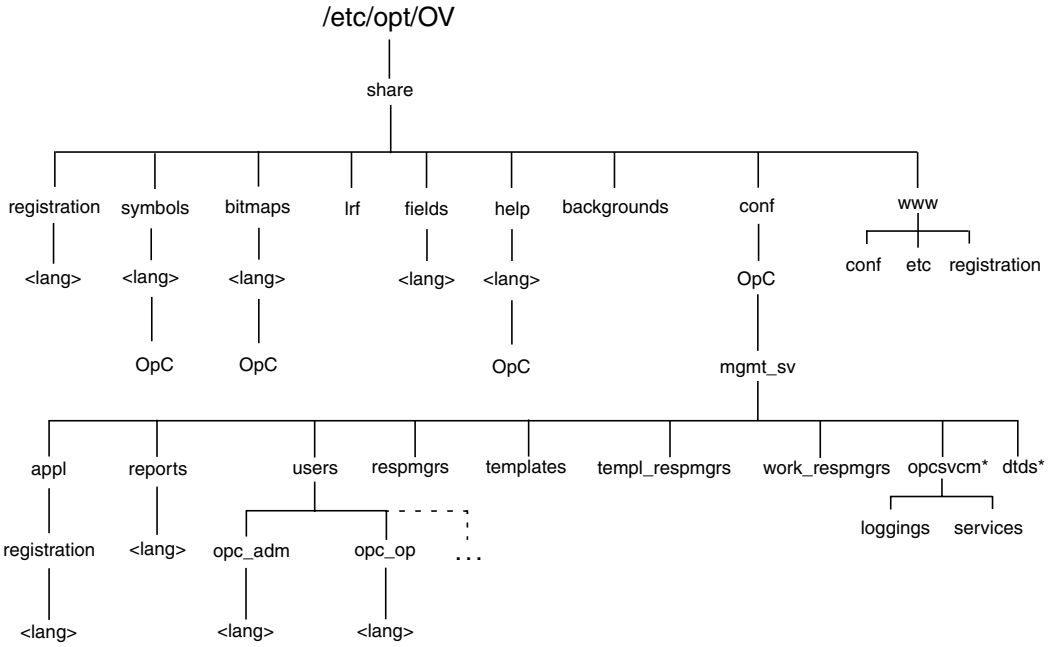
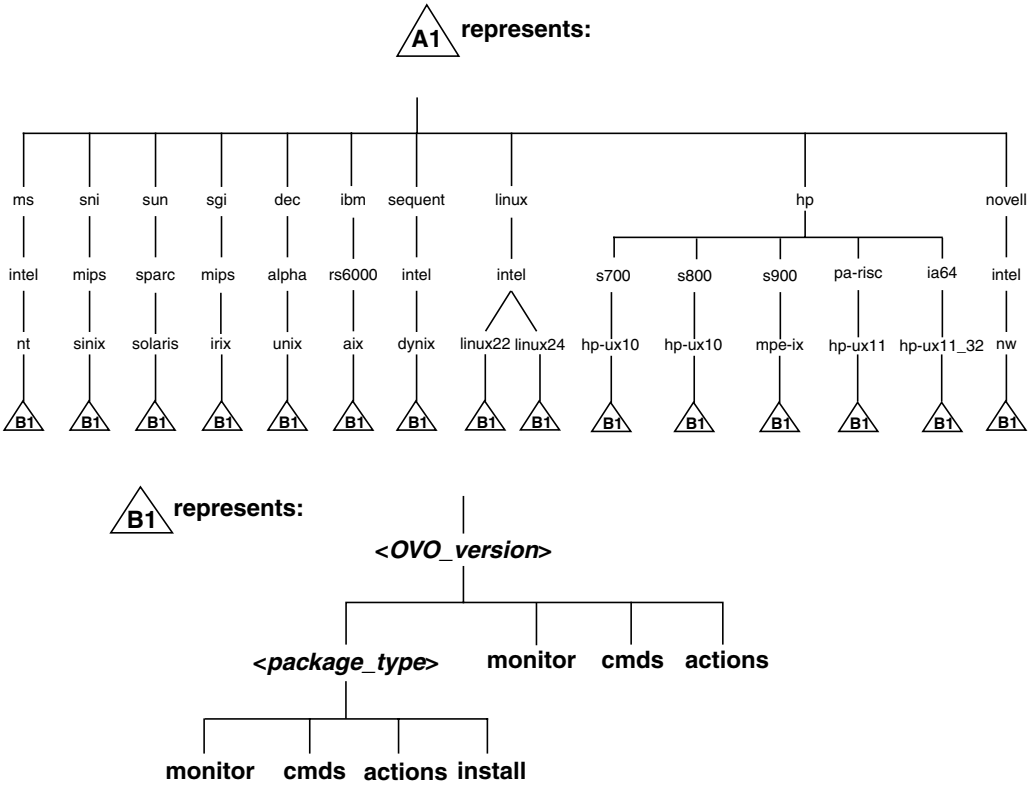


Figure 2-3 File Tree on the Management Server (/etc/opt/OV Branch)



* Only if HP OpenView Service Navigator is installed

Figure 2-4 Vendor-specific OVO Software Sub-tree on Management Server



Where:

<*OVO_version*>. Version of OVO that supports a particular agent platform (for example A.08.00).

OVO can manage several different OVO versions for each agent platform. For more information about OVO version management, see the *OVO DCE Agent Concepts and Configuration Guide*.

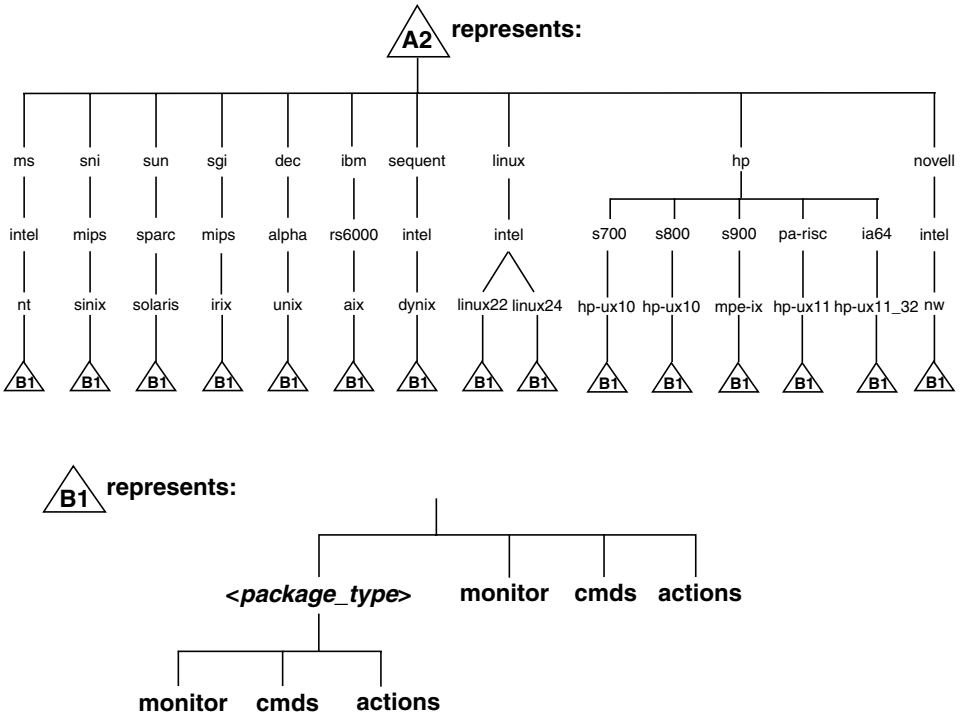
<*package_type*>. Communication type used by the remote procedure calls (RPC) of a particular agent platform, for example:

- RPC_NCS
- RPC_DCE_TCP
- RPC_DCE_UDP

NOTE When DCE managed nodes communicate with the management server over a fast network (LAN), choose DCE RPC (UDP) in preference to DCE RPC (TCP) as the communication protocol for the best performance.

The customer sub-tree is similar to the vendor sub-tree, without the OVO version. You can integrate your additional scripts, including individual scripts and binaries, in the **monitor**, **cmds** and **actions** subdirectories. These files are automatically distributed to the managed node by OVO.

Figure 2-5 Customer-specific OVO Software Sub-tree on Management Server



HP-UX Agent Filesets

Table 2-3 OVO **Generic HP-UX Agent Filesets in OVOPC-CLT**

<platform_selector>	Fileset	Description
hp/pa-risc/hp-ux11	OVOPC-UX11-CLT	Managed node functions for HP 9000 Technical Workstation or Enterprise Server systems running HP-UX 11.0 or 11.11 [a]
hp/ia64/hp-ux11_32	OVOPC-UXIA-CLT	Managed node functions for HP IA64 Technical Workstation or Enterprise Server systems running HP-UX 11.22 or 11.23

a. Never delete this agent platform on an HP-UX 11.x management server.

Table 2-4 **OVO English-only HP-UX Agent Filesets in OVOPC-CLT-ENG**

<platform_selector>	Fileset	Description
hp/s900/mpe-ix	OVOPC-MPE-CLT	Managed-node functions for systems running MPE/iX

For more information about the contents of these filesets, see the *OVO Installation Guide for the Management Server*.

HP-UX Agent Subproducts

Table 2-5 OVO English and Spanish Components in the Subproducts

OVO Product	Filesets in Product	Description of Fileset
OVOPC-CLT	OVOPC-AIX-CLT	Agent software for IBM RS/6000 systems running on AIX.
	OVOPC-LIN-CLT	Agent software for Intel-based PCs running Linux.
	OVOPC-NT-CLT	Agent software for Intel-based PCs running MS Windows NT/2000.
	OVOPC-OSF-CLT	Agent software for DEC Alpha systems running Tru64 UNIX.
	OVOPC-SOL-CLT	Agent software for Sun SPARC systems running Solaris
	OVOPC-UX10-CLT	Agent software for HP 9000 Series 700/800 systems running HP-UX 10.x
	OVOPC-UX11-CLT	Agent software for HP 9000 Series 700/800 systems running HP-UX 11.0 or 11.11
	OVOPC-UXIA-CLT	Agent software for HP IA64 systems running HP-UX 11.22
OVOPC-PA-CLT	OVPPC-PA-HP10	Deployable subagent, OpenView Performance Agent for HP-UX 10.20
	OVOPC-PA-HP11	Deployable subagent, OpenView Performance Agent for HP-UX 11.0 or 11.11
	OVOPC-PA-SOL	Deployable subagent, OpenView Performance Agent for Solaris
	OVOPC-PA-HPIA	Deployable subagent, OpenView Performance Agent for HP-UX 11.22

Installing and De-installing Agents

This section describes how to install and de-install HP-UX 11.x managed nodes.

Methods for Installing Agents

To install OVO agents on HP-UX managed nodes, use one of the following methods:

- **Standard Installation**

  See “Installing Agents with Standard Installation” on page 85.

- **SD-UX Installation**

  See “Installing Agents with SD-UX” on page 86.

- **Manual Installation**

  See “Installing Agents Manually” on page 90.

Tips for Installing Agents

When installing HP-UX managed nodes, follow these guidelines:

- **Manual Root Passwords**

  Make sure you know all the root passwords of all the managed nodes when you install the OVO agent software.

- **Automatic Root Passwords**

  On UNIX managed nodes, passwords are not required if an `.rhosts` entry for root has been made or if the management server is included in `/etc/hosts.equiv` (HP-UX 11.x).

- **Name of Management Server**

  The name of the management server must be known to the managed node. That is, the name of the management server must be registered on the name server or in the local host table:

  `/etc/hosts`.

  You can verify the name of the management server with the `nslookup` command.

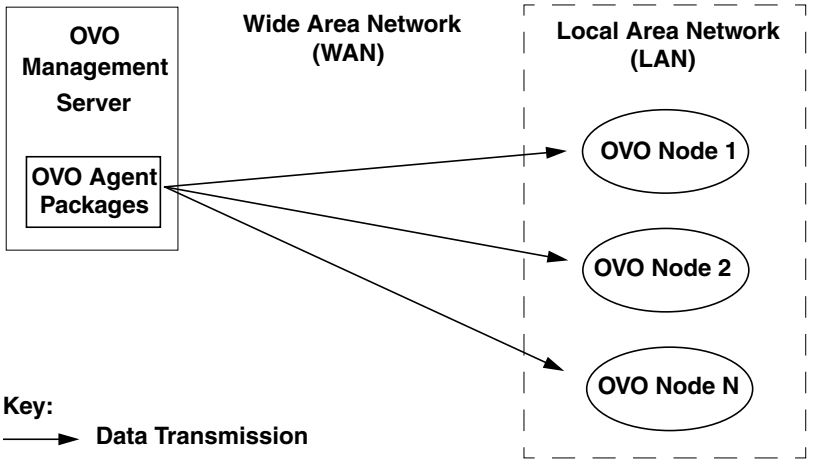
❑ **Installation on NIS Clients**

If the managed node is a Network Information Service (NIS or NIS+) client, you must add the OVO default operator `opc_op` as a member of the group `opcgrp` on the NIS server before installing the OVO software on a managed node. This ensures that the OVO default operator `opc_op` is used by OVO and is consistent on all systems. If you do not add the OVO default operator `opc_op` on the NIS server, the installation will create a user `opc_op` with the group `opcgrp` locally on the node.

Installing Agents with Standard Installation

Figure 2-6 shows the standard OVO installation method.

Figure 2-6 Standard OVO Agent Installation Method



For general administration instructions, see the *OVO Administrator's Reference*.

If errors occur during the installation, check the local installation logfiles:

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

`/var/adm/sw/swinstall.log`

Installing Agents with SD-UX

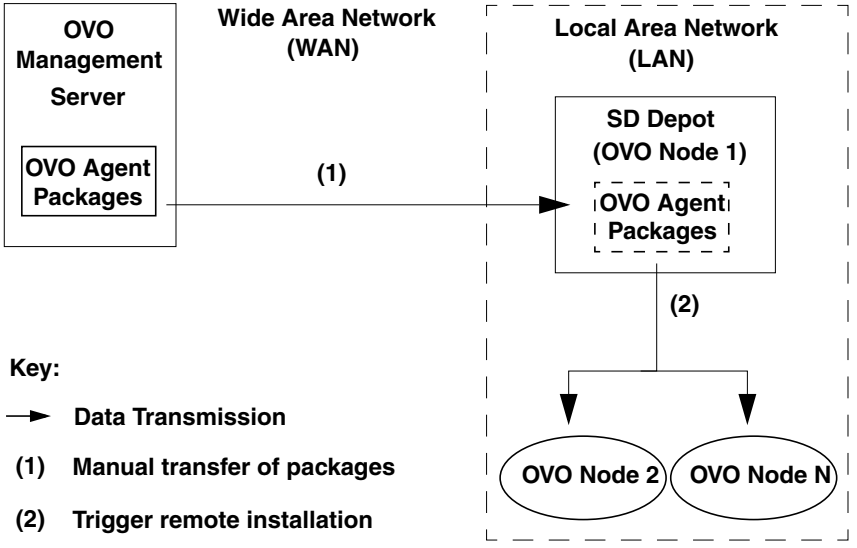
To save time and money, you can install OVO on HP-UX 11.x platforms using the advanced features of HP Software Distributor (HP SD-UX). You use this method to install the OVO agent software packages from a software depot on a node other than the OVO management server.

Installing Agents from a SD-UX Depot Node

Installing the OVO agent software packages from a software depot on a node other than the OVO management server is especially useful in an environment where a LAN of managed nodes is managed by a management server over a WAN. Instead of transferring “x” number of agent packages over the WAN line, the packages are installed once on a depot node in the remote LAN. Subsequent agent installations then get the packages from the local depot.

Figure 2-7 shows how to install OVO agents on HP-UX 11.x managed nodes with the HP Software Distributor (SD-UX) from a remote software depot.

Figure 2-7 HP SD-UX Remote Software Depot Installation Method



Creating a SD-UX Depot on a Remote Node

To create an HP-UX 11.x Software Distributor (SD-UX) depot for installing OVO managed nodes, follow these steps:

1. **Copy the OVO agent locally.**

   If you do not have additional SD-UX licenses for transferring the software to the managed node, copy the packages locally. If this is the case on the depot node, transfer the OVO software packages from the management server over the WAN to the depot node using FTP and register the depot.

   The OVO agent requires these software packages:

   - `opc_pkg.Z`
   - `comm_pkg.Z`
   - `perf_pkg.Z`

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

   - *HP-UX 11.0 and 11.11 managed nodes*

     ```
     /var/opt/OV/share/databases/OpC/mgd_node/vendor/hp/\
     pa-risc/hp-ux11/A.07.10/RPC_DCE_[TCP|UDP]/
     ```

   - *HP-UX IA64 11.22 managed nodes*

     ```
     /var/opt/OV/share/databases/OpC/mgd_node/vendor/hp/\
     ia64/hp-ux11_32/A.07.10/RPC_DCE_[TCP|UDP]/
     ```

2. **Create a temporary, uncompressed depot.**

   To get a *compressed* depot, you must first create a temporary, *uncompressed* depot.

   Copy the *uncompressed* packages into the `/tmp` directory and execute as follows:

   ```
   swcopy -d -s /tmp/opc_pkg -x source_type=tape -x \
   enforce_dependencies=false ITOAgent @ /depot1

   swcopy -d -s /tmp/comm_pkg -x source_type=tape -x \
   enforce_dependencies=false OVOPC-AGT @ /depot1

   swcopy -d -s /tmp/perf_pkg -x source_type=tape -x \
   enforce_dependencies=false OVOPC-AGT @ /depot1
   ```

   If the SD-UX depot does not exist, it is created automatically.

3. **Compress the depot on another depot.**

   Copy temporary, *uncompressed* depot to another depot, and specify the options `-x compress_files=true` in the `swcopy` command:

   ```
   swcopy -d -s /depot1 -x enforce_dependencies=false
   ITOAgent @ <depot>
   ```

   If the SD-UX depot does not exist, it is created automatically.

4. **Remove the OVO agent from the HP SD-UX depot node.**

   To remove the agent from the HP SD-UX depot on the depot node, enter the following on the depot node:

   ```
   swremove -d ITOAgent @ depot2
   ```

   If the product is the last software in the depot, the depot is automatically unregistered by the `swremove` command. This does not remove the OVO agent software from the node.

Installing Agents from the SD-UX Depot

After the SD-UX depot is established, all OVO agents within the LAN can retrieve the OVO binary packages from the SD-UX depot instead of from the management server, as shown in Figure 2-6 on page 85 and Figure 2-7 on page 86. This part of the installation process is performed automatically.

You initiate the install operation from the administrator GUI on the OVO management server. The management server contacts the managed node and issues the install command locally on the managed node. The target managed node then retrieves the software packages from the SD-UX depot using the `swinstall` command, for more information, see the `swinstall(1M)` man page.

You can also manually retrieve the software packages from the OVO management server (see "Installing Agents Manually" on page 90).

Enabling SD-UX

To enable SD-UX, configure the node name for the SD-UX depot using the `Add/Modify Node: Node Communication Options` window in the OVO administrator GUI.

You can choose between the following installation methods:

- **Standard Installation**

  See "Installing Agents with Standard Installation" on page 85.

- **SD-UX Installation**

  See "Installing Agents with SD-UX" on page 86.

Installing Agents Manually

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

You can install an agent on an HP-UX managed node from an SD-UX tape file or from an SD-UX depot:

- **SD-UX Tape File**

  To install the agent without a depot or a network connection, copy an SD-UX tape file to the node. For instructions, see “To Install an Agent Manually from the SD-UX Tape Files” on page 91.

- **SD-UX Depot**

  To pre-install many agents, create and use a depot. For instructions, see “Creating a SD-UX Depot on a Remote Node” on page 87.

To Install an Agent Manually from the SD-UX Tape Files

To install an agent on an HP-UX managed node from an SD-UX tape file, follow these steps:

1. **Copy the OVO agent packages and installation script to a temporary directory on the managed node.**

   On the management server, these are the following files:

   - `opc_pkg.Z`
   - `comm_pkg.Z`
   - `perf_pkg.Z`
   - `opc_inst`

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

   - *HP-UX 11.0 and 11.11 managed nodes*

     ```
     /var/opt/OV/share/databases/OpC/mgd_node/vendor/hp/\
     pa-risc/hp-ux11/A.07.10/RPC_DCE_[TCP|UDP]/
     ```

   - *HP-UX IA64 11.22 managed nodes*

     ```
     /var/opt/OV/share/databases/OpC/mgd_node/vendor/hp/\
     ia64/hp-ux11/A.07.10/RPC_DCE_[TCP|UDP]/
     ```

2. **Install the Agent.**

   a. Change the permissions of the agent installation script to ensure that it can be executed:

      ```
      chmod +x /tmp/opc_inst
      ```

   b. Start the agent installation script by entering:

      ```
      /tmp/opc_inst
      ```

3. **Examine the logfile for the node:**

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

   If any errors occurred during installation, correct the problems and reinstall.

To Install an Agent Manually from an SD-UX Depot

To install an agent on an HP-UX managed node from an SD-UX depot, follow these steps:

1. **Install the agent packages:**

   Install the agent packages on the node by entering:

   `swinstall -s <depot_host:depot_path> ITOAgent`

2. **Examine the logfile for the node:**

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

   If any errors occurred during installation, correct the problems and reinstall.

TIP

Installing the agent from the command line is somewhat faster than installing the agent with the SD-UX GUI. However, the command-line installation does not notify you of any warnings found in the analysis phase unless run it twice, setting the `-p` option in the first run. If you would like to use the GUI, simply omit the name of the agent package when you enter the `swinstall` command.

Installing the agent packages will produce dependency errors, because the packages do not hold all the files necessary for the agent to run.

If you want verify that all these files exist, use the following command to get a list of all software that is installed on the node:

`/usr/sbin/swlist -l product`

Activating the Managed Node

After the node with the pre-installed agent is connected to the network (“To Activate the Node from the Command Line” on page 95), you can activate and register the managed node.

You can you can activate the managed node from the following:

- ❏ OVO GUI
- ❏ Command Line

To Activate the Node from the OVO GUI

To activate the node from the OVO GUI, follow these steps:

1. **Add the pre-installed nodes to the OVO Node Bank window.**

   Use the following menu sequence:

   `Actions-> Node-> Add`.

2. **Add the node to an OVO node group.**

   Drag and drop the node onto a node group in the `OVO Node Group Bank window`.

3. **Open the Install/Update OVO Software and Configuration window.**

   Use the following menu sequence:

   `Actions-> Agents-> Install / Update SW & Config`.

4. **Update all components.**

   In the `Install/Update OVO Software and Configuration` window, do the following:

   a. Select all components.

CAUTION

Do not check `[Force Update]`. If you check this option, the management server re-installs the agent.

   b. Click `[OK]`.

   Depending on whether you have pre-installed the agent, the management server does the following:

   - If you have pre-installed the agent on the node, the management server activates the node, and installs the selected components.
   - If you have *not* pre-installed the agent software, the management server installs the agent.

5. **Verify that the control, message, and action agents are all running on the managed node.**

   Enter the following:

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

To Activate the Node from the Command Line

To activate the agent on the node from the command line, follow these steps:

1. **Install the agent on the node manually.**

   To find out how to install the agent manually, see “Installing Agents Manually” on page 90.

Add the pre-installed nodes to the `OVO Node Bank` window.

Use the following menu sequence:

`Actions-> Node-> Add`.

2. **Add the node to an OVO node group.**

   Drag and drop the node onto a node group in the `OVO Node Group Bank` window.

3. **Activate the node.**

   Enter the following:

   ```
   /opt/OV/bin/OpC/install/opcactivate -s <OVO_mgt_server> \
   -cs <server.codeset> -cn <agent.codeset>
   ```

   This command activates the agent, which then attempts to send messages to the management server.

   - Specifying the `-s` option with the `opcactivate` command is optional. This option starts the `/opt/OV/bin/OpC/install/upd_res.sh` script which integrates the OVO agent into the system startup and shutdown scripts, for example the `/sbin/init.d/opcagt` file.
   - `-cs <server_codeset>` is the character set for the OVO management server.
     `-cn <agent codeset>` is the character set for this agent.

     For more information about codesets, see the *OVO Administrator’s Reference* and the man page *opcactivate(1M)*.

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

   After the node is connected to the network, enter the following command on the management server:

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

   The templates, monitors, commands, and so on must still be installed from the management server GUI. For instructions, see “To Activate the Node from the OVO GUI” on page 93-

De-installing Agents

You can de-install agents from HP-UX managed nodes automatically or manually.

De-installing Agents Automatically

To find out how to de-install agents automatically, see the *OVO Administrator’s Reference*.

To De-install an Agent Manually

To de-install an OVO agent from an HP-UX managed node manually, follow these steps:

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

   ```
   swremove ITOAgent
   ```

If Errors Occur During De-installation

If errors occur during the de-installation, check the local de-installation logfiles:

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

About Preconfigured Elements

This section describes preconfigured templates, template groups, and applications used by OVO on HP-UX managed nodes.

Types of Preconfigured Template Groups

OVO uses the following preconfigured template groups:

- HP-UX 11.x
- HP-UX 11.x IA64

Types of Default opcmsg Message Templates

Table 2-6 shows the opcmsg message templates that are available for HP-UX managed nodes.

Table 2-6 opcmsg Message Templates on HP-UX Managed Nodes

Name	Description
`opcmsg(1|3)`	Default interception of messages submitted by `opcmsg(1)`, `opcagtmsg_send(3)`, and `opcmsg(3)`.

Types of Default Logfile Templates

Table 2-7 shows encapsulated logfiles and associated template used on HP-UX managed nodes.

Table 2-7 Encapsulated Logfiles on HP-UX Managed Nodes

Logfile	Description	Name
`/var/adm/cron/log`	`cron(1M)` clock daemon logfile	`Cron (10.x/11.x HP-UX)`
`/var/adm/btmp` (binary format)	History of bad login attempts	`Bad Logs (10.x/11.x HP-UX)`

About SNMP Trap and Event Interception

By default, OVO intercepts SNMP traps from any application sending traps to the `opctrapi` daemon running on the management server and on all managed nodes where the OpenView trap daemon (`ovtrapd`) is running, or where port 162 can be accessed directly. For details about which traps are intercepted by default, see the SNMP trap templates in the `Message Source Templates` window of the OVO administrator GUI.

Types of SNMP Traps

The following kinds of SNMP traps can be intercepted:

- **Well-defined Traps**

  Example: system cold start, network interface up and down, and so on

- **Internal HP OpenView Traps**

  Example: Traps originating from `netmon`.

NOTE Local event interception is supported only with Network Node Manager (NNM) version 6.2.

About OVO Distributed Event Interception

OVO Distributed Event Interception enables you to intercept SNMP traps on systems other than the OVO management server. This trap interception enables messages to be processed locally, thereby improving system performance. Automatic actions, for example, can be triggered and executed directly on the node or in the subnet, instead of being first forwarded to the management server.

To Configure Basic Event Interception

To configure basic OVO Distributed Event Interception, follow these steps:

1. **Configure SNMP devices or the NNM collection station.**

   Make sure that one of the following is true:

   - *SNMP Devices*

     SNMP devices have only one SNMP destination.

     Set the destination systems for SNMP devices on HP-UX nodes in the following file:

     `/etc/SnmpAgent.d/snmpd.conf`

     Use the following statement:

     `trap-dest:<nodename>`

   - *NNM Collection Station*

     There is only one system serving as the NNM collection station for the management server. This station should be connected through the fastest network.

2. **Set the SNMP session mode.**

   If NNM is not running on the node where you want to intercept events, add the following line to the `opcinfo` file on that node:

   `SNMP_SESSION_MODE NO_TRAPD`

3. **Assign and distribute the trap template to the node.**

To Avoid Duplicate Messages in Event Interception

To avoid duplicate messages, make sure that an OVO agent (and thereby, an OVO event interceptor) runs on all NNM collection stations. Use the Print Collection Station application in the NNM Tools application group to verify which managed nodes are set up as NNM collection stations.

To Configure Event Interception with ECS

By default, `opctrapi` connects to the correlated event flow of `pmd`. You can change this behavior by adding a statement to the `opcinfo` file on the managed node.

Syntax:

```
SNMP_EVENT_FLOW [ALL|RAW|CORR]
```

The `opctrapi` process connects to the default ECS stream of `pmd`.

If needed, you can configure `opctrapi` to connect to a specific ECS stream of `pmd` by specifying the ECS stream in the `opcinfo` file:

```
SNMP_STREAM_NAME <stream_name>
```

Types of Default Applications

On HP-UX systems, OVO can start two version of the System Administrator (SAM) graphical user interface (GUI):

- Motif SAM
- ASCII SAM

NOTE For a list of default applications available for UNIX managed nodes, see the *OVO Administrator's Reference*.

About Motif SAM

The Motif version of System Administrator GUI uses the following:

Command Issued. **`sam`**

Default User. **`root`**

Default Password. None is required. Application is started by the OVO action agent. If the default user has been changed by the operator, you must supply a password.

About ASCII SAM

The ASCII version of System Administrator GUI uses the following:

Command Issued. **`sam`**

Default User. **root**

Default Password. None is configured.

Start in window (input/output).

Distributing Scripts and Programs

For HP-UX managed nodes, the platform selectors and architecture identifiers are the following:

- **HP-UX 11.0 or 11.11**

  `hp/pa-risc/hp-ux11`

- **HP-UX 11.22 (IA64)**

  `hp/ia64/hp-ux11_32`

Location of User Scripts and Programs

Table 2-8 shows the location of user scripts and programs provided on the management server.

Table 2-8 Location of User Scripts and Programs on the Management Server

Script/Program	Location
Automatic actions, operator-initiated actions, and scheduled actions	`/var/opt/OV/share/databases/OpC\ /mgd_node/customer/<arch>/actions/*`
Monitoring scripts and programs used by the monitoring agent and the logfile encapsulator	`/var/opt/OV/share/databases/OpC\ /mgd_node/customer/<arch>/monitor/*`
Scripts and programs called through command broadcast or started from the Application Desktop	`/var/opt/OV/share/databases/OpC\ /mgd_node/customer/<arch>/cmds/*`

About Temporary Directories

Table 2-9 shows the temporary directories for distributed scripts and programs on the managed nodes.

Table 2-9 Temporary Directories for Distributed Scripts and Programs on the Managed Nodes

Managed Node	Operating System	Temporary Directory

HP 9000/[78]00	HP-UX 11.0 or 11.11	`/var/opt/OV/tmp/OpC/bin/actions`
		`/var/opt/OV/tmp/OpC/bin/cmds`
		`/var/opt/OV/tmp/OpC/bin/monitor`

HP IA64	HP-UX 11.22	`/var/opt/OV/tmp/OpC/bin/actions`
		`/var/opt/OV/tmp/OpC/bin/cmds`
		`/var/opt/OV/tmp/OpC/bin/monitor`

About Target Directories

Table 2-10 shows the target directories for distributed scripts and programs on the managed nodes.

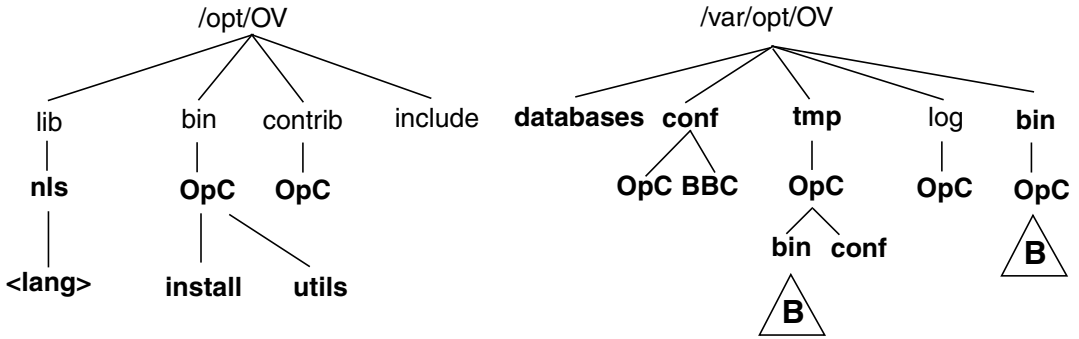
Table 2-10 Target Directories for Distributed Scripts and Programs on the Managed Nodes

Managed Node	Operating System	Target Directory	Access Rights
HP 9000/700 HP 9000/800	HP-UX 11.0 or 11.11	`/var/opt/OV/bin/OpC/actions`	`rwxr – r –` (owner: root)
		`/var/opt/OV/bin/OpC/cmds`	`rwxr-xr-x` (owner: root)
		`/var/opt/OV/bin/OpC/monitor`	`rwxr – r –` (owner: root)
HP IA64	HP-UX 11.22	`/var/opt/OV/bin/OpC/actions`	`rwxr – r –` (owner: root)
		`/var/opt/OV/bin/OpC/cmds`	`rwxr-xr-x` (owner: root)
		`/var/opt/OV/bin/OpC/monitor`	`rwxr – r –` (owner: root)

Organization of Managed Nodes

Figure 2-8 shows how OVO software is organized on HP-UX 11.0 and 11.11 managed nodes.

Figure 2-8 OVO Software on HP-UX 11.0 and 11.11 Managed Nodes



Key:

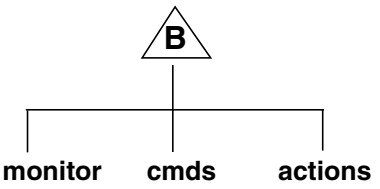
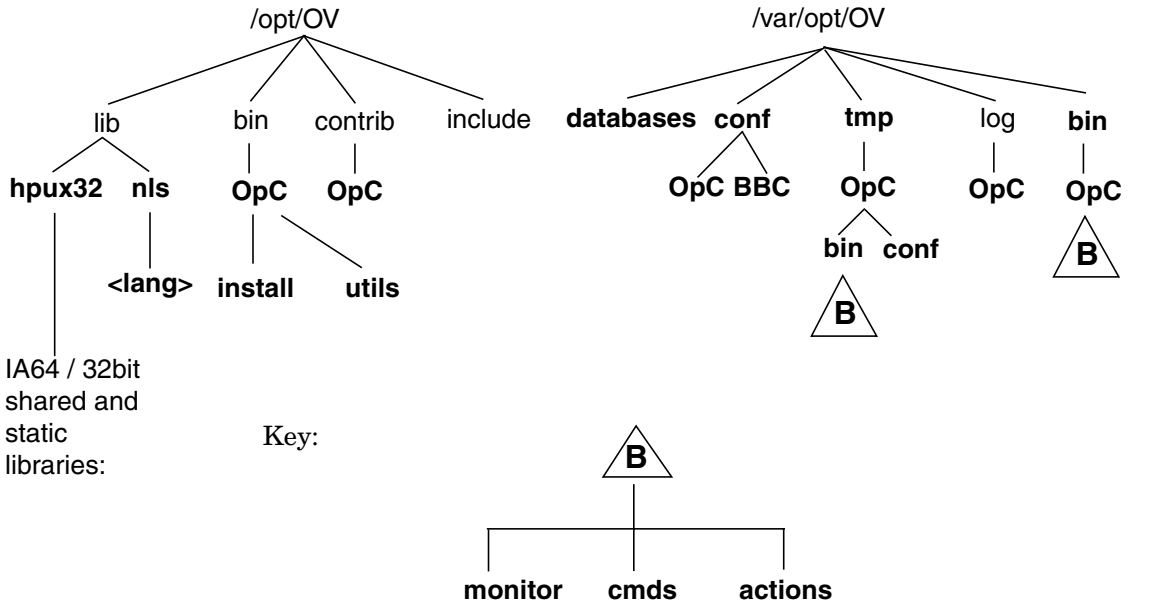


Figure 2-9 OVO Software on HP-UX 11.22 Managed Nodes



If HP OpenView NNM is also installed on the managed node, only those directories displayed in boldface type are created by OVO.

At installation, the software trees (shown in Figure 2-8) on the management server (which also acts as a managed node) is combined with the management server file tree. For a diagram of the management server file tree, see the *OVO Installation Guide for the Management Server*.

Location of Files

On HP-UX 11.x managed nodes, files are located as follows:

- **Process-related Files**

  `/var/opt/OV/tmp/OpC`

- **Agent Configuration Files**

  `/var/opt/OV/conf/OpC`

About the Default OVO Operator

The default OVO operator, `opc_op`, owns `/home/opc_op` as home directory. By default, the operators use the Korn Shell (`/bin/ksh`) and are not allowed to log into the system directly (that is, enter * in `/etc/passwd`).

If the managed node is a Network Information Service (NIS or NIS+) client, you must add the OVO default operator `opc_op` as a member of the group `opcgrp` on the NIS server before installing the OVO software on a managed node. This ensures that the OVO default operator `opc_op` is used by OVO and is consistent on all systems. If you do not add the OVO default operator `opc_op` on the NIS server, the installation will create a user `opc_op` with the group `opcgrp` locally on the node.

Types of System Resources

OVO applies changes in the following system resource files:

`/etc/passwd`.	Default OVO operator entry.
`/etc/group`.	Default OVO operator group entry.
`/sbin/init.d/opcagt` .	OVO startup and shutdown script.
`/etc/rc.config.d/opcagt` .	OVO startup and shutdown configuration script
`/sbin/rc2.d`.	Creates link `K059opcagt` to `/sbin/init.d/opcagt` is created. This link determines when `opcagt` is killed during the shutdown sequence.

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

Types of Libraries

Table 2-11 describes the managed node libraries for OVO A.05.xx, A.06.xx, and A.7.xx.

Table 2-11 Libraries for the OVO Managed Nodes

		Item	OVO A.05.xx	OVO A.06.xx	OVO A.07.xx
HP-UX 11.x	DCE	Library	**libopc_r.sl**	**libopc_r.sl**	**libopc_r.sl**
		Libraries linked to the OVO library.	/usr/lib/libdcekt.1 /usr/lib/libpthread.1 /usr/lib/libnsl.1 /usr/lib/libc.1	/usr/lib/libdcekt.1 /usr/lib/libpthread.1 /opt/OV/lib/libnsp.sl /opt/OV/lib/libas.sl /usr/lib/libnsl.1 /usr/lib/libc.1	/usr/lib/libdcekt.1 /usr/lib/libpthread.1 /usr/lib/libnsl.1
		Link and compile options	-lopc_r	-lopc_r	-lopc_r, -lnsp
HP-UX 11.0 or 11.11	DCE	Description	The HP-UX 11.x agent is a native 11.x agent and uses Kernel Threads which cannot be intermixed with Posix/DCE Threads. Since Kernel Threads were not available on HP-UX 10.x and because the HP-UX 11.x object format is incompatible with the HP-UX 10.x object format, applications that were integrated with the OVO version A.04.02 software *must* be re-compiled on HP-UX 11.0 before the can be integrated with OVO version A.08.00.	N/A	N/A

Table 2-11 Libraries for the OVO Managed Nodes (Continued)

		Item	OVO A.05.xx	OVO A.06.xx	OVO A.07.xx
HP-UX IA64 (HP-UX 11.22)	DCE	Library	N/A	N/A	`libopc_r.so`

		Libraries linked to the OVO library.			`/usr/lib/hpux32/libdcekt.so.1`
					`/usr/lib//hpux32/libpthread.so.1`
					`/usr/lib//hpux32/libnsl.so.1`

		Link and compile options			
		Description			The HP-UX 11.22 agent is a native 32 bit Itanium application. It cannot be intermixed with PA-RISC 1.1 or 2.0 code. Applications that were integrated with OVO version 10.x, 11.0 or 11.11 must be recompiled on HP-UX 11.22 before they can be integrated with OVO version A.08.00

About the Include File

On an HP 9000/700, HP 9000/800 or an HP IA64 platform with HP-UX 11.x managed nodes, use the following include file:

```
/opt/OV/include/opcapi.h
```

About the Makefiles

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

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

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

- `Makef.hpux11`
- `Makef.hpuxIA32`

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

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

Monitoring Events

The Event Monitoring Service (EMS) enables you to monitor system resources on HP-UX, and send notifications about these system resources when they change in an observable way. EMS provides information that is not immediately accessible to OVO. For example, EMS monitors the status of peripheral components. EMS is supplied by DART. Integration into OVO is supported only by EMS version 3.x.

To use EMS, you can use the following:

- **OVO Threshold Monitor Templates**

  Monitor EMS-provided resources.

- **opcmsg (1|3) Message Interceptor Template**

  Receives EMS notifications.

Before you set up OVO threshold monitor templates or use the OVO EMS opcmsg templates, you must install EMS.

For more information about EMS, see the documentation supplied with the EMS product.

About EMS Threshold Monitoring[1]

OVO provides a monitor executable, `opc_get_ems_resource`, that you can call in threshold monitor templates. The `opc_get_ems_resource` executable queries EMS for a resource instance or all instances of a resource class, and reports the current values to OVO. By setting up conditions for a threshold monitor template, you can set different thresholds for these values and react accordingly (for example, with different automatic or operator-initiated actions).

You can use only numeric and enumerated data types for threshold monitoring. To find out how to use the `Object Pattern` field in the `Condition No.` window to monitor multiple instances of a monitored object (for example, a resource class), see the *OVO Concepts Guide*.

1. EMS threshold monitoring is not available for the HP-UX 11.22 agent.

Types of Data Returned by the Monitor Executable

The monitor executable, `opc_get_ems_resource`, returns the following data:

- **Current Value of the Resource Instance**

  Available through the OVO variable:

  `<$VALUE>`

  Sample output:

  `1`

- **Name of the Resource Instance**

  Available through the OVO variable:

  `<$MSG_OBJECT>`

  Sample output:

  `/vg/vg00/lv/status/lvol1`

- **Readable Interpretation of the Enumerated Value**

  If the resource instance is of the type enumerated, this value is available through the OVO variable:

  `<$OPTION(EMS_ENUM)>`

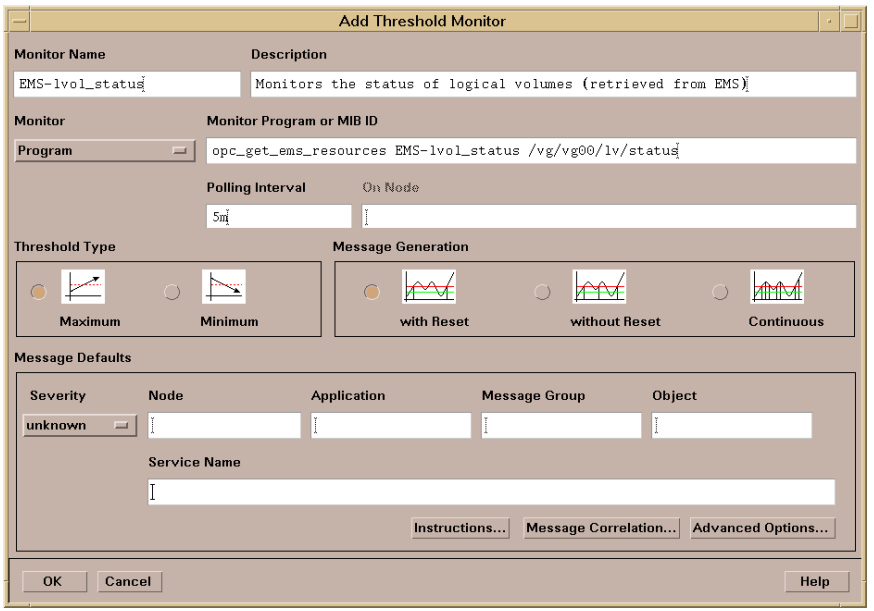
  Sample output:

  `UP`

Setting up a Threshold Monitor Template

Figure 2-10 shows how to set up a threshold monitor template with `opc_get_ems_resource`.

Figure 2-10 Setting up a Threshold Monitor for EMS Resources



In the `Monitor Program or MIB ID` field, enter the following:

- **Name of the Program Monitor**

  `opc_get_ems_resource`

- **Name of the Threshold Monitor Template**

  This name tells `opc_get_ems_resource` where to send the result of the query.

  Example:

  `EMS-lvol_status`

- **EMS Resource Instance or Class**

  Example:

  `/vg/vg00/lv/status`

Viewing the Resource Hierarchy in the EMS GUI Client

You can view the resource instances and classes that are available in EMS with the EMS GUI client, which is integrated into SAM, the HP-UX system administration tool.

To Start the EMS GUI

To start the EMS GUI, follow these steps:

1. Start SAM.

   For example, start SAM from the `OVO Application Bank` window.

2. Double-click the `Resource Management` icon
3. Double-click the `Event Monitoring Service` icon.

To View Resource Instances in the EMS GUI

To see a description and a list of all possible values, click `[Show Instance Description…]`.

To Close the EMS GUI

When you have finished browsing through the resource hierarchy, click `[Cancel]` rather than `[OK]` because you do not want to add the request.

Types of EMS Resource Instances

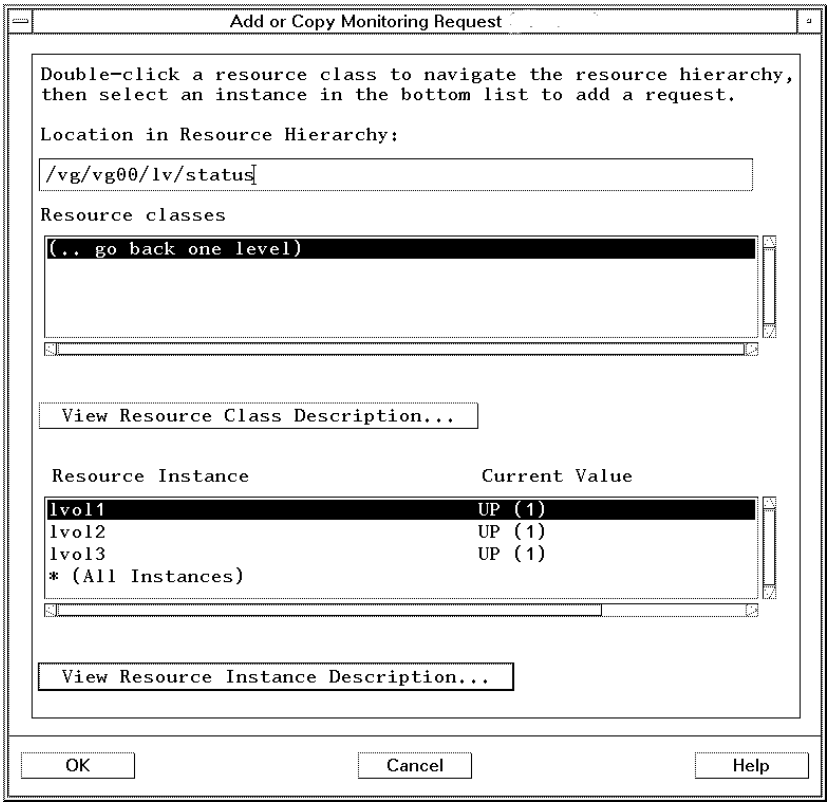
Figure 2-11 on page 117 shows all resource instances of the following resource class:

```
/vg/vg00/lv/status
```

These resource instances include the following, as well as their current values:

- `lvol1`
- `lvol2`
- `lvol3`

Figure 2-11 Browsing the EMS Resource Hierarchy



Viewing the Resource Hierarchy in the OVO Application Bank

Instead of using the EMS GUI client in SAM to browse the resource hierarchy, you can also execute the application `EMS Resources` (application group `OSSPI`) in the `OVO Application Bank` window.

About the EMS Resources Application

When you execute `EMS Resources`, it opens a terminal window and calls `opc_get_ems_resource -d -r`. By default, `EMS Resources` displays all resources starting with the root directory (/). You can modify `EMS Resources` to start at a specific level in the resource hierarchy (for example, at `/vg/vg00/lv/status`).

Sample Output from the EMS Resources Command

The output is displayed in the terminal window and may look like the following example:

```
/vg/vg00/lv/status
/vg/vg00/lv/status/lvol1 = 1 ("UP")
/vg/vg00/lv/status/lvol2 = 1 ("UP")
/vg/vg00/lv/status/lvol3 = 1 ("UP")
```

Syntax for the EMS Resource Command

The command `opc_get_ems_resource` requires the following syntax:

```
opc_get_ems_resource [-r] [-t <secs>] [-d |
<ito_monitor_name>] [<resource> ...]
```

`-r`.	Recursively traverses class and instance tree.
`-t`.	Sets timeout to <*secs*> seconds. Default is 30 seconds.
`-d`.	Displays on `stdout`.
<*ito_monitor_name*>	Monitor name to be used when providing the resource value to OVO.
<*resource*>	Name of the resource instance and class to be monitored and displayed Default is root (`/`).

If Error Occur with EMS

If you encounter problems with EMS or `opc_get_ems_resource`, check the logfiles in the following directory for more information:

```
/etc/opt/resmon/log
```

Viewing the Resource Hierarchy from the Command Line

To get information about configured resources, you can use the command line tool:

```
/opt/resmon/bin/resls
```

For details, see the man page *resls(1)*.

Sending EMS Notifications to OVO

To configure event monitoring requests for EMS through `opcmsg`, use the EMS GUI client in SAM and the `opcmsg` message source template. The message source template `opcmsg(3)` is integrated into the EMS GUI. In the EMS GUI, you can select `opcmsg(3)` as a notification target for EMS events.

Configuring OVO EMS Templates

Using the OVO threshold monitor mechanism is more effective than receiving EMS notifications from `opcmsg`. Not only do you have to use the OVO administrator GUI *and* the SAM GUI to configure EMS, you also have to do this locally on each managed node. If you are using threshold monitoring, you can configure the templates centrally on your OVO management server and distribute them to the managed nodes that have EMS installed.

High Availability Support on HP-UX

OVO offers MC/ServiceGuard support on both the management server and the managed nodes.

For installation and configuration instructions, see the *OVO Installation Guide for the Management Server*

For additional information for system administrators working with OVO in MC/ServiceGuard environments, see the *OVO DCE Agent Concepts and Configuration Guide*.

About the Supplied Perl Interpreter

The managed node software includes a custom binary Perl 5.6.1 distribution.

The Perl is embedded in the Perl interpreter and the monitoring agent, and is designed to be used internally by OVO. Some OVO policies deployed by OpenView Operations for Windows management servers include Perl scripts (for example, some schedules and measurement threshold policies). Perl scripts are also used by some HP-supplied Smart Plug-ins (SPIs).

The Perl interpreter and other binaries are automatically installed into the `$OV_CONTRIB/perl` directory. A basic set of modules is installed in the /opt/OV/nonOV/perl/a/lib/5.6.1/File/ directory. Pre-existing Perl installations are not altered as a result of installing a managed node.

If you want to use the Perl distribution for additional purposes beyond its internal use within OVO, you should first check which modules are included by listing the `.pl` and `.pm` files within the `/opt/OV/nonOV/perl/a/lib/5.6.1/` directory.

For further information about Perl or if you need to add additional modules, go to the following web site:

`http://www.perl.com`

NOTE

Perl is supplied "as is" with no warranties whether express or implied according to the Perl artistic license agreement. Hewlett-Packard is not responsible for errors in Perl, which is public domain software and not produced by HP. Hewlett-Packard does not support any modifications to the provided Perl distribution. This software is licensed, not sold, and your use of the software is subject to the license terms contained in the license agreement."

3 About Linux Managed Nodes

In This Chapter

This chapter explains how to install and configure HP OpenView Operations (OVO) on Linux managed nodes and on RedHat Enterprise Linux Advanced Server 2.1 (RedHat AS 2.1) cluster systems.

Installation Requirements

This section explains OVO hardware and software requirements for Linux managed nodes.

Hardware Requirements

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

- **Disk Space**

  33 MB (about 66 MB is required during software installation).

- **Additional Swap Space**

  None

- **Additional RAM**

  20 MB

Software Requirements

The following software *must* be installed on Linux managed nodes:

❑ **Operating System and Parameters**

Supported operating system and kernel versions are listed in Table 3-2 on page 132 and Table 0-1 on page HIDDEN.

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_PROC_FS`

  Proc file system support

NOTE

The following kernel fetaures must be enabled only on RedHat Enterprise Linux Advanced Server 2.1 (RedHat AS 2.1) cluster systems:

- `CONFIG_SCSI_LOGGING`
- `CONFIG_SYSCTL`

❑ **Packages**

The following packages *must* be installed on every platform:

- `bash`
- `gawk`

The following table lists all packages that *must* also be installed depending on the operating system and version.

Table 3-1 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	
	RedHat 8.0	
	RedHat 9.0	
	RedHat AS 2.1[a]	
	RedHat AS 3.0	
	SuSE 6.4	`compat` `shlibs`
	SuSE 7.0	
	SuSE 7.2	`compat` `glibc`
	SuSE 7.3	
	SuSE 8.0	
	SuSE 8.1	`compat-2002` `glibc`
	Debian 3.0	`libstdc++2.9-glibc2.1` `libc6`

Table 3-1 Required Packages for Different Operating Systems and Versions (Continued)

Language	Operating System and Version	Packages

Japanese	RedHat 6.2J	`libstdc++`
		`ldconfig`
		`glibc`

	RedHat 7.0.1J	`compat-libstdc++` `glibc`
	RedHat 7.1J	
	RedHat 7.2J	
	RedHat 7.3	
	RedHat 8.0	
	RedHat 9.0	

	Turbolinux 6.0J Workstation	`libstdc++-compat`
		`ldconfig`
		`glibc`

	Turbolinux 6.1J Server	
	Turbolinux 6.5J Server	
	Turbolinux 7.0J Workstation	`libstdc++-compat` `glibc`
	Turbolinux 8.0	`libstdc++-compat` `glibc`

a. RedHat Enterprise Linux Advanced Server 2.1

- **DCE RPC**

  Delivered with the OVO DCE agent packages.

- **RedHat Package Manager (RPM)**

  Must be installed on Debian systems.

- **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.

The following table and Table 0-1 on page HIDDEN show the operating system and kernel version supported by OVO for Linux managed nodes.

Table 3-2 Supported Operating System and Kernel Versions (English)

Language	Operating System and Version	Kernel	glibc
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	2.4.x x can be 7	2.2.4
	RedHat 7.3	2.4.x x can be 18	2.2.5
	RedHat 8.0 RedHat 9.0	2.4.x x can be 18	2.2.93
	RedHat AS 2.1	2.4.x x can be 19	2.2.4

Table 3-2 Supported Operating System and Kernel Versions (English)

Language	Operating System and Version	Kernel	glibc
English	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 7.2	2.4.x x can be 4	2.2.2
	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
	SuSE 8.1 SuSE 8.2	2.4.x x can be 19	2.2.5-161
	Debian 3.0	2.4.x x can be 18	2.2.5

Table 3-3 Supported Operating System and Kernel Versions (English)

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	2.4.x x can be 7	2.2.4
	SuSE 6.2	2.2.x x can be 10	2.1.1 2.1.2 2.1.3
	SuSE 6.3	2.2.x x can be 13	2.1.2 2.1.3
	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	2.4.x x can be 0 2.2.x x can be 18	2.2
	SuSE 7.2	2.4.x x can be 4	2.2.2
	SuSE 7.3	2.4.x x can be 10	2.2.4
	Debian 2.2	2.2.x x can be 17	2.1.3

Installing and De-installing Agents

This section describes how to install and de-install Linux managed nodes.

Tips for Installing Agents

When installing Linux managed nodes, follow these guidelines:

❏ **Installation Methods**

You can install agents in one of two ways:

- *Remotely*

  From the management server.

  For details, see "Installing Agents" on page 136.

- *Manually*

  Locally on the Linux managed nodes.

  For details, see "To Install an Agent Manually" on page 137.

❏ **Remote Installation**

Before installing agents remotely, you *must* set up the management server and provide remote logins. For details, see "Before Installing Agents Remotely" on page 136.

❏ **Hostnames of Management Server**

The name of the management server *must* be known to the managed node. If DNS is *not* configured, the name of the management server *must* be registered on the name server or in the local host table:

`/etc/hosts`

You can verify the name of the management server with the `nslookup` command.

TIP

When checking running processes with the Linux `ps` command, OVO processes may be reported several times because the Linux `ps` command reports all threads associated with a process. This duplication is the normal Linux behavior, and is *not* related to OVO.

Use the command `ps fax` to get a more detailed listing of all running processes and their dependencies.

Installing Agents

You can install agents on Linux managed nodes remotely from the OVO management server or locally on Linux managed nodes.

Before Installing Agents Remotely

Before installing agents remotely, you *must* do the following:

- **Establish "remsh" or "ssh" Services**

  Enable `remsh` (`rsh`) or `ssh` services so you can install the agent software remotely from the OVO management server on a Linux managed node.

- **Enable Automatic (De-)Installation**

  In the `Add Node` window on the management server, select `Automatic (De-)Installation` option for the managed node.

- **Provide User Name**

  On the management server, provide a user name for the installation.The `root` user name is used by default.

- **Add tty Devices for Remote Logins**

  Add `tty` devices for remote logins (for example, `ttyp0`, `ttyp1`, and so on) to the following file:

  `/etc/securetty`

Installing Agents with Standard Installation

For general installation instructions, see the *OVO Administrator's Reference*.

To Install an Agent Manually

In some situations, you may want to install the Linux agent software without using the management server. Manual installation prepares the system to become an OVO managed node when it is later connected to the network. This approach is useful if you are preparing many systems in a central location, or if you want to avoid using the `root` connection over the network that is necessary for a standard agent installation.

To install the OVO agent on an OVO Linux system that will become an OVO managed node, follow these steps:

1. **Verify hardware and software requirements.**

   Make sure that your Linux managed node meets the hardware and software requirements described in "Installation Requirements" on page 127. Also, review the installation tips offered in "Tips for Installing Agents" on page 135.

2. **Copy the OVO agent packages and installation script to a temporary directory on the managed node.**

   On the management server, these are the following files:

   - `opc_pkg.Z`
   - `comm_pkg.Z`
   - `perf_pkg.Z`
   - `opc_inst`

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

- *Linux RedHat 6.2, 7.0, SuSE 6.x, 7.0, Turbolinux 6.x, and Debian 2.2*

  /var/opt/OV/share/databases/OpC/mgd_node/vendor/\
  linux/intel/linux22/<*OVO_version*>/RPC_DCE_TCP/

- *Linux RedHat 7.1, 7.2, 7.3 and 8.0, RedHat AS 2.1, SuSE 7.1, 7.2, 7.3, 8.0 and 8.1, Turbolinux 7.0, Turbolinux 8.0 and Debian 3.0*

  /var/opt/OV/share/databases/OpC/mgd_node/vendor/\
  linux/intel/linux24/<*OVO_version*>/RPC_DCE_TCP/

In these directories, <*OVO_version*> is the version of OVO (for example, A.08.00).

3. **Add the managed node to the OVO Node Bank window.**

   Use the OVO administrator GUI to add the managed node to the OVO Node Bank.

4. **Install the OVO agent software.**

   On the Linux managed node, do the following:

   a. **Install the Agent.**

      A. Change the permissions of the agent installation script to ensure that it can be executed:

         chmod +x /tmp/opc_inst

      B. Start the agent installation script by entering:

         /tmp/opc_inst

   b. **Activate the agent.**

      Enter the following:

      **/opt/OV/bin/OpC/install/opcactivate [-s] **
      **<*OVO_mgt_server*> [-cs <*server.codeset*>] **
      [-cn <*agent.codeset*>]

      In this command, <*OVO_mgt_server*> is the hostname of your OVO management server.

- Specifying the `-s` option with the `opcactivate` command is optional. This option starts the `/opt/OV/bin/OpC/install/upd_res.sh` script which integrates the OVO agent into the system startup and shutdown scripts, for example the `/etc/init.d` file.

  `-cs <server_codeset>` is the character set for the OVO management server.
  `-cn <agent codeset>` is the character set for this agent.

  For more information about codesets, see the *OVO Administrator's Reference* and the man page *opcactivate(1M)*.

If Errors Occur During Installation

If errors occur during the installation, check the local installation logfile:

`/tmp/rpm.log`

This file is empty if the installation had no errors.

De-installing Agents

You can de-install agents from Linux managed nodes automatically or manually.

De-installing Agents Automatically

For general de-installation instructions, see the *OVO Administrator's Reference*.

To De-install an Agent Manually

To de-install an agent manually, follow these steps:

1. Stop all OVO agents running on the managed node.

   Enter the following:

   ```
   opcagt -kill
   ```

2. De-install the OVO agent software by entering:

   ```
   rpm -e OPCPERF OPC OPCCOMM
   ```

NOTE If you are removing an older version of the agent, use the following command: `rpm -e OPC dce`.

3. De-install DCE if it is not used by any other application.

   Enter the following:

   ```
   rpm -e dce
   ```

Removing Older Agents

If older OVO agent packages are no longer required and are *not* installed on any managed node, you can remove them with the following commands:

- **Linux RedHat 6.2, 7.0, SuSE 6.x, 7.0, Turbolinux 6.x, and Debian 2.2**

  ```
  /opt/OV/bin/OpC/install/rm_opc.sh linux/intel/linux22/\
  <OVO_version>
  ```

- **Linux RedHat 7.1, 7.2, 7.3 and 8.0, RedHat AS 2.1, SuSE 7.1, 7.2, 7.3, 8.0 and 8.1, and Turbolinux 7.0 and Debian 3.0**

  ```
  /opt/OV/bin/OpC/install/rm_opc.sh linux/intel/linux24/\
  <OVO_version>
  ```

In these commands, *<OVO_version>* is the version of OVO that supports this agent platform (for example, `A.08.00`).

About Preconfigured Elements

This section describes preconfigured templates, template groups, and applications used by OVO on Linux managed nodes.

Preconfigured Template Groups

OVO uses the following preconfigured template groups:

- `Linux (RedHat)`
- `Linux (Turbolinux)` (Japanese management server only)

Types of Default Logfile Templates

Table 3-4 shows encapsulated logfiles and associated template used on Linux managed nodes.

Table 3-4 Encapsulated Logfiles on Linux Managed Nodes

Logfile	Description	Template Name
`/var/log/cron`	Cron logfile	`Cron (RedHat Linux)`[a]

a. `Cron (RedHat Linux)` template name also applies to Turbolinux.

No SNMP Trap and Event Interception

The OVO event interceptor is *not* supported on Linux managed nodes.

Types of Default Applications

For a list of default applications available for UNIX managed nodes, see the *OVO Administrator's Reference*.

Distributing Scripts and Programs

For Linux managed nodes, the platform selectors and architecture identifiers are the following:

- **Linux RedHat 6.2 and 7.0, SuSE 6.x, 7.0, Turbolinux 6.x, and Debian 2.2**

  `linux/intel/linux22`

- **Linux RedHat 7.1, 7.2, 7.3, and 8.0, RedHat AS 2.1, SuSE 7.1, 7.2, 7.3, 8.0, and 8.1, and Turbolinux 7.0 and Debian 3.0**

  `linux/intel/linux24`

Location of User Scripts and Programs

Table 3-5 shows the location of user scripts and programs provided on the management server.

Table 3-5 Location of User Scripts and Programs on the Management Server

Script/Program	Location

Automatic actions, operator-initiated actions, and scheduled actions	Linux RedHat 6.2, 7.0, SuSE 6.x, 7.0, Turbolinux 6.x, and Debian 2.2:
	`/var/opt/OV/share/databases/OpC/mgd_node/customer/\ linux/intel/linux22/actions/*`
	Linux RedHat 7.1, 7.2, 7.3 and 8.0, RedHat 2.1, SuSE 7.1, 7.2, 7.3, 8.0, and 8.1, and Turbolinux 7.0, and Debian 3.0:
	`/var/opt/OV/share/databases/OpC/mgd_node/customer/\ linux/intel/linux24/actions/*`

Monitoring scripts and programs used by the monitoring agent and the logfile encapsulator	Linux RedHat 6.2, 7.0, SuSE 6.x, 7.0, Turbolinux 6.x, and Debian 2.2:
	`/var/opt/OV/share/databases/OpC/mgd_node/customer/\ linux/intel/linux22/monitor/*`
	Linux RedHat 7.1, 7.2, 7.3, and 8.0, RedHat AS 2.1, SuSE 7.1, 7.2, 7.3, 8.0, and 8.1, and Turbolinux 7.0 and Debian 3.0:
	`/var/opt/OV/share/databases/OpC/mgd_node/customer/\ linux/intel/linux24/monitor/*`

Scripts and programs called through command broadcast or started from the Application Desktop	Linux RedHat 6.2, 7.0, SuSE 6.x, 7.0, Turbolinux 6.x, and Debian 2.2:
	`/var/opt/OV/share/databases/OpC/mgd_node/customer/\ linux/intel/linux22/cmds/*`
	Linux RedHat 7.1 7.2, 7.3, and 8.0, RedHat AS 2.1, SuSE 7.1, 7.2, 7.3, 8.0, and 8.1, and Turbolinux 7.0 and Debian 3.0:
	`/var/opt/OV/share/databases/OpC/mgd_node/customer/\ linux/intel/linux24/cmds/*`

About Temporary Directories

Table 3-6 shows the temporary directories for distributed scripts and programs on the managed nodes.

Table 3-6 Temporary Directories for Distributed Scripts and Programs on Managed Nodes

Managed Node	Operating System	Temporary Directory

Intel Pentium	Linux	`/var/opt/OV/tmp/OpC/bin/actions`
		`/var/opt/OV/tmp/OpC/bin/cmds`
		`/var/opt/OV/tmp/OpC/bin/monitor`

About Target Directories

Table 3-7 shows the target directories for distributed scripts and programs on the managed nodes.

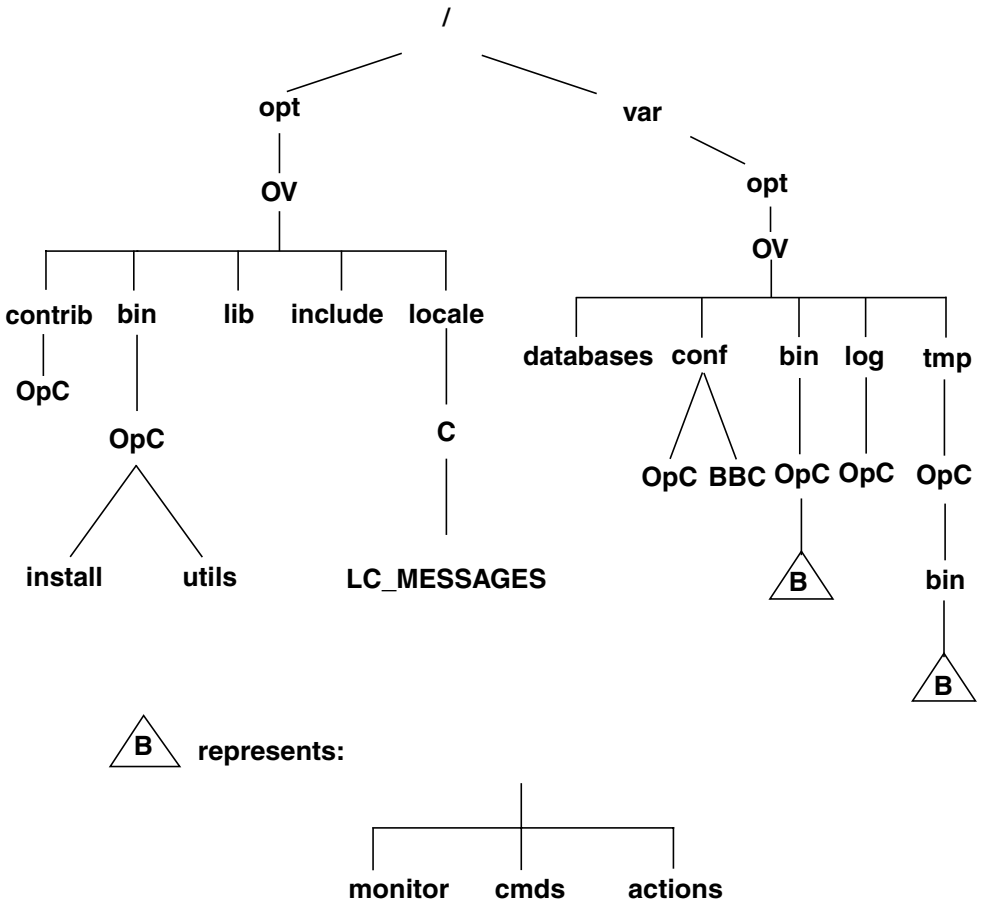
Table 3-7 Target Directories for Distributed Scripts and Programs on the Managed Nodes

Managed Node	Operating System	Target Directory	Access Rights
Intel Pentium	Linux	`/var/opt/OV/bin/OpC/actions`	`rwxr-xr-x` (owner: `root`)
		`/var/opt/OV/bin/OpC/cmds`	`rwxr-xr-x` (owner: `root`)
		`/var/opt/OV/bin/OpC/monitor`	`rwxr-xr-x` (owner: `root`)

Organization of Managed Nodes

Figure 3-1 shows how OVO software is organized on Linux managed nodes.

Figure 3-1 OVO Software on Linux Managed Nodes



Location of Files

On Linux managed nodes, files are located as follows:

- **Process-related Files**

  `/var/opt/OV/tmp/OpC`

- **Agent Configuration Files**

  `/var/opt/OV/conf/OpC`

About the Default OVO Operator

If they do *not* already exist, the default OVO operator `opc_op` and group `opcgrp` are created.

About Default OVO Operator Entries

The default OVO operator is added in the following file on Linux managed nodes:

`/etc/passwd`

Fields include the following:

`User Name` `opc_op`

`Encrypted Password` `*` (no login)

`User-ID` `777` (if still available) or next possible free number

`Group-ID` `77` (if still available) or next possible free number

`Description` Default OVO operator

`Home Directory` `/home/opc_op`

`Login Shell` `/bin/bash` (POSIX shell)

About Default OVO Operator Group Entries

The default OVO operator group is added to the following directory on Linux managed nodes:

`/etc/group`

Fields include the following:

`Group Name`	`opcgrp`
`Encrypted Password`	Empty
`Group-ID`	`77` or higher
`Users`	`opc_op`
`Description`	Default OVO operator group

Types of Libraries

Table 3-8 describes the managed node libraries for OVO A.05.xx, A.06.xx, and A.07.xx.

Table 3-8 Libraries for the OVO Managed Nodes

	OVO Version	OVO A.05.xx	OVO A.06.xx	OVO A.07.xx
DCE	Library	**libopc_r.so**	**libopc_r.so**	**libopc_r.so**
	Libraries linked to the OVO library.	RedHat 5.x: libdcerpc.so libdcethread.so libpthread.so libuuid.so libcrypt.so.1 libstdc++.so.2.8 RedHat 6.x, 7.x, SuSE 6.x, 7.x and Turbolinux 6.x: libdcerpc.so libdcethread.so libpthread.so libuuid.so libcrypt.so.1 libstdc++-libc6.1-1.so.2	RedHat 5.x: libdcerpc.so libdcethread.so libpthread.so libuuid.so libcrypt.so.1 libstdc++.so.2.8 libopcas.so RedHat 6.x, 7.x, SuSE 6.x, 7.x and Turbolinux 6.x: libdcerpc.so libdcethread.so libpthread.so libuuid.so libcrypt.so.1 libstdc++-libc6.1-1.so.2 libopcas.so	RedHat 6.x, 7.x, SuSE 6.x, 7.x, Turbolinux 6.x, Debian 2.2, and Turbolinux 7.0: libdcerpc.so libdcethread.so libpthread.so libuuid.so libcrypt.so.1 libstdc++-libc6.1-1.so.2 libopcas.so
	Link and compile options	-D_REENTRANT -lopc_r -lnsp -lpthread	-D_REENTRANT -lopc_r -lnsp -lpthread	-D_REENTRANT -lopc_r -lnsp -lpthread
	Description	The LD_LIBRARY_PATH variable has to be exported or ldconfig has to be executed.	The LD_LIBRARY_PATH variable has to be exported or ldconfig has to be executed.	The LD_LIBRARY_PATH variable has to be exported or ldconfig has to be executed.

About the Include File

On an Intel Pentium platform with Linux managed nodes, use the include file:

```
/opt/OV/include/opcapi.h
```

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

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

About the Makefile

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

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

To build an executable with correct compile and link options, use the following makefile:

```
Makef.linux
```

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

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

About the Supplied Perl Interpreter

The managed node software includes a custom binary Perl 5.6.1 distribution.

The Perl is embedded in the Perl interpreter and the monitoring agent, and is designed to be used internally by OVO. Some OVO policies deployed by OpenView Operations for Windows management servers include Perl scripts (for example, some schedules and measurement threshold policies). Perl scripts are also used by some HP-supplied Smart Plug-ins (SPIs).

The Perl interpreter and other binaries are automatically installed into the `$OV_CONTRIB/perl` directory. A basic set of modules is installed in the `/opt/OV/lib` directory. Pre-existing Perl installations are not altered as a result of installing a managed node.

If you want to use the Perl distribution for additional purposes beyond its internal use within OVO, you should first check which modules are included by listing the `.pl` and `.pm` files within the `/opt/OV/nonOV/perl/a/lib/5.6.1/` directory.

For further information about Perl or if you need to add additional modules, go to the following web site:

`http://www.perl.com`

NOTE

Perl is supplied "as is" with no warranties whether express or implied according to the Perl artistic license agreement. Hewlett-Packard is not responsible for errors in Perl, which is public domain software and not produced by HP. Hewlett-Packard does not support any modifications to the provided Perl distribution. This software is licensed, not sold, and your use of the software is subject to the license terms contained in the license agreement."

4 About MPE/iX Managed Nodes

In this Chapter

This chapter explains how to install and configure HP OpenView Operations (OVO) on MPE/iX managed nodes.

Installation Requirements

This section explains OVO hardware and software requirements for MPE/iX managed nodes.

Hardware Requirements

Before installing OVO, make sure the MPE/iX systems you select as managed nodes meet the following hardware requirements:

- **Disk Space**

  10 MB (about 20 MB is required during software installation)

- **Additional Swap Space**

  None

- **Additional RAM**

  None

Software Requirements

Before installing OVO, make sure the following software is installed on MPE/iX managed nodes:

- **Operating System**

  For a list of operating system versions supported by OVO, see the *OVO Installation Guide for the Management Server*.

- **DCE RPC**

  CE RPC 1.0.2 or DCE RPC 1.2.1

- **NS Services**

Requirements for the Management Server

You must install the vt3k package on the management server. The vt3k package is available on the HP-UX Application Software CD-ROMs.

Required MPE/iX Patches

You must install the following MPE/iX patches:

Table 4-1 Required MPE/iX Patches

MPE/iX	Patch ID	Description
6.0	MPEKXE5	Adds routines to the system `SL.PUB.SYS` that the console interceptor requires to operate.
	ITOED07A	Provides routines to the `XL.PUB.SYS` to allow the OVO agent to call various NCS routines.
6.5	FRILXX7A	Enables the OVO agent to register at the DCE rpcd. This patch is required if the basic DCE client is installed that comes free with MPE FOS.
	DCELXX6A	This patch is required if DCE is installed that has to be purchased separately.
	ITOED07B	Provides routines to the `XL.PUB.SYS` to allow the OVO agent to call various NCS routines.
7.0	FRILXX7A	Enables the OVO agent to register at the DCE rpcd. This patch is required if the basic DCE client is installed that comes free with MPE FOS.
	DCELXX6A	This patch is required if DCE is installed that has to be purchased separately.
	ITOED07C	Provides routines to the `XL.PUB.SYS` to allow the OVO agent to call various NCS routines.

Installing and De-installing Agents

This section describes how to install and de-install MPE/iX managed nodes.

Tips for Installing Agents

This section includes tips for installing MPE/iX managed nodes.

About the Management Server Name

Before installing agents, the name of the management server must be known to the managed node. This means that it must be registered on the name server or in the local host table, `HOSTS.NET.SYS`.

About Daemons

Before installing agents on the managed node, the DCE RPC Daemon (`dced` or `rpcd`) must be running.

If this daemon is not running, the OVO services cannot be started. Automatic startup and integration of the startup functionality in the boot procedure is performed by OVO only for the `dced/rpcd` daemon, and only if you have selected the `Automatic Update of System Resource Files` option, see the `Add/Modify Node` window in the OVO administrator GUI.

An example of a system resource file is the following:

```
SYSSTART.PUB.SYS
```

About the Default OVO Operator

If you do not need the functionality of the default OVO operator on your managed nodes (except on the management server), you can purge the related information (that is, purge the account OVOPR).

About Login and Logout UDCs

Before installing software, disable the login and logout UDCs for the following, if they are present:

- manager.sys
- mrg.ovopc
- agent.ovopc

NOTE Interactive login and logout UDCs are not supported by OVO. For this reason, you must disable login and logout UDCs during software installation and application startup using the vt3k connection.

About Languages

Before starting the OVO agent software installation, always set LANG to C.

About IP Addresses

To check IP addresses, use the following:

NSLOOKUP.HPDCE.SYS

For more information, see the *OVO Administrator's Reference*.

About Domain Name Resolution

In its current release, OVO supports only the domain name service for IP address resolution. Therefore the (fully qualified) management server system must be known by the domain name resolver (as configured in `RESLVCNF.NET.SYS` on the managed node). Or, if no name server is running, the management server name must be locally registered in `HOSTS.NET.SYS`.

IP address resolution through the following are *not* supported:

- Network Directory (`NSDIR.NET.SYS`)
- Probe (and Probe Proxy)

About the Logging Group

The logging group on MPE/iX is where the files `opcmsglg` (local message logfile) and `opcerror` reside. This logging group must belong to the account `OVOPC`. If the logging group it does not belong to OVOPC, OVO services cannot write or create files in that group. For more information, see the *OVO Administrator's Reference*.

About OVO Agent Jobs

OVO agents run in the job, **OPCAGTJ,AGENT.OVOPC**. For this reason, you should probably adapt **HPJOBLIMIT** to ensure that all jobs, including OVO agents, can be started (for example, when *not* running OVO intelligent agents).

The OVO action agent also streams separate jobs for application startup and command broadcasting. Adapt the **HPJOBLIMIT** accordingly.

About Executable Libraries

Before you install agents, the executable library, `SNMPXL.NET.SYS`, must be available, and OVO must have execution rights. If the executable library is not available or if OVO does not have execution rights, the OVO Monitor Agent will not operate.

About Time Zones

Before installing software, you must set the **TIMEZONE** variable to correct differences between the various time resources used by OVO C routines and MPE/iX intrinsics and commands. If you do not set this variable, messages, error trace files, and trace logfiles receive the wrong creation time stamp. These incorrect time stamps can cause problems when you work with multiple management servers. Incorrect time stamps also disrupt the timing of follow-the-sun, which switches message routing.

Insert the following call at a global location (for example, at the logon UDC or `SYSSTART.PUB.SYS`):

```
call: setvar TZ,"TIMEZONE"
```

For possible `TIMEZONE` values, see `tztab.lib.sys`. Set the variable according to your country or region.

If hardware time and system time are still misaligned, you can correct them with the `setclock` command. for values for all MPE/iX clocks, see `showclks.pubxl.telesup`. For example, to align the clocks, see "help setclock operation."

About Spool Files

When tasks are executed in a job (for example, scheduled actions, broadcast commands, or X-applications), the spool files generated from these tasks are automatically deleted. If you want to retain the spool file, set the following variables in the file `OPCINFO.BIN.OVOPC` to the following:

```
OPC_MPE_CREATE_SPOOL_FILE TRUE
```

To define the outfence for spool files, set the following variable:

```
OPC_MPE_OUTCLASS_STRING <outcalls_string>
```

Example:

```
OPC_MPE_OUTCLASS_STRING ,1,1
```

About Streamed Jobs

You can use the system boot file, SYSSTART.PUB.SYS, to set up a normal user environment automatically when OVO is started.

Parameters for SYSSTART.PUB.SYS

The contents of this file should include command parameters for your environment, such as the following:

- Standard limits for job sessions
- Spooler start commands
- Stream device identification
- Outfence priorities
- Event logging

Excluding Network Commands from SYSSTART.PUB.SYS

A SYSSTART file can contain selected MPE/iX commands (and their parameters) that the system manager is allowed to execute. Networking commands are excluded.

You should exclude networking commands from the following:

- Jobs streamed from SYSSTART
- Logon UDC for OPERATOR.SYS

Starting a Streamed Job

If you have used the Add/Modify Node window to select the Automatic Update of System Resource Files option for the managed node, SYSSTART.PUB.SYS is created or updated.

NOTE SYSSTART.PUB.SYS is not created if the Automatic Update of System Resource Files option for the managed node already contains a pre-existing OVO entry.

SYSSTART.PUB.SYS contains the start sequence for the job *stream* OPCSTRTJ.BIN.OVOPC. This job is used for starting the DCE RPC Daemon (dced or rpcd) and the OVO agents. (In this job, *stream* refers to the standard **STREAM** commands, or to the node-specific *stream* utility configured in the administrator GUI, using the Advanced Options window, accessed from the Add/Modify Node window.)

Before starting OVO agents, you must ensure that the network services are running.

For an example of this streamed job, see the following file:

```
/var/opt/OV/share/databases/OpC/mgd_node/\
vendor/hp/s900/mpe-ix/A.06.00/sysstrtj.
```

To Set up a Customized Job Stream Facility

To avoiding hard-coded passwords and thereby improve security, you can set your own *stream* facility.

To set up a customized job stream facility, follow these steps:

1. Open the Add/Modify Node or Node Defaults window.
2. Open the Node Advanced Options window.
3. Do one of the following:
   - *Set up a customized job stream facility.*

     No passwords are placed in the OVO job files. Control over the job is given to your own *stream* facility.
   - *Use the OVO default.*

     If you leave the default, passwords remain unencrypted and the file OPCSTRTJ.BIN.OVOPC contains the AGENT.OVOPC password.

Preparing OVO for a Customized Job Stream Facility

If you want to use your own customized job stream facility, check the MPE/iX startup file SYSSTART.PUB.SYS before installing OVO A.06.00 software. If there is an entry for OVO (the installation process checks for the keyword **OperationsCenter**), that entry will not be modified.

You can modify the line that streams the OVO startup job OPCSTRTJ.BIN.OVOPC manually so that it will not be changed by later software installation.

For example, the change the following line:

- **Change**

  ```
  STREAM OPCSTRTJ.BIN.OVOPC
  ```

- **To**

  ```
  my job-stream facility> OPCSTRTJ.BIN.OVOPC
  ```

In this line, <*my job-stream facility*> could be the Maestro **mstream**.

If there is no entry for OVO in SYSSTART.PUB.SYS, the automatic software installation inserts an entry for OVO in SYSSTART.PUB.SYS. The major parts of the entry looks like this:

```
comment    ...     OperationsCenter
<customer-defined stream-facility> OPCSTRTJ.BIN.OVOPC
```

Installing Agents

See the *OVO Administrator's Reference* for general installation instructions.

In an error occurs (for example, if the installation process could not be reviewed in a terminal window), check the following logfile management server for errors or warnings:

```
/var/opt/OV/log/OpC/mgmt_sv/install.log
```

De-installing Agents

For general de-installation instructions, see the *OVO Administrator's Reference*.

About Preconfigured Elements

MPE/iX preconfigured elements are described in greater detail in the *Supplementary Guide to MPE/iX Templates*:

`http://<management_server>:3443/ITO_DOC/C/manuals/MPETemplates.pdf`

In this URL, <*management_server*> is the fully qualified hostname of your management server.

Intercepting Messages

OVO is able to intercept messages that are sent to the MPE/iX console. Some of these messages already have a predefined message classification, which OVO maps where possible to a message group and severity level.

About Default Message Mapping

Table 4-2 shows how MPE/iX classifications are mapped to OVO Message Groups.

Table 4-2 Default Message Mapping on MPE/iX Managed Nodes

MPE/iX Classification	OVO Message Group
Database	Misc
DTC	Misc
Hardware	Hardware
Jobs	Job
Logging	Misc
MPE/iX	OS
Network	Network
Performance	Performance
Printer	Output
Security	Security
Spooler	Output
Storage	Backup

For details about the MPE/iX console messages that are intercepted, see the following:

- MPE/iX console template `MPE Console Messages` in the `Message Source Templates` window
- *Supplementary Guide to MPE/iX Templates*

Mapping Messages to OVO Security Levels

Table 4-3 on page 166 shows how MPE/iX messages are mapped to the OVO severity levels.

Table 4-3 MPE/iX and OVO Message Mapping Severity

MPE/iX Severity Level	OVO Severity Level
0	Normal
1	Normal
2	Warning
3	Critical

Mapping NMEV Markers

Messages from the MPE/iX operating system might contain so-called Node Management Event (NMEV) markers. OVO uses these markers to map MPE/iX console messages to the severity, message group, application, and object fields for OVO messages.

NMEV markers have the format `NMEV#pcc@aaa`, where:

`p` MPE/iX Message Severity mapped to OVO severity. If the severity is not in the range of 0 to 3, it is an invalid marker and the pattern is treated as normal text. (See Table 4-3 on page 166 for the possible values.)

`cc` MPE/iX Message Class mapped to the OVO Object field (optional: values from 0 to 99). The MPE/iX message class is currently not used by MPE/iX. If this field is omitted, the default 00 is used.

`aaa` MPE/iX Application ID identifying the source of the message, mapped to the OVO Application field (optional: values from 0 to 310).

If the `@aaa` portion is omitted, it is set to the default value of @310. This maps the message to the message group `Misc` and the application `Console Event`.

Table 4-4 shows how NMEV markers are mapped in OVO.

Table 4-4 NMEV Marker Mapping

MPE/iX Application ID	OVO Message Group	Application/Operating System Subsystem
052	Performance	Laser/RX
053	Database	Allbase/SQL
194	Network	Public Networking
195	Network	Network-OSI
196	Network	Network-NS
198	Network	Network-SNA
200	Output	Ciper Devices
206	OS	I/O Services
211	Output	Native Mode Spooler
212	Output	Page Printer
213	Output	Device Manager
214	Storage	Printer,Tape,Spool
215	Storage	Software Resiliency
216	OS	Threshold Manager
217	Storage	Store/Restore
218	Job	Jobs/Sessions
220	OS	Process Mgr
221	Logging	System Logging
222	OS	Transaction Mgmt
224	Logging	User Logging
225	Hardware	SPU Switchover

Table 4-4 NMEV Marker Mapping (Continued)

MPE/iX Application ID	OVO Message Group	Application/Operating System Subsystem
226	OS	Reply Info Table
227	OS	System Manager
228	Output	High End Printer
229	Hardware	Diagnostic-System
230	OS	Command Interpreter
231	OS	System & Error Mgmt
232	OS	Label Management
233	Storage	Magneto-Optic Lib
234	DTC	Terminal I/O
235	DTC	DCC Surrogate
236	Storage	Labeled Tape
237	Security	MPE/iX Security
238	OS	Native Language
239	Hardware	UPS Monitoring
310	Misc	Console Event

Some of the entries in the OVO Message Group column are not configured as default OVO message groups when OVO is installed. Messages sent to those message groups are routed to the message group `Misc` as described in Table 4-3 on page 166. Create these message groups if you want those messages to be routed to groups other than `Misc`.

For example, the marker `NMEV#200@214` would generate a message with the severity `Warning`, in the message group `Storage`, concerning the application `Printer,Tape,Spool`.

If no OVO-to-MPE/iX mapping is available for an MPE/iX console message intercepted by OVO, the original MPE/iX classification is used as a default value and the message is displayed in the message group `Misc` until you configure a message group that more accurately suits your requirements. If you need different mapping, you can apply the OVO concept of message regrouping.

The OVO attribute mapping is defined in the following file:

`CONSDESC.COMMANDS.OVOPC`

This file is delivered by default with the MPE/iX agent installation.

For more information about how to configure this file to map NMEVs other than the ones defined in Table 4-4 on page 167, see “Generating a New NMEV Marker” on page 169.

Generating a New NMEV Marker

The OVO Console Interceptor supports all methods of generating NMEV event messages.

An NMEV event marker can be generated in the following ways:

- **TELLOP**

  Inserting the marker into the text of a `TELLOP` command.

- **PRINTOP**

  Inserting the marker into a parameter for calling the `PRINTOP` command.

- **NMEVENT**

  Calling the `NMEVENT` intrinsic by way of a program.

The NMEV marker string can be placed in `TELLOP` messages. This string can be useful for generating messages to OVO from within jobs or sessions. The `PRINTOP` intrinsic can also be used to send the NMEV marker to the console from programs. In both cases, the MPE/iX Console Interceptor processes the message. In all cases, the valid NMEV marker is stripped from the text of the message before the messages is forwarded to the message browser.

The NMEVENT intrinsic performs a function similar to `opcmsg(3)`. Some networking and other third-party applications may use this intrinsic. However, it is recommended that all applications generating OVO events use the `opcmsg(3)` call instead of the NMEVENT API.

You can add new NMEV markers to the `consdesc` file so that OVO can map user-defined NMEV markers to user-defined OVO message groups, application, and object fields. You should not create user-defined IDs because it is possible that the user-defined application IDs could conflict with HP-defined ID if HP added entries to the default `consdesc file` in the future.

The default `consdesc` file is located in the following directory on the management server:

```
/var/opt/OV/share/databases/OpC/mgd_node/vendor/hp/s900\
/mpe-ix/<ito_version>/cmds/consdesc.Z
```

This file is compressed. You must uncompress it before you can start editing it. Place your customized version of this file into the following directory on the management server

```
/var/opt/OV/share/databases/OpC/mgd_node/customer/hp\
/s900/mpe-ix/cmds/consdesc
```

Distribute the default `consdesc` file using the `Install / Update OVO Software and Configuration` window. You do not need to compress it. OVO does that for you.

After distribution, the file is located on the MPE/iX managed node at:

```
CONSDESC.COMMANDS.OVOPC
```

NOTE

You must restart the MPE/iX console interceptor on your MPE/iX managed node to activate the changes in the following file:

```
CONSDESC.COMMANDS.OVOPC
```

To restart the MPE/iX console interceptor on your MPE/iX managed node, enter the following:

```
/opt/OV/bin/OpC/opcagt -start
```

No SNMP Trap and Event Interception

The OVO event interceptor is not supported on MPE/iX managed nodes.

Types of Default Monitored Objects

For information about the default monitored objects used by OVO on MPE/ix managed nodes, see the *Supplementary Guide to MPE/iX Templates*.

Tips for Configuring File Names

You can provide `actions/cmds/monitor` command files for MPE/iX managed nodes on the management server in:

```
/var/opt/OV/share/databases/OpC/mgd_node/\
customer/hp/s900/mpe-ix
```

If you do so, keep the following in mind:

- **Character Length**

  Make sure the file names are not longer than 8 characters.

- **Special Characters**

  The characters underscore (_) and dash (-) are not allowed.

- **Case**

  MPE/iX does not distinguish between uppercase and lowercase letters.

- **ASCII Format**

  Only ASCII files are supported. Binaries for automatic distribution to MPE/iX are not supported because the MPE/iX file code is not known to the management server.

Types of Default Applications

The following default applications are available for MPE/ix managed nodes:

- ❏ Broadcast
- ❏ Disk Space
- ❏ Lan Console
- ❏ Monitor Console
- ❏ Physical Terminal
- ❏ Print Status
- ❏ Processes
- ❏ Virtual Terminal
- ❏ Vt3K (Block Mode)
- ❏ Vt3K (Type Ahead)

NOTE *All applications except Physical Terminal and Virtual Terminal:*

If the default user has been changed by the operator, you must supply a password.

For more information, see the *OVO Administrator's Reference* and the *Supplementary Guide to MPE/iX Templates*.

About "Broadcast"

OVO application that enables you to issue the same command on multiple systems in parallel.

Default User `MGR.OVOPR`

Default Password None is required. Application is started through the OVO action agent.

About “Disk Space”

OVO shows the current disk usage.

Command Issued **discfree d**

Default User MGR.OVOPC

About “Lan Console”

OVO allows the user to use all console commands.

Command Issued **netcons.bin.ovopc lancon**

Default User MANAGER.SYS

About “Monitor Console”

OVO displays all messages sent to the MPE/iX console.

Command Issued **netcons.bin.ovopc**

Default User AGENT.OVOPC

About “Physical Terminal”

The script defined as the `Physical Terminal` command in the `Managed Node Configuration` window is called when starting the physical terminal application.

Default User MANAGER.SYS

Default Password None is configured.

About “Print Status”

Shows the current status of spooling systems.

Command Issued **listspf**

Default User MGR.OVOPC

Default Password None required. Application is started through the OVO action agent.

About "Processes"

OVO displays the status of the running processes.

Command Issued **`showproc; pin=1;system;tree`**

Default User `MANAGER.SYS` because `showproc` requires SM capability.

About "Virtual Terminal"

For a virtual terminal connection to MPE/iX systems, OVO uses **vt3k** as virtual terminal emulator for HP 3000 nodes running MPE/iX. For ARPA host name to NS node name mapping, see the section in the *OVO DCE Agent Concepts and Configuration Guide*.

Default User `MGR.OVOPR`

Distributing Scripts and Programs

For MPE/ix managed nodes, the platform selector and architecture identifier is the following:

```
hp/s900/mpe-ix
```

Location of User Scripts and Programs

Table 4-5 shows the location of user scripts and programs provided on the management server.

Table 4-5 Location of User Scripts and Programs on the Management Server

Script/Program	Location
Automatic actions, operator-initiated actions, and scheduled actions	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /hp/s900/mpe-ix/actions/*`
Monitoring scripts and programs used by the monitoring agent and the logfile encapsulator	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /hp/s900/mpe-ix/monitor/*`
Scripts and programs called through command broadcast or started from the Application Desktop	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /hp/s900/mpe-ix/cmds/*`

About Temporary Directories

Table 4-6 shows the temporary directories for distributed scripts and programs on the managed nodes.

Table 4-6 Temporary Directories for Distributed Scripts and Programs on the Managed Nodes

Managed Node	Operating System	Temporary Directory
HP 3000/900	MPE/iX	TMPACT.OVOPC TMPCMDS.OVOPC TMPMON.OVOPC .ZOVOPC (for compressed files)

About Target Directories

Table 4-7 shows the target directories for distributed scripts and programs on the managed nodes.

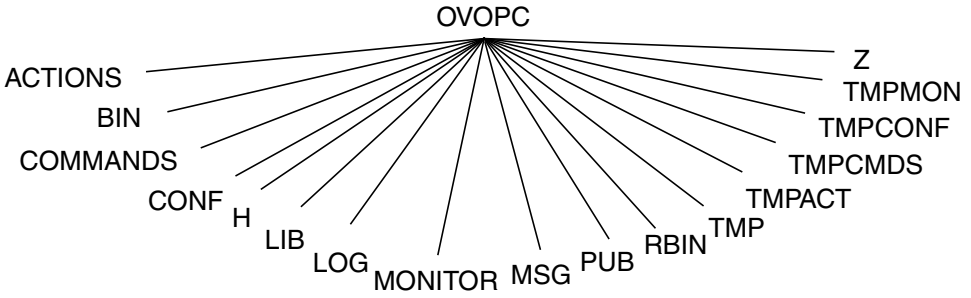
Table 4-7 Target Directories for Distributed Scripts and Programs on Managed Nodes

Managed Node	OS	Directory	Access Rights
HP 3000/900	MPE/iX	ACTIONS.OVOPC cap=BA,IA,PM,MR,DS,PH	R,X,L,A,W,S:AC
		COMMANDS.OVOPC cap=BA,IA,PM,MR,DS,PH	R,X:ANY;L,A,W,S:AC
		MONITOR.OVOPC cap=BA,IA,PM,MR,DS,PH	R,X,L,A,W,S:AC

Organization of Managed Nodes

Figure 4-1 shows how software is organized on MPE/iX managed nodes.

Figure 4-1 OVO Software on MPE/iX Managed Nodes



During installation, OVO creates the accounts OVOPC and OVOPR. The group PUB.OVOPC is not used by OVO.

Location of Files

On MPE/iX managed nodes, files are located as follows:

- **Process-related Files**

  TMP.OVOPC

- **Agent Configuration Files**

  CONF.OVOPC

About the Default OVO Operator

On MPE/iX, the default operator, MGR.OVOPR, is assigned the dummy group, PUB.OVOPR, as home group. The MPE/iX default capabilities and access rights are applied for this account and group.

About the System Resource File

OVO applies changes in the following system resource file:

`SYSSTART.PUB.SYS`

This resource is used for OVO agent startup. You can modify it only if you have set the `Automatic Update of System Resource Files` option.

Mapping ARPA Host Names to NS Node Names

Table 4-8 describes ARPA hostname to NS node name mapping.

Table 4-8 ARPA to NS Node Name Mapping

ARPA Hostname	NS Node Name	Comment
`hpbbli`	`smarty`	Different node names but same domain
`hpsgmx18.sgp.hp.com`	`hpsgmx18.sgp.hpcom`	Same node names, but managed node belongs to different domain than management server
`topaz.sgp.hp.com`	`nstopaz.mis.hpsg`	Node names and domains differ

About the vt3k Operation

OVO uses the **vt3k** operation for the following:

- **Software (De-)Installation**

  Installing and de-installing software on an MPE/iX managed node.

- **Virtual Terminal Connection**

  Connecting a virtual terminal from the operator Application Desktop or the administrator Application Bank to an MPE/iX managed node.

The **vt3k** operation requires the HP Network Services (NS) node name of the remote HP 3000. However, nodes selected from the map are identified by the ARPA hostname. By default, the ARPA hostname of a selected node is truncated after the first dot (`.`). The first part of the ARPA hostname becomes the NS node name for the vt3k operation. This mechanism assumes that the truncated name identifies a node in the same NS domain as the management server because a fully qualified NS node name is unavailable.

NOTE You can configure the `vt3k.conf` file at any time. You do not have to exit the OVO GUI or restart any OVO services.

Problems with ARPA Hostnames and NS Node Names

Two problems can occur when mapping ARPA hostnames to NS node names:

- Truncated ARPA host name differs from the NS node name.
- MPE/iX managed node belongs to a different NS domain.

Avoiding Problems with the OVO Mapping File

To avoid problems with ARPA hostnames and NS node names, OVO supports the mapping file below:

`/etc/opt/OV/share/conf/OpC/mgmt_sv/vt3k.conf`

This file can be a symbolic link to one of the following files:

- `/etc/xnmvt3k.conf`
- `/etc/opt/OV/share/conf/xnmvt3-k.conf`

The latter file is used by OVO for remote logins on HP 3000 systems through vt3k.

Resolving ARPA Hostname to NS Node Names

OVO resolves the ARPA host name to NS node name as follows:

1. **Searches for the full ARPA hostname.**

   OVO searches for the first line in the `vt3k.conf` file that begins with a matching ARPA hostname. If it finds a matching name, OVO adds the NS node name in the second column of the vt3k operation.

2. **Searches for the truncated ARPA hostname.**

   If OVO does not find a matching ARPA hostname in the `vt3k.conf` file, it repeats the search with only the first part of the ARPA host name (the part preceding the first dot). If it finds a matching name, OVO adds the NS node name in the second column to the **vt3k** operation.

3. **Adds the truncated ARPA hostname.**

   If OVO does not find a matching name in the `vt3k.conf` file. or if the mapping file does not exist (the default case), OVO adds the truncated hostname to the **vt3k** operation. In this case, the name identifies a node in the same NS domain as the management server. A fully qualified NS node name is missing.

Types of Libraries

Table 4-9 describes the managed node libraries for OVO A.05.xx, A.06.xx, and A.07.xx.

Table 4-9 Libraries for the OVO Managed Nodes

	Item	OVO A.05.xx	OVO A.06.xx	OVO A.07.xx
DCE	Library	**libapixl.lib.ovopc**	**libapixl.lib.ovopc**	**libapixl.lib.ovopc**
	Libraries linked to the OVO library	N/A	N/A	N/A
	Link and compile options	info="Ih" link cap=pm,ia,ba,mr,ds; & rl=libcinit.lib.sys ;& xl=opcapixl.lib	info="Ih" link cap=pm,ia,ba,mr,ds; & rl=libcinit.lib.sys ;& xl=opcapixl.lib	info="Ih" link cap=pm,ia,ba,mr,ds; & rl=libcinit.lib.sys ;& xl=opcapixl.lib
	Description	N/A	N/A	N/A

About the Include File

On a HP 3000/900 platform running MPE/iX managed nodes, use the following include file:

```
OPCAPI.H.OVOPC
```

About the Makefiles

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

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

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

```
Makef.mpe-ix
```

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

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

5 About Novell NetWare Managed Nodes

In this Chapter

This chapter explains how to install and configure HP OpenView VantagePoint Operations (OVO) on Novell NetWare managed nodes.

Installation Requirements

This section explains OVO hardware and software requirements for Novell NetWare managed nodes.

Hardware Requirements

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

- **Server**

  Novell NetWare Server 4.1x, 5, and 5.1 and 6

- **Disk Space**

  - *NetWare Server*

    10 MB on each NetWare server in the `SYS: volume`

  - *Software Depot*

    20 MB disk space for the software depot on the Windows 95/98/NT/2000 server.

- **Additional RAM**

  - *NetWare Server*

    7 MB additional free RAM on the NetWare server:

    — 4 MB for the OVO agent

    — 1 MB for TIRPC

    — 0.5 to 2 MB for the NetWare Management Agent and XCONSOLE (*optional*)

    At least 32 MB of server RAM is suggested for fair performance (depending on the OS version).

  - *OVO Agent*

    16 MB additional free RAM for the OVO agent if you are using NetWare SFT III file servers.

Software Requirements for the Managed Nodes

Before installing OVO, make sure the following software is installed on Novell NetWare managed nodes:

- **Operating System**

  For a list of operating system versions supported by OVO, see the *VPO Installation Guide for the Management Server*.

- **TIRPC**

  If it is not already present on the system, TIRPC is supplied with the OVO agent software. It is installed during OVO agent installation.

NOTE

On NetWare 6, PKERNEL service and TIRPC *cannot* run concurrently. This means that NFS and NDPS services will be unavailable while OVO Agent is running. The OVO Agent installation will disable starting of PKERNEL in `AUTOEXEC.NCF` file if it is present.

- **TCP/IP Services**

  TCP/IP services must be configured (including name resolution), running, and started automatically.

- **Network FRAMING Types**

  Network FRAMING types must be configured. Ethernet II frame type is required.

- **CLIB.NLM**

  `CLIB.NLM` version 4.10 or higher must be installed.

- **SNMP Daemon** (optional)

  SNMP daemon must be configured, running, and started automatically if monitoring and trap interception is required.

- **XCONSOLE** (optional)

  `XCONSOLE.NLM` must be installed and configured on each server only if you want remote access from the Management Server. XCONSOLE is part of Novell products like Flex-IP and NetWare/IP. XCONSOLE must be configured and running. Remote console access (through telnet) must be allowed.

- **Novell NMA** (*optional*)

  If Novell NMA is installed and configured on the NetWare server, it is recommended that Trap Interceptor templates from group NetWare are deployed on the NetWare managed node. Those templates will take advantage of information provided by NMA and forward the events detected by it to the management server message browser. In this case, it is recommended that Monitor Agent templates are *not* deployed on the managed node.

- **DSEVENT.NLM**

  Default OVO instrumentation (`VENDOR.NLM`) requires the presence of `DSEVENT.NLM` on the system in order to catch events raised by the NDS system. This module is distributed by default with the operating system and should *not* be removed from the system.

Software Requirements for the Depot Server

Before installing OVO, make sure the following software is installed on Novell NetWare depot server system:

- **Microsoft Windows**

  Microsoft Windows 95, 98, NT or 2000 Operating System.

- **Novell Client**

  Novell Client 32 for Windows must be installed on the system to be used as the depot server.

Installing and De-installing Agents

This section describes how to install and de-install Novell NetWare managed nodes.

Tips for Installing Agents

When installing Novell NetWare managed nodes, follow these guidelines:

- **Installation Logfiles**

  Each step of the installation is recorded in the logfile `vpoinst.log` on the NetWare depot server system.

  The file is placed in the base directory of the OVO NetWare depot:

  `C:\Program Files\VPO`

  By default, the location can be changed during depot installation.

  If you encounter problems during the installation, check this logfile for warnings and errors, and retry the installation.

- **Novell Directory Services (NDS)**

  The installation process creates the following file on each managed node:

  `SYS:/OPT/OV/BIN/OPC/INSTALL/NDSINFO`

  This file contains information about the position of the managed node in the NDS directory tree so that the OVO agent. The NLMs can log in to NDS when they are started.

- **Changed Configuration Files**

  Each configuration file on the NetWare server that is changed by the OVO installation process (for example, `AUTOEXEC.NCF`) is stored in the same directory with the extension.`VPO` in case you need to restore the old system. This is also done during OVO agent de-installation.

- **OVO Event Interceptor and SNMPLOG.NLM**

  The OVO event interceptor and the Novell `SNMPLOG.NLM` *cannot* be used together. If you experience problems with the OVO event interceptor, make sure the `SNMPLOG.NLM` is not loaded. If you need `SNMPLOG.NLM` to report traps, disable the OVO event interceptor.

❏ **UDP Echo Services**

The OVO agent monitors the connection from the NetWare server to OVO management server by sending the UDP echo packages. The UDP echo service must, therefore, be enabled on the OVO management server. Verify that the echo service is *not* disabled in the following file:

`/usr/adm/inetd.sec`

The echo service is enabled if it is not listed in the `inetd.sec` file.

❏ **UDP Protocol**

If you use UDP protocol for agent-server communication, set the data array size to 2048 bytes or less. If the data array size is not set in this way, the communication fails for larger messages.

To set the size of data array, use the following in the in `opcinfo` file:

`OPC_RPC_ARRAY_SIZE`

When using the UDP protocol, the default value for data array size is 2048 bytes.

❏ **PATH**

`PATH` cannot be changed during runtime on Novell NetWare managed nodes. All actions, monitors, and commands must be either fully qualified or must reside in `PATH`. `PATH` must be set before the OVO agents are started.

❏ **Unsupported OVO Agent Functionality**

A subset of the OVO agent functionality is *not* supported or is implemented in a slightly different way on the NetWare platform.

- *opcmsg*

  The `opcmsg(1)` command and `opcmsg(3)` API are not implemented.

- *opcmon*

  The `opcmon(1)` command is not implemented. The `opcmon(3)` API is implemented.

- *MSI*

  MSI on the managed node is not implemented.

- *Message Interceptor*

  The message interceptor is not implemented.

- *Event Correlation*

  Event Correlation is not implemented.

- *ANS*

  Advanced Network Security is not implemented.

- *opcswitchuser*

  The `opcswitchuser` command is not implemented.

- *Security Level*

  Only the regular level of security is implemented.

- *Subagent Registration File*

  The subagent registration file is not encrypted:

  `SYS:/VAR/OPT/OV/CONF/OPC/AGTREG`

- *Tracing*

  Tracing cannot be switched on and off during agent operation.

- *vpofiles*

  During the installation, a file `SYS:/VAR/OPT/OV/CONF/OPC/VPOFILES` is created. It contains the files that will be removed during deinstallation of the agent. Do *not* remove this file, otherwise deinstallation of the OVO Agent will fail.

- *RPCNET.CFG (on NetWare 6)*

  To prevent problems with RPC configuration on NetWare 6, TIRPC configuration file `RPCNET.CFG` has been moved from `SYS:\ETC` to OVO configuration directory `SYS:/VAR/OPT/OV/CONF/OPC`. This file should *not* be modified or deleted.

  `RPCNET.CFG` will be removed upon de-installation of the OVO agent from the NetWare server.

- *opcagt*

  The `opcagt(1)` command implementation differs from the implementation on other platforms. Only one instance of the `opcagt` command can be started on NetWare. Starting the `opcagt(1)` command starts the OVO agent service. It is a common practice in NetWare that a service opens its own virtual screen on the console screen. The operator uses this to control the service. The OVO agent opens a separate virtual screen on NetWare server console when started. By selecting the options in the menu of the OVO agent screen the operator is able to start and stop the OVO agents and query the agents status.

  The following actions can be executed by the OVO agent processes:

  `Display OVO Agent Status` Prints the status of OVO agents to the console.

  `Start OVO Agents` Starts or re-initializes the other OVO Agent processes (equivalent to `opcagt -start`).

  `Stop OVO Agents` Stops all OVO agent processes except for the message agent and the control agent functionality (equivalent to `opcagt -stop`).

  `Kill OVO Agents` Stops all OVO agent processes (equivalent to `opcagt -kill`).

  The console user interface is implemented with the standard NWSNUT services so that the standard NetWare console look-and-feel is achieved.

- Multi-Byte Locales

  Netware agent is *not* supported in multi-byte locales - such as Japanese, Korean, etc.

About the Installation Process

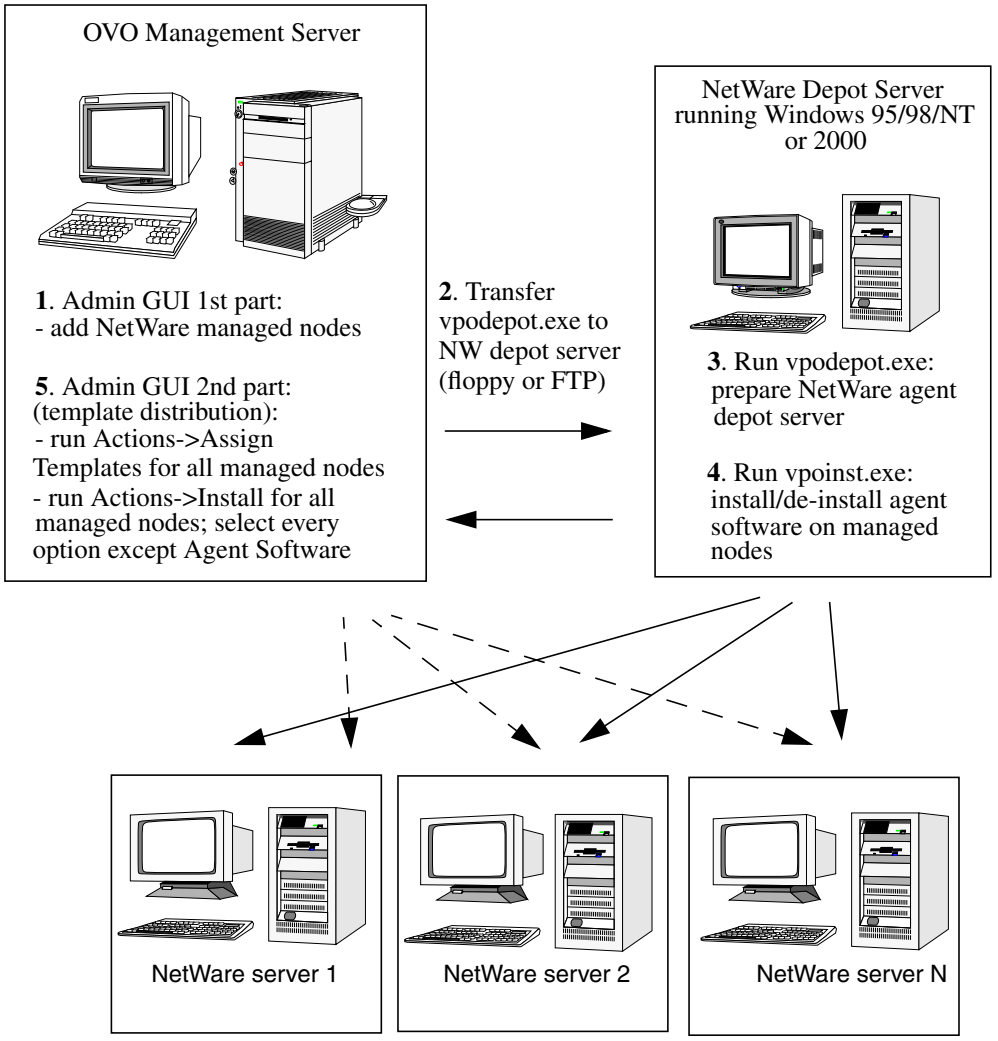
The process for installing the OVO agent software on Novell NetWare managed nodes differs from the standard installation process used for other platforms. The NetWare agent installation is semi-automated and depot-server-based.

The process for installing the OVO agent software on Novell NetWare managed nodes takes place in two locations:

- **OVO Administrator GUI**
  - Adding the managed nodes to the `OVO Node Bank`.
  - Assigning and transferring templates to the managed nodes.
- **NetWare Depot Server**
  - Running `vpodepot` on the depot server installs OVO installation software on Windows machine.
  - Installing the OVO agent software on the managed nodes by running `vpoinst.exe`.

Figure 5-1 on page 195 shows all installation steps made on the OVO management server and on the Novell NetWare depot server.

Figure 5-1 Installing the OVO Novell NetWare Agent Package



To Install Agents

To install OVO agents on Novell NetWare managed nodes, follow these steps:

1. **Make sure the Novell NetWare nodes are known to OVO and are accessible.**

   From the OVO administrator GUI, add your Novell NetWare managed nodes to the `OVO Node Bank` window.

NOTE

The agent software package is *not* automatically copied to the NetWare depot server. This must be done manually as explained in the following step.

2. **Copy the installation package to the NetWare depot server.**

   The installation package (`vpodepot.exe`) is located in the following directory on the management server:

   ```
   /var/opt/OV/share/databases/OpC/mgd_node/vendor/\
   novell/intel/nw/A.07.10/RPC_SUN_TCP/vpodepot.exe
   ```

   From the OVO Management Server, copy `vpodepot.exe` to depot server.

3. **Install the installation package on the NetWare depot server.**

   On the depot server, execute the `vpodepot.exe` file.

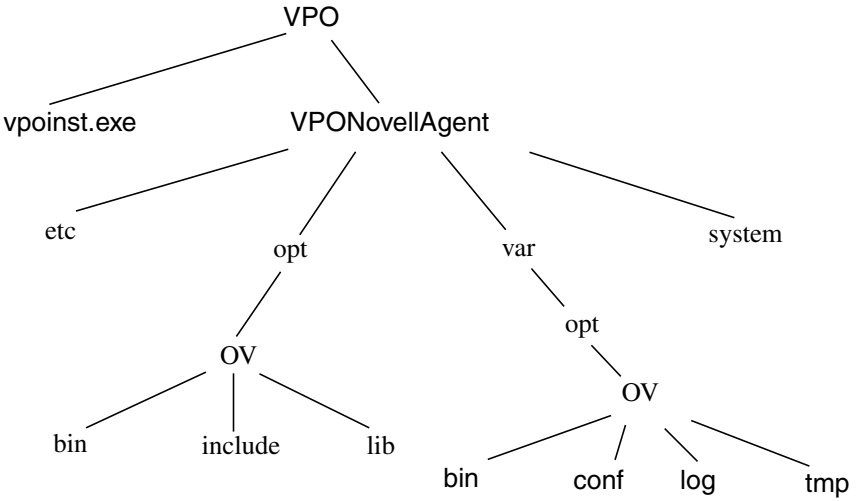
   The InstallShield installation program, unless it is changed during the installation, creates the following directory:

   `C:\Program Files\VPO`

   InstallShield also adds the `vpoinst.exe` program to the Windows `Start` menu.

   Figure 5-2 shows the file tree layout of the directory `C:/ Program Files` after `vpodepot.exe` has been executed.

Figure 5-2 File Tree Layout of the OVO NetWare Depot Server



4. **Install the OVO agent software on the Novell NetWare managed nodes.**

CAUTION

Do *not* stop the OVO management server processes when installing the OVO agent software.

On the depot server, do the following:

a. **Execute the vpoinst.exe file.**

In the initial dialog box, the following menu options are displayed:

`Install`	Installs the OVO agent, and gives the additional option of backing up any already-installed OVO agent in the case of future reinstallation.
`Deinstall`	Automatically de-installs the OVO agent from selected NetWare servers. It is possible to reinstall the previous version of the OVO agent, if there is one on the target server, and reinstate the previous version of the OVO agent. The deinstallation procedure will restore system files to the same state as before the last installation of the OVO agent. If `Restore old VPO version` is selected, and an old OVO installation is available on the NetWare server, it will be restored.
`Exit`	Immediately exits the procedure.
`Next>>`	Proceeds to the next step.

b. **Start the installation.**

Select the `Install` option and click on `Next>>`.

The `Select NetWare Nodes` dialog box appears. The names of all available NetWare servers detected on the network are shown in the box on the left.

NOTE

In order to avoid having multiple `OPC_OP/OPC_GRP` in the lower directory contexts, it is possible to create a single `OPC_OP/OPC_GRP` user/group in the upper level of the directory structure. In that case make sure that the box `Do not create OPC_OP/OPC_GRP` is checked while installing the NetWare agent.

c. **Add NetWare nodes.**

Use the following menu options:

`Add>>` Adds individual nodes to the list. You add a NetWare server by highlighting it and clicking `Add>>`. The server then appears in the box on the right.

`Add all` Adds all nodes to the list.

`<<Remove` Removes individual nodes from the list. You remove a NetWare server by highlighting it and clicking `<<Remove`. The server then appears in the box on the left.

`Preserve old VPO Installation (if available)` Saves the existing installation, if one exists, on the target servers for future restoration.

Only one version of OVO can be preserved using this option.

`Install in batch mode` Causes the installation of the OVO agent on the specified servers to proceed automatically, with only one prompt for specific OVO configuration which will be applied to all NetWare nodes. If you choose this option, all NetWare managed nodes specified must belong to the same management server.

If you choose this option, the next two windows will appear only once, and their contents will be used for all selected nodes.

Then click `Next>>` to proceed to the `VPO Agent Configuration` screen.

d. **Select the user and group to be used for running actions on the managed node.**

From the VPO Agent Configuration screen, you can select the user and group which will be used for running actions on the managed node.

NOTE

It is possible to use an existing user with administrative rights. However, all applications in the Application Bank in the OVO management server *must* be updated to include the correct username and password.

In the Management Server field, you must enter the name of the management server which will be used to manage the OVO agent on the NetWare node.

e. **Optional: Configure OPCINFO flags.**

Click on Advanced Options to configure options in the OPCINFO file on the managed node.

The Advanced Options screen enables certain OPCINFO flags to be automatically distributed to all NetWare nodes without the need to manually update the configuration files.

In this screen you are presented with the following checkboxes:

OPC_IP_ADDRESS Adds OPC_IP_ADDRESS to the OPCINFO file.

OPC_RESOLVE_IP Adds the OPC_RESOLVE_IP to the OPCINFO file.

Edit OPCINFO Enables you to manually edit the contents of the OPCINFO file.

CAUTION

Use the Edit OPCINFO option at your own risk.

f. **Copy the files to the NetWare server.**

The installation checks if it is necessary and possible to create the user selected in the `Configuration` dialog box. If it is possible, the installation creates the requested user in the current context and set the administrative rights for that user. The installation also checks if the OVO agent is already running on the target node. If so, this node is skipped.

When the configuration is complete, the installation copies OVO modules and files to the NetWare server, with the old installation preserved, if you selected this option. The installation also prepares and copies `OPCINFO` and `NDSINFO` (for executing actions) to the appropriate directory.

5. **Inform the management server that the agent software has been successfully installed on the new OVO managed nodes.**

In the management server command line, enter the following:

```
/opt/OV/bin/OpC/opcsw -installed <node_name>
/opt/OV/bin/OpC/opchbp -on <node_name>
```

TIP

At this point you should assign your templates to the NetWare managed nodes, and distribute the templates, actions, monitors, and commands. For more information about assigning and distributing templates, see the *VPO Administrator's Guide to Online Information*.

After successfully installing the OVO agent, TIRPC is restarted, if necessary, and the OVO agent is started on the managed nodes.

Removing Older Agents

If an older OVO agent package is no longer required and is not installed on any managed node, you can remove it by running the following:

```
/opt/OV/bin/OpC/install/rm_opc.sh novell/intel/nw \
<VPO_version>
```

In this command, *<VPO_version>* is the version of OVO that supports this agent platform (for example, A.07.10).

About Preconfigured Elements

This section describes preconfigured templates, template groups, and applications used by OVO on Novell NetWare managed nodes.

About SNMP Trap and Event Interception

The OVO event interceptor is supported on Novell NetWare 4.1x, 5.x, and 6.0 with NMA 2.1, 2.6 or 2.7.

There are two preconfigured templates for Novell NetWare:

- **NetWare NMA 2.1/2.6 Threshold Traps**

  Filter traps originating from the NetWare NMA when one of the 24 NMA thresholds is exceeded.

- **NetWare NMA 2.1/2.6 Traps**

  Filter the 378 traps that can be generated by the NMA module when an important event on the NetWare server occurs.

NOTE Local event interception is supported only with Network Node Manager (NNM) version 6.2.

Types of Default Applications

This section describes the default applications in the following application groups:

- **NetWare Tools**

  See “Monitoring Performance” on page 206.

- **NetWare Config**

  See “About the NetWare Config Window” on page 206.

- **NetWare Performance**

  See “About the NetWare Performance Window” on page 207.

About Novell NetWare Management Agent (NMA)

If NMA is present on the managed node, it is recommended that Trap Interceptor templates are deployed to the managed node. It is *not* advisable to deploy Monitor Agent templates together with the Trap Interceptor templates to the same managed node. If NMA is *not* present, Monitor Agent templates provide the appropriate substitute. NMA is not required for NetWare managed node monitoring.

You can obtain current and historical trend data and set alarm thresholds for trend parameters on NMA 2.1 NetWare file servers. You can also obtain information about the server’s configuration, NLM files, memory usage, adapters, network interfaces, disks, disk controllers, volumes, queues, users, connections, open files, and installed software.

For print servers, NMA 2.1 or later provides queue information that is not available for servers running older versions of NMA.

About the NMA 2.1 Agent

The NMA provides real-time server performance information about the NetWare server alarms. These alarms are sent to the network and system management consoles. Or the alarms are processed locally by the OVO agent, and then forwarded to the OVO management console.

The NMA 2.1 agent is a set of NetWare agent NLMs that must be deployed on each NetWare server that you want to manage from the OVO console or Novell ManageWise console.

The NetWare agent NLMs include the following:

- **NWTRAP.NLM**

  Over 400 traps with Novell NetExpert help text

- **HOSTMIB.NLM**

  NetWare Server SNMP Host Resources MIB

- **SERVINST.NLM**

  NetWare Server SNMP instrumentation

- **NTREND.NLM**

  NetWare Server server-based trending

All NetWare servers from Novell, including all 4.x, 5.x and 6 NetWare servers, SFT III servers, SMP servers, and Mirrored Servers, are supported by NMA. These agents are all provided and supported by Novell and can be purchased as a separate part numbers from the Novell ManageWise console.

Monitoring Performance

Novell NMA 2.1 Agent NLMs enable you to monitor performance statistics, such as CPU utilization and the number of users and connections, as well as memory and disk usage (including permanent and allocated memory, and dirty and allocated cache buffers).

Server faults are managed by monitoring the server's key parameters. These conditions are monitored directly at the server and then passed to the OVO agent through SNMP traps.

You can enable NMA monitoring by configuring the following NMA configuration files on the NetWare server:

- `NWTREND.INI`
- `TRAPTARG.CFG`

Configuration of these files is *not* part of the OVO configuration and distribution framework.

In addition to the monitors provided by NMA, you can also create your own OVO templates to monitor any integer MIB variables supported by NMA. With these templates you can monitor NetWare server variables not monitored internally by the NMA.

About the NetWare Config Window

The following application icons are available by default in the `NetWare Config` window:

- `Down & Reboot`
- `Down & Restart`
- `Restart NMA`

NOTE You *cannot* start `Down & Reboot` and `Down & Restart` on NetWare SFT III systems.

The user `opc_op` (or any other user with administrator's rights) can execute these application on the NetWare server.

About the NetWare Performance Window

In the `NetWare Performance` window, the following application icons are available by default:

- `Allocated Memory`
- `Cache Buffers`
- `Code & Data Memory`
- `CPU Utilization`
- `Logged-in Users`
- `Dirty Cache Buffers`
- `File Reads`
- `File Cache Hits`
- `File Writes`
- `File KReads`
- `File KWrites`
- `Free Redir Area`
- `KPackets Recvd #min`
- `KPackets Sent #min`
- `Memory Monitor`
- `Packets Recvd #min`
- `Packets Sent #min`
- `Queue Wait Time`
- `Ready Queue Jobs`
- `Ready Jobs (avg. KB)`
- `Total Packets Recvd`
- `Total Packets Sent`
- `Trend Graph`
- `Volume Free Space`

Applications from this bank execute as user `root` on the server, and make `SNMP GET` calls to collect performance data from the NetWare server.

About the NetWare Tools Window

From the In `NetWare Tools` window, the user `opc_op` (or any other user with administrator's rights) can execute all of the applications on the NetWare server except the Xconsole application, which is only used to run a NetWare console in an X window on the OVO console.

NOTE On NetWare SFT III systems, starting applications belonging to the NetWare Tools application group on the secondary IO Engine can cause problems if the secondary IO Engine is already in the state down. The secondary IO Engine may abend.

Types of NetWare Tools Applications

In `NetWare Tools` window, the following application icons are available by default:

- **Adapters**

  Determines I/O port address or interrupt conflicts by viewing a list of adapters.

  Default: **`adapinfo <server_name>`**

- **Boot the NetWare Server (NCF)**

  Stops and restarts (cold boots) the NetWare server, but does not exit the server.

  Default: **`itodown.ncf`**

- **Bound Protocols**

  Lists all the protocols bound to each network board in a server.

  Default: **`protocls <server_name>`**

  The number of packets sent and received over each protocol is also listed. By viewing the Bound Protocols object group, you can see which protocols have the most traffic.

- **Cold Boot the NetWare Server (NCF)**

  Stops and restarts the NetWare server. This is done by removing DOS before exiting.

  Default: **`itoreset.ncf <server_name>`**

- **Connections**

  Monitors the status of users and user connections.

  Default: **`conninfo <server_name>`**

  The difference between the data returned by the Connections action and by the Users action is the emphasis of the Connection action on data relating specifically to connections. This emphasis enables you to determine how busy the server really is and which connections and users are the busiest.

- **CPU Info**

  Returns information about devices including the CPU speed.

  Default: **`cpuinfo <server_name>`**

- **Disks**

  Enables you to get detailed information about the disk drives in a managed server.

  Default: **`diskinfo <server_name>`**

  Part of the detailed information provided by this action concerns the fault tolerance of a given disk partition. This information enables you to determine whether a hard disk is losing data integrity. A number in the redirected area indicates the number of data blocks that have been redirected to the Hot Fix™ Redirection Area to maintain data integrity.

  If you are checking NetWare SFT III systems, the disks from both file servers are displayed.

- **Display a File**

  Displays a file. That is, it copies the content of a file to standard output. This command is similar to the UNIX `cat` command.

  Default: **`showfile <file_name>`**

  You must start this command through the customized startup application so you can enter the additional parameters (for example, the name of an NLM).

- **Installed Software (NW)**

  Displays those products that have been installed on the server using `PINSTALL`.

  Default: **`instlsw <server_name>`**

  `PINSTALL` is a product from Novell used to install software packages such as NMA on NetWare Servers.

- **Load/Unload an arbitrary NLM**

  Loads a NLM.

  Default: **`itoload <nlm_name>`**

  Unloads a NLM.

  Default: **`itounload <nlm_name>`**

  You can start arbitrary NLMs with the `itoload` and `itounload` commands. You must started these commands through a customized startup so you can enter the additional parameters.

- **Memory Use**

  Monitors memory use.

  Default: **`meminfo <server_name>`**

  The memory-use action displays the following data:

  - `Alloc Memory Pool (KB)`
  - `Cache Buffer (KB)`
  - `Cache Movable Memory (KB)`
  - `Cache Non-Movable Memory (KB)`
  - `Code and Data Memory (KB) in NetWare 4.0 or higher`
  - `Permanent Memory Pool (KB) in NetWare 3.11 and 3.12 only`

- **Mirrored Devices**

  Provides information about mirrored devices.

  Default: **`mirrdevs <server_name>`**

- **NCP Info**

  Provides statistics about NetWare Core Protocol (NCP).

  Default: **`ncpinfo <server_name>`**

- **NetWare Agent Actions**

  The OVO NetWare agent includes some preconfigured actions. Most of the preconfigured actions are located in the file `VENDOR.NLM` in the vendor file tree. This is different to the approach usually adopted on Unix-like platforms and on NT, where each action is stored in a separate script or is executable. However, calling conventions for NMA preconfigured actions are the same as for Unix-like platforms. Actions can be called from templates and from applications in the `NetWare Application Bank` window.

  Some NetWare NCF scripts are implemented in addition to the actions provided in `VENDOR.NLM`.

NOTE For preconfigured actions that require an additional parameter *<server_name>*, enter the name of the NetWare server where the actions are being executed.

Types of NMA Applications

The NMA actions are described below.

NOTE Some actions take a while to execute. These actions are marked with an asterisk (*).

- **Network Interfaces**

  Displays interface information for each network board in a server.

  Default: **`netintrf <server_name>`**

  Use Network Interfaces as a troubleshooting tool to determine why a user cannot log in to a file server. If the frame types are different, you can change the frame type in the user's `NET.CFG` file, edit the user's frame type to match the server's frame type, and restart the user's system.

- **NLM Files***

  Determines which NLM files are currently loaded on the server. Includes NLM file version, release date and amount of memory used by the NLM.

  Default: **`currnlms <server_name>`**

- **ODI Info**

  Provides statistics about buffers for packets received and ECB requests.

  Default: **`odiinfo <server_name>`**

- **Open Files**

  Enables you to see which files are currently open, what volume they are reside in, who opened the files, and which connections are being used.

  Default: **`openfils <server_name>`**

- **Print Server**

  Displays information about printers and queues attached to print servers.

  Default: **`presvinfo <server_name>`**

- **Running Software***

  Displays currently running NLMs and their memory usage.

  Default: **`runsw <server_name>`**

- **Queues**

  Monitors queues, jobs in the queues, and servers attached to the queues.

  Default: **`quesinfo <server_name>`**

- **Set Parameters***

  Displays all settings for the server configuration.

  Default: **`setparms <server_name>`**

  This is the same information as is returned from the console `SET` command.

- **Trend Parameters***

  Displays information on the current trend parameters.

  Default: **presvinfo <*server_name*>**

- **System Summary**

  Returns information about the server name and uptime, as well as a description of the operating system.

  Default: **sysumary <*server_name*>**

- **Users**

  Monitors user activity to determine, amongst other things, the optimum server shutdown time:

  Default: **userinfo <*server_name*>**

- **Volume**

  Enables you to determine the exact amount of space available on every volume in the server.

  Default: **volinfo <*server_name*>**

  NetWare server disk storage space is divided into volumes. The Volume action enables you to view information about the volumes in a server running NMA software (for example, size, free space, how the volumes are distributed across disks, and who is using the space.

- **XCONSOLE**

  Opens a NetWare virtual terminal connection to node.

  This application requires only the remote console password (which may be different from the `opc_op` password).

  For NetWare SFT III servers, add another XCONSOLE application that calls the primary IO Engine rather than the MS Engine as in the default XCONSOLE application.

NOTE

The user name for the Xconsole application is `xconsole`. This is *not* a NetWare user name. It is only present in the OVO database as a warning that the password for the remote console access may be different from the user `opc_op` password.

Configuration Distribution and Update

For Novell NetWare managed nodes, the platform selector and architecture identifiers is the following:

```
novell/intel/nw
```

Location of User Scripts and Programs

Table 5-1 shows the location of user scripts and programs provided on the management server.

Table 5-1 Location of User Scripts and Programs on the Management Server

Script/Program	Location
Automatic actions, operator-initiated actions, and scheduled actions	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /novell/intel/nw/actions/*`
Monitoring scripts and programs used by the monitoring agent and logfile encapsulator	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /novell/intel/nw/monitor/*`
Scripts and programs called through command broadcast or started from the Application Desktop	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /novell/intel/nw/cmds/*`

About Temporary Directories

Table 5-2 shows the temporary directories for distributed scripts and programs on the managed nodes.

Table 5-2 Temporary Directories for Distributed Scripts and Programs on Managed Nodes

Managed Node	Operating System	Temporary Directory

Intel 486 or higher	Novell NetWare	`sys:/var/opt/OV/tmp/OpC/bin/actions`
		`sys:/var/opt/OV/tmp/OpC/bin/cmds`
		`sys:/var/opt/OV/tmp/OpC/bin/monitor`

About Target Directories

Table 5-3 shows the target directories for distributed scripts and programs on the managed nodes.

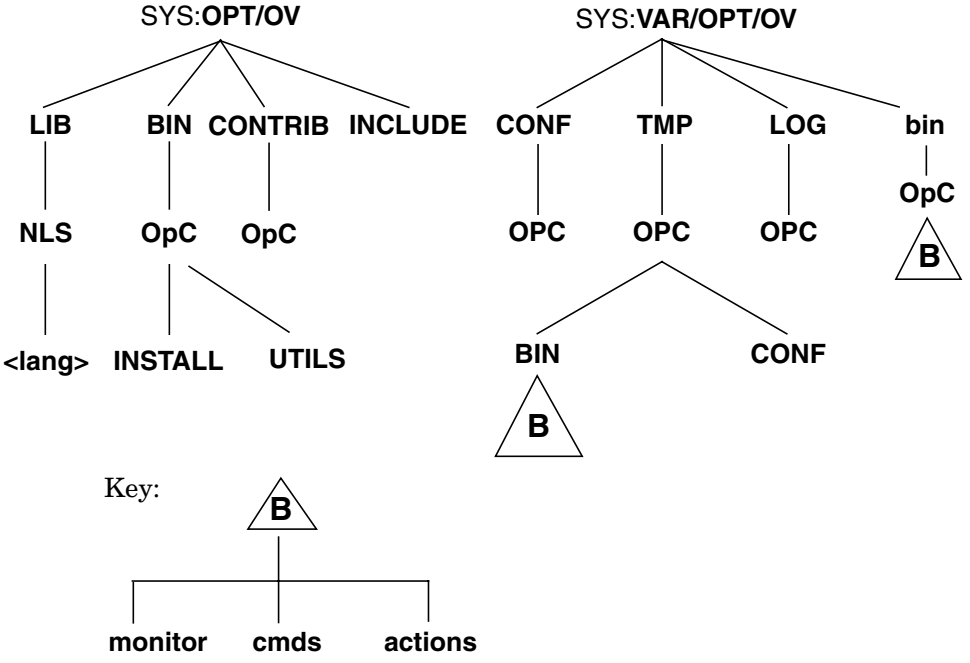
Table 5-3 Target Directories for Distributed Scripts and Programs on the Managed Nodes

Managed Node	Operating System	Target Directory	Access Rights
Intel 486 or higher	Novell NetWare	`sys:/var/opt/OV/tmp/OpC/bin/\ actions`	Administrator (full access)
		`sys:/var/opt/OV/tmp/OpC/bin/\ cmds`	Administrator (full access)
		`sys:/var/opt/OV/tmp/OpC/bin/\ monitor`	Administrator (full access)

Organization of Managed Nodes

Figure 5-3 shows how OVO software is organized on Novell NetWare managed nodes.

Figure 5-3 OVO Software on Novell NetWare Managed Nodes



During installation, OVO creates the `opc_op` account, which has the same security level as the user `ADMIN`. The `opc_op` account is a normal user account used to execute applications.

Location of Files

On Novell NetWare managed nodes, files are located as follows:

- **Process-related Files**

  `SYS:/var/opt/OV/tmp/OpC`

- **Agent Configuration Files**

  `SYS:/var/opt/OV/conf/OpC`

About the Default OVO Operator

During the installation of OVO agents, user OPC_OP and group OPC_GRP are added into NDS. User OPC_OP is used to run applications on the managed node. If you want, you can remove this user from NDS.

CAUTION If you remove OPC_OP, all applications in the Application Bank must be reconfigured to use an existing user with sufficient rights.

On Novell NetWare managed nodes, the OVO entry in the User Manager for Domains includes the following fields:

User Name	OPC_OP
Encrypted Password	Must be entered manually. Use NETADMIN or NWADMIN.
User-ID	N/A.
Group-ID	N/A
Description	Special user with rights equivalent to NetWare system administrator ADMIN.
Home Directory	Not set.
Login Shell	None assigned. NetWare works with login scripts.

Types of System Resources

During the agent software installation, OVO adds the agent startup command OPCAGT.NCF to the AUTOEXEC.NCF file.

The following resources are changed during installation:

SYS:/SYSTEM/AUTOEXEC.NCF

The following changes are made to this resource:

OPCAGT.NFC	Added to invoke the OVO agent for NetWare software if this command is not already present in this file.

Table 5-4 shows the TIRPC modules installed by OVO on Novell NetWare managed nodes.

Table 5-4 TIRPC modules installed by OVO on Novell NetWare

Module	Version
local_nd.nlm	1.10y
lwpnfsd.nlm	1.10y
netdir.nlm	1.10y
rpcbstub.nlm	1.10y
rpcinfo.nlm	1.10y
rpcstart.ncf	N/A
rpcstop.ncf	N/A
spx_nd.nlm	1.10y
tcp_nd.nlm	1.10y
tirpc.nlm	1.10y

About APIs

NOTE

The OVO commands and APIs `opcmon(1)`, `opcmack(1)`, and `opcmsg(1)` are *not* supported for Novell NetWare managed nodes.

OVO provides a set of application program interfaces (APIs) for Novell NetWare agents. These APIs facilitate interprocess communication (in particular, the parent-child relationship) between OVO agents and the custom NLMs.

Types of APIs

OVO provides the following APIs on Novell NetWare managed nodes:

`OVnlm_init()` Must be the first function called in the `main()` function of a OVO-enabled NetWare Loadable Module (NLM). This function initializes the OVO-related variables and returns a handle that must be used in all subsequent calls in this NLM.

`OVnlm_exit()` Must be used to terminate the execution of OVO-enabled NLM instead of the usual `exit()` function. This function is required to inform the parent OVO Agent NLM that the custom NLM has finished, and to provide exit code to the parent.

Examples of OVO-enabled NLMs

An example of an action, `HELLO.NLM`, is shown below. This action is executed by the OVO action agent and the output is captured as a OVO annotation.

```
#define OPC_NLM
#include "opcnwapi.h"
main( int argc, char **argv )
{
int handle;
    OVnlm_init( argc, argv, &handle );
    printf( "%s: Hello world!\n", argv[0] );
    OVnlm_exit( handle, 0 );
}
```

Another example of an action is contained in the following file on the management server:

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

Types of Libraries

Table 5-5 describes the managed node libraries for OVO A.05.xx, A.06.xx, and A.07.xx.

Table 5-5 Libraries for the OVO Managed Nodes

	Item	OVO A.05.xx	OVO A.06.xx	OVO A.07.xx
EZ-RPC	Library	**libopc.lib**	**libopc.lib**	**libopc.lib**
	Libraries linked to the OVO library.	No libraries linked.	libov.lib	libov.lib
	Link and compile options	-DOPC_NW -DNW -DCSM_ONC	-DOPC_NW -DNW -DCSM_ONC	-DOPC_NW -DNW -DCSM_ONC
	Description	libopc.lib is only used as archive library for API developers. It is not used at runtime.	libopc.lib and libov.lib are only used as archive libraries for API developers. They are not used at runtime.	libopc.lib and libov.lib are only used as archive libraries for API developers. They are not used at runtime.

About the Include File

On an Intel 486 or higher platform with Novell NetWare managed nodes, use the following include file:

```
SYS:.opt/OV/include/opcapi.h,opcnwapi.h
```

About the Makefile

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

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

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

```
Makef.nw
```

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

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

6 About Sequent DYNIX Managed Nodes

In this Chapter

This chapter explains how to install and configure HP OpenView Operations (OVO) on Sequent DYNIX managed nodes.

Installation Requirements

This section explains OVO hardware and software requirements for Sequent DYNIX managed nodes.

Hardware Requirements

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

- **Disk Space**

  10 MB (about 20 MB is required during software installation)

- **HPFS Partition**

  OVO agent must be installed on an HPFS partition. FAT partitions are not supported for OVO agent installation and operation.

- **Additional Swap Space**

  None

- **Additional RAM**

  4 MB

Software Requirements

Before installing OVO, make sure the following software is installed on Sequent DYNIX managed nodes:

- **Operating System**

  For a list of operating system versions supported by OVO, see the *OVO Installation Guide for the Management Server*.

- **System Parameters**

  For a list of kernel parameters, see the *OVO Administrator's Reference*. You can check and change the system parameters using the `menu` tool.

- **Sequent LAN**

  Sequent local area network product ptx/LAN version 4.0.1. or higher.

- **Sequent TCP/IP**

  Sequent TCP/IP product ptx/TCP/IP version 4.0.3 or higher.

- **Gradient NCS 1.5.1 NckNidl**

  If NCS is not found on the managed node, OVO installs `llbd` and `lb_admin` during the OVO agent software installation.

Installing and De-installing Agents

This section describes how to install and de-install Sequent DYNIX managed nodes.

Tips for Installing Agents

When installing Sequent DYNIX managed nodes, follow these guidelines:

- **Name of Management Server**

  The name of the management server must be known to the managed node. You must register the name of the management server on the name server or in the local host table:

  `/etc/hosts`

  You can verify this by using the `nslookup` command.

- **OVO Agent Software**

  The OVO agent software is installed on the `/opt` file tree. An empty `/opt` file tree is created during installation of the Sequent DYNIX/ptx operating system. By default, this file tree is positioned on the root file system. If there is not enough space for the installation of the OVO agents, create a symbolic link before installing OVO.

  For example, if `/bigdisk` is a local file system with enough free space, you would create the symbolic link as follows:

  ```
  mkdir -p /bigdisk/OV

  ln -s /bigdisk/OV /opt/OV
  ```

  In a cluster environment, make sure that `/bigdisk` is accessible from all cluster clients. That is, make sure that it is mounted from all client nodes. For example, the local file system `/bigdisk` on a cluster client must be mounted to exported file system `/bigdisk` on cluster server.

Installing Agents

For general installation instructions, see the *OVO Administrator's Reference*.

If errors occur during the installation, check the local installation logfile:

```
/tmp/pkgadd.log
```

De-installing Agents

For general de-installation instructions, see the *OVO Administrator's Reference*.

If errors occur during the de-installation, check the local de-installation logfile:

```
/tmp/pkgrm.log
```

About Preconfigured Elements

This section describes preconfigured templates, template groups, and applications used by OVO on Sequent DYNIX managed nodes.

No SNMP Trap and Event Interception

The OVO event interceptor is not supported on Sequent DYNIX/ptx managed nodes.

Types of Default Applications

For a list of default applications available for UNIX managed nodes, see the *OVO Administrator's Reference*.

Distributing Scripts and Programs

For Sequent DYNIX managed nodes, the platform selector and architecture identifier is the following:

```
sequent/intel/dynix
```

Location of User Scripts and Programs

Table 6-1 shows the location of user scripts and programs provided on the management server.

Table 6-1 Location of User Scripts and Programs on the Management Server

Script/Program	Location
Automatic actions, operator-initiated actions, and scheduled actions	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /sequent/intel/dynix/actions/*`
Monitoring scripts and programs used by the monitoring agent and the logfile encapsulator	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /sequent/intel/dynix/monitor/*`
Scripts and programs called through command broadcast or started from the Application Desktop	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /sequent/intel/dynix/cmds/*`

About Temporary Directories

Table 6-2 shows the temporary directories for distributed scripts and programs on the managed nodes.

Table 6-2 Temporary Directories for Distributed Scripts and Programs on the Managed Nodes

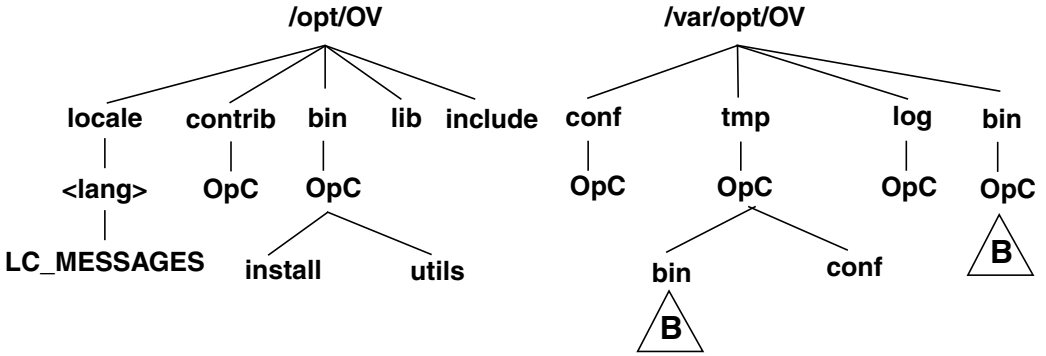
Managed Node	Operating System	Temporary Directory

Intel 486 or higher	Sequent DYNIX/ptx	`/var/opt/OV/tmp/OpC/bin/actions`
		`/var/opt/OV/tmp/OpC/bin/cmds`
		`/var/opt/OV/tmp/OpC/bin/monitor`

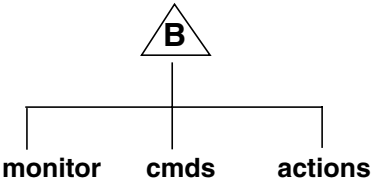
Organization of Managed Nodes

Figure 6-1 shows how OVO software is organized on Sequent DYNIX/ptx managed nodes, based on the typical SVR4 platforms.

Figure 6-1 OVO Software on Sequent DYNIX/ptx Managed Nodes



Key:



Location of Files

On Sequent DYNIX/ptx managed nodes, files are located as follows:

- **Process-related Files**

  `/var/opt/OV/tmp/OpC`

- **Agent Configuration Files**

  `/var/opt/OV/conf/OpC`

About the Default OVO Operator

If they do not already exist, the default OVO operator `opc_op` and group `opcgrp` are created.

About Default OVO Operator Entries

The default OVO operator is added to the following directory on Sequent DYNIX/ptx managed nodes:

`/etc/passwd`

Fields include the following:

`User Name` `opc_op`

`Encrypted Password` `*` (no login)

`User-ID` `777` (if still available) or next possible free number

`Group-ID` `77` (if still available) or next possible free number

`Description` Default OVO operator

`Home Directory` `/home/opc_op`

`Login Shell` `/bin/sh`

About Default OVO Operator Group Entries

The default OVO operator group is added to the following directory on Sequent DYNIX/ptx managed nodes:

`/etc/group`

Fields include the following:

`Group Name` `opcgrp`

`Encrypted Password` Empty

`Group-ID` `77` or higher

`Users` `opc_op`

`Description` Default OVO operator group

Types of System Resources

OVO makes changes in the following system resource files during installation:

`/etc/passwd`
`/etc/shadow` (if present) Entry for the default OVO operator and Protected Password Database (if present).

`/etc/group` Group entry for the default OVO operator

`/etc/init.d/opcagt` OVO startup and shutdown script.

`/etc/rc0.d` Creates the `K07opcagt` file.

`/etc/rc2.d` Creates the `S93opcagt` file.

`/etc/init.d/ncs` NCS startup and shutdown script.

`/etc/rc0.d` Creates the `K52ncs` file.

`/etc/rc2.d` Creates the `S76ncs` file.

Types of Libraries

Table 6-3 describes the managed node libraries for OVO A.05.xx, A.06.xx, and A.07.xx.

Table 6-3 Libraries for the OVO Managed Nodes

	Item	OVO A.05.xx	OVO A.06.xx	OVO A.07.xx
NCS	Library	**libopc.so**	**libopc.so**	**libopc.so**
	Libraries linked to the OVO library	/usr/lib/libnck.a /usr/lib/libinet.so /usr/lib/libnsl.so /usr/lib/librpc.so /usr/lib/libsec.a /usr/lib/libseq.a /usr/lib/libsocket.so /usr/coff/lib/libintl.a	/usr/lib/libnck.a /usr/lib/libinet.so /usr/lib/libnsl.so /usr/lib/librpc.so /usr/lib/libsec.a /usr/lib/libseq.a /usr/lib/libsocket.so /usr/coff/lib/libintl.a	/usr/lib/libnck.a /usr/lib/libnsl.so /usr/lib/librpc.so /usr/lib/libsec.a /usr/lib/libseq.a /usr/lib/libsocket.so /usr/coff/lib/libintl.a
	Link and compile options	-lopc -lnsp -lsocket	-lopc -lnsp -lsocket	-lopc -lnsp -lsocket
	Description	N/A	N/A	N/A

About the Include File

On an Intel 486 or higher platform with Sequent DYNIX/ptx managed nodes, use the following include file:

```
/opt/OV/include/opcapi.h
```

About the Makefile

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

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

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

```
Makef.ptx
```

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

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

7 About SGI IRIX Managed Nodes

In this Chapter

This chapter explains how to install and configure HP OpenView Operations (OVO) on Silicon Graphics Indigo (SGI) IRIX managed nodes.

Installation Requirements

This section explains OVO hardware and software requirements for SGI IRIX managed nodes.

Hardware Requirements

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

- **Disk Space**

  10 MB (about 20 MB is required during software installation)

- **Additional Swap Space**

  None

- **Additional RAM**

  None

Software Requirements

Before installing OVO, make sure the following software is installed on SGI IRIX managed nodes:

- **Operating System**

  For a list of operating system versions supported by OVO, see the *OVO Installation Guide for the Management Server*.

- **System Parameters**

  For a list of kernel parameters, see the *OVO Administrator's Reference*. You can check and change the system parameters using the `sysmgr` tool.

- **NCS**

  For SGI IRIX 6.2 or higher, install the following NCS 1.5.1 package:

  `license_eoe.sw.netls_server`

  If neither NCS nor DCE are found on the managed node, OVO installs `llbd` and `lb_admin` during OVO software installation.

- **NFS**

  For diskless operations, install SGI IRIX NFS on a cluster server.

Installing and De-installing Agents

This section describes how to install and de-install SGI IRIX managed nodes.

Tips for Installing Agents

When installing SGI IRIX managed nodes, follow these guidelines:

- **Name of Management Server**

  The name of the management server must be known to the managed node. You must register the name of the management server on the name server or in the local host table:

  `/etc/hosts`

  You can verify this by using the `nslookup` command.

- **OVO Agent Software**

  The OVO agent software is installed on the `/opt` file tree. If there is not enough space for the installation of the OVO agents, create a symbolic link before installing OVO.

  For example, if `/bigdisk` is a local file system with enough free space, you would create the symbolic link as follows:

  ```
  mkdir -p /bigdisk/OV
  ln -s /bigdisk/OV /opt/OV
  ```

  In a cluster environment, make sure that `/bigdisk` is accessible from all cluster clients. That is, make sure that it is mounted from all client nodes. For example, the local file system `/bigdisk` on a cluster client must be mounted to exported file system `/bigdisk` on cluster server.

- **Installation on NIS Clients**

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

Installing Agents

For general installation instructions, see the *OVO Administrator's Reference*.

If errors occur during the installation, check the local installation logfile:

```
/tmp/inst.log
```

De-installing Agents

For general de-installation instructions, see the *OVO Administrator's Reference*.

If errors occur during the de-installation, check the local de-installation logfile:

```
/tmp/inst.log
```

Removing Agents

If you no longer need an older OVO agent package, and the package is not installed on any managed node, you can remove it by running:

**/opt/OV/bin/OpC/install/rm_opc.sh sgi/mips/irix **
<OVO_version>

In this command, *<OVO_version>* is the version of OVO that supports this agent platform (for example, A.08.00).

About Preconfigured Elements

This section describes preconfigured templates, template groups, and applications used by OVO on SGI IRIX managed nodes.

Types of Default Logfile Templates

No SNMP Trap and Event Interception

The OVO event interceptor is not supported on SGI IRIX managed nodes.

Types of Default Applications

For a list of default applications available for UNIX managed nodes, see the *OVO Administrator's Reference*.

Distributing Scripts and Programs

For SGI IRIX managed nodes, the platform selector and architecture identifier is the following:

```
sgi/mips/irix
```

Location of User Scripts and Programs

Table 7-1 shows the location of user scripts and programs provided on the management server.

Table 7-1 Location of User Scripts and Programs on the Management Server

Script/Program	Location
Automatic actions, operator-initiated actions, and scheduled actions	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /sgi/mips/irix/actions/`
Monitoring scripts and programs used by the monitoring agent and the logfile encapsulator	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /sgi/mips/irix/monitor/`
Scripts and programs called through command broadcast or started from the Application Desktop	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /sgi/mips/irix/cmds/`

About Temporary Directories

Table 7-2 shows the temporary directories for distributed scripts and programs on the managed nodes.

Table 7-2 Temporary Directories for Distributed Scripts and Programs on the Managed Nodes

Managed Node	Operating System	Temporary Directory

Silicon Graphics	SGI IRIX	`/var/opt/OV/tmp/OpC/bin/actions`
		`/var/opt/OV/tmp/OpC/bin/cmds`
		`/var/opt/OV/tmp/OpC/bin/monitor`

About Target Directories

Table 7-3 shows the target directories for distributed scripts and programs on the managed nodes.

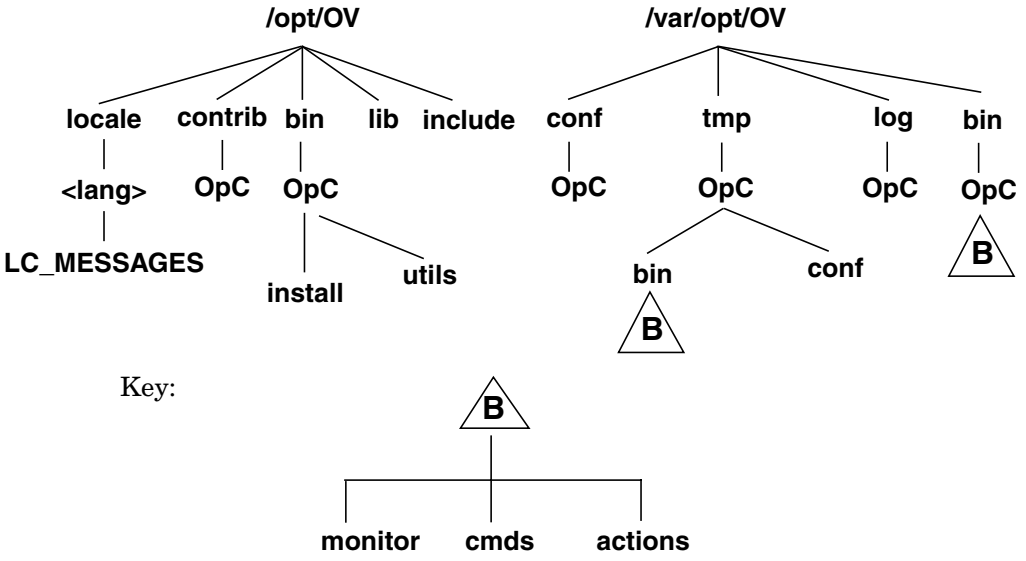
Table 7-3 Target Directories for Distributed Scripts and Programs on the Managed Nodes

Managed Node	Operating System	Target Directory	Access Rights
Silicon Graphics	SGI IRIX	`/var/opt/OV/bin/OpC/actions`	`rwxr-xr-x` (owner:root)
		`/var/opt/OV/bin/OpC/cmds`	`rwxr-xr-x` (owner:root)
		`/var/opt/OV/bin/OpC/monitor`	`rwxr-xr-x` (owner:root)

Organization of Managed Nodes

Figure 7-1 shows how OVO software is organized on SGI IRIX managed nodes, based on the typical SVR4 platforms.

Figure 7-1 OVO Software on SGI IRIX Managed Nodes



Location of Files

On SGI IRIX managed nodes, files are located as follows:

- **Process-related Files**

  `/var/opt/OV/tmp/OpC`

- **Agent Configuration Files**

  `/var/opt/OV/conf/OpC`

About the Default OVO Operator

If they do not already exist, the default OVO operator `opc_op` and group `opcgrp` are created.

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

About Default OVO Operator Entries

The default OVO operator is added to the following directory on SGI IRIX managed nodes:

`/etc/passwd`

Fields include the following:

`User Name` `opc_op`

`Encrypted Password` `*` (no login)

`User-ID` `777` (if still available) or next possible free number

`Group-ID` `77` (if still available) or next possible free number

`Description` Default OVO operator

`Home Directory` `/var/people/opc_op`

`Login Shell` `/bin/sh` (POSIX shell)

About Default OVO Operator Group Entries

The default OVO operator group is added to the following directory on SGI IRIX managed nodes:

`/etc/group`

Fields include the following:

`Group Name` `opcgrp`

`Encrypted Password` Empty

`Group-ID` `77` or higher

`Users` `opc_op`

`Description` Default OVO operator group

Types of System Resources

OVO makes changes in the following system resource files during installation:

`/etc/passwd`
`/etc/shadow` (if present) Entry for the default OVO operator and Protected Password Database (if present).

`/etc/group` Group entry for the default OVO operator

`/etc/init.d/opcagt` OVO startup and shutdown script.

`/etc/rc0.d` Creates the `K09opcagt` file.

`/etc/rc2.d` Creates the `S89opcagt` file.

`/etc/exports` Cluster server only. Entry for export of `/opt` directory.

`/etc/exports` Cluster client only. Entry for mount `/opt` directory.

`/etc/int.d/grad_nck` NCS startup and shutdown script.

`/etc/rc0.d` Creates the `K35nck` file.

`/etc/rc2.d` Creates the `S40nck` file.

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

Types of Libraries

Table 7-4 describes the managed node libraries for OVO A.05.xx, A.06.xx, and A.07.xx.

Table 7-4 Libraries for the OVO Managed Nodes

	Item	OVO A.05.xx	OVO A.06.xx	OVO A.07.xx
NCS	Library	**libopc.so**	**libopc.so**	**libopc.so**
	Libraries linked to the OVO library.	/opt/OV/lib/libnsp.so /usr/lib/libnck.a /usr/lib/libnsl.so /usr/lib/libc.so	/opt/OV/lib/libnsp.so /usr/lib/libnck.a /usr/lib/libnsl.so /usr/lib/libc.so	/opt/OV/lib/libnsp.so /usr/lib/libnck.a /usr/lib/libnsl.so /usr/lib/libc.so
	Link and compile options	-lopc -lsocket -lnsl	-lopc -lsocket -lnsl	-lopc -lsocket -lnsl
	Description	N/A	N/A	N/A

About the Include File

On a Silicon Graphics Indigo platform with SGI IRIX managed nodes, use the following include file:

```
/opt/OV/include/opcapi.h
```

About the Makefile

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

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

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

```
Makef.irix
```

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

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

8 About SINIX RM/Reliant Managed Nodes

In this Chapter

This chapter explains how to install and configure HP OpenView Operations (OVO) on Siemens-Nixdorf SINIX RM/Reliant managed nodes.

Installation Requirements

This section explains OVO hardware and software requirements for SINIX RM/Reliant managed nodes.

Hardware Requirements

Before installing OVO, make sure the SINIX RM/Reliant systems you select as managed nodes meet the following hardware requirements:

- **Disk Space**

  14 MB (about 28 MB is required during software installation)

- **Additional Swap Space**

  None

- **Additional RAM**

  None

Software Requirements

Before installing OVO, make sure the following software is installed on SINIX RM/Reliant managed nodes:

- **Operating System**

  For a list of operating system versions supported by OVO, see the *OVO Installation Guide for the Management Server*.

- **System Parameters**

  For a list of kernel parameters, see the *OVO Administrator's Reference*. You can check and change the system parameters using the `sysadm` tool.

- **Siemens-Nixdorf Networking Packages (5.43)**

  - `tcp`
  - `SImac596`

❏ **Communication Software**

- *NCS 1.5.1*

  If NCS is chosen as the `Node Type` in the OVO GUI, and NCS 1.5.1 is not found on the managed node, OVO installs `llbd` and `lb_admin` during the OVO agent software installation.

- *DCE-CLNT 2.0*

  If the communication type is set to DCE RPCS (TCP or UDP), DCE-CLNT must be installed on the managed node.

NOTE

You can purchase DCE at additional cost for SINIX/Reliant platforms from the platform vendor or from a third-party supplier.

❏ **Package: attcmd**

❏ **Package: SIsnmpd**

This package is necessary if you want to run the OVO monitoring agent.

The 64-bit version of SINIX 5.45 includes this software package only for version V5.45A30 or higher.

If you have a 64-bit SINIX 5.45 system with a lower version, you can either upgrade, take this package from the V5.45A30 release, or take the following files from a 32-bit SINIX 5.45 system:

- `/opt/lib/snmpd/snmplib/libsnmp.so`
- `/opt/lib/snmpd/snmplib/libsnmpio.so`
- `/opt/lib/snmpd/snmplib/libsnmpuser.so`
- `/opt/snmp/lib/libsnmpapi.so`

and copy them to the `/opt/OV/lib` directory.

Installing and De-installing Agents

This section describes how to install and de-install SINIX RM/Reliant managed nodes.

Tips for Installing Agents

When installing SINIX RM/Reliant managed nodes, follow these guidelines:

- **Name of Management Server**

  The name of the management server must be known to the managed node. You must register the name of the management server on the name server or in the local host table:

  `/etc/hosts`

  You can verify this by using the `nslookup` command.

- **OVO Agent Software**

  The OVO agent software is installed on the `/opt` file tree. If there is not enough space for the installation of the OVO agents, create a symbolic link before installing OVO.

  For example, if `/bigdisk` is a local file system with enough free space, you would create the symbolic link as follows:

  ```
  mkdir -p /bigdisk/OV
  ln -s /bigdisk/OV /opt/OV
  ```

  In a cluster environment, make sure that `/bigdisk` is accessible from all cluster clients. That is, make sure that it is mounted from all client nodes. For example, the local file system `/bigdisk` on a cluster client must be mounted to exported file system `/bigdisk` on cluster server.

- **Logfile Encapsulator**

  By default, some of the logfiles checked by the logfile encapsulator are not present on SINIX/Reliant managed nodes (for example, `/var/adm/loginlog`). It is important that you manually create all logfiles that are checked by the logfile encapsulator agent. For example, if bad login attempts are to be monitored by OVO, you must first create the file `/var/adm/loginlog` with read and write permissions for the owner only. The owner must be `root` and the group `sys`. After five unsuccessful attempts to log in, a message is written to `/var/adm/loginlog`.

  The `Su` and `Cron` templates assume that the default setup is used for the `/etc/default/su` and `/etc/default/cron` files. If the default setup is not used, you must adapt the logfile paths in the templates to match the actual file names.

- **DNS**

  If you want to configure the Domain Name Server (DNS) on a SINIX/Reliant managed node, you must do the following:

  1. Edit the following file:

     `/etc/resolv.conf`

  2. Add the following line to the `hosts` files:

     <*nodename*> (uname -n)

     You must add this line to the following files:

     - `/etc/net/ticlts/hosts`
     - `/etc/net/ticots/hosts`
     - `/etc/net/ticotsord/hosts`

     If <*nodename*> is not defined in these three files, the OVO installation will fail because the `opcnsl` program will be unable to determine the management server.

- **Installation on NIS Clients**

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

❑ **Monitor Agent (opcmona)**

n SINIX RM/Reliant managed nodes, after having installed the OVO agent software, the monitor agent does not start. The following error message is generated:

```
"Can't find libsnmpapi.so"
```

If you want to run the OVO monitor agent, you need the package `SIsnmpd` on the managed node. The 64 bit version of SINIX 5.45 includes this software package only for version V5.45A30 or higher.

If you have a 64 bit SINIX 5.45 system with a lower version, you can do one of the following:

- Upgrade to version V5.45A30.
- Take this package from the V5.45A30 release.
- Copy the following files from a 32-bit SINIX 5.45 system to the directory `/usr/lib/snmpd/snmplib`:

  — `/opt/lib/snmpd/snmplib/libsnmp.so`
  — `/opt/lib/snmpd/snmplib/libsnmpio.so`
  — `/opt/lib/snmpd/snmplib/libsnmpuser.so`
  — `/opt/snmp/lib/libsnmpapi.so`

  If the following link does not yet exist, create it on your Sinix system:

  ```
  ln -s /opt/snmp/lib/libsnmpapi.so\
  /opt/OV/lib/libsnmpapi.so
  ```

  Then restart the OVO agents.

Configuring DCE

This section explains how to set up a new DCE configuration and remove an existing DCE configuration on SINIX RM/Reliant managed nodes.

To Configure DCE

To configure DCE on SINIX RM/Reliant managed nodes, follow these steps:

1. To start the `dce_config` program, enter the following:

   `/etc/dce_config`

2. Select `2. CONFIGURE`.
3. Select `3. DCE Client`.
4. If you are asked about removing all remnants of a previous DCE configuration, enter **`y`**.
5. When prompted, enter **`y`**.

   The `dce_config` program then checks the local clock against the `dtsd` server.
6. Enter the name of the system where a DTS server running.
7. Enter the Cell Administrator's principal name (for example, **`cell_admin`**) and password.
8. Enter the name of the system that is the CDS server.
9. Do *not* create a LAN profile.
10. Enter one of the following

    - **`clerk`**

      If you want to configure DTS.
    - **`none`**

      If you do *not* want to configure DTS.

This procedure configures the managed nodes as a DCE client and starts the DCE daemon `dced`.

To Remove an Existing DCE Configuration

To remove an existing DCE configuration from SINIX RM/Reliant managed nodes, follow these steps:

1. From the main menu, choose `5. UNCONFIGURE`.
2. Choose `6. REMOVE`.

Installing Agents

To install agents on SINIX RM/Reliant managed nodes, you can use standard or manual installation methods.

Installing Agents with Standard Installation

For standard installation instructions, see the *OVO Administrator's Reference*.

If errors occur during the installation, check the local installation logfile:

```
/tmp/pkgadd.log
```

Installing Agents Manually

For manual installation instructions, see "To Install an Agent Manually" on page 280.

NOTE

The agent package `opc_pkg.Z` on the OVO management server for the SINIX/Reliant platform is the following:

```
/var/opt/OV/share/databases/OpC/mgd_node/vendor/sni\
mips/sinix/A.08.00/RPC_[NCS|DCE_TCP|DCE_UDP]/opc_pkg.Z
```

De-installing Agents

To de-install agents on SINIX RM/Reliant managed nodes, you can use standard or manual de-installation methods. You can also remove older agent packages from the managed nodes.

De-installing Agents with Standard De-installation

For standard de-installation instructions, see the *OVO Administrator's Reference*.

If errors occur during the de-installation, check the local de-installation logfile:

```
/tmp/pkgrm.log
```

To De-install an Agent Manually

To de-install an agent manually, follow these steps:

1. Stop all OVO agents running on the managed node.
2. De-install the OVO agent software from SINIX/Reliant managed nodes by entering:

   pkgrm OPC

Removing Older Agents

If an older OVO agent package is no longer required and is not installed on any managed node, you can remove it by running script on the management server:

/opt/OV/bin/OpC/install/rm_opc.sh sni/mips/sinix \ <*OVO_version*>

In this command, *<OVO_version>* is the version of OVO that supports this agent platform (for example A.08.00).

About Preconfigured Elements

This section describes preconfigured templates, template groups, and applications used by OVO on SINIX RM/Reliant managed nodes.

No SNMP Trap and Event Interception

The OVO event interceptor is not supported on SINIX RM/Reliant managed nodes.

Distributing Scripts and Programs

For SINIX RM/Reliant managed nodes, the platform selector and architecture identifier is the following:

```
sni/mips/sinix
```

Location of User Scripts and Programs

Table 8-1 shows the location of user scripts and programs provided on the management server.

Table 8-1 Location of User Scripts and Programs on the Management Server

Script/Program	Location
Automatic actions, operator-initiated actions, and scheduled actions	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /sni/mips/sinix/actions/*`
Monitoring scripts and programs used by the monitoring agent and the logfile encapsulator	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /sni/mips/sinix/monitor/*`
Scripts and programs called through command broadcast or started from the Application Desktop	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /sni/mips/sinix/cmds/*`

About Temporary Directories

Table 8-2 shows the temporary directories for distributed scripts and programs on the managed nodes.

Table 8-2 Temporary Directories for Distributed Scripts and Programs on the Managed Nodes

Managed Node	Operating System	Temporary Directory

Siemens Nixdorf	SINIX	`/var/opt/OV/tmp/OpC/bin/actions`
		`/var/opt/OV/tmp/OpC/bin/cmds`
		`/var/opt/OV/tmp/OpC/bin/monitor`

About Target Directories

Table 8-3 shows the target directories for distributed scripts and programs on the managed nodes.

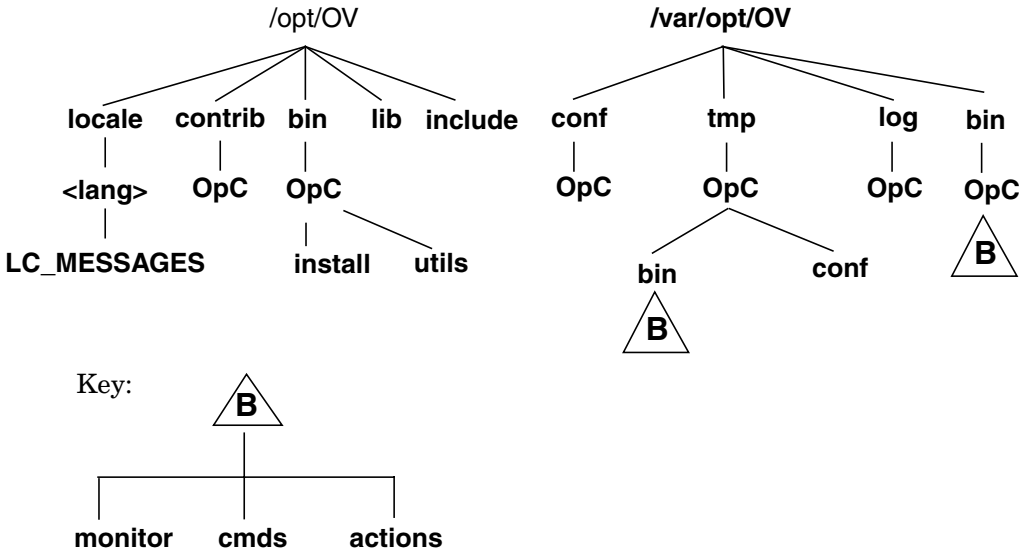
Table 8-3 Target Directories for Distributed Scripts and Programs on the Managed Nodes

Managed Node	Operating System	Target Directory	Access Rights
Siemens Nixdorf	SINIX	`/var/opt/OV/bin/OpC/actions`	`rwxr-xr-x` (owner:root)
		`/var/opt/OV/bin/OpC/cmds`	`rwxr-xr-x` (owner:root)
		`/var/opt/OV/bin/OpC/monitor`	`rwxr-xr-x` (owner:root)

Organization of Managed Nodes

Figure 8-1 shows how OVO software is organized on SINIX RM/Reliant managed nodes, based on the typical SVR4 platforms.

Figure 8-1 OVO Software on SINIX/Reliant Managed Nodes



Location of Files

On SINIX RM/Reliant managed nodes, files are located as follows:

- **Process-related Files**

  `/var/opt/OV/tmp/OpC`

- **Agent Configuration Files**

  `/var/opt/OV/conf/OpC`

About the Default OVO Operator

If they do not already exist, the default OVO operator `opc_op` and group `opcgrp` are created.

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

About Default OVO Operator Entries

The default OVO operator is added to the following directory on SINIX RM/Reliant managed nodes:

`/etc/passwd`

Fields include the following:

`User Name` `opc_op`

`Encrypted Password` `*` (no login)

`User-ID` `777` (if still available) or next possible free number

`Group-ID` `177` (if still available) or next possible free number

`Description` Default OVO operator

`Home Directory` `/home/opc_op`

`Login Shell` `/bin/sh`

About Default OVO Operator Group Entries

The default OVO operator group is added to the following directory on SINIX RM/Reliant managed nodes:

`/etc/group`

Fields include the following:

`Group Name` `opcgrp`

`Encrypted Password` Empty

`Group-ID` `177` or higher

`Users` `opc_op`

`Description` Default OVO operator group

Types of System Resources

OVO makes changes in the following system resource files during installation on SINIX RM/Reliant managed nodes:

`/etc/passwd`
`/etc/shadow` (if present) Entry for the default OVO operator and Protected Password Database (if present).

`/etc/group` Group entry for the default OVO operator

`/etc/init.d/opcagt` OVO startup and shutdown script.

`/etc/rc0.d` Creates the `K09opcagt` file.

`/etc/rc1.d` Creates the `K09opcagt` file.

`/etc/rc2.d` Creates the `S89opcagt` file.

`/etc/int.d/ncs` NCS startup and shutdown script (if it is not already present and the communciation type is NCS RPC).

`/etc/rc0.d` Creates the `K52ncs` (if it is not already present and the communciation type is NCS RPC).

`/etc/rc1.d` Creates the `K52ncs` file (if it is not already present and the communciation type is NCS RPC).

`/etc/rc2.d` Creates the `S76ncs` file (if it is not already present and the communciation type is NCS RPC).

`/usr/lib/snmplib/libsnmpapi.so -> \`
`/opt/lib/snmpd/snmplib/libsnmpuser.so` Creates symbolic link (if it is not already present).

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

Types of Libraries

Table 8-4 describes the managed node libraries for OVO A.05.xx, A.06.xx, and A.07.xx.

Table 8-4 Libraries for the OVO Managed Nodes

	OVO Version	OVO A.05.xx	OVO A.06.xx	OVO A.07.xx
DCE	Library	**libopc_r.so**	**libopc_r.so**	**libopc_r.so**
	Libraries linked to the OVO library	thr_cc is used which comes with its own libraries	thr_cc is used which comes with its own libraries	thr_cc is used which comes with its own libraries
	Link and compile options	-lopc_r -lnsp -ldce -lsocket_r -lresolv_r -lm_r -lc -lnsl_r_i	-lopc_r -lnsp -ldce -lsocket_r -lresolv_r -lm_r -lc -lnsl_r_i	-lopc_r -lnsp -ldce -lsocket_r -lresolv_r -lm_r -lc -lnsl_r_i
	Description	N/A	N/A	N/A
NCS	Library	**libopc.so**	**libopc.so**	**libopc.so**
	Libraries linked to the OVO library	mips_cc is used which comes with its own libraries	mips_cc is used which comes with its own libraries	mips_cc is used which comes with its own libraries
	Link and compile options	-lopc -lnck -lnsp -lsocket -lnsl -lc -lucb	-lopc -lnck -lnsp -lsocket -lnsl -lc -lucb	-lopc -lnck -lnsp -lsocket -lnsl -lc -lucb
	Description	N/A	N/A	N/A

About the Makefile

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

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

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

- `Makef.sinix`
- `Makef.sinix-dce`

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

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

9 About Sun Solaris Managed Nodes

In this Chapter

This chapter explains how to install and configure HP OpenView Operations (OVO) on Sun Solaris managed nodes.

Installation Requirements

This section explains OVO hardware and software requirements for Sun Solaris managed nodes.

Hardware Requirements

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

- **Disk Space**

  65 MB (about 65 MB is required during software installation)

  - *NCS*

    10 MB

    About 20 MB is required during software installation.

  - *DCE*

    20 MB free disk space

    — 10 MB for OVO agent

    — 10 MB for HP Lightweight DCE software

    About 40 MB is required during software installation.

- **Additional Swap Space**

  None

- **Additional RAM**

  None

Software Requirements

Before installing OVO, make sure the following software is installed on Sun Solaris managed nodes:

- **Operating System**

  For a list of operating system versions supported by OVO, see the *OVO Installation Guide for the Management Server*.

- **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.

  See also the section “Problems Caused by Missing OS Patches for Sun Solaris” on page 279 for information about patches that must not be installed on Sun Solaris managed nodes.

Table 9-1 Required Patches for Sun Solaris Managed Nodes

OS Version	Patch ID	Description
Solaris 2.6	107733-09	SunOS 5.6: Linker patch
	105591-11	SunOS 5.6: Shared library patch for C++
	106429-02	SunOS 5.6: /kernel/drv/mm patch
	105181-29	SunOS 5.6: Kernel update patch
	105210-38	SunOS 5.6: libaio, libc & watchmalloc patch
	105568-23	SunOS 5.6: /usr/lib/libthread.so.1 patch
	105633-59	OpenWindows 3.6: Xsun patch
	106841-01	OpenWindows 3.6: Keytables patch
	106842-09	SunOS 5.6: Feature patch for Euro currency support in Solaris 2.6

Table 9-1 Required Patches for Sun Solaris Managed Nodes (Continued)

OS Version	Patch ID	Description
Solaris 7	106950-15	SunOS 5.7: Linker patch
	106327-10	SunOS 5.7: 32-Bit Shared library patch for C++
	107544-03	SunOS 5.7: /usr/lib/fs/ufs/fsck patch
	106541-17	SunOS 5.7: Kernel update patch
	106980-17	SunOS 5.7: libthread patch
Solaris 8	109147-09	SunOS 5.8: Linker patch
	108434-03	SunOS 5.8: Shared library patch for C++
	108827-11	SunOS 5.8: libthread patch

❑ **Kernel Parameters**

It is recommended that you set the following kernel parameters for Sun Solaris managed nodes:

Table 9-2 Recommended Kernel Parameters for Sun Solaris Managed Nodes

Parameter	Description	Minimum value
semmap	This parameter is no longer used on Solaris 8.	
semmni	Number of semaphore identifiers	30
semmns	Number of semaphores in system	200 or greater
semmsl	Maximum number of semaphores per ID	100

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

❑ **Communication Software**

- *NCS*

  If NCS is chosen as the `Communication Type` in the OVO GUI, and NCS version 1.5.1 is *not* found on the managed node, OVO installs `llbd` and `lb_admin` during the OVO agent software installation.

- *DCE*

  If the communication type is set to DCE RPC (TCP or UDP) and 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. Refer to Table 9-3 for more information regarding supported DCE packages.

Table 9-3 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.

Installing and De-installing Agents

This section describes how to install and de-install Sun Solaris managed nodes.

Tips for Installing Agents

When installing Sun Solaris managed nodes, follow these guidelines:

- **Name of Management Server**

  The name of the management server must be known to the managed node. You must register the name of the management server on the name server or in the local host table:

  `/etc/hosts`

  You can verify this by using the `nslookup` command.

- **Name of System**

  The system name `uname -s` must be set to one of the following:

  - `SunOS`
  - `Solaris`

- **Package SUNWaccu**

  The package `SUNWaccu` must be installed on the system if process table and CPU utilization are to be monitored by OVO. If this package is *not* installed, and monitoring templates `proc_util` and `cpu_util` are configured, warning messages will be displayed in the `Message Browser` window stating that the corresponding shell scripts failed to execute.

- **Bad Logins**

  If bad login attempts are to be monitored by OVO, the file `/var/adm/loginlog` must first be manually created. By default, `loginlog` does *not* exist, so no logging is done. To enable logging, the logfile must be created with read and write permission for the owner `root` and group `sys`. You can then configure the logfile template `Bad Logs (Solaris)` for the node.

- **OVO Agent Software**

  The OVO agent software is installed on the `/opt` file tree. If there is *not* enough space for the installation of the OVO agents, create a symbolic link before installing OVO.

  For example, if `/bigdisk` is a local file system with enough free space, you would create the symbolic link as follows:

  ```
  mkdir -p /bigdisk/OV
  ln -s /bigdisk/OV /opt/OV
  ```

  In a cluster environment, make sure that `/bigdisk` is accessible from all cluster clients. That is, make sure that it is mounted from all client nodes. For example, the local file system `/bigdisk` on a cluster client must be mounted to exported file system `/bigdisk` on the cluster server.

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**

  If the DCE communication type is used, make sure you have the following patches installed:

  Solaris 2.6

  Use the following patches:

  105181-16

  105210-24

  105568-14

NOTE See also the section “Software Requirements” on page 274 for a list of required patches for Sun Solaris managed nodes.

Installing Agents

To install agents on Sun Solaris managed nodes, you can use standard or manual installation methods.

Installing Agents with Standard Installation

For standard installation instructions, see the *OVO Administrator's Reference*.

If errors occur during the installation, check the local installation logfile:

```
/tmp/pkgadd.log
```

To Install an Agent Manually

In some situations, you may want to install the Sun Solaris agent software without using the management server. Manual installation prepares the system to become an OVO managed node when it is later connected to the network. Manual installation is useful if many systems are prepared in a central location, or if you want to avoid using the root connection over the network that is necessary for a standard agent installation.

To install the OVO agent on a Sun Solaris system that will become a OVO managed node, follow these steps:

1. **Copy the OVO agent packages and installation script to a temporary directory on the managed node.**

   On the management server, these are the following files:

   - `opc_pkg.Z`
   - `comm_pkg.Z`
   - `perf_pkg.Z`
   - `opc_inst`

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

   ```
   /var/opt/OV/share/databases/OpC/mgd_node/vendor/sun/\
   sparc/solaris/A.08.00/RPC_[NCS|DCE_TCP|DCE_UDP]/
   ```

2. Set umask, enter:

   ```
   umask 022
   ```

3. **Install the Agent.**

   a. Change the permissions of the agent installation script to ensure that it can be executed:

      ```
      chmod +x /tmp/opc_inst
      ```

   b. Start the agent installation script by entering:

      ```
      /tmp/opc_inst
      ```

You can now activate the Sun Solaris managed node. For instructions, see “Activating Agents” on page 282.

Activating Agents

To activate agents on Sun Solaris managed nodes, you can use the command line or the OVO GUI.

To Activate a Node from the Command Line

To activate a Sun Solaris managed node over the network from the command line, follow these steps:

1. Add the pre-installed node to the `OVO Node Bank`.

   Use the following menu sequence:

   `Actions:Node->Add`

2. Add the node to an OVO node group.

   Drag and drop the node onto a node group in the `OVO Node Group Bank` window.

3. Install the OVO agent on the node manually.

   For instructions, see “To Install an Agent Manually” on page 280.

4. After manually installing the agent on the node, enter the following:

   `/opt/OV/bin/OpC/install/opcactivate -s <OVO_mgt_server>\ -cs <server_codeset> -cn <agent_codeset>`

   The agent then attempts to send messages to the management server.

   - Specifying the `-s` option with the `opcactivate` command is optional. This option starts the `/opt/OV/bin/OpC/install/upd_res.sh` script which integrates the OVO agent into the system startup and shutdown scripts, for example the `/etc/init.d` file.
   - `-cs <server_codeset>` is the character set for the OVO management server.
     `-cn <agent codeset>` is the character set for this agent.

     For more information about codesets, see the *OVO Administrator’s Reference* and the man page *opcactivate(1M)*.

5. After the node is connected to the network, execute the following command on the management server:

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

To Activate the Node from the OVO GUI

After the node with the pre-installed agent is connected to the network, you can activate and register the managed node from the OVO GUI.

To activate and register the managed node from the OVO GUI, follow these steps:

1. Add the pre-installed nodes to the `OVO Node Bank`.

   Use the following menu sequence:

   `Actions:Node->Add`

2. Add the node to an OVO node group.

   Drag and drop the node onto a node group in the `OVO Node Group Bank` window.

3. Distribute the OVO configuration to the node:

   a. Select `Actions:Agents->Install / Update SW & Config` from the menu bar of the `OVO Node Bank`.

      The `Install / Update OVO Software and Configuration` window opens.

   b. Select all components.

   c. Click `[OK]`.

CAUTION

Do *not* check `[Force Update]`. If you do, the management server will re-install the agent.

If the agent is pre-installed on the node, the management server will activate the node, and install the selected components.

CAUTION

If the agent software is *not* pre-installed, the management server will install the agent.

4. To verify that the control, message, and action agents are all running on the managed node, enter the following:

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

De-installing Agents

To de-install agents on Sun Solaris managed nodes, you can use standard or manual de-installation methods. You can also remove older agent packages from the managed nodes.

De-installing Agents with Standard De-installation

For general de-installation instructions, see the *OVO Administrator's Reference*.

If errors occur during the de-installation, check the local de-installation logfile:

`/tmp/pkgrm.log`

To De-install an Agent Manually

To de-install an agent manually, follow these steps:

1. Stop all OVO agents running on the managed node.
2. De-install the OVO agent software from the managed nodes by entering:

   `/usr/sbin/pkgrm OPC OPCCOMM OPCPERF`

NOTE If you are de-installing an older version of the agent, use: `/usr/sbin/pkgrm OPC`.

3. If you installed DCE communication type, you must also de-install the `HPlwdce` package.

   Enter the following:

   `/usr/sbin/pkgrm HPlwdce`

Removing Older Agents

If older OVO agent packages are no longer required and are *not* installed on any managed node, you can remove them from the management server by running:

```
/opt/OV/bin/OpC/install/rm_opc.sh sun/sparc/solaris \
<OVO_version>
```

In this command, <OVO_version> is the version of OVO that supports this agent platform (for example, A.08.00).

About Preconfigured Elements

This section describes preconfigured templates, template groups, and applications used by OVO on Sun Solaris managed nodes.

One Preconfigured Template Group

OVO uses the following preconfigured template group:

- `Solaris`

Types of Default opcmsg Message Templates

Table 9-4 shows the opcmsg message templates that are available for Sun Solaris managed nodes.

Table 9-4 opcmsg Message Templates on Sun Solaris Managed Nodes

Name	Description
`opcmsg(1|3)`	Default interception of messages submitted by `opcmsg(1)`, `opcagtmsg_send(3)`, and `opcmsg(3)`.

Types of Default Logfile Templates

Table 9-5 shows encapsulated logfiles and associated template used on Sun Solaris managed nodes.

Table 9-5 Encapsulated Logfiles on Sun Solaris Managed Nodes

Logfile	Description	Template Name
`/var/cron/log`	Cron logfile	`Cron (Solaris)`

About SNMP Trap and Event Interception

By default, OVO intercepts SNMP traps from any application sending traps to the `opctrapi` daemon running on the management server and on all managed nodes where the OpenView trap daemon (`ovtrapd`) is running, or where port 162 can be accessed directly. For details about which traps are intercepted by default, see the SNMP trap templates in the `Message Source Templates` window of the OVO administrator GUI.

Types of SNMP Traps

The following kinds of SNMP traps can be intercepted:

- **Well-defined Traps**

  Example: system cold start, network interface up and down, and so on.

- **Internal HP OpenView Traps**

  Example: Traps originating from `netmon`.

NOTE Local event interception is supported only with Network Node Manager (NNM) version 6.2.

About OVO Distributed Event Interception

OVO Distributed Event Interception enables you to intercept SNMP traps on systems other than the OVO management server. This trap interception enables the messages to be processed locally, thereby improving system performance. Automatic actions, for example, can be triggered and executed directly on the node or in the subnet, instead of being first forwarded to the management server.

To Configure Basic Event Interception

To configure basic OVO Distributed Event Interception, follow these steps:

1. **Configure SNMP devices or the NNM collection station.**

   Make sure that one of the following is true:

   - *SNMP Devices*

     SNMP devices have only one SNMP destination.

     Set the destination systems for SNMP devices on Sun Solaris nodes in the following file:

     `/etc/SnmpAgent.d/snmpd.conf`

     Use the following statement:

     `trap-dest:<nodename>`

   - *NNM Collection Station*

     There is only one system serving as the NNM collection station for the management server. This station should be connected through the fastest network.

2. **Set the SNMP session mode.**

   If NNM is *not* running on the node where you want to intercept events, add the following line to the `opcinfo` file on that node:

   `SNMP_SESSION_MODE NO_TRAPD`

3. **Assign and distribute the trap template to the node.**

To Avoid Duplicate Messages in Event Interception

To avoid duplicate messages, make sure that an OVO agent (and thereby, an OVO event interceptor) runs on all NNM collection stations. Use the `Print Collection Station` application in the NNM Tools application group to verify which managed nodes are set up as NNM collection stations.

To Configure Event Interception with ECS

By default, `opctrapi` connects to the correlated event flow of `pmd`. You can change this behavior by adding a statement to the `opcinfo` file on the managed node.

Syntax:

```
SNMP_EVENT_FLOW [ALL|RAW|CORR]
```

The `opctrapi` process connects to the default ECS stream of `pmd`.

If needed, you can configure `opctrapi` to connect to a specific ECS stream of `pmd` by specifying the ECS stream in the `opcinfo` file:

`SNMP_STREAM_NAME <stream_name>`

Types of Applications

For a list of default applications available for UNIX managed nodes, see the *OVO Administrator's Reference*.

Distributing Scripts and Programs

For Sun Solaris managed nodes, the platform selector and architecture identifier is the following:

```
sun/sparc/solaris
```

Location of User Scripts and Programs

Table 9-6 shows the location of user scripts and programs provided on the management server.

Table 9-6 Location of User Scripts and Programs on the Management Server

Script/Program	Location
Automatic actions, operator-initiated actions, and scheduled actions	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /sun/sparc/solaris/actions/*`
Monitoring scripts and programs used by the monitoring agent and the logfile encapsulator	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /sun/sparc/solaris/monitor/*`
Scripts and programs called through command broadcast or started from the Application Desktop	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /sun/sparc/solaris/cmds/*`

About Temporary Directories

Table 9-7 shows the temporary directories for distributed scripts and programs on the managed nodes.

Table 9-7 Temporary Directories for Distributed Scripts and Programs on the Managed Nodes

Managed Node	Operating System	Temporary Directory

Sun SPARC
Fujitsu-Siemens SPARC
	Sun Solaris	`/var/opt/OV/tmp/OpC/bin/actions`
		`/var/opt/OV/tmp/OpC/bin/cmds`
		`/var/opt/OV/tmp/OpC/bin/monitor`

About Target Directories

Table 9-8 shows the target directories for distributed scripts and programs on the managed nodes.

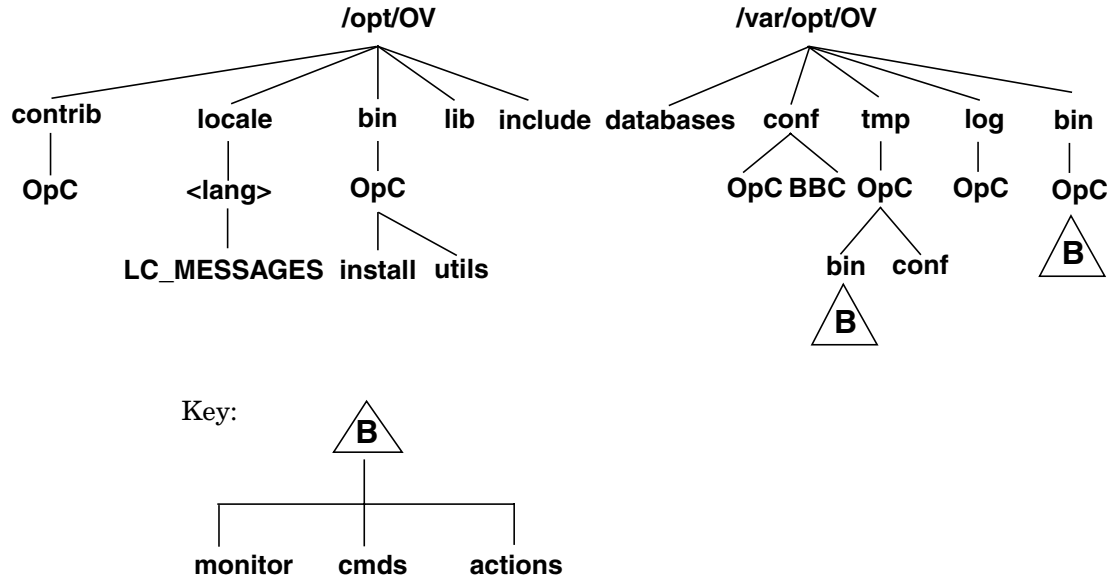
Table 9-8 Target Directories for Distributed Scripts and Programs on the Managed Nodes

Managed Node	Operating System	Target Directory	Access Rights
Sun SPARC Fujitsu-Siemens SPARC	Sun Solaris	`/var/opt/OV/bin/OpC/actions`	`rwxr-xr-x` (owner: `root`)
		`/var/opt/OV/bin/OpC/cmds`	`rwxr-xr-x` (owner: root)
		`/var/opt/OV/bin/OpC/monitor`	`rwxr-xr-x` (owner: `root`)

Organization of Managed Nodes

Figure 9-1 shows how OVO software is organized on Sun Solaris managed nodes.

Figure 9-1 OVO Software on Sun Solaris Managed Nodes



The path `/var/sadm/pkg/OPC` is used by the `pkgadd` utility for software maintenance.

Location of Files

On Sun Solaris managed nodes, files are located as follows:

- **Process-related Files**

  `/var/opt/OV/tmp/OpC`

- **Agent Configuration Files**

  `/var/opt/OV/conf/OpC`

About the Default OVO Operator

The default OVO operator, opc_op, owns /export/home/opc_op as home directory. By default, the operator uses the Korn Shell (/bin/ksh), and is locked until the passwd command is executed. User opc_op belongs to the group opcgrp.

You add user opc_op and group opcgrp only locally on the managed node (with useradd or groupadd).

If the managed node is a Network Information Service (NIS or NIS+) client, the OVO installation checks if user opc_op is already in the NIS database:

- If opc_op is in the NIS database, no additional user is installed.
- If opc_op is *not* in the NIS database, opc_op is added only locally on the managed node.

Types of System Resources

OVO makes changes in the following system resource files during installation on Sun Solaris managed nodes:

/etc/passwd /etc/shadow	Entry for the default OVO operator.
/etc/group	Group entry for the default OVO operator.
/etc/init.d/opcagt	OVO startup and shutdown script.
/etc/rc3.d/S99opcagt	Creates file.
/etc/rc0.d/K09opcagt	Creates file.
/etc/rc1.d/K09opcagt	Creates file.
/etc/vfstab	On cluster client only, entry for mount /opt directory.
/etc/init.d/ncs	NCS startup script (if not already present).
/etc/rc3.d/S76ncs	Creates file (if not already present).
/etc/rc0.d/K52ncs	Creates file (if not already present).
/etc/rc2.d/K52ncs	Creates file (if not already present).

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

Types of Libraries

Table 9-9 describes the managed node libraries for OVO A.05.xx, A.06.xx and A.07.xx.

Table 9-9 Libraries for the OVO Managed Nodes

	Item	OVO A.05.xx	OVO A.06.xx	OVO A.07.xx
NCS	Library	**libopc.so**	**libopc.so**	**libopc.so**
	Libraries linked to the OVO library.	libov.a and libovutil.a are statically linked into libopc.so /usr/lib/libw.so.1 /usr/lib/libsocket.so.1 /usr/lib/libnsl.so.1 /usr/lib/libc.so.1 /usr/lib/libdl.so.1 /usr/lib/libmp.so.2 /usr/platform/SUNW,\ Ultra-5_10/lib/libc_psr.so.1	libov.a and libovutil.a are statically linked into libopc.so /usr/lib/libw.so.1 /usr/lib/libnck.a /usr/lib/libsocket.so.1 /usr/lib/libnsl.so.1 /opt/OV/lib/libopcas.so.1	/usr/lib/libsocket.so.1 /usr/lib/libnsl.so.1 /usr/lib/libw.so.1 /opt/OV/lib/libopcas.so /usr/lib/libc.so.1 /usr/lib/libdl.so.1 /usr/lib/libmp.so.2 /usr/platform/SUNW,\ Ultra-5_10/lib/libc_psr.so.1
	Link and compile options	-lopc -lnsp -lsocket -lnsl	-lopc -lnsp -lsocket -lnsl	-lopc -lnsp -lsocket -lnsl
	Description	N/A	N/A	N/A

Table 9-9 Libraries for the OVO Managed Nodes (Continued)

	Item	OVO A.05.xx	OVO A.06.xx	OVO A.07.xx
DCE	Library	**libopc_r.so**	**libopc_r.so**	**libopc_r.so**
	Libraries linked to the OVO library.	/opt/OV/dce/lib/libdce.so /opt/OV/dce/lib/libdcecrypt.so /usr/lib/libsocket.so.1 /usr/lib/libnsl.so.1 /usr/lib/libw.so.1 /usr/lib/libc.so.1 /usr/lib/libdl.so.1 /usr/lib/libmp.so.2 /usr/platform/SUNW,\ Ultra-5_10/lib/libc_psr.so.1	/usr/lib/libm.so.1 /usr/lib/libthread.so.1 /opt/OV/dce/lib/libdce.so /opt/OV/lib/libopcas.so /opt/OV/dce/lib/ \ libdcecrypt.so /usr/lib/libsocket.so.1 /usr/lib/libnsl.so.1 /usr/lib/libw.so.1 /usr/lib/libc.so.1 /usr/lib/libdl.so.1 /usr/lib/libmp.so.2 libc_psr.so.1[a]	/opt/OV/dce/lib/libdce.so /opt/OV/dce/lib/ \ libdcecrypt.so /usr/lib/libsocket.so.1 /usr/lib/libnsl.so.1 /usr/lib/libw.so.1 /opt/OV/lib/libopcas.so /usr/lib/libthread.so.1 /usr/lib/libm.so.1 /usr/lib/libc.so.1 /usr/lib/libdl.so.1 /usr/lib/libmp.so.2 /usr/platform/SUNW,\ Ultra-5_10/lib/libc_psr.so.1
	Link and compile options	-lopc_r -lnsp -lnsl -ldce -lsocket -lthread -lm -lw	-lopc_r -lnsp -lnsl -ldce -lsocket -lthread -lm -lw	-lopc_r -lnsp -lnsl -ldce -lsocket -lthread -lm -lw
	Description	N/A	N/A	N/A

a. Location of the library `libc_psr.so.1` is platform dependent.

About the Include File

On a Sun SPARCstation platform with Sun Solaris managed nodes, use the include file:

`/opt/OV/include/opcapi.h`

About the Makefile

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

/opt/OV/OpC/examples/progs

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

- **NCS**

  `Makef.solaris`

- **DCE**

  `Makef.solarisdce`

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

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

Support for Sun Enterprise E10000

The Sun Enterprise E10000 platform is an extremely powerful and highly reliable server system:

- **Dynamic System Domains**

  System boards within the platform may be logically grouped into separately bootable systems called Dynamic System Domains, or simply domains. Up to eight domains may exist simultaneously on a single E10000 platform. The domain is able to run its own operating system (Sun Solaris 2.6, 7 or 8), and can handle its own workload. Domains can be created and deleted without interrupting the operation other domains.

- **Sun Service Processor**

  Sun Service Processor (SSP) is the central console that monitors the E10000 system and enables the operator to perform management and maintenance procedures. The SSP enables you to control and monitor the domains as well as the platform itself.

Monitoring and Managing E10000 Systems

Standard instrumentation provided with OVO A.08.00 version enables you to monitor and manage the Sun Enterprise E10000 platform with the following:

- **Remote Monitoring and Managing**

  Monitoring and managing the SSP system remotely.

- **Proxy Agent**

  There is no OVO agent installed on the SSP system. OVO agent on another node (Sun Solaris or HP-UX) takes a proxy agent role. The SSP system must be added to `OVO Node Bank` as `Message Allowed` node.

- **SNMP Traps**

  Monitoring the E10000 platform is based on intercepting SNMPv1 traps, which are generated by the SSP `snmpd` daemon on the SSP system.

- **Monitor and Logfile Templates**

  Additional monitor and logfile templates are provided to monitor the SSP `cbs` daemon process and the SSP logfiles.

- **SSP Administration**

  SSP administration windows `hostview` and `netcontool` can be launched remotely from the `OVO Application Bank`.

About Software and OS Versions for E10000 Systems

OVO for Sun Enterprise E10000 supports the following software and operating system versions:

- **SSP Software**

  Sun Enterprise 10000 SSP 3.x

- **Operating System**

  Sun Solaris 2.6, 7 and 8

- **OVO Agent Packages**

  Installed on Sun Solaris or HP-UX system

About Preconfigured Elements for E10000 Systems

This section describes preconfigured templates, template groups, and applications provided by OVO for monitoring and managing the Sun Enterprise E10000 platform.

One Preconfigured Template Group

OVO uses the following preconfigured template group for Sun Enterprise E10000:

- `SSP`

About SNMP Trap Interception

A SNMP trap template is used to intercept all SSP snmpd traps.

Because there is no OVO agent installed on the SSP system, you must do the following to intercept SSP traps:

- **Reconfigure**

  You must reconfigure the SSP `snmpd` daemon. For instructions, see “Configuring the SSP System for E10000 Systems” on page 307.

- **Assign and Distribute**

  You must assign and distribute the SNMP trap template to the node with OVO agent installed.

About Encapsulated Logfiles

OVO provides the SSP Logfile Template for monitoring the domain- and platform-specific SSP logfiles shown in Table 9-10.

Table 9-10 Encapsulated SSP Logfiles

Logfile	Description	Template Name
`/var/opt/SUNWssp/adm/<domain_name>/messages`	Domain specific	`SSP Logfile`
`/var/opt/SUNWssp/adm/<domain_name>/netcon`	`netcon` logfile	`SSP Logfile`
`/var/opt/SUNWssp/adm/messages`	Platform specific	`SSP Logfile`

To monitor the SSP logfiles, you must export and then manually mount the following SSP logfile directory on the OVO agent node:

`/var/opt/SUNWssp/adm`

For more information, see “To Reconfigure the SSP snmpd Daemon” on page 307.

About Monitored Objects

The control board server (cbs) daemon provides access to the Sun Enterprise 10000 system control board for client programs running on the SSP system. The SSP monitor template is provided to check if the cbs daemon is running.

Table 9-11 shows the object thresholds on the SSP system.

Table 9-11 Object Thresholds on the SSP system

Object	Description	Threshold	Polling Interval (Minutes)
cbs	Monitors the cbs (control board server) daemon	0.5	3

You must establish remote equivalence between the SSP system and the node with OVO agent installed. For details, see “To Establish Remote Host Equivalence” on page 308.

About SSP Tools

OVO provides an additional application group, `SSP Tools`, for monitoring and managing the E10000 system.

`SSP Tools` consists of the following applications:

`hostview`	Launches the SSP administration X window application - `hostview`, the primary graphical user interface (GUI) to the E10000 system. This GUI is used to monitor the E10000 hardware and software configuration and status. It enables you to perform dynamic reconfiguration operations. The application is started on the management server.
`netcontool`	Launches SSP administration X window application - `netcontool`, the graphical user interface (GUI) to the `netcon` command. This GUI enables a remote connection to the domain console window (that is, the console window for a specified domain). The application is started on the management server.
`SSP Config`	Uses a vi text editor to open and edit the template configuration file: `/var/opt/OV/conf/OpC/ssp` The file must be edited to determine which SSP nodes are to be monitored. The application is started on the node where the OVO agent is running.

Configuring the SSP System for E10000 Systems

To configure the Sun Service Processor (SSP) system, perform these procedures:

1. Reconfigure the SSP `snmpd` daemon.

   See “To Reconfigure the SSP snmpd Daemon” on page 307.

2. *Optional:* Establish remote host equivalence.

   See “To Establish Remote Host Equivalence” on page 308.

3. *Optional:* Export the SSP logfiles directory.

   See “To Establish Remote Host Equivalence” on page 308.

To Reconfigure the SSP snmpd Daemon

To intercept SSP traps on the node with OVO agent installed, the SSP `snmpd` daemon must be reconfigured and restarted.

To reconfigure the SSP `snmpd` daemon, follow these steps:

1. Edit the SSP `snmpd` configuration file:

   ```
   /etc/opt/SUNWssp/snmp/agt/\
   Ultra-Enterprise-10000.snmpd.cnf
   ```

   At the end of the file, add the following lines:

   ```
   #OVO start

   trap snmptrap <OVO_agent_IP_address> 162

   #OVO end
   ```

   Where:

   <OVO_agent_IP_address> is the IP address of the node where OVO agent with SSP SNMP trap template is installed.

2. Restart the `snmpd` daemon.

   a. Stop the running `snmpd` daemon.

   b. Wait for the automatic restart.

3. Determine an `snmpd` PID, then stop the process:

   ```
   ps -e -opid,user,args |grep root | grep snmpd

   kill <snmpd_PID>
   ```

To Establish Remote Host Equivalence

NOTE This procedure is required if you want to monitor the SSP `cbs` daemon.

To establish a remote host equivalence between the SSP system and the node with OVO agent installed, follow these steps:

1. In the `/export/home/ssp` directory, create a `.rhosts` file with the following contents:

   ***<OVO_agent_node_name>* root**

   Where:

   <OVO_agent_node_name> is the IP address of the node where OVO agent with SSP SNMP trap template is installed.

2. Change the permission attributes for the file:

   chmod 400 /export/home/ssp/.rhosts

To Export the SSP Logfiles Directory

NOTE This procedure is required if you want to monitor the SSP logfiles.

1. Add the following directory to the list of directories to be NFS exported at system boot time:

   /var/opt/SUNWssp/adm

2. Edit the `/etc/dfs/dfstab` file by adding the following line:

   share -F nfs -o -ro /var/opt/SUNWssp/adm

3. Export the directory by executing the following command:

   share -F nfs -o -ro /var/opt/SUNWssp/adm

Installing the OVO Agent for E10000 Systems

This section explains how to prepare a node for SSP system monitoring, then install and configure the OVO agent on the node you selected.

Before Installing the OVO Agent

Before installing the OVO agent packages, you must do the following:

1. Choose a node for SSP system monitoring.

   Determine which node will be used for monitoring the SSP system. The OVO agent (for the purpose of monitoring the SSP system) must be installed either on a Sun Solaris or an HP-UX node.

2. Mount the SSP logfiles directory.

   On the node chosen for SSP system monitoring, mount the previously NFS exported SSP logfiles directory:

   `/var/opt/SUNWssp/adm`

To Install the OVO Agent

NOTE This procedure must be performed on the OVO management server.

To install OVO agent packages on the selected node, follow these steps:

1. Add the SSP system to `OVO Node Bank`.

   Use the following menu sequence:

   `Actions:Node->Add`.

2. Distribute the OVO configuration to the selected node.

   In the `OVO Node Bank` window select `Actions:Agents->Install`. You only need to distribute `Software` and `Commands`.

3. Edit the templates configuration file:

   `/var/opt/OV/conf/OpC/ssp`

   a. In the `Application Group - SSP Tools` window, execute the `SSP Config` application. This must be done on the node, where the agent which monitors the SSP is installed.

      This application opens the SSP templates configuration file in a vi text editor tool. The templates configuration file lists nodes to be monitored by the OVO agent. The entries are checked by the monitor and the logfile shell scripts.

   b. Add the SSP node name to the configuration file.

      Observe the following syntax rules:

      `hostname {main|backup} [logfiles]`

`hostname`	Name of a remote host where SSP is running.
`{main|backup}`	Only entries with the keyword `main` are used. All other entries are ignored. That is, only nodes with the keyword `main` are monitored. Backup entries can be used for quick change from monitoring main SSP host to a backup host.
`[logfiles]`	Space-separated list of SSP logfiles that are monitored.

NOTE You must restart the OVO agent to activate the changes in the templates configuration file.

4. Assign and distribute templates to the selected OVO agent node.

   In the `OVO Node Bank` window select `Actions:Agents->Assign Templates`, and assign the `SSP` template group to the selected node.

Reconfiguring the SSP Templates

You must reconfigure the SSP templates each time a change from main to backup SSP node occurs. To reconfigure the SSP templates, execute the `SSP Config` application, and edit the templates configuration file as described in “To Install the OVO Agent” on page 309.

About the OVO Integration Package for Sun Management Center

The OVO integration package for Sun Management Center is available as a separate add-on.

For detailed installation and configuration instructions, see the *HP OpenView Operations Integration for Sun Management Center User's Guide*.

The manual is available as an Acrobat Portable Document Format (PDF) document on the management server or on the Internet:

- **Management Server**

  `/opt/OV/doc/C/OpC`

- **Internet**

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

High Availability Support on Sun Solaris

This version of OVO offers the following High Availability (HA) solutions for Sun Solaris on the management server and managed nodes:

- **Sun Enterprise Cluster Support**

  OVO version A.08.00 offers Sun Enterprise Cluster support on both the management server and the managed nodes.

  For installation and configuration instructions, see the *OVO Installation Guide for the Management Server*

  For additional information for system administrators working with OVO in Sun Cluster environments, see the *OVO DCE Agent Concepts and Configuration Guide*.

- **VERITAS Cluster Server Support**

  This version of OVO introduces VERITAS Cluster Server Support on both the management server and the managed nodes.

  For installation and configuration instructions, see the *OVO Installation Guide for the Management Server*.

  For additional information for system administrators working with OVO in VERITAS Cluster Server environments, see the *OVO DCE Agent Concepts and Configuration Guide*.

About the Supplied Perl Interpreter

The managed node software includes a custom binary Perl 5.6.1 distribution.

The Perl is embedded in the Perl interpreter and the monitoring agent, and is designed to be used internally by OVO. Some OVO policies deployed by OpenView Operations for Windows management servers include Perl scripts (for example, some schedules and measurement threshold policies). Perl scripts are also used by some HP-supplied Smart Plug-ins (SPIs).

The Perl interpreter and other binaries are automatically installed into the `$OV_CONTRIB/perl` directory. A basic set of modules is installed in the /opt/OV/nonOV/perl/a/lib/5.6.1/File directory. Pre-existing Perl installations are not altered as a result of installing a managed node.

If you want to use the Perl distribution for additional purposes beyond its internal use within OVO, you should first check which modules are included by listing the `.pl` and `.pm` files within the `/opt/OV/nonOV/perl/a/lib/5.6.1/` directory.

For further information about Perl or if you need to add additional modules, go to the following web site:

`http://www.perl.com`

NOTE

Perl is supplied "as is" with no warranties whether express or implied according to the Perl artistic license agreement. Hewlett-Packard is not responsible for errors in Perl, which is public domain software and not produced by HP. Hewlett-Packard does not support any modifications to the provided Perl distribution. This software is licensed, not sold, and your use of the software is subject to the license terms contained in the license agreement."

10 About Tru64 UNIX Managed Nodes

In this Chapter

This chapter explains how to install and configure HP OpenView Operations (OVO) on Tru64 UNIX managed nodes and TruCluster systems.

HP Tru64 UNIX

Earlier versions of **HP Tru64 UNIX** were known as **Digital UNIX**. It began its existence with the name **DEC OSF/1**.

Definitions

The following terms, used throughout this chapter, are defined here:

- **Tru64 UNIX system**

  An AlphaServer running the Tru64 UNIX operating system. This system may be either a single system or a TruCluster system.

- **Tru64 UNIX managed node**

  A Tru64 UNIX system that has the OVO agent software installed and is being monitored. This system may be either a single system or a TruCluster member.

- **Tru64 UNIX single system**

  A standalone Tru64 UNIX operating system, that is, not part of a cluster.

- **TruCluster system**

  A highly integrated synthesis of the HP Tru64 UNIX operating system software, AlphaServer systems, and storage devices that operate as a single virtual system. TruCluster members can share resources, data storage, and cluster-wide file systems under a single security and management domain, yet they can boot or shut down independently without disrupting client services.

- **TruCluster member**

  An individual Tru64 UNIX system that operates as part of a TruCluster system.

Installation Requirements

This section explains OVO hardware and software requirements for Tru64 UNIX managed nodes.

Hardware Requirements

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

- **Disk Space**

  35 MB (about 60 MB is required during software installation)

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

- **Additional Swap Space**

  None

- **Additional RAM**

  None

NOTE Before you install OVO A.07.12 agent software package, you must first de-install any of the previous agent software packages installed on the managed nodes. For de-installation instructions, see the *OVO Administrator's Reference*.

Software Requirements

Before installing OVO, make sure the following software is installed on Tru64 UNIX managed nodes:

- **Operating System**

  For a list of operating system versions supported by OVO, see the *OVO Installation Guide for the Management Server*.

  For TruCluster systems, the operating system version should be V5.1 or higher.

- **Required Patch for the Tru64 UNIX Managed Nodes**

  The `CXXREDIST632V11.tar` patch is required for the Tru64 UNIX managed nodes.

  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 ftp patch site:

  ftp://ftp.compaq.com/pub/products/c-cxx/tru64/cxx/

- **Kernel Parameters**

  For a list of kernel parameters, see the *OVO Administrator's Reference*. You can verify and change the kernel parameters using the `setup` tool.

NOTE

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_per_user` to:
default + (Number_of_Templates * 2).

- **Basic Networking Services**

  OSFCLINET4*xxx* Basic Networking Services. The operating system determines the value of *xxx*.

- **DCE Runtime Kit**

NOTE DCE Runtime Kit software is required only if you choose DCE as communication type.

Table 10-1 DCE Runtime Kit Requirements

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 only	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

NOTE OVO supports DCE versions supplied with the Tru64 UNIX operating system. However, although the 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.

- **Japanese Base System**

  `IOSJPBASE4xxx` Japanese Base System. This system is only for managed nodes running Tru64 UNIX in a Japanese environment.

- **Package: OSFINCLUDExxx**

  OSFINCLUDExxx Standard Header Files package is required for building executables on Tru64 UNIX nodes. The operating system determines the value of *xxx*.

TruCluster System Notes and Recommendations

This section is a capsulation of the features, notes, and recommendations for monitoring applications on a TruCluster system.

- For TruCluster systems, the operating system version should be V5.1 or higher.
- DCERTS410 DCE Runtime Services V4.1 and DCERTS420 DCE Runtime Services and V4.2 are the only valid DCE runtime kits for TruCluster systems.
- NCS RPC communication is supported on single Tru64 UNIX managed nodes, but it is not supported on TruCluster managed nodes.
- Only the OVO A.06.xx and OVO A.07.xx agent software have been validated on TruCluster systems.
- You must create an OVO node group for your TruCluster system and add the TruCluster members to this node group.

  See the section “Tips for Installing Agents” on page 323 for more information.
- Installing or de-installing the agent software must be done on one TruCluster member; the software is added to or deleted from the other TruCluster members automatically.
- The `/usr/opt/OV` and `/var/opt/OV` directories are Context Dependent Symbolic Links (CDSLs). The pathnames for these directories are `/usr/cluster/members/{memb}/opt/OV` and `/var/cluster/members/{memb}/opt/OV`, where `{memb}` is used to access member-specific files in a TruCluster system.
- You must execute the `/opt/OV/bin/OpC/install/cluster_deploy.sh` shell script on the management server with the TruCluster node group name parameter to start the heartbeat polling on all TruCluster members.

- If TruCluster members were either down during the agent installation and were subsequently brought up or were added after the agent software installation, they must be activated. See “Activating Subsequent TruCluster Members” on page 333 for more information.
- Before a highly available CAA application can be monitored by OVO, changes need to be made in the action script for the monitoring to relocate during failover. Refer to the section titled “Relocating the Monitoring of a Single-Instance Application during a Failover (TruCluster Systems)” for specific information.

Installing and De-installing Agents

This section describes how to install and de-install OVO on Tru64 UNIX managed nodes, including TruCluster managed nodes.

NOTE Before you install OVO A.07.12 agent software package, you must first de-install any of the previous agent software packages installed on the managed nodes. For de-installation instructions, see the *OVO Administrator's Reference*.

Tips for Installing Agents

When installing Tru64 UNIX managed nodes, follow these guidelines:

❑ **General TruCluster Installation Procedure**

The following procedure is a general procedure for installing the agent software on a TruCluster system; additional information is located in the remainder of this section. Be sure to perform all the following steps in the order given.

On TruCluster members:

1. Ensure that legacy agent software is not present on the TruCluster members. See the section titled "De-installing Agents" on page 334 for more information.

On the management server:

2. Create an OVO node group for the TruCluster system.
3. Add the TruCluster members to this OVO node group.
4. Distribute the Agent software on only one TruCluster member; the agent software is propagated to the other TruCluster members automatically. Also, all the TruCluster members are activated.
5. Execute the `/opt/OV/bin/OpC/install/cluster_deploy.sh` shell script with the TruCluster node group name parameter to start the heartbeat polling on all the TruCluster members.

6. Assign templates to each TruCluster member or to the TruCluster OVO node group.
7. Distribute the templates to each TruCluster member or to the TruCluster OVO group node.

❑ **Management Server**

The name of the management server must be known to the managed node.

That is, the name of the management server must be registered on the name server or in the local host table:

`/etc/hosts`

You can verify the name of the management server with the `nslookup` command.

❑ **Agent Software**

The OVO agent software is installed on the following file tree:

`/usr/opt`

If there is not enough space for installation of the OVO agents, create a symbolic link *before* installing OVO.

- Single system

  For single systems, consider the following example if `/bigdisk` s is a local file system with enough free space:

  ```
  mkdir -p /bigdisk/OV

  ln -s /bigdisk/OV /usr/opt/OV
  ```

- TruCluster system

  For TruCluster systems, increase the size of the `/usr` filesystem by using the Advanced File System (AdvFS) `advol` command.

- **Logfile Encapsulator**

  By default, some logfiles monitored by the logfile encapsulator are *not* present on Tru64 UNIX managed nodes.

  For example:

  `/var/adm/messages`, `/usr/adm/lplog` or `/var/adm/sialog`.

  To add `/var/adm/messages` and `/usr/adm/lplog` to the managed node, add the following to the `/etc/syslog.conf` file:

  `kern.debug /var/adm/messages`

  `lpr.debug /usr/adm/lplog`

  To add `/var/adm/sialogr` to the managed node, enter the corresponding command:

  `touch /var/adm/sialogr` for single systems

  `mkcdsl /var/adm/sialog` for TruCluster systems

- **DCE RPC and NCS RPC**

  Before installing the OVO agent software on Tru64 UNIX managed nodes, make sure to set up and configure DCE RPC or NCS RPC correctly. Tru64 UNIX managed nodes support both DCE RPC and NCS RPC as communication types. Single Tru64 UNIX managed nodes support both DCE RPC and NCS RPC as communication types. TruCluster managed nodes support only DCE RPC communication.

NOTE NCS communication type is not supported on TruCluster systems.

- **Installation on NIS Clients**

  If the managed node is a Network Information Service (NIS or NIS+) client, the OVO installation checks if user `opc_op` is already in the NIS database:

  - If `opc_op` is in the NIS database, no additional user is installed.
  - If `opc_op` is *not* in the NIS database, `opc_op` is added only locally on the managed node.

  The OVO operator `opc_op` must be a member of the `opcgrp` group.

Configuring DCE on the Managed Nodes

NOTE For TruCluster systems, you must configure DCE on each TruCluster member.

To configure DCE, follow these steps:

1. In a terminal window, enter the following:

   `dcesetup`

   This command starts the `dcesetup` program.

2. Choose the following menu option:

   `1) Configure.`

3. When prompted, enter **`y`** to confirm the selection.
4. When prompted, enter **`y`** to reconfigure the DCE client.
5. Select the option that best suits your needs:

   - *RPC Only*

     If you have installed DCE 3.x but do *not* want advanced DCE features, select this option:

     `6) Configure this system for RPC only.`

   - *DCE Client*

     If you have installed DEC 2.x or 3x and want advanced DCE features, do this:

     a. Select this option:

        `1) Configure this system as a DCE Client.`

        You are then prompted with the following question:

        `Would you like to search the LAN for known cells?`

b. Respond to the prompt as follows:

- *Automatic Setup*

  If you have configured cells and want the DCE setup utility to find them, enter **`y`**. When prompted with additional questions, accept the default answers offered by `dcesetup`.

- *Manual Setup*

  If you want to manually configure a client to use an existing cell, enter **`n`** and the name of the cell: **`ito`**. This cell must be configured on the DCE server.

  When prompted, do the following:

  1. Enter the hostname of the Master CDS Server.
  2. Indicate that the cell you are configuring can broadcast to the Master CDS Server by entering **`y`**.
  3. If the time displayed is correct, enter **`y`**.
  4. Choose whether you want run Distributed Time Service (DTS) on the node.
  5. Choose whether you want to enable DCE SIA.
  6. Enter the principal name (for example, **`cell_admin`**) and password for the DCE server.
  7. Enter **`y`** to delete the principals.

6. When prompted, enter **`y`** to verify the configuration.

   OVO configures the managed nodes as a DCE client and starts the DCE daemon `dced`.

Removing an Existing DCE Configuration

To remove an existing DCE configuration, use the following options from the main menu:

- ❏ `6) Clean`
- ❏ `7) Clobber`

Installing Agent Software and Activating the Managed Nodes

To install the agent software and activate it on the managed node, you have the choice of using either OVO GUI, or install and activate the managed node manually.

If errors occur during the installation, check the local installation logfile:

```
/var/adm/smlogs/setld.log
```

Installing and Activating Agent Using OVO GUI

For standard installation instructions, see the *OVO Administrator's Reference*.

To activate the node from the OVO GUI, perform the following steps on the management server:

1. **Add the pre-installed nodes to the OVO Node Bank window:**

   Use the following menu sequence:

   ```
   Actions-> Node-> Add
   ```

2. **For TruCluster systems, create an OVO node group.**

3. **Add the node to an OVO node group.**

   Drag and drop the node onto a node group in the OVO Node Group Bank window.

   For TruCluster systems, drag and drop the nodes for all the TruCluster members into the OVO node group

4. **Open the Install/Update OVO Software and Configuration window.**

   Use the following menu sequence:

   ```
   Actions-> Agents-> Install / Update SW & Config
   ```

5. **Update all components.**

   In the `Install/Update OVO Software and Configuration` window, do the following:

   a. Select all components.

NOTE

For TruCluster systems, you need to select all the components for only the first TruCluster member. For the other TruCluster members, select all the components except the agent software.

CAUTION

Do not check `[Force Update]` unless this is the initial installation on a TruCluster system. If you check this option, the management server re-installs the agent.

   b. Click `[OK]`.

   Depending on whether you have pre-installed the agent, the management server does the following:

   - If you have pre-installed the agent on the node, the management server activates the node, and installs the selected components.
   - If you have *not* pre-installed the agent software, the management server installs the agent.

   On TruCluster systems, the agent software is propagated to the other TruCluster members at this time. Also, all the TruCluster members are activated.

6. **For TruCluster systems, update the database and start heartbeat polling. Otherwise skip this step.**

   Execute the `/opt/OV/bin/OpC/install/cluster_deploy.sh` shell script on the management server with the TruCluster node group name parameter.

7. **Verify that the control, message, and action agents are all running on the managed node.**

   Enter the following:

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

Installing the Agents Manually

In some situations, you may want to install the OVO Tru64 UNIX agent software without using the management server. This manual installation enables you to prepare the system to become an OVO managed node when it is later connected to the network. Manual installation is useful if you are preparing many systems in a central location, or if you want to avoid the network root connection necessary for standard installation.

For TruCluster systems, install the agents on any TruCluster member; the agent software is propagated automatically.

1. **Copy the OVO agent packages and installation script to a temporary directory on the managed node.**

   On the management server, these are the following files:

   - `opc_pkg.Z`
   - `comm_pkg.Z`
   - `perf_pkg.Z`
   - `opc_inst`

The files are located in one of the following directories on the management server, depending on the operating system and DCE versions installed on your managed node:

- Tru64 UNIX version V5.1A and DCE version V4.2

  ```
  /var/opt/OV/share/databases/OpC/mgd_node/vendor/ \
  dec/alpha/unix51A+/A.08.00/RPC_DCE_[TCP|UDP]/
  ```

- Tru64 UNIX versions V5.1 or earlier and DCE version V4.1 or earlier

  ```
  /var/opt/OV/share/databases/OpC/mgd_node/vendor/ \
  dec/alpha/unix/A.08.00/RPC_DCE_[TCP|UDP]/
  ```

For a list of supported operating system versions and DCE Runtime Kit versions, see Table 10-1 on page 319.

2. **Install the Agent.**

   a. Change the permissions of the agent installation script to ensure that it can be executed:

      `chmod +x /tmp/opc_inst`

   b. Start the agent installation script by entering:

      `/tmp/opc_inst <arguments>`

   All arguments passed to the `opc_inst` command (except `-h`) are passed to the `opcactivate` command. See Step 4 of the section "Activating the Managed Nodes Manually" on page 331. This command also activates the managed node; for a TruCluster system, this activates all the TruCluster members.

   On TruCluster systems, the agent software is propagated to the other TruCluster members at this time.

Activating the Managed Nodes Manually

After you install the agent software, activate the agent software on the node by following these steps:

3. **Add the pre-installed nodes to the OVO Node Bank window.**

   Use the following menu sequence:

   ```
   Actions-> Node-> Add
   ```

4. **For TruCluster systems, create an OVO node group on the management server.**
5. **On the management server, add the node to an OVO node group.**

   Drag and drop the node onto a node group in the `OVO Node Group Bank window`.

   For TruCluster systems, drag and drop the nodes for all the TruCluster members into the OVO node group.
6. **Activate the managed node with the opcactivate command, issued on the managed node.**

NOTE

If you entered any arguments to the `/tmp/opc_inst` command in Step 2 of "Installing the Agents Manually" on page 330, you may skip this step.

Enter the following:

```
/opt/OV/bin/OpC/install/opcactivate -s <OVO_mgt_server> \
-cs <server_codeset> -cn <agent_codeset>
```

NOTE

For TruCluster systems, you must activate all TruCluster members individually.

This command activates the agent, which then attempts to send messages to the management server.

a. Specifying the `-s` option with the opcactivate command is optional. This option starts the `/opt/OV/bin/OpC/install/upd_res.sh` script which integrates the OVO agent into the system startup and shutdown scripts, such as startup script in the `/etc/init.d` file.

b. `-cs <server_codeset>` is the character set for the OVO management server.

c. `-cn <agent codeset>` is the character set for this agent.

For more information about codesets, see the *OVO Administrator's Reference* and the man page *opcactivate(1M)*.

7. **On the management server, update the database and start heartbeat polling for the managed node.**

   For TruCluster systems, execute the **`/opt/OV/bin/OpC/install/cluster_deploy.sh`** shell script on the management server.

   For single systems, enter the following command on the management server after the node is connected to the network:

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

   The templates, monitors, commands, and so on must still be installed using the OVO GUI.

Activating Subsequent TruCluster Members

It may be necessary to activate TruCluster members in the following cases:

- ❏ TruCluster members were down during the installation and were subsequently brought up.
- ❏ TruCluster members were added after the agent software installation.

The agent software is propagated automatically to the TruCluster member. Use these steps to activate them:

1. On the management server, add the TruCluster member to the node group for the TruCluster system.
2. On the managed node, (that is the TruCluster member), run the following command:

   ```
   /opt/OV/bin/OpC/install/opcactivate -s <OVO_mgt_server> \
   -cs <server_codeset> -cn <agent_codeset>
   ```

3. On the management server, run the following commands:

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

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

Verification

After the templates have been assigned and distributed, verify the installation by executing the `/usr/opt/OV/bin/OpC/utils/submit.sh` shell script on all TruCluster members and examine the messages in the Message Browser.

De-installing Agents

For TruCluster systems, you need to de-install the agents only on one TruCluster member. The agent software is de-installed on all the other TruCluster members automatically.

De-installing Agents with Standard De-installation

For standard de-installation instructions, see the *OVO Administrator's Reference*.

If errors occur during the de-installation, check the local de-installation logfile:

`/var/adm/smlogs/setld.log`

To De-install an Agent Manually

To de-install an agent manually, follow these steps:

1. Stop all OVO agents running on the managed node.

   For TruCluster systems, you need to stop the agents on all TruCluster members.

2. De-install the OVO agent software from the managed nodes by entering:

   `setld -d OPCPERFAGT000 OPCCOMMAGT000 OPCAGT000`

About Preconfigured Elements

This section describes preconfigured templates, template groups, and applications used by OVO on Tru64 UNIX managed nodes.

To Modify a Logfile Template

For detailed information about encapsulated logfiles, see the template in the OVO GUI.

NOTE Logfile templates are configured to collect information from logfiles that are produced by standard installations. If you are monitoring a non-standard installation, you should modify the templates to suit your special situation.

Before editing `syslog.conf` on your Tru64 UNIX system, read the man page *syslog.conf(1M)*.

To modify a logfile template, follow these steps:

1. If `/var/adm/messages` is not already included in the `/etc/syslog.conf` file, add the following line (using tabs, *not* spaces):

   `kern.debug /var/adm/messages`

2. Create the following file:

   `/var/adm/messages`

   For example, use the `touch` or the `mkcdsl` command with the following ownership and permission:

   ```
   -rw-r-----   1 root     adm messages
   ```

3. Restart the `syslogd` process.

No SNMP Event Interception

The OVO event interceptor is *not* supported on Tru64 UNIX managed nodes.

Types of Default Applications

For a list of default applications available for UNIX managed nodes, see the *OVO Administrator's Reference*.

Distributing Scripts and Programs

For Tru64 UNIX managed nodes, the platform selector and architecture identifier is the following:

```
dec/alpha/unix
```

Location of User Scripts and Programs

Table 10-2 shows the location of user scripts and programs provided on the management server.

Table 10-2 Location of User Scripts and Programs on the Management Server

Script/Program	Location
Automatic actions, operator-initiated actions, and scheduled actions	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /dec/alpha/unix/actions/*`
Monitoring scripts and programs used by the monitoring agent and the logfile encapsulator	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /dec/alpha/unix/monitor/*`
Scripts and programs called through command broadcast or started from the Application Desktop	`/var/opt/OV/share/databases/OpC/mgd_node/customer\ /dec/alpha/unix/cmds/*`

About Temporary Directories

Table 10-3 shows the temporary directories for distributed scripts and programs on the managed nodes.

Table 10-3 Temporary Directories for Distributed Scripts and Programs on the Managed Nodes

Managed Node	Operating System	Temporary Directory

DEC Alpha AXP	Tru64 UNIX	`/var/opt/OV/tmp/OpC/bin/actions`
		`/var/opt/OV/tmp/OpC/bin/cmds`
		`/var/opt/OV/tmp/OpC/bin/monitor`

About Target Directories

Table 10-4 shows the target directories for distributed scripts and programs on the managed nodes.

Table 10-4 Target Directories for Distributed Scripts and Programs on the Managed Nodes

Managed Node	Operating System	Target Directory	Access Rights
DEC Alpha AXP	Tru64 UNIX	`/var/opt/OV/bin/OpC/actions`	`rwxr-xr-x` (owner:root)
		`/var/opt/OV/bin/OpC/cmds`	`rwxr-xr-x` (owner:root)
		`/var/opt/OV/bin/OpC/monitor`	`rwxr-xr-x` (owner:root)

Relocating the Monitoring of a Single-instance Application during a Failover (TruCluster Systems)

Cluster Application Availability (CAA) is used to start a single-instance application on an individual TruCluster member and relocate it during failover to another cluster member. This section explains how to use CAA to relocate application monitoring during a failover.

❏ **References**

For more information on CAA, refer to the *Cluster Highly Available Applications* manual in the Tru64 UNIX TruCluster documentation set. Chapter 2, Using CAA for Single-Instance Application Availability, is particularly useful.

For more information on TruCluster system administration, refer to the *Cluster Administration* manual in the Tru64 UNIX TruCluster documentation set.

Tru64 UNIX documentation is available online at the following URL: `http://www.tru64unix.compaq.com/docs/pub_page/doc_list.html`

❏ **Procedure**

Perform the following:

1. Make the application a highly available CAA resource as follows:
   a. Create the CAA resource profile and action script for the application, either through the `SysMan` menu or by using the `caa_profile` command. This step creates the `/var/cluster/caa/profile/<name>.cap` and `/var/cluster/caa/scripts/<name>.scr` files, respectively.
   b. Test the action script.
   c. Validate the resource profile.
   d. Register the resource with CAA.
   e. Start the resource.

2. From the OVO server, assign the template that you created to monitor your application to all TruCluster members.
3. From the OVO server, distribute this template to all cluster members.
4. After the initial distribution of the template, use the `opctemplate -d` command to disable the template for all cluster members on which the application does not run.

   `opctemplate -d <template-name>`

   where *<template-name>* is the name of the template.

   On subsequent template distributions, the template state is maintained on the managed TruCluster members. Hence, this step is required only after the initial template distribution.
5. Edit the application action script.

   There are three main routines of the action script: start, stop, and list.

   a. Enable the template in start routine with the `opctemplate -e` command.

   b. Disable the template in stop routine with the `opctemplate -d` command.

   c. List all templates with type, name and status with the `opctemplate -l` command. This is the default task of the `opctemplate` command.

   Consider the examples at the end of this section.

   With these changes, if the TruCluster member on which the application is running fails, or if a particular required resource fails, CAA does the following:

   - Disables the monitoring of the application.
   - Relocates or fails over the application to another member that either has the required resources available or on which the required resource can be started.
   - Starts monitoring the application on that other member.

❑ **Examples**

- **Sample Application**

  The following is a simple `Tcl/Tk` application named `xhostname` that will be monitored by OVO:

```
#!/usr/bin/wish
set hname [exec hostname -s]
set clarg [lindex $argv 0]

wm minsize . 350 30
wm title . "$argv0 on $hname $clarg"

button .hostname -font helvb24 -text $hname -command { exit
}
pack .hostname -padx 10 -pady 10
```

- **CAA Profile**

  The following is the CAA profile for the `xhostname` application:

```
NAME=xhostname
TYPE=application
ACTION_SCRIPT=xhostname.scr
ACTIVE_PLACEMENT=0
AUTO_START=0
CHECK_INTERVAL=60
DESCRIPTION=xhostname
FAILOVER_DELAY=0
FAILURE_INTERVAL=0
FAILURE_THRESHOLD=0
HOSTING_MEMBERS=
OPTIONAL_RESOURCES=
PLACEMENT=balanced
REQUIRED_RESOURCES=
RESTART_ATTEMPTS=1
SCRIPT_TIMEOUT=60
```

- **CAA Action Script**

  The following is the CAA action script for the `xhostname` application. This script contains annotations to show you where you need to modify the existing code.

```
#!/usr/bin/ksh -p
#
# ****************************************************************
# *                                                              *
# *    Copyright (c) Digital Equipment Corporation, 1991, 1998   *
# *                                                              *
# *   All Rights Reserved.  Unpublished rights  reserved  under  *
# *   the copyright laws of the United States.                   *
# *                                                              *
# *   The software contained on this media  is  proprietary  to  *
# *   and  embodies  the  confidential  technology  of  Digital  *
# *   Equipment Corporation.  Possession, use,  duplication  or  *
# *   dissemination of the software and media is authorized only *
# *   pursuant to a valid written license from Digital Equipment *
# *   Corporation.                                               *
# *                                                              *
# *   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  DFARS  252.227-7013, *
# *   or  in  FAR 52.227-19, as applicable.                      *
# *                                                              *
# ****************************************************************
#
# HISTORY
#
# @(#)$RCSfile$ $Revision$ (DEC) $Date$
#
# This is the CAA action script for the xhostname application.
```

```
# This action script has been modified so that the monitoring
# of the application fails over along with the application.
#
# The start and stop routines of the script have been enhanced
# to enable the monitoring template in the start routine and disable
# the monitoring template in the stop routine. This is done using
# the "opctemplate -e | -d" command.  If the enabling and
# disabling of the monitoring template was not successful
# a message is sent to the OVO management server. In order
# that the message is sent, the opcmsgi agent should be
# running on the managed nodes (Assign and Distribute the
# Default Digital UNIX (Tru64 UNIX) opcmsg(1|3) template onto all
# the TruCluster nodes).
#

PATH=/sbin:/usr/sbin:/usr/bin
export PATH
XHOSTNAME=/usr/bin/xhostname
export DISPLAY="<hostname>:0"
```

(You need to add this next block of code from here ...

```
# PATH for the opctemplate and opcmsg command
OPCTEMPLATE=/usr/opt/OV/bin/OpC/opctemplate
OPCMSG=/usr/opt/OV/bin/OpC/opcmsg

# Monitoring template for the Xhostname application
# that has been assigned and distributed to all the
# TruCluster nodes.
TEMPLATE=Xhostname
```

... to here)

```
case $1 in
```

```
    'start')
# Start the xhostname application
        if [ -x $XHOSTNAME ]; then
            if $XHOSTNAME &
            then
```

(You need to add this next block of code from here ...

```
# Check if the opctemplate command exists. Enable the template.
               if [ -x $OPCTEMPLATE ]; then
                  $OPCTEMPLATE -e $TEMPLATE
# Check if the enabling of the template was successful
# else send a message to the OVO management server.
                  if [ `$OPCTEMPLATE -l $TEMPLATE |
                     grep -c enabled` -ne 1 ]
                  then
# Check if the opcmsgi agent is running. This agent is needed to
# send the message to the OVO management server.
                       if [ `ps -eaf | grep -v grep |
                             grep -c opcmsgi` -ne 0 ]
                       then
                          $OPCMSG appl=$TEMPLATE \
                          msg_grp=OS \
                          object=daemon \
                          msg_text="Template $TEMPLATE not enabled" \
                          sev=warning
                       fi
                  fi
               fi
```

... to here)

```
                       fi
        fi
```

```
        exit 0
    ;;

    'stop')
```

(You need to add this next block of code from here ...

```
# Check if the opctemplate command exists and disable the template
        if [ -x $OPCTEMPLATE ]; then
           $OPCTEMPLATE -d $TEMPLATE
# Check if the disabling of the template was successful else send a
# message to the OVO management server.
           if [ `$OPCTEMPLATE -l $TEMPLATE |grep -c disabled` -ne 1 ]
           then
# Check if the opcmsgi agent is running. This agent is needed to
# send the message to the OVO management server.
                if [ `ps -eaf |grep -v grep |grep -c opcmsgi` -ne 0 ]
                then
                   $OPCMSG appl=$TEMPLATE \
                   msg_grp=OS \
                   object=daemon \
                   msg_text="Unable to disable template $TEMPLATE" \
                   sev=warning
                fi
           fi
        fi
```

... to here)

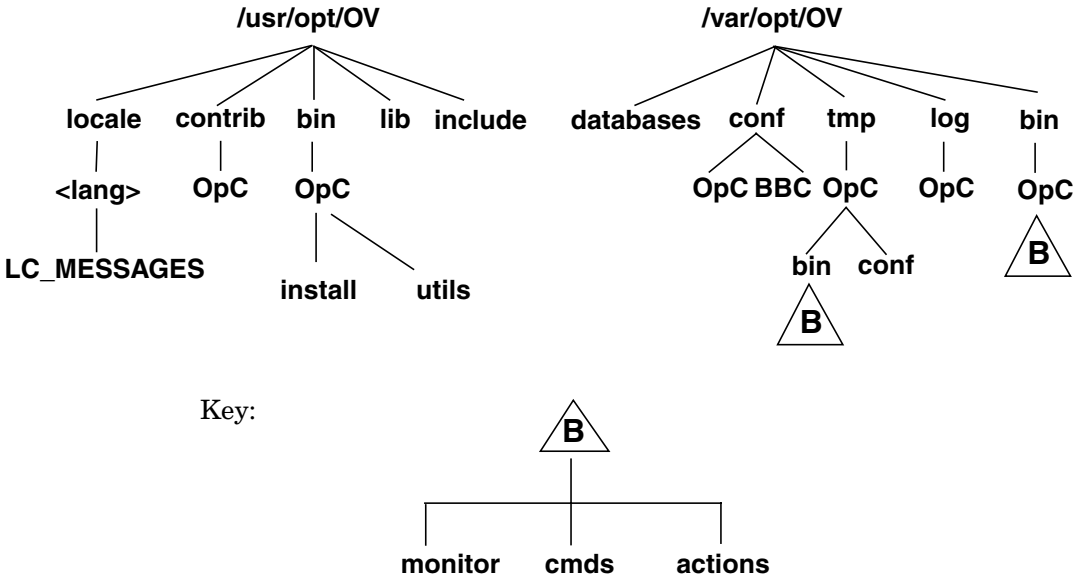
```
# Check if the xhostname application is running and stop it.
        ps -eu 0 -o pid,command | grep -v grep |
        grep -E '/usr/bin/xhostname' | cut -f1 -d' ' | \
        xargs kill -KILL
```

```
        exit 0
    ;;

    'check')

        PID=`ps -eu 0 -o command | grep -v grep | grep -E
'/usr/bin/xhostname' `
        if [ -z "$PID" ] ; then
            exit 1
        fi

        exit 0
    ;;

    *)
        $ECHO "usage: $0 {start|stop|check}"
        exit 1
    ;;
esac
```

Organization of Managed Nodes

Figure 10-1 shows how OVO software is organized on Tru64 UNIX managed nodes.

Figure 10-1 OVO Software on Tru64 UNIX Managed Nodes



Location of Files

On Tru64 UNIX managed nodes, files are located as follows:

- **Process-related Files**

  `/var/opt/OV/tmp/OpC`

- **Agent Configuration Files**

  `/var/opt/OV/conf/OpC`

About the Default OVO Operator

If they do not already exist, the default OVO operator `opc_op` and group `opcgrp` are created. You add user `opc_op` and group `opcgrp` only locally on the managed node (with `useradd` or `groupadd`).

If the managed node is a Network Information Service (NIS or NIS+) client, the OVO installation checks if user `opc_op` is already in the NIS database:

- If `opc_op` is in the NIS database, no additional user is installed.
- If `opc_op` is *not* in the NIS database, `opc_op` is added only locally on the managed node.

The OVO operator `opc_op` must be a member of the `opcgrp` group.

About Default OVO Operator Entries

The default OVO operator is added to the following directory:

`/etc/passwd`

Fields include the following:

`User Name`	`opc_op`
`Encrypted Password`	`*` (no login)
`User-ID`	Either `777` (if still available) or next possible free number
`Group-ID`	Either `77` (if still available) or next possible free number
`Description`	Default OVO operator
`Home Directory`	`/usr/users/opc_op`
`Login Shell`	`/bin/sh`

About Default OVO Operator Group Entries

The default OVO operator group is added to the following directory:

`/etc/group`

Fields include the following:

`Group Name`	`opcgrp`
`Encrypted Password`	Empty
`Group-ID`	`77` or higher
`Users`	`opc_op`
`Description`	Default OVO operator group

Types of System Resources

During installation, OVO makes changes in the following system resource files:

`/etc/passwd` `/etc/shadow` (if present)	Default OVO operator entry and Protected Password Database (if present).
`/etc/group`	Default OVO operator group entry.
`/sbin/init.d/opcagt`	OVO startup and shutdown script.
`/sbin/rc0.d`	Creates the `K01opcagt` file.
`/sbin/rc2.d`	Creates the `K01opcagt` file.
`/sbin/rc3.d`	Creates the `S97opcagt` file.

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

Types of Libraries

Table 10-5 describes the managed node libraries for OVO A.05.xx, A.06.xx, and A.07.xx.

Only the OVO A.06.xx and OVO A.07.xx libraries are valid for TruCluster systems.

Table 10-5 Libraries for the OVO Managed Nodes

	Item	OVO A.05.xx	OVO A.06.xx	OVO A.07.xx
DCE	Library	**libopc_r.so**	**libopc_r.so**	**libopc_r.so**
	Libraries linked to the OVO library	/usr/shlib/libiconv.so /usr/shlib/libdce.so /usr/shlib/libdce_r.so (optional) /usr/shlib/libphtreads.so /usr/shlib/libpthread.so /usr/shlib/libmach.so /usr/shlib/libexc.so /usr/shlib/libc.so /usr/shlib/libcxx.so	/usr/shlib/libiconv.so /usr/shlib/libdce.so /usr/shlib/libdce_r.so (optional) /usr/shlib/libphtreads.so /usr/shlib/libpthread.so /usr/shlib/libmach.so /usr/shlib/libexc.so /usr/shlib/libc.so /usr/shlib/libcxx.so	/usr/shlib/libiconv.so /usr/shlib/libdce.so /usr/shlib/libdce_r.so (optional) /usr/shlib/libphtreads.so /usr/shlib/libpthread.so /usr/shlib/libmach.so /usr/shlib/libexc.so /usr/shlib/libc.so /usr/shlib/libcxx.so /usr/opt/OV/lib/libnsp.so
	Link and compile options	-lopc_r	-lopc_r	-lopc_r
	Description	N/A	N/A	N/A

Table 10-5 Libraries for the OVO Managed Nodes (Continued)

	Item	OVO A.05.xx	OVO A.06.xx	OVO A.07.xx
NCS	Library	N/A	**libopc.so**	**libopc.so**
	Libraries linked to the OVO library	N/A	/usr/lib/libnck.a /usr/lib/libc.a /usr/shlib/libiconv.so /usr/shlib/libcxx.so	/usr/lib/libnck.a /usr/lib/libc.a /usr/shlib/libiconv.so /usr/shlib/libcxx.so
	Link and compile options	N/A	-lopc	-lopc
	Description	N/A	N/A	N/A

NOTE NCS RPC communication is supported on single Tru64 UNIX managed nodes, but it is not supported on TruCluster managed nodes.

About the Include File

On an HP AlphaServer platform with Tru64 UNIX managed nodes, use the include file:

```
/usr/opt/OV/include/opcapi.h
```

About the Makefile

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

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

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

- `Makef.dec`

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

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

NOTE For building executables on Tru64 UNIX nodes, `OSFINCLUDExxx` Standard Header Files package is required. See the *Installation Guide* in the Tru64 UNIX documentation set for more information.

About the Supplied Perl Interpreter

The managed node software includes a custom binary Perl 5.6.1 distribution.

The Perl is embedded in the Perl interpreter and the monitoring agent, and is designed to be used internally by OVO. Some OVO policies deployed by OpenView Operations for Windows management servers include Perl scripts (for example, some schedules and measurement threshold policies). Perl scripts are also used by some HP-supplied Smart Plug-ins (SPIs).

The Perl interpreter and other binaries are automatically installed into the `$OV_CONTRIB/perl` directory. A basic set of modules is installed in the /opt/OV/nonOV/perl/a/lib/5.6.1/File directory. Pre-existing Perl installations are not altered as a result of installing a managed node.

If you want to use the Perl distribution for additional purposes beyond its internal use within OVO, you should first check which modules are included by listing the `.pl` and `.pm` files within the `/opt/OV/nonOV/perl/a/lib/5.6.1/` directory.

For further information about Perl or if you need to add additional modules, go to the following web site:

`http://www.perl.com`

NOTE

Perl is supplied "as is" with no warranties whether express or implied according to the Perl artistic license agreement. Hewlett-Packard is not responsible for errors in Perl, which is public domain software and not produced by HP. Hewlett-Packard does not support any modifications to the provided Perl distribution. This software is licensed, not sold, and your use of the software is subject to the license terms contained in the license agreement."

11 About Windows NT/2000 Managed Nodes

In this Chapter

This chapter explains how to install and configure HP OpenView Operations (OVO) on Microsoft Windows NT/2000 managed nodes.

NOTE In this manual, the term “Windows” refers to both the Windows 2000 and Windows NT operating systems.

Installation Requirements

This section explains OVO hardware and software requirements for Microsoft Windows NT/2000 managed nodes.

Hardware Requirements

Before installing OVO, make sure that all involved systems meet these hardware requirements.

Requirements for the OVO Management Server

Make sure your OVO management server meets the following requirements:

❏ **Client Software**

The OVO management server *must* be installed with the client software fileset `OVOPC-CLT`.

Check that the DCE-based client package is installed on the management server, by entering the following:

```
swlist -l product OVOPC-CLT
```

If the DCE-based client package is installed, the output should be similar as the following:

```
OVOPC-CLT      A.07.10         OVO Localized RPC-Based Agents
```

❏ **Kernel Parameter Maxfiles**

Use the following settings for kernel parameter maxfiles:

- *35 or Less Windows Managed Nodes*

  If your installation includes 35 or less Windows managed nodes, use the setting for the kernel parameter maxfiles described in the *OVO Installation Guide for the Management Server*.

- *36 or More Managed Nodes*

  If your installation includes 36 or more Windows managed nodes, increase the setting of maxfiles by the following:

  ```
  3*Number_of_additional_NT_nodes + 15
  ```

Requirements for the Windows Installation Server

If you are using a Windows Installation Server, make sure it meets the following requirements:

- ❑ **Agent Processes**

  15 MB memory for agent processes.

- ❑ **Local Drive**

  35 MB free disk space must be temporarily available on the drive that contains the FTP directory during installation.

- ❑ **NTFS Disk**

  A total fo 65 MB of free disk space must be available on the NTFS-formatted disk:

  - 50 MB for the installed agent files.
  - 15 MB for the agent packages to be transferred to the managed nodes.

- ❑ **Domain Controller**

  The Installation Server must be a domain controller.

Requirements for the Windows Managed Node

Make sure your OVO managed nodes meet the following requirements:

- ❑ **Agent Processes**

  15 MB memory for agent processes.

- ❑ **Local Drive**

  35 MB free disk space must be temporarily available on the drive that contains the FTP directory during installation.

- ❑ **NTFS Disk**

  50 MB of space must be free on the NTFS-formatted disk for the installed agent files.

Software Requirements

Before installing OVO, make sure the following software is installed on Windows managed nodes:

❏ **Operating System**

For a list of operating system versions supported by OVO, see the *OVO Installation Guide for the Management Server*.

❏ **Service Packs**

The following Service Packs are required:

- *Windows NT*

  Service Pack 5 or 6A

- *Windows 2000*

  No Service Pack, Service Pack 1,2,3 or 4

- *Windows NT Terminal Server Edition*

  Service Pack 5 or 6A

NOTE

For information about software requirements for a combination of Windows NT Terminal Server Edition and Citrix MetaFrame, see “About Citrix MetaFrame Integration” on page 433.

❏ **FTP**

FTP Service must be running (required during “FTP Agent Package” installation). The FTP service must have read/write permission for the FTP home directory and must not allow anonymous FTP access if the `Administrator` account is used.

❏ **Name of Management Server**

The name of the management server must be known to the managed node. You can verify this by using the `ping` command.

❏ **Default OVO Operator**

The default OVO operator `HP ITO account` may not be removed from Windows managed nodes because the agents normally run under the operator’s account.

- **Schedule Service**

  Schedule service may *not* be disabled (required during installation)

- **TCP/IP Services**

  TCP/IP services must be running and started automatically.

- **RPC Services**

  RCP services (that is, the (Remote Procedure Call Service) must be running and started automatically.

- **SNMP Services**

  SNMP services must be running if you plan to use discovery and other SNMP features of OVO.

- **DHCP Service**

  DHCP (dynamic address service for Windows clients) may *not* be used because OVO relies on the IP address to identify the managed nodes.

Installing and De-installing Agents

This section describes how to install and de-install Microsoft Windows NT/2000 managed nodes.

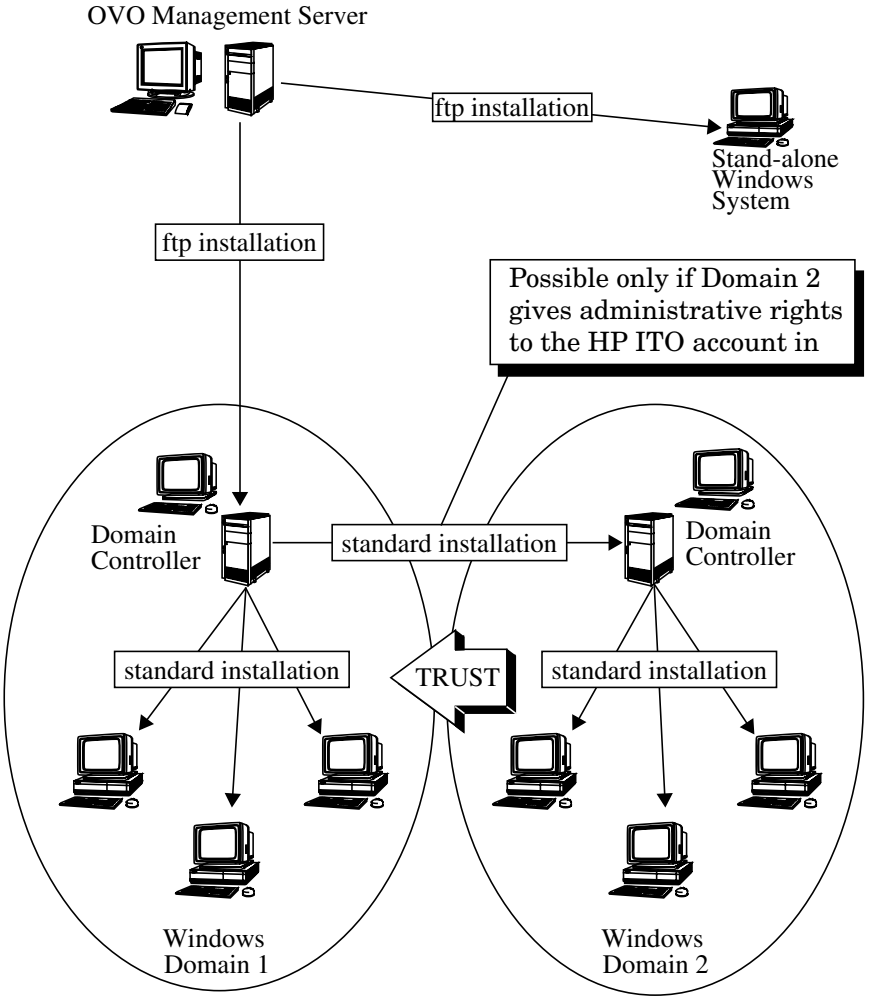
About Installation

NOTE In this manual, a Windows **installation server** is an NT primary or backup domain controller with the OVO agent package installed, or a Windows 2000 domain controller with Active Directory installed.

NOTE If you are using Active Directory in your environment, it is recommended to install the OVO Agent using the `SYSTEM account` instead of the default `HP ITO account`.

Figure 11-1 shows how to install Windows managed nodes.

Figure 11-1 Installing the OVO Windows Agent Package



Methods for Installing Agents

Depending on how your network is configured, you can use one of the following methods to install the OVO agent package on Windows managed nodes:

- **FTP Installation**

  Use this method to install or upgrade agents on system with FTP services running.

  See "Installing Agents through FTP" on page 367.

- **Standard Installation**

  Use this method to install or upgrade agents on the following:

  - System that has an installation server in its domain.
  - System in a domain that gives administrative rights to the `HP ITO account` on an installation server in another domain.

  See "Installing Agents with Standard Installation" on page 373.

- **FTP Re-installation**

  Use this method to re-install agents on the following:

  - System that already has an agent running.
  - System with FTP services running.

  See "Re-installing Agents through FTP" on page 378.

- **Manual Installation**

  Use the standard installation method to install or upgrade agents on the following:

  - Windows system that is not yet connected to the network.
  - Windows system that is connected to a network where an FTP connection with write permission is either impossible or inadvisable.
  - Windows system on which the OVO agents should run under an account other than the `HP ITO account`.

  See "Pre-installing Agents Manually" on page 382.

About OVO Agent Accounts

By default, the OVO agents are installed and run under the account `HP ITO account`. If required, the agents can run under alternative accounts. See the following sections for more information about the `HP ITO account` and about what you should consider if you choose alternative account.

About the "HP ITO account"

By default, the standard installation of the OVO agent package on a Windows managed node installs the `HP ITO account` as a member of the `Administrators` group. As a result, the standard installation gives the account all those user rights that are available under Windows.

Although it is essential that the `HP ITO account` be a member of the `Administrators` group, only those user rights listed in Table 11-1 are required by the account to function correctly. All other user rights associated with the `HP ITO account` by membership in the `Administrators` group may be removed or granted as required.

NOTE Taking away user rights directly from the `HP ITO account` will result in reduced functionality.

Table 11-1 Required User Rights for the "HP ITO account"

User Right	Required in OVO
Access a computer from the network.	By Windows installation server.
Act as part of the operating system.	By OVO action agent to switch user.
Increase quotas.	By the action agent to switch user for application execution.
Log in as a service.	By OVO agent, which runs as a service.
Manage auditing and security log.	During action execution.
Replace a process-level token.	By the action agent to switch user.
Shut down the system.	By the shutdown application.

About Alternative Accounts

The OVO agents can be installed and run under any account, including the SYSTEM account. If you want to choose an account other than the HP ITO account, you must install the agents using the manual or FTP installation method. See “Pre-installing Agents Manually” on page 382 for more information about the installation procedure.

When choosing an alternative account, beware of the following implications:

- **Applications and monitors**

  Applications that are configured to run under the account opc_op or HP ITO account must be changed manually. Specify the same account that you choose for the OVO agents.

  All monitor executables run under the account specified for the OVO agents. This may restrict some of the access rights to monitored applications.

  The SYSTEM account does not have any network access capabilities.

- **Choosing the SYSTEM account**

  If you choose the SYSTEM account, OVO does not create any account, not even the account opc_op.

  If you choose the SYSTEM account for a Domain Controller, you can no longer install the OVO agents on remote systems using the Domain Controller as the installation server because the SYSTEM account does not have any access rights for remote systems. To enable remote installations, configure the HP ITO Installation Service on the Domain Controller to run as a domain user that has domain admin user rights.

- **Choosing a new account**

  If you choose a new account, the account will be created as a member of the Administrators group and the agents will be installed using the specified account name. If an agent with a different account already exists on the system, the new agent will be installed under the new account name. Remove the existing account manually if you no longer need it.

- **Choosing an existing account**

  If the specified account already exists on the system but, the passwords do not match, the existing account is removed and recreated with the same name but a different internal user ID.

- **No account specified**

  If no account is specified, the installation will check for an existing agent installation. If an agent already exists, the same user account will be used for the installation. If no agent is detected, the installation will create the default `HP ITO account`.

Installing Agents through FTP

This section explains how to use the File Transfer Protocol (FTP) to install the agent package from the OVO management server to a Windows domain controller that does not currently have the agent running.

Installing the First Agent

Use the FTP installation method for your first Windows agent package installation, or if you need to create an installation server in a domain that does not give administrative rights to the `HP ITO account` on an installation server in another domain. You must perform this type of installation at least once. The installation method requires FTP services and one manual step on the Windows system.

Installing Additional Agents

If an installation server is already available, and you want to install OVO agent software on additional Windows nodes, see “Installing Agents with Standard Installation” on page 373.

To Install an Agent through FTP

To install an OVO agent on Windows managed nodes using the standard installation method, follow these steps:

1. Make sure that your systems meet all installation requirements.

   Check the “Installation Requirements” on page 357.

2. Select `Window: Node Bank` from any submap to display the `OVO Node Bank` window.

3. Select `Actions: Node: Add...` to display the `Add Node` window.

4. In the `Add Node` window, fill in the following fields:

   `Label` — Enter the name of the node as you want it to be displayed in the `OVO Node Bank`.

   Example:

   `ntserver`

   `Hostname` — Enter the complete hostname of the Windows domain controller that you want to set up as the Windows installation server.

   Example:

   `ntserver.com`

   After you enter this name and press **Return**, OVO looks up and verifies the IP address, as well as the net type, machine type, and operating system name.

   If SNMP services are running on the Windows node, the HTTPS agent is selected by default. Make sure that you select `MS Windows` (without HTTPS).

   If SNMP services are not running on the Windows node, OVO cannot detect the machine type and operating system name. Select `MS Windows` (without HTTPS) and continue with the installation.

`As User` Enter the administrator's user name, or even **anonymous** if the FTP server allows it.

If you are using the administrator's user name, anonymous FTP access must be disabled on the node.

5. Click `[Communication Options]` to display the `Node Communication Options` window.
6. In the `Node Communication Options` window, fill in the following fields:

   `Installation Drive` Enter the letter of an NTFS drive with 10 megabytes of disk space for the agent software. If the drive that you specify does not have enough space, or if you leave this field blank, OVO searches the available local drives for an NTFS drive that has enough free space.

   `Installation Server` Leave this field blank. An installation server is not yet available for this domain. Remember, you are creating an installation server with this procedure. If you enter anything in this field, OVO generates an error message when the installation script runs.

7. Click `[Close]` to dismiss the `Node Communication Options` window, then `[OK]` to dismiss the `Add Node` window.

   The `OVO Node Bank` window now shows a new symbol with the label you entered in the `Label` field (for example, **ntserver**).

8. Add the new node to a node group so that it can be managed by an OVO operator:

   a. Open the `OVO Node Group Bank` window.

   b. Double-click the node group to which you want to add the node.

      Add a new node group if you do not want to use one of the OVO default node groups. Remember to assign any new node groups to an operator.

   c. Drag the node from the `OVO Node Bank` window and drop it into the submap of the node group.

9. Reload the message browser.

10. Display the `Install/Update OVO Software and Configuration` window:
    a. Click the new icon to highlight it.
    b. Choose `Actions:Agents->Install/ Update SW & Config...`
11. Under `Target Nodes`, do this:
    a. Select `[Nodes in list requiring update]`.
    b. Click `[Get Map Selection]`.

    The node name is displayed in the window.
12. Under `Components`, do this:
    a. Select `[Agent Software]`.
    b. Click `[OK]`.

    The installation begins. A new shell opens and starts the installation script.
13. When prompted for the `as user` password, give the password of the Windows system administrator.
14. When prompted for the password of the `HP ITO account`, do one of the following:
    - Specify a password.
    - Press **Enter**.

      OVO creates a password for you.

CAUTION

If you are installing the OVO agent software on a **domain controller**, do *not* let OVO create a password for you. Instead, specify your own password. You will need this password again when installing on another domain controller.

The installation script then installs the agent package on the Windows system.

IMPORTANT

You perform the next five steps on the Windows system. If the Windows system is not physically near you, you can ask someone at the system to perform these steps.

15. On the Windows system, log in as the administrator and open an MS-DOS command prompt.

    If you have read/write access to the FTP home directory drive, you can also install the agent through anonymous FTP with the username **ftp** and the password **ftp**.

16. On the Windows system, switch to the FTP home drive and directory.
17. On the Windows system, change directory to:

    ```
    temp
    ```

18. On the Windows system, enter the following:

    ```
    cscript opc_inst.vbs
    ```

    This command invokes a script that takes about two minutes to execute. The script sets up the domain controller as the Windows managed node. This managed node can also function as the installation server for all other Windows nodes.

    The installation is complete when you see the following line:

    ```
    INSTALLATION SUCCESSFUL
    ```

19. If the installation fails, check the contents of the installation logfile:

    `%SYSTEMROOT%\temp\inst.log`

    to find the cause of the terminated installation, examine the logfile for lines that begin with

    `E->`

    You can also verify the installation by checking the Windows services window and looking for the entry `HP ITO Agent`, which should be running. (The `HP ITO installation service` will not be running. The `HP ITO installation service` runs only when you install the agent on another Windows system, which is a Domain Controller.)

IMPORTANT

You perform the next step on the OVO management server.

20. On the OVO management server, verify that the agent is running on the Windows node:

    a. Click the node icon.

    b. Double-click the `OVO Status` application in the `OVO Application Bank` window.

    This application returns the status of the OVO agent processes. If the agent processes are running, you know that the Windows agent is installed and that the Windows domain controller is functioning as the Windows installation server.

Installing Agents with Standard Installation

This section describes how to install OVO agents on managed nodes in a Windows system using the standard installation method. To learn about other installation methods, see “Methods for Installing Agents” on page 363. For general OVO installation instruction, see the *OVO Administrator’s Reference*.

Domain Requirements for a Standard Installation

Before you begin the standard installation, make sure a Windows installation server is available in one of the following domains:

- Domain of the system you are installing.
- Some other domain where the `HP ITO account` has administrative rights for the system on which you want to install the agent.

If an installation server that meets these requirements is not available, create one by using the procedure explained in “Installing Agents through FTP” on page 367.

OVO Requirements for a Standard Installation

Make sure that the latest version of the OVO agent software is installed on the installation server. For details, see “Hardware Requirements” on page 357.

Although an installation server *can* install the agent package on systems in other domains, you should install the agent package only on systems in the domain of the installation server. The process of creating an installation server automatically installs the `HP ITO account` on the domain controller, where it has the necessary rights throughout the domain. If the `HP ITO account` does not have administrative rights throughout the domain, you have to manually assign them on each system where you install the agent.

For more information on rights and permissions for the `HP ITO account`, see “About the “HP ITO account”” on page 364.

FTP Requirements for a Standard Installation

A standard installation does not require FTP services, and can be performed on any Windows system within the domain of the installation server domain. You can perform a standard installation on the primary or backup domain controller of any domain that grants administrative rights to the `HP ITO account` of another installation server. The primary or backup domain controller can thus be used to create other installation servers in other domains.

To Install an Agent with Standard Installation

To install an OVO agent on Windows managed nodes using the standard installation method, follow these steps:

1. Make sure that your systems meet all installation requirements.

   Check the “Installation Requirements” on page 357.

2. Select `Window: Node Bank` from any submap to display the `OVO Node Bank` window.
3. Select `Actions: Node->Add...` to display the `Add Node` window.
4. In the `Add Node` window, fill in the following fields:

   `Label` — Enter the name of the node as it should be displayed in the `OVO Node Bank`.

   Example:

   `ntworkstation`

`Hostname` Enter the complete hostname of the Windows system where you want to install the agent.

Example:

ntworkstation.com

After you enter this name and press **Return**, OVO looks up and verifies the IP address, as well as the net type, machine type, and operating system name.

If SNMP services are running on the Windows node, the HTTPS agent is selected by default. Make sure that you select `MS Windows` (without HTTPS).

If SNMP services are not running on the Windows node, OVO cannot detect the operating system name, net type, and so on. Select `MS Windows` (without HTTPS) and continue with the installation.

5. Click `[Communication Options]` to display the `Node Communication Options` window.
6. In the `Node Communication Options` window, fill in the following fields:

   `Installation Drive` Enter the letter of an NTFS drive with 10 MB of disk space for the agent software. If the drive that you specify does not have enough disk space, or if you leave this field blank, OVO searches the available drives for an NTFS drive that has enough free disk space.

   `Installation Server` Enter the name of an Windows domain controller that has been set up as an installation server (and is in the same domain, or has administrative rights for the `HP ITO account` in this domain).

   Example:

   ntserver.com

7. Click `[Close]` to close the `Communication Options` window.
8. Click `[OK]` in the `Add Node` window.

9. Add the new node to a node group so that it can be managed by an OVO operator:

   a. Open the `OVO Node Group Bank` window.

   b. Double-click the node group to which you want to add the node.

      Add a new node group if you do not want to use one of the OVO default node groups. Remember to assign any new node groups to an operator.

   c. Drag the node from the `OVO Node Bank` window and drop it into the submap of the node group.

10. If you added a new group, configure the message browser to receive messages from this new group:

    - If the message browser is open, it prompts you for a restart when you finish the step above.
    - If the message browser is *not* open, add the new node group and open the message browser now.

NOTE You can monitor the rest of the installation by looking at messages received in the message browser.

11. Display the `Install/Update OVO Software and Configuration` window:

    a. Click the new icon to highlight it.

    b. Choose `Actions:Agents->Install/ Update SW & Config...`.

12. Under `Target Nodes`, do this:

    a. Select `[Nodes in list requiring update]`.

    b. Click `[Get Map Selection]`.

    The node name is displayed in the window.

13. Under `Components`, do this:

    a. Select `[Agent Software]`.

    b. Click `[OK]`.

    The installation begins. A new shell opens and starts the installation script.

14. When prompted for the password of the `HP ITO account`, do one of the following:

    - Specify a password.
    - Press **Enter**.

      OVO creates a password for you.

CAUTION

If you are installing the OVO agent software on a **domain controller**, do *not* let OVO create a password for you. Instead, specify your own password. You will need this password again when installing on another domain controller.

When installing the agent on another **domain controller**, use the password of the `HP ITO account` on the domain controller where you first installed the agent software.

The installation script then installs the agent package on the Windows system.

15. Verify that the agent is running on the Windows node.

    a. Clicking the node icon.

    b. Double-click the `OVO Status` application in the `OVO Application Bank` window.

       This application returns the status of the OVO agent processes. If they are running, you know that the Windows agent is installed and that the Windows domain controller is functioning as the Windows installation server.

If an Error Occurs During a Standard Installation

If errors occur during a standard installation, check the local installation logfile:

```
%SYSTEMROOT%\temp\inst.log
```

NOTE

NT Terminal Server Edition only:

If, for some reason, the OVO agents were not correctly installed and do not work properly, manual installation is recommended. For instructions, see “Pre-installing Agents Manually” on page 382

Re-installing Agents through FTP

This section explains how to use a Windows installation server to re-install or upgrade the agent package that was originally installed on Windows systems using the FTP installation method (see “Installing Agents through FTP” on page 367). To learn about other installation methods, see “Methods for Installing Agents” on page 363.

Re-installing the First Agent or an Installation Server

Use the FTP re-installation method to re-install or upgrade the following:

- **Agent Package**

  Re-install or upgrade the agent package on the first Windows primary or backup domain controller.

- **Installation Server**

  Re-install or upgrade an installation server in a domain that grants administrative rights to an `HP ITO account` in another domain that contains an available installation server.

Re-installing Additional Agents

If an installation server is already available, and you want to re-install or upgrade OVO agent software on additional Windows nodes, see “Installing Agents with Standard Installation” on page 373.

To Re-install an Agent through FTP

To re-install or upgrade an OVO agent on Windows managed nodes using the FTP re-installation method, follow these steps:

1. Make sure that your systems meet all the listed requirements.

   Check the “Installation Requirements” on page 357.

2. Select `Window: NodeBank` from any submap to display the `OVO Node Bank` window.
3. Select `Actions:Node:Modify...` to display the `Modify Node` window.
4. Click `[Communication Options]` to display the `Node Communication Options` window
5. In the `Node Communication Options` window, fill in the following fields:

   `Installation Drive` Enter the letter of an NTFS drive with 10 MB of disk space for the agent software:

   - If the drive that you specify does not have enough space, or if you leave this field blank, OVO searches the available local drives for a disk that has enough free space.
   - If you are re-installing the OVO agent software, enter the letter of the NTFS drive where the agent software was installed.
   - If you want to re-install on a different NTFS drive, de-install the OVO agent software first, and then proceed with the ftp installation.

   `Installation Server` Enter the complete hostname of the Windows system where you want to install the agent.

   Example:

   `ntsystem.com`

6. Click `[Close]` to close the `Node Communication Options` window.
7. Click `[OK]` to close the `Modify Node` window.

8. Display the `Install/Update OVO Software and Configuration` window:
   a. Click the new icon to highlight it.
   b. Choose `Actions:Agents->Install/ Update SW & Config...`
9. Under `Target Nodes`, do this:
   a. Select `[Nodes in list requiring update]`.
   b. Click `[Get Map Selection]`.

   The node name is displayed in the window.
10. Under `Components`, do this:
    a. Select `[Agent Software]`.
    b. Click `[OK]`.

    The installation begins. A new shell opens and starts the installation script.

    When prompted for the Administrator password, give the password of the Windows system administrator.

    When prompted for the password of the `HP ITO account`, do one of the following:

    - Specify a password
    - Press **Enter**.

    OVO creates a password for you.

CAUTION

If you are installing the OVO agent software on a **domain controller**, do not let OVO create a password for you. Instead, specify your own. You will need this password again when installing on another domain controller.

The installation script then installs the agent package on the Windows node. You will not receive any installation messages in the message browser until the installation is complete.

11. Verify that the agent is running on the Windows node:

    a. Click the node icon.

    b. Double-click the `OVO Status` application in the `OVO Application Bank` Window.

    This application returns the status of the OVO agent processes. If they are running, you know that the Windows agent is installed and that the Windows domain controller is functioning as the Windows installation server.

Pre-installing Agents Manually

In some situations, you may want to pre-install the OVO Windows agent software on a Windows PC without using the management server.

When to Pre-install Agents Manually

Pre-installation makes it possible to prepare the PC to become an OVO managed node when it is later connected to the network. Preparing the PC in this way may be useful if a large number of PCs are prepared in some central location, or if you want to avoid using the root connection over the network that is necessary for a standard agent installation.

The manual installation method also enables you to specify an agent account other than the standard `HP ITO account`.

To Pre-install a Windows Agent on a Windows PC

To pre-install an OVO Windows agent on an OVO Windows PC that will become an OVO managed node, follow these steps:

1. Copy files from the management server to the managed node:

   - *Source Directory on the Management Server*

     ```
     /var/opt/OV/share/databases/OpC/mgd_node/vendor/ms\
     /intel/nt/A.07.10/RPC_DCE_TCP/
     ```

   - *Destination Directory on the Managed Node*

     ```
     C:\temp
     ```

   - *Files to be Copied*

     — `opc_pkg.Z`
     — `comm_pkg.Z`
     — `perf_pkg.Z`
     — `opc_pre.bat`
     — `unzip.exe`
     — `unzip.txt`
     — `opcsetup.inf`
     — `opc_inst.vbs`

     Rename the `*.Z` files to `*.zip`.

2. Edit the `opcsetup.inf` file.

   Change the entries for `Setup Drive` and `Management Server` as appropriate:

```
[Setup Drive]
 C:
[Management Server]
 management_server.domain.com
[Account Password]
(empty by default)
...
```

NOTE

If you leave the password line empty, OVO generates a random password.

If you want to use a specific password, encrypt it on the OVO management server with the `opcpwcrpt` tool under:

```
/opt/OV/bin/OpC/install
```

If you are installing the OVO agent software on a **domain controller**, do not let OVO create a random password for you. Instead, specify your own password. You will need this password again when installing on another domain controller.

Add the following entries to the `opcsetup.inf` file if you want to install the OVO agents under an account other than the `HP ITO account`:

```
[Agent User]
 account name
```

Where *`account name`* is the name of the account to be used. Specify `SYSTEM` to use the built-in accounts. Note that account names may not contain space characters. See “About Alternative Accounts” on page 365 for more information.

3. Create the following file on the managed node:

   - *Directory*

     `C:\temp`

   - *File*

     `nodeinfo`

   - *Contents*

     `OPC_NODE_TYPE CONTROLLED`
     `OPC_MGMTSV_CHARSET iso885915` (or `sjis` for Japanese)
     `OPC_NODE_CHARSET acp1252` (or `acp932` for Japanese)
     `OPC_COMM_TYPE RPC_DCE_TCP`

4. From a command prompt on the Windows PC, run the setup batch file:

   `C:`

   `cd \temp`

   `opc_pre.bat`

5. On the management server, add the Windows node to the node group.

6. When the Windows PC is connected to the OVO management server, update the database and start hearbeat polling for the Windows node:

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

De-installing Agents

This section describes how to de-install OVO agents on Windows managed nodes.

NOTE

If you are de-installing the OVO agent software from a Windows Domain Controller, the accounts for the domain users `HP ITO account` and `opc_op` must be deleted manually after the de-installation of the OVO agent software.

De-installing Agents with Standard De-installation

For standard de-installation instructions, see the *OVO Administrator's Reference*.

To De-install an Agent Manually

To de-install the OVO agent software manually from Windows managed nodes, follow these steps:

1. Stop all OVO agents running on the managed node.
2. Run the following command:

```
\usr\OV\bin\OpC\opcsetup -u
```

If Errors Occur During De-installation

If errors occur during the de-installation, check the local de-installation logfile:

```
%SYSTEMROOT%\temp\inst.log
```

About Preconfigured Elements

This section describes preconfigured templates, template groups, and applications used by OVO on Windows managed nodes.

NOTE For detailed descriptions of the default applications in the `OVO Application Bank` window, see “Types of Default Applications” on page 394.

Monitoring Eventlogs on Windows Managed Nodes

You can set up logfile templates to monitor Eventlogs.

Syntax for Eventlogs

When setting up the templates, set up the fields as follows:

`Logfile` Must have the name of a Windows EventLog with the following syntax:

`%<NAME>_LOG%`

Example:

`%SYSTEM_LOG%`

`File to be executed` Should be empty if you are monitoring a Windows eventlog.

`File to be read` Should be empty if you are monitoring a Windows eventlog.

`Polling Interval` Ignored.

`Logfile Character set` Must be one of the following:

- `ACP1252`

  English/Spanish language nodes

- `ACP932`

  Japanese language nodes

`Read from Last File Position` Should be selected.

Viewing Eventlogs in the Message Browser

Table 11-2 shows how eventlog fields are displayed in the message browser.

Table 11-2 Eventlog to Message Browser Field Correlation

Eventlog Field	Message Browser Field	Comments
Date	Date	The date that the event was created on managed node.
Time	Time	The time the event was created on managed node.
Event ID	Message Text	The Event ID will be displayed before any additional message text[a].
Source	Application	None
Type *error* *information* *warning*	Severity *critical* *normal* *warning*	None
Category	Object	None
Description	Message Text	All other message text (after the Event ID).
User	Not mapped	Not mapped.
Computer	Node	The name of the node as it is known to the management server.
	Msg Group	Empty.

a. Formatted as: `EventID: 0xnnnnnnnn (ai) - description text`

About SNMP Trap and Event Interception

By default, OVO intercepts SNMP traps from any application sending traps to the `opctrapi` daemon running on the management server and on all managed nodes where the OpenView trap daemon (`ovtrapd`) is

running, or where port 162 can be accessed directly. For details about which traps are intercepted by default, see the SNMP trap templates in the `Message Source Templates` window of the OVO administrator GUI.

Types of SNMP Traps

The following kinds of SNMP traps can be intercepted:

- **Well-defined Traps**

  Example: System cold start, network interface up and down, and so on.

- **Internal HP OpenView Traps**

  Example: Traps originating from `netmon`.

NOTE Local event interception is supported only with Network Node Manager (NNM) version 6.2.

About OVO Distributed Event Interception

OVO Distributed Event Interception enables you to intercept SNMP traps on systems other than the OVO management server. This trap interception enbales the messages to be processed locally, thereby improving system performance. Automatic actions, for example, can be triggered and executed directly on the node or in the subnet, instead of being first forwarded to the management server.

To Configure Basic Event Interception

To configure basic OVO Distributed Event Interception, follow these steps:

1. **Configure SNMP devices or the NNM collection station.**

   Make sure that one of the following is true:

   - *SNMP Devices*

     SNMP devices have only one SNMP destination.

     Set the destination systems for SNMP devices on HP-UX nodes in the following file:

     `/etc/SnmpAgent.d/snmpd.conf`

     Use the following statement:

     `trap_dest:<nodename>`

   - *NNM Collection Station*

     There is only one system serving as the NNM collection station for the management server. This station should be connected through the fastest network.

2. **Set the SNMP session mode.**

   If NNM is not running on the node where you want to intercept events, add the following line to the `opcinfo` file on that node:

   `SNMP_SESSION_MODE NO_TRAPD`

3. **Assign and distribute the trap template to the node.**

To Avoid Duplicate Messages in Event Interception

To avoid duplicate messages, make sure that an OVO agent (and thereby, an OVO event interceptor) runs on all NNM collection stations. Use the `Print Collection Station` application in the `NNM Tools` application group to verify which managed nodes are set up as NNM collection stations.

Monitoring Windows Objects

To Monitor Windows Objects

To monitor Windows objects, follow these steps:

1. Set the Monitor to `Program`.
2. In the `Monitor Program or MIB ID` field, enter the following:

   `NTPerfMon\\`

Guidelines for Object and Counter Values

When entering Object and Counter values, follow these guidelines:

- **Fixed Labels**

  The values are fixed labels that can be found for each object you want to monitor.

- **Case-insensitive Labels**

  The labels are not case-sensitive, but must include any spaces.

Guidelines for Parent Instance and Instance Values

When entering Parent Instance and Instance values, follow these guidelines:

- **Valid Values**

  The values vary according to what is being monitored.

- **Question Marks**

  The fields may also be filled with a question mark (**?**), which will allow the string to match any valid value.

- **Parent Instances**

  A parent instance may or may not exist. If there is no parent instance, simply omit it from the syntax.

Locating Objects

OVO will attempt to locate the objects when the agent is started, or when a new template is assigned to the node. If OVO cannot immediately locate the object, it will wait for two minutes and then search again. If OVO cannot locate the object after five attempts, it will send a message to the message browser, notifying the administrator that the object could not be found. The monitor will not begin to search again until the agent is restarted, or the template is reinstalled.

Types of Default Applications

This section describes the default Intel-based applications in the `OVO Application Bank` window, naming the executable that is invoked, and the user-configurable switches, if any. This section is useful if you want to learn how existing Windows applications can be customized for your particular situation and requirements.

About “Cancel Reboot”

This application will cancel a system reboot command that was issued from the OVO reboot application for the selected Windows node.

Default

```
itosdown.exe /a
```

Description of Values Returned

See “About “Reboot”” on page 408.

About “Diagnostics”

This application collects general diagnostic information for the selected Windows node.

Default

`itodiag.exe` (returns all information listed below)

User Configurable Parameters

`osversion` Returns operating system information.

`hardware` Returns hardware information:

- BIOS information
- Processor type:
  - 386
  - 486
  - 586 (Pentium)
  - x686 (Pentium Pro)
- Number of processors in the system

`memory` Returns the following memory information:

- Total paging file size (Windows swap file)
- Available paging file
- Physical location of the page file and its limits (minimum, maximum)

`network` Returns network information.

`nonwdrives` Stops `itodiag` from collecting information about `NAME`, `FILE SYSTEM`, `TOTAL`, and `FREE` for each mapped network drive. Useful in conjunction with the `drives` parameter.

This is useful when the agent user account (`HP ITO account`) has no permissions on one of the drives and the collection causes a login failure on the node that provides the network drive.l.

`drives` Returns the information listed below for each drive:

`DRIVE` Returns current drive letter.

`NAME` Returns any name that is assigned to that drive.

`TYPE` Returns one of these four types of drive:

- `REMOVABLE`

  Floppy drive

- `REMOTE`

  Network connection

- `FIXED`

  Local hard drive

- `CD-ROM`

  CD disk drive

`FILE SYSTEM` Returns one of these file system types:

- `NTFS`
- `NTFAT`
- `DOS`
- `HPFS`
- `OS/2`

`TOTAL` Returns the total size of the drive in MB.

`FREE` `N/A` is reported for the name, file system, and total and free space if the drive is not fixed and the disk is currently not inserted (floppy drive or CD- ROM) or if there is a network connection that requires a password (which is case for administrator connections `C$`, `D$`, and so on).

`processes` Returns the following process information:

- ID
- Name
- Priority (higher number is higher priority) and other information

`cpuload` Returns CPU load information for each processor on the system:

`Processor time` Returns the percentage of elapsed time that a processor is busy executing a non-idle thread. This can be regarded as the fraction of the time spent doing useful work. Each processor is assigned an idle thread in the idle process that consumes those unproductive processor cycles not used by any other threads.

`Private time` Returns the percentage of processor time spent in Privileged Mode in non-idle threads. The Windows service layer, the Executive routines, and the Windows Kernel execute in Privileged Mode.

`User Time` Returns the percentage of processor time spent in User Mode in non-idle threads. All application code and subsystem code executes in User Mode.

`Interrupts/s` Returns the number of device interrupts the processor is experiencing. A device interrupts the processor when it has completed a task or when it otherwise requires attention.

`Ipconfig` Returns the Windows IP Configuration.

This consists of the following:

- Ethernet adapter card name
- IP Address
- Subnet Mask
- Default Gateway

Description of Values Returned:

Refer to the User Configurable Parameters for this application.

About “Installed Software”

This application returns the names of the software that has been entered in the registry on the selected Windows node. Only Windows software that has created a subtree in the registry is listed. Older software (for example, Windows NT 3.51) is not shown.

This function returns all the subtrees from the registry “local machine” under the key “Software”. All software written for Windows create a subkey under “Software” to store external parameters. The `itoreg.cfg` file is used to filter out unwanted information. For a sample `itoreg.cfg` file, see “About “Reg Viewer”” on page 409.

Default

```
itoreg.exe /enum 3 /key Software /initkey lm
```

User Configurable Parameters

`/enum X`	Returns the subtrees from the specified key. Information is printed out to the depth specified by `X`.
`/key <NAME>`	Defines the starting point of the subtree to be processed.
`/initkey`	Defines in which registry have to search for `<key>`.

NOTE For a full description of the Windows registry, see the Windows documentation.

Description of Values Returned

See the User Configurable Parameters for this application, as well as the Windows documentation.

About “Job Status”

This application returns a list of the scheduled jobs entered by the `at` function. If the schedule service has not been started, the message `The service has not been started` is returned. If nothing is scheduled on the target node, the message `There are no entries in the list` is displayed. Otherwise a list of commands is displayed along with the times at which they are scheduled to run.

Default

`at.exe`

User Configurable Parameters

For a full description of creating and removing scheduled jobs, see the Windows documentation.

About “LM Sessions”

This application lists sessions between the selected Windows node and other computers on the network. If the selected system is acting as a logon server, it shows sessions of the users for which it has validated logins. If no user name is shown by the entry, it indicates that a service has created this session connection.

Default

`net.exe sessions`

User Configurable Parameters

For a full description of `net.exe`, see the Windows documentation.

Description of Values Returned

`Computer`	The name of the system that has made the connection.
`User name`	Name of the user. If this field is blank it means that the Windows system has a connection, which is typical when a service has made a log-on.
`Opens`	The number of open resources associated with the connection.
`Idle time`	Time since this connection was last used.

About “Local Users”

This application prints the name of the user who is locally logged onto the selected Windows node. If you need more information about the users and sessions, use the Show Users application.

Default

```
itouser.exe /local
```

User Configurable Parameters

See “About “Show Users”” on page 419.

Description of Values Returned

See “About “Show Users”” on page 419.

About “Memory Load”

This application returns information about the current memory usage of the selected Windows node. If you need more information about the Windows node, use the Diagnostics application.

Default

```
itodiag.exe /memory
```

User Configurable Parameters

See“About “Diagnostics”” on page 395.

Description of Values Returned

See “About “Diagnostics”” on page 395.

About “NetBios Sessions”

This application displays protocol statistics and current TCP/IP connections using NBT (NetBIOS over TCP/IP) for the selected Windows node.

Default

```
nbstat.exe -s
```

User Configurable Parameters

For a full description of `nbstat.exe`, see the Windows documentation.

About "PerfMon Objects"

This application returns all of the performance objects that are defined on the selected Windows node. A non-English Windows installation returns the objects in both the local language and the default language (US English). This application is used mostly by the administrator to make the configuration of threshold monitors on Windows systems easier.

Default

`opcprfls.exe`

User Configurable Parameters

`/a`	By default, returns all the performance monitor objects found on the system.
`/o <string>`	Returns only objects that match the string, starting from the beginning of the object. For example, **`/o s`** returns the objects **`system`**, **`server`** and **`server work queues`**, while **`/o sy`** returns **`system`** and **`/over`** matches nothing and returns an error message.
`/s`	By default, returns a maximum of ten instances. If more are defined it will print out the message "`MULTIPLE INSTANCES, TOO MANY TO LIST`".
`/f`	Returns a full list and prints all instances, no matter how many are defined.

NOTE

The performance objects are always stored in both US English *and* the local language if the local language is not also US English. For example, on a German Windows system, names are defined for all the objects in both US English and German. If `opcprfls.exe` finds a second language, the message "`Second Language found`" is displayed, and each object, counter, or instance thereof is returned in both US English and the local language. If an object does not have a local language name, only the US English name is printed. The OVO agent can monitor any of the performance objects in either US English or the local language, but US English is valid on all Windows machines, regardless of the local language.

Description of Values Returned

Refer to the “User Configurable Parameters” section for this application.

About "Process Kill"

This application kills all processes that are running under the configured name on the selected Windows node. If the user does not have the rights to kill the process, an error is returned.

Default

`itokill.exe`

User Configurable Parameters

`/pid <process id>`	Kill process with `id` *`<process id>`*
`/name <process name>`	Kill *all* processes with `name` *`<process name>`*.
`/f`	Forced kill without notification.
`/l`	List all processes. Because this function uses the registry to get all the process names, it does not show the extension `.exe` after executable files. This information is not stored in the registry.

NOTE Under Windows, a user with administrator rights can kill any process, but normal users can kill only processes that are running under their account name. If you want the OVO operator to be able to kill any process, configure the application to run under `HP ITO account`.

Description of Values Returned

See the "User Configurable Parameters" section for this application.

About “Reboot”

This application will shutdown and reboot the selected Windows nodes.

Default

```
itosdown.exe /t 120 /r /w
```

User Configurable Parameters

`/m <msg>`	Returns shutdown `<msg>` in a popup window on the node.
`/t <sec>`	Specifies the delay (in seconds) before the system shutdown occurs.
`/a`	Aborts an OVO initiated system shutdown.
`/r`	Automatic reboot after shutdown. If this option is not set, the system shuts down. It can then only be restarted manually.
`/f`	Force system shutdown. Processes are not allowed to delay the shutdown for local user interaction (for example, to query whether data should be saved). Without this option, the shutdown might not occur because of processes running on the system.
`/w`	Pop up a notification window. This allows the local user to cancel the shutdown process. If the local user cancels the shutdown process, the management server receives an error message.

Description of Values Returned

See the “User Configurable Parameters” section for this application.

About "Reg Viewer"

This application returns the values and subkeys for the define key of the Selected Windows node.

For example, to view the OVO agent configuration, modify the application to use the following:

```
/enum 1 /initkey LM /\
key Software\Hewlett-Packard\OpenView\ITO
```

Default

None. This application requires an entry listed in Table 11-3.

Table 11-3 Registry Viewer Application Options

To view a key/value: **/view /initkey lm|cu|cr|us /key <path> [/valuename <name>]**
To set a key or value: **/set /initkey lm|cu|cr|us /key <path> [/valuename <name> /value <value> /type REG_SZ|REG_DWORD]**
To delete a key or value: **/delete /initkey lm|cu|cr|us /key <path> [/valuename <name>] [/force] [/set]**
To scan registry for pattern: **/scan <pattern> /initkey lm|cu|cr|us /key <path> [/view]**
To enumerate a registry tree (thereby printing out registry keys to the set depth: `enum` uses a config file that verifies keys that should not be processed): **/enum <depth> /initkey lm|cu|cr|us /key <path> [/view]**
To execute a registration script: **/file <filename> /initkey lm|cu|cr|us**

User Configurable Parameters

`/initkey lm|cu|cr|us` Define initial registry key:

	`lm`	`KEY_LOCAL_MACHINE`
	`cu`	`KEY_CURRENT_USER`
	`cr`	`KEY_CLASSES_ROOT`
	`us`	`KEY_USERS`
`<pattern>`	`*`	Matches any sequence of characters (zero or more).
	`?`	Matches any character.
	`[SET]`	Matches any character in the specified set.
	`[!SET]` or `[^SET]`	Matches any character not in the specified set.
	`\`	Escape a character like ‘]’ or ‘-’.

Use the **`/view`** option to scan values.

`/type <type>` Define an entry type:

- `REG_DWORD`
- `REG_SZ`

`/valuename <name>` Define a value.

`/enum`

The configuration file name is `itoreg.cfg`.

Example of exclusion of specific registry keys used for the display of the installed software:

```
Exclusions = {

Classes;

Program Groups;

Secure;

Windows 3.1 Migration Status;

Description;

}
```

About "Server Config"

This application displays settings for the Server service for the selected Windows node.

Default

`net.exe config server`

User Configurable Parameters

For a full description of `net.exe`, see the Windows documentation.

Description of Values Returned

`Server Name` Name of the server

`Comment` Comment for the server that is displayed in Windows Screens and with the `NET VIEW` command.

`Software version` Version number.

`Server is active on` Network connections that the server is using.

`Server hidden` Specifies whether the server's computer name appears on display listings of servers. Hiding a server does not alter the permissions on that server.

`Maximum Logged On Users` Maximum open files per session.

About “Server Stats”

This application displays in-depth statistics about the Server service for the selected Windows node.

Default

```
net.exe statistics server
```

User Configurable Parameters

For a full description of `net.exe`, see the Windows documentation.

Description of Values Returned

For a full description of `net.exe`, see the Windows documentation.

About “Shares”

This application lists the external connections that are available on the selected Windows node. All shares ending with a dollar sign (**$**) are hidden shares that the Windows system makes available for remote administration by default.

Default

`net.exe share`

User Configurable Parameters

None.

Description of Values Returned

`Share name`	Full name of the available netbios share.	
`Resource`	Location of the share on the local system.	
`Remark`	Common remarks:	
	`Default share`	These shares are for remote administration and are available only to users of the Administrators (or Domain administrators) group. They are created by default at startup.
	`Remote IPC`	Share for default IPCs.
	`Remote Admin`	Share to the local Windows system location.

About “Show Drivers”

This application lists all drivers that are present on the selected Windows node.

Default

```
itomserv.exe /list d
```

User Configurable Parameters

See “About “Show Services”” on page 416.

Description of Values Returned

`NAME` — True name of the service. To perform actions on the service, use this name.

`DISPLAY` — Description of the service. This is the name that is normally seen when working with the control panel.

`STATUS` — The status of a service can be one of the following:

- `Started` (that is, Running)
- `Paused`
- `Stopped` (represented by a blank entry)

`STARTUP` — The startup type of a service can be:

`Automatic`, `boot`, or `system`	Service starts every time the system starts.
`Manual`	Service can be started by a user or a dependent service.
`Disabled`	Service cannot be started.

About "Show Services"

This application returns a list of the services that are configured on the selected Windows system. If the OVO user does not have the rights to obtain information about a service, "NA" is returned for the service details.

Default

```
itomserv.exe /list s
```

User Configurable Parameters

`/start <servicename>` Start service <*servicename*>.

`/stop <servicename>` Stop service <*servicename*>.

`/pause <servicename>` Pause service <*servicename*>.

`/continue <servicename>` Continue service <*servicename*>.

`/status <servicename>` Print the status of service <servicename>.

`/list s | d | a` Print a list of installed services:

`s`	List all Windows system services.
`d`	List all Windows device drivers.
`a`	List all installed services.

`/width <servicename> <description>`

<*servicename*> defines the width of the service to be displayed.

<*description*> defines the width of the description of a service.

The width option can be used together with the `/list` or `/status` options.

The following example lists service names with a width of 30 characters and hides the description:

```
itomserv.exe /list s /width 30 0
```

`/e`	Set the exit status to a numerical value:

0	RUNNING
1	NOT_RUNNING
2	START_PENDING
3	STOP_PENDING
4	CONTINUE_PENDING
5	PAUSE_PENDING
6	PAUSED

NOTE Although the `/e` parameter is not useful from the `OVO Application Bank`, it is included here because it may be useful for use with monitor scripts

Description of Values Returned

`Name` Internal name of the service.

`Display` Name that is normally displayed to the user.

`Status` Status of a service can be one of the following:

- Started
- Paused
- Stopped (indicated by a blank entry)

`Startup` The startup type of a service can be:

`Automatic`	Service starts every time the system starts.
`Manual`	Service can be started by a user or a dependent service.
`Disabled`	Service cannot be started.
`N/A`	User does not have the rights to obtain in-depth information about the service.

About “Show Users”

This application displays information about local users and sessions on the selected Windows Node.

Default

```
itouser.exe /u
```

User Configurable Parameters

`/u` Returns user information for the system, including:

- Name of the current user
- Domain this user is logged into
- Server that validated the log-in

`/s` Returns full session information for the system, including:

- System name
- Net BIOS name
- Current local user name
- Type of the client
- Number of open sessions
- Idle time

`/nu` Returns number of users logged on by the system.

`/ns` Returns number of sessions on the system.

`/local` Returns the name of user logged into the local system.

Description of Values Returned

See the “User Configurable Parameters” section for this application.

About “Start Services”

This application starts the requested service on the selected Windows node. If a service is disabled (as opposed to being stopped) this application cannot enable the service. Services may not be enabled remotely. They must be enabled on the target system.

Default

```
itomserv.exe /start <service name>
```

User Configurable Parameters

See “About “Show Services”” on page 416.

About “Stop Services”

This application stops the requested service. Since administrative rights are required to stop and start Windows services, the user must be defined as HP ITO Account, not opc_op.

Default

```
itomserv.exe /stop <service name>
```

User Configurable Parameters

See “About “Show Services”” on page 416.

About "TCP/IP Status"

This application displays protocol statistics and current active TCP/IP network connections for the selected Windows node.

Default

`netstat.exe`

User Configurable Parameters

See the Windows documentation.

Description of Values Returned

`Proto`	Protocol that is used for the connection.
`Local Address`	Local system name and port number.
`Foreign Address`	Full name and port number of the system to which the node is connected. The port number can also be **`nbsession`**, which is a netbios connection over TCP/IP.
`State`	Current state of the connection.

About "Used Shares"

This application returns a list of connections that the selected Windows node has made. If the status is disconnected, a connection is automatically established as soon as the local user switches to this drive.

Default

`net.exe use`

User Configurable Parameters

For a full description of `net.exe`, see the Windows documentation.

Description of Values Returned

`Status`	State of the connection (for example, `OK`, `Disconnected` means that the drive connection is defined but not connected).
`Local`	Letter of the local drive used to access the connection.
`Remoted`	Name of the system and the share that is used.
`Network`	Type of network that is providing the connection (for example, Microsoft Windows Network, or 3rd party NFS software).

About "Virtual Terminal PC"

This application opens a terminal with command-line capabilities to the target Windows system. All output is redirected to the Virtual Terminal on the management server. Calling an application with a user interface is not supported. You should use a third party application for screen redirection, if terminal emulation or UI applications are required.

`Virtual Term (PC)` does *not* support the following:

- ❏ Terminal emulation.
- ❏ Applications that use a textual user interface.
- ❏ Applications that use a graphical user interface.

Default

`opcvterm.exe`

User Configurable Parameters

None.

Telnet on Windows 2000

On Windows 2000, the built-in Telnet Service can be used instead of the Virtual Terminal (PC).

You can change the setting directly in the Windows registry under:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\TelnetServer\1.0\NTLM`

To enable remote login from a UNIX system, follow these steps:

1. From the `Control Panel`, select `Administrative Tools: Telnet Server Administration`.
2. Enter **3** to select the option `3) Display/ change registry settings....`
3. Enter **7** to select the option `7) NTLM`.
4. Change this setting to `0` by replying appropriately to all prompts.
5. Use the menu options `5` (Stop Service) and `4` (Start Service) to stop and restart the Telnet Service

Windows 2000 allows remote login from UNIX systems.

About “OVO Install Log”

This application returns the contents of the OVO installation log from the selected Windows node.

Default

```
cmd.exe /c “type %SYSTEMROOT%\temp\inst.log”
```

User Configurable Parameters

None.

About “Workst Stats”

This application displays in-depth statistics about the workstation service for the selected Windows node.

Default

```
net.exe statistics workstation
```

User Configurable Parameters

For a full description of `net.exe`, refer to the Windows documentation.

Description of Values Returned

For a full description of `net.exe`, refer to the Windows documentation.

Distributing Scripts and Programs

For Windows NT/2000 managed nodes, the platform selector and architecture identifier is the following:

```
ms/intel/nt
```

Location of User Scripts and Programs

Table 11-4 shows the location of user scripts and programs provided on the management server.

Table 11-4 Location of User Scripts and Programs on the Management Server

Script/Program	Location
Automatic actions, operator-initiated actions, and scheduled actions	`/var/opt/OV/share/databases/OpC/mgd_node/customer/ /ms/intel/nt/actions/*`
Monitoring scripts and programs used by the monitoring agent and the logfile encapsulator	`/var/opt/OV/share/databases/OpC/mgd_node/customer/ /ms/intel/nt/monitor/*`
Scripts and programs called through command broadcast or started from the Application Desktop	`/var/opt/OV/share/databases/OpC/mgd_node/customer/ /ms/intel/nt/cmds/*`

About Temporary Directories

Table 11-5 shows the temporary directories for distributed scripts and programs on the managed nodes.

Table 11-5 Temporary Directories for Distributed Scripts and Programs on the Managed Nodes

Managed Node	Operating System	Temporary Directory

Intel 486 or higher	Windows	`\usr\OV\tmp\OpC\bin\actions`
		`\usr\OV\tmp\OpC\bin\cmds`
		`\usr\OV\tmp\OpC\bin\monitor`

About Target Directories

Table 11-6 shows the target directories for distributed scripts and programs on the managed nodes.

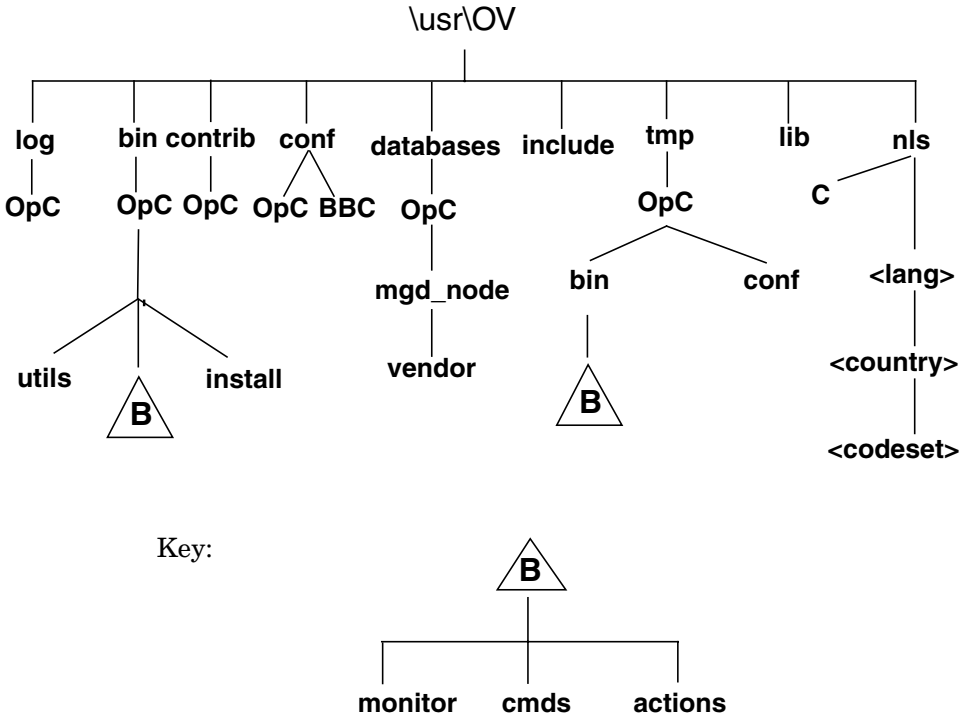
Table 11-6 Target Directories for Distributed Scripts and Programs on the Managed Nodes

Managed Node	Operating System	Directory	Access Rights
Intel 486 or higher	Windows	`\usr\OV\bin\OpC\actions`	Administrator (full access) Everyone (rx)
		`\usr\OV\bin\OpC\cmds`	Administrator (full access) Everyone (rx)
		`\usr\OV\bin\OpC\monitor`	Administrator (full access) Everyone (rx)

Organization of Managed Nodes

Figure 11-2 shows how OVO software is organized on Windows NT/2000 managed nodes.

Figure 11-2 OVO Software on Windows Managed Nodes



During installation, OVO creates the `HP ITO account`, which has all rights and privileges that are required for the OVO agent software. It also creates the `opc_op` account, which is a normal user account and is used to execute applications.

NOTE The directories represented in Figure 11-2 by the letter “B” are created by the control agent if necessary.

Location of Files

On Windows managed nodes, files are located as follows:

- **Process-related Files**

  `\usr\OV\tmp\OpC`

- **Agent Configuration Files**

  `\usr\OV\conf\OpC`

About the Default OVO Operator

Table 11-7 shows the OVO user accounts on Windows managed nodes.

Table 11-7 OVO User Accounts on Windows Managed Nodes

Field	Entry	
User Name	`HP ITO account`	`opc_op`
Password	Defined during installation	Same as `HP ITO account`[a]
Group	`Administrators`[b] or `Domain Administrator`[c]	Users or Domain Users
Description	HP OVO *agent* account	HP OVO *operator* account
Login Shell	None	None

a. All other properties assume the default value
b. Standalone or domain members
c. Domain Controller

Types of System Resources

System Environment Variables

OVO sets the following system environment variables, which can be used in scripts, when setting up automatic actions in templates, and so on:

Table 11-8

Variable	Explanation	Example
%OvAgentDir%	The installation directory for the Windows agent.	C:\usr\OV
%OvPerlBin%	The absolute path to the Perl interpreter.	C:\usr\OV\bin\perl.exe

Registry Keys

OVO inserts several keys in the Windows Registry.

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

%SystemRoot%\System32\regedt32.exe

The Windows Registry Editor shows the following keys for OVO:

- HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\ITO
- HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\Control\Lsa\MSV1_0
- HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\Services\HP ITO Agent

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

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

OVO Managed Node Libraries

Table 11-9 describes the managed node libraries for OVO A.05.xx, A.06.xx, and A.07.xx.

Table 11-9 Libraries for the OVO Managed Nodes

Item	OVO A.05.xx	OVO A.06.xx	OVO A.07.xx
Library	**libopc.dll** **opcapi.dll**	**libopc.dll** **opcapi.dll**	**libopc.dll** **opcapi.dll** **opcas.dll** **libnsp.dll** **pdh.dll**
Libraries linked to the OVO library	N/A	N/A	N/A
Link and compile options	N/A	N/A	N/A
Description	Use `*.mak` files to build	Use `*.dsp` files to build	Use `*.dsp` files to build

About the Include File

On an Intel platform with Windows NT/2000 managed nodes, use the following include file:

```
\usr\OV\include\opcapi.h
```

About the Makefile

To built an executable correctly, use Microsoft Developer Studio 6.0 or higher.

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

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

About Citrix MetaFrame Integration

You can install Citrix MetaFrame as an extension of Windows Terminal Server with additional client and server functionality, including:

- ❏ Support for heterogeneous computing environments
- ❏ Support for enterprise-scale management
- ❏ Seamless desktop integration

NOTE For detailed descriptions of the default Citrix MetaFrame applications that can be used with OVO, see “Types of Citrix MetaFrame Applications” on page 438.

Supported Versions of Citrix MetaFrame

OVO supports the English version of Citrix MetaFrame 1.8 on Windows NT 4.0 Terminal Server Edition Service Pack 4.

Software Requirements for Citrix MetaFrame

The following software is required for Citrix MetaFrame on Windows managed nodes:

- ❏ **Windows NT Service Pack**

  Windows NT 4.0 Terminal Server Edition: Service Pack 5 or 6A

- ❏ **Citrix MetaFrame**

  Citrix MetaFrame 1.8 or higher

Integrating Citrix MetaFrame into OVO

To integrate Citrix MetaFrame into OVO, perform these procedures:

1. **Install the Citrix MetaFrame agent.**

   You can install the Citrix MetaFrame agent using one of the following installation methods:

   - *Standard Installation*

     Use this method if the OVO agents are correctly installed. For instructions, see "To Install an Agent with Standard Installation" on page 374.

   - *Manual Installation*

     Use this method if the OVO are not correctly installed and do not function correctly. For instructions, see "To Pre-install a Windows Agent on a Windows PC" on page 382.

NOTE

During manual installation, the logfile is stored in the `C:\temp` directory. Or, if that directory does not exist, the logfile is put in the directory where the installation was started

2. **Configure the Citrix MetaFrame agent.**

   To find out how to configure the Citrix MetaFrame agent, see "To Configure the Citrix MetaFrame Server" on page 435.

To Configure the Citrix MetaFrame Server

To configure the Citrix MetaFrame server, follow these steps:

1. **Upload the configuration.**

   On the management server, enter the following command:

   ```
   opccfgupld -add TS_MF
   ```

   The `swinstall` installation process automatically installs the commands and monitors directly into your OVO software sub-tree platform.

2. **Assign and distribute templates to the MetaFrame managed nodes.**

   Do this:

   a. Make sure the Terminal Server or MetaFrame server is present in the `OVO Node Bank`, and that the agent software is running on the node.

   b. Assign the Terminal Server or MetaFrame templates to the agent on the managed node.

NOTE

If you are using Terminal Server, use the templates from the `Terminal Server` group. If you are using Terminal Server and MetaFrame, assign the `MetaFrame` group.

   c. Distribute the assigned templates, monitors, and commands to the node.

About the ICA Browser Service

The ICA Browser service is specific to Citrix MetaFrame managed nodes. ICA browsing is central to MetaFrame license pooling, load balancing, and application publishing. The ICA Browser service enables you to control browser parameters (for example, backup ICA Browsers, ICA Gateways, and update and refresh intervals). You can also configure which servers become the master ICA Browser.

About the Program Neighbourhood Service

The Program Neighbourhood service provides a new means of application access and management for the enterprise: the Server Farm. A Server Farm can contain all Citrix servers within your organization, regardless of the previous boundaries of local subnets and NT Domains.

Types of MetaFrame Monitored Objects

Table 11-10 describes the default monitored objects used by OVO on Citrix MetaFrame managed nodes.

Table 11-10 Object Thresholds on Citrix MetaFrame Managed Nodes

Object	Description	Threshold	Polling Interval (Minutes)
`TS_Licensing`	Checks if Terminal Server licensing service is running.	1	5
`TS_Service`	Checks if Terminal Server service is running.	1	5
`MF_ICA_Browser`	Checks if MetaFrame ICA Browser service is running.	1	5
`MF_Prog_Neighbourhood`	Checks if the MetaFrame ICA Program Neighbourhood service is running.	1	5

Types of MetaFrame Logfile Templates

Table 11-11 shows encapsulated logfiles and associated templates used on Citrix MetaFrame managed nodes.

Table 11-11 Encapsulated Logfiles on Managed Nodes running Windows NT Terminal Server and Citrix MetaFrame

Logfile	Description	Template Name
SYSTEM_LOG	NT system eventlog for Terminal Server	System Log (Terminal Server)
SYSTEM_LOG	NT system eventlog for MetaFrame	System Log (MetaFrame)

NOTE Although there is a logfile template available for NT Terminal Server, you should only use the logfile template for Citrix MetaFrame.

Types of Citrix MetaFrame Applications

Citrix MetaFrame has an additional application group, `MetaFrame Tools`. The implementation is similar to using the MetaFrame Tools/Citrix Server Administrator GUI directly on the MetaFrame system.

This section describes the applications in the MetaFrame Tools application group.

About "ACL Info"

Displays file and directory permissions that give excessive access to users and groups. This application can be used to verify the security of the MetaFrame server, and also reports potential security exposures on a MetaFrame server.

NOTE This application is supported only on Windows NT.

Default

`acl info <path> </files_only | /registry_only>`

User Configurable Parameters

<path>

Path of director and file.

`/files_only` Reduces scope of application to files only.

`/registry_only` Reduces scope of application to registry only.

About "Auditlog"

Processes the Windows NT EventLog and generates reports of login and logout activity.

Default

`auditlog`

User Configurable Parameters

`username`	Returns the name of the user.
`session`	Returns the session duration.
`/FAIL`	Returns a status report for specified parameters.

NOTE To use Auditlog, you must enable Windows NT login and logout event logging with User Manager for Domains.

About "Disconnect"

Used to disconnect a terminal server session.

NOTE This application must be passed with the parameters listed under "Default."

Default

`disconnect <sessionid | sessionname>`

About "Flush"

Equates the client drive mapping cache. This equation forces the MetaFrame server and the client to re-synchronize all disk data.

Default

`flush`

About "License"

Shows information about currently present licenses on the network. By default, the application shows how many licenses exist on the network, how many are in use on the entire network, and how many licenses are in use on the node:

Default

`license`

About “Processes”

Displays the status of all user processes, one process per line.

Default

`processes`

User Configurable Parameters

`sessionname`	Returns the name of the session.
`processid`	Returns the process ID.
`username`	Returns the username.
`programname`	Returns the name of the program associated with selected object.

About “Send Message”

Sends messages to ICA client users.

NOTE This application must be passed with the parameters listed under “Default.”

Default

`send message <`*`username`* | *`sessionname`* | *`sessionid`*`> <`*`message`*`>`

About “Servers”

Displays the available Terminal Servers on the network.

Default

`servers`

User Configurable Parameters

</DOMAIN:domain>

Returns information for the specified domain.

About "Sessions"

Displays information about currently logged users. By default, it shows all sessions on the current server:

Default

`sessions <username> </SERVER:server_name>`

User Configurable Parameters

<username>

Returns all sessions for the specified username.

/SERVER:server_name

Returns the users logged on the specified server.

About "Users"

Displays information about currently logged users. By default, it shows all users with sessions on the current server:

Default

`users </SERVER:server_name>`

User Configurable Parameters

/SERVER:server_name

Returns the users logged on the specified server.

About SMS Integration

The OVO/SMS integration is a collection of monitors and templates that enable the OVO Windows agent to monitor an SMS installation in the PC subnet of an IT environment. This integration enables OVO users to monitor the environment of Windows nodes, and to restart SMS services if they fail.

Windows agents installed on every Site Server report SMS information about the entire SMS hierarchy *without* using any SMS mechanisms.

Supported Versions of SMS

OVO supports both the English and the Japanese System Management Server (SMS) 1.2 on Microsoft Windows NT Server 4.0.

Integrating SMS into OVO

The OVO/SMS integration has two parts:

- **SMS**

  Specific SMS application event log template and fourteen threshold monitors.

- **Windows**

  Standard Windows application event log template.

This sections explains how to set up and install these templates and monitors.

To Integrate SMS into OVO

To integrate SMS into OVO, follow these steps:

1. **Assign the SMS monitors and templates to the Windows servers.**

   The SMS integration contains fourteen threshold monitors that monitor SMS services.

   Each service has an `UP` and `DWN` monitor:

`UP`	Sends OVO a message when the service is running again. This monitor never has an associated action.
`DWN`	Sends OVO a message when the service that it monitors is down, and either automatically restarts the service, or provides the operator with the command that will restart it.

   The SMS services and their associated `UP` and `DWN` monitors are shown in Table 11-12.

   Assign one or both of these `UP` and `DWN` monitors to the Windows systems that run the services that the templates will monitor.

   You must assign the Application Event Log template, `NT SMS`, to any SMS Site Server of the SMS hierarchy. However, you cannot assign NT SMS to the `logon`, `distribution`, or `helper` servers because duplicate reprocessing of problems will result. These servers are also logged into the Windows application event log of the Site Server. The Application Event Log template *must* be on a Site Server, even if the site is distributed.

2. **Customize the conditions for the templates.**

   You must consider two templates when customizing the template conditions for the SMS Site Server:

   - *SMS*

     SMS-specific application event log template.

     A `suppress unmatched` condition is the first condition of the SMS application event log template. This condition suppresses all Windows application event log entries that are not SMS-related, thus ensuring that the entire set of 586 match conditions is not checked unnecessarily for non-SMS log entries.

- *Windows*

  Default Windows application event log template.

  The default Windows Logfile encapsulator template, `dflt_ApplEvLog`, has a `forward unmatched` flag set by default. If both templates are installed on an SMS Site Server, two messages will be generated for each SMS-related event log entry: one by the SMS template and one by the default Windows Logfile template. To avoid this problem, add one additional `suppress matched` condition at the beginning of the default Windows Logfile template that suppresses SMS-related messages. This condition needs to match the string SMS in the application field of the message.

  This additional condition is needed only if you assign both templates to the same node and if the you keep the `forward unmatched` condition set in the default template.

3. **Distribute the templates.**

   Distribute the agent as well, if it is not already installed.

Types of OVO-SMS Monitors for SMS Services

Table 11-12 shows The SMS services and their associated `UP` and `DWN` monitors.

Table 11-12 OVO-SMS Monitors for SMS Services

OVO-SMS Monitors	SMS Service	Restart[a]
NT_DWN_SMS_CLIENT_CONFIG_MANAGER	Client Configuration Manager	OA
NT_UP_SMS_CLIENT_CONFIG_MANAGER		none
NT_DWN_SMS_EXECUTIVE	Executive	OA
NT_UP_SMS_EXECUTIVE		none
NT_DWN_SMS_HIERARCHY_MANAGER	Hierarchy Manager	AA
NT_UP_SMS_HIERARCHY_MANAGER		none
NT_DWN_SMS_INVENTORY_AGENT	Inventory Agent	OA
NT_UP_SMS_INVENTORY_AGENT		none
NT_DWN_SMS_PACKAGE_COMMAND_MANAGER	Package Command Manager	OA
NT_UP_SMS_PACKAGE_COMMAND_MANAGER		none
NT_DWN_SMS_SITE_CONFIG_MANAGER	Site Configuration Manager	AA
NT_UP_SMS_SITE_CONFIG_MANAGER		none
NT_DWN_SMS_TRAP_FILTER	Trap Filter	none
NT_UP_SMS_TRAP_FILTER		none

a. OA = Operator Action; AA= Automatic Action

Mapping SMS Messages

When OVO reports SMS messages in the message browser, it assigns a Message Group and Message Object corresponding to the message. The tables below show how the SMS messages will be mapped in OVO.

Assigning SMS Messages to OVO Message Groups

Table 11-13 shows how OVO assigns SMS messages to Message Groups.

Table 11-13 SMS Message Assignment to OVO Message Groups

SMS Message	OVO Message Group
All messages containing one of the following words: • Compress • Instruction • Inventory • Job • Package	Jobs
All SMS network errors that are not related to jobs.	Network
All SMS security errors that are not related to jobs.	Security
All SMS database errors that are not related to jobs.	DB
All remaining errors.	OS

Assigning SMS Messages to OVO Message Objects

Table 11-14 shows how OVO assigns SMS messages to Message Objects.

Table 11-14 SMS Event Assignment to OVO Message Objects

SMS Events	OVO Message Objects
All events that are related to setup, installation, and configuration.	Configuration
All events that can be related to inventory collection.	Inventory
All events that can be related to package distribution.	Distribution
All events that can be related to application errors.	Application
All remaining events.	Miscellaneous

About the Supplied Perl Interpreter

The managed node software includes a custom binary Perl 5.6.1 distribution.

The Perl is embedded in the Perl interpreter and the monitoring agent, and is designed to be used internally by OVO. Some OVO policies deployed by OpenView Operations for Windows management servers include Perl scripts (for example, some schedules and measurement threshold policies). Perl scripts are also used by some HP-supplied Smart Plug-ins (SPIs).

The Perl interpreter and other binaries are automatically installed into the `%OvAgentDir%\in` directory. A basic set of modules is installed in the `%OvAgentDir%\in` directory. Pre-existing Perl installations are not altered as a result of installing a managed node.

If you want to use the Perl distribution for additional purposes beyond its internal use within OVO, you should first check which modules are included by listing the `.pl` and `.pm` files within the `/opt/OV/nonOV/perl/a/lib/5.6.1` directory.

For further information about Perl or if you need to add additional modules, go to the following web site:

`http://www.perl.com`

NOTE

Perl is supplied "as is" with no warranties whether express or implied according to the Perl artistic license agreement. Hewlett-Packard is not responsible for errors in Perl, which is public domain software and not produced by HP. Hewlett-Packard does not support any modifications to the provided Perl distribution. This software is licensed, not sold, and your use of the software is subject to the license terms contained in the license agreement."

12 Administration of the OVO Management Server in a Cluster Environment

In this Chapter

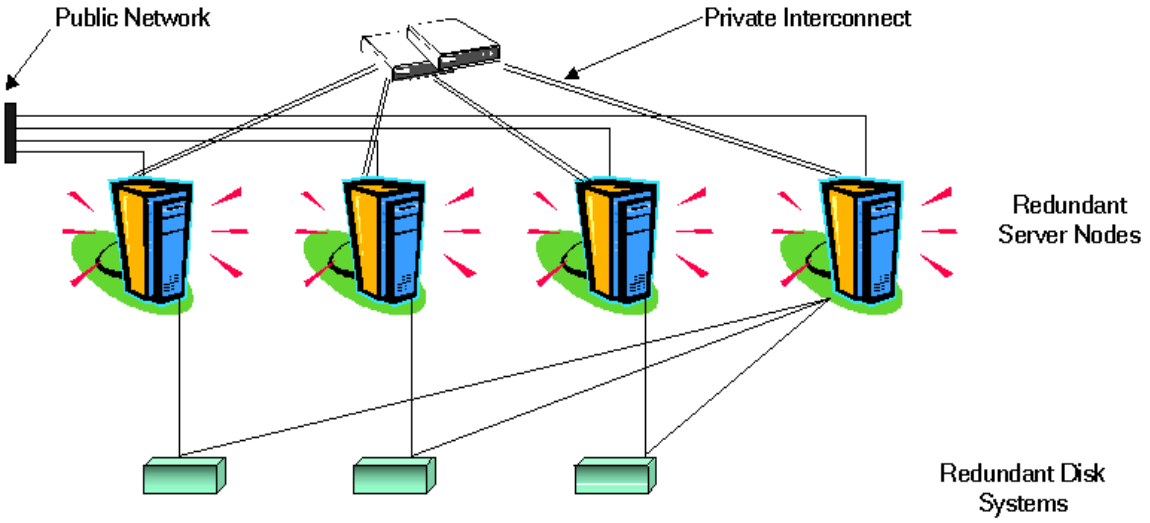
This chapter provides information for system administrators working with OVO in a cluster environment. It assumes that you are familiar with the general concepts of OVO and with High Availability concepts.

For detailed information about Sun Cluster, VERITAS Cluster Server, and MC/ServiceGuard, see appropriate chapters in the *OVO Installation Guide*.

About the Cluster Architecture

Cluster architecture provides a single, globally coherent process and resource management view for the multiple nodes of a cluster. Figure 12-1 shows an example of a cluster architecture.

Figure 12-1 Architecture of a High Availability Cluster



Each node in a cluster is connected to one or more public networks, and to a *private interconnect*, representing a communication channel used for transmitting data between cluster nodes.

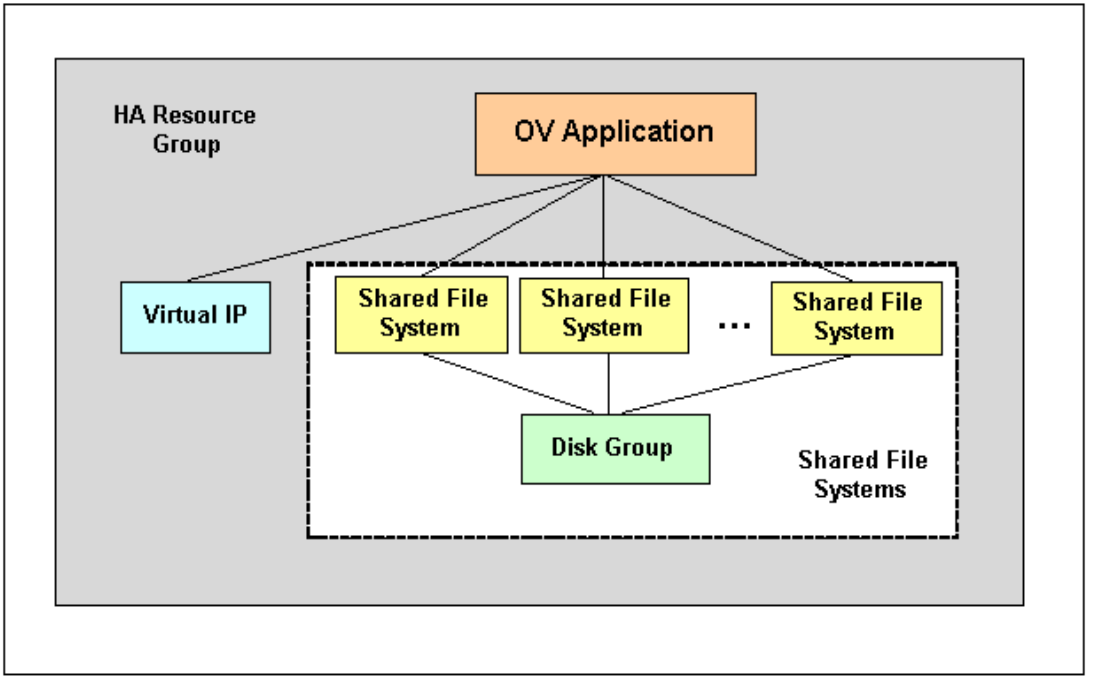
Applications running in a cluster environment are configured as HA Resource Groups. HA Resource Group is a generic term for cluster objects representing HA Applications.

The OVO Management Server Running as an HA Resource Group

Concepts

In modern cluster environments such as VERITAS Cluster, Sun Cluster or MC/ServiceGuard, applications are represented as compounds of resources, simple operations enabling application to run in a cluster environment. The resources construct a **Resource Group**, which represents an application running in a cluster environment.

Figure 12-2 Typical HA Resources Group Layout



The HA Resource Group is differently represented by the various cluster environments. Table 12-1 indicates these differences.

Table 12-1 Resource Group in Cluster Environments

Cluster Environment	Abbreviation	HA Resource Group Represented As...
MC ServiceGuard	MC/SG	Package
VERITAS Cluster Server	VCS	Service Group
Sun Cluster	SC	Resource Group

Instead of cluster specific terms, HA Resource Group is used in this document as a generic term that designates set of resources in a cluster environment.

Starting, Stopping, and Switching HA Resource Group

Administration of the HA Resource Group is performed by using the command:

```
/opt/OV/bin/ovharg_config
```

To Start the HA Resource Group

To start the HA Resource Group, enter:

`/opt/OV/bin/ovharg_config ov-server -start <node name>`

where <*node name*> is name of the node on which the HA Resource Group should be started.

NOTE The Resource Group name is normaly `ov-server`, but you can also choose an alternative name.

You will get the following return codes:

`0` - if the OVO Application was started successfully, or

`1` - if the start operation failed.

To Stop the HA Resource Group

To stop the HA Resource Group, enter:

/opt/OV/bin/ovharg_config ov-server -stop <*node name*>

where <*node name*> is name of the node on which the HA Resource Group should be stopped.

You will get the following return codes:

`0` - if the OVO Application was stopped successfully, or

`1` - if the stop operation failed.

To Switch the HA Resource Group

To switch the HA Resource Group from one node to another, enter:

/opt/OV/bin/ovharg_config ov-server -switch <*node name*>

where <*node name*> is name of the node to which the HA Resource Group should be switched.

You will get the following return codes:

`0` - if the OVO Application was switched successfully, or

`1` - if the switch operation failed.

Manual Operations for Starting, Stopping and Monitoring OVO Management Server in a Cluster Environment

The OVO management server in a cluster environment is represented as the OV application which is a part of the the HA Resource Group, containing resources which perform all necessary operations for starting, stopping and monitoring the OV application.

The `/opt/OV/lbin/ovharg` utility is used for starting, stopping, and monitoring the OVO management server running as OV application in a cluster environment.

To Start OVO Management Server

To start the OVO management server, enter:

/opt/OV/lbin/ovharg -start ov-server

You will get the following return codes:

`0` - if the OVO management server was started successfully, or

`1` - if the start operation failed.

To Stop OVO Management Server

To stop the OVO management server, enter:

```
/opt/OV/lbin/ovharg -stop ov-server
```

You will get the following return codes:

`0` - if the OVO management server was stopped successfully, or

`1` - if the stop operation failed.

To Monitor OVO Management Server

Cluster Manager permanently monitors the OVO management server by using the following action:

```
/opt/OV/lbin/ovharg -monitor ov-server
```

If the OVO management server is running properly, this command returns `0`, otherwise it returns `1`, which causes switching of the `ov-server` HA Resource Group to another cluster node.

However, there are situations in which you need the OVO management server to be stopped, while all other parts of the HA Resource Group should continue to run. In such situations, you will need to disable monitoring manually.

To disable the OVO management server monitoring manually, use the `disable` option:

```
/opt/OV/lbin/ovharg -monitor ov-server disable
```

When the monitoring process is disabled manually, you will be able to stop the OVO management server. This will *not* cause the HA Resource Group to be switched to another cluster node. The Cluster Manager will *not* detect this event, because the return code of the monitor command will still be `0`.

NOTE After you have finished the manual OVO management server administration, you *must* restart the OVO management server.

To check whether the OVO management server runs properly, use the following command:

```
/opt/OV/bin/OpC/opcsv
```

- If the management server is running, enable monitoring again by using the following command:

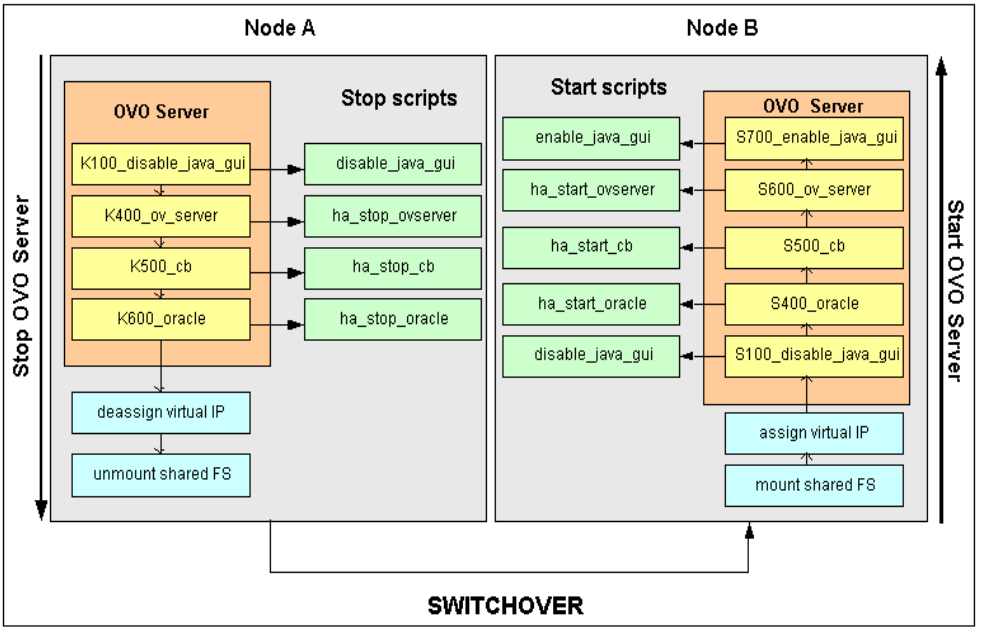
  ```
  /opt/OV/lbin/ovharg -monitor ov-server enable
  ```

- If the OVO management server is *not* running properly, you have to perform additional manual steps in order to put it in a running state.

Switchover example

The example illustrates the switchover procedure in a two node cluster in which the HA Resource Group `ov-server` is currently active on cluster system `Node A`. The cluster initiates switchover from `Node A` to the remaining `Node B`. The Resource Group `ov-server` is stopped on `Node A` and started on `Node B`. The switchower procedure is shown on Figure 12-3.

Figure 12-3 Switchover Procedure



Switchover Procedure

When a system failure occurs on `Node A`, the cluster initiates switchover of the Resource Group `ov-server` from `Node A`. The Resource Group is stopped on `Node A` and started on `Node B`. The procedure is conducted as follows:

1. On `Node A`:
   a. Cluster Manager stops the OVO management server running as OV Application by performing the following action:

      ```
      /opt/OV/lbin/ovharg -stop ov-server
      ```

      The `ovharg` script reads all stop links and executes stop scripts in the appropriate sequence.

   b. Cluster Manager deassigns the virtual IP and unmounts shared file systems.
2. On `Node B`:
   a. Cluster Manager assigns the virtual IP and mounts shared file systems.
   b. Cluster Manager starts the OVO management server running as OV Application by performing the following action:

      ```
      /opt/OV/lbin/ovharg -start ov-server
      ```

      The `ovharg` script reads all start links and executes start scripts in the appropriate sequence.

The Resource Group `ov-server` is now active on `Node B`.

Troubleshooting OVO in a Cluster Environment

HA Resource Group Cannot Be Started on Particular Cluster Node

Using the Tracing Option

If HA Resource Group cannot be started on one of cluster nodes, first try to resolve this problem by enabling the trace option. Perform the following steps:

1. Make sure that HA Resource Group is not running on any cluster node. If the HA Resource Group is running, stop it with the following command:

   /opt/OV/lbin/ovharg_config ov-server -stop <*node name*>

2. Enable tracing by entering:

   /opt/OV/lbin/ovharg -tracing ov-server enable

3. Enter the following command:

   /opt/OV/lbin/ovharg_config ov-server -start <*node name*>

If you receive the output `0`, the OVO management server has been successfully started. If the output is `1`, the start operation failed. To find out more about the causes of the problem, check the output of the trace file:

`/var/opt/OV/hacluster/ov-server/trace.log`

If the OVO management server failed to start, perform the steps described in the section entitled “Manual Operations” on page 460.

Manual Operations

If the OVO management server could not be started properly, it is possible to start the whole OVO management server or parts of it manually.

To start the whole management server manually, perform the following steps:

1. Mount shared file systems:
   - file system for the OVO server database
   - file system for `/etc/opt/OV/share`
   - file system for `/var/opt/OV/share`
   - file system for `/var/opt/OV/shared/server`
2. Assign the virtual host to the network interface.
3. Run the command:

   `/opt/OV/lbin/ovharg -start ov-server`

If you receive the output `0`, the OVO management server has been successfully started. If the output is `1`, the start operation failed. Check the output of the trace file to find out the problem causes.

If you failed to start the whole OVO management server, perform the steps described in the section entitled "Using Links".

Using Links

You can start any of the OVO management server components by using links placed in the `/var/opt/OV/hacluster/ov-server`. In this directory, there are several links that point to the special scripts. When activated, these scripts perform start, stop, and monitor operations for the OVO management server components. The links are given in the following format:

`S<`*`index`*`>_<`*`name`*`>` for start links

`K<`*`index`*`>_<`*`name`*`>` for stop links

`M<index>_<`*`name`*`>` for monitor links,

where `S`, `K`, or `M` designate action to be executed (start, stop, or monitor), `<`*`index`*`>` is represented by a number which indicates sequence of execution, while `<`*`operation name`*`>` indicates operation to be executed.

NOTE It is very important to execute links in the correct sequence defined by *<index>*.

Tables given below show links used within the cluster High Availability concept.

Table 12-2 Start Links

Link Name	Script Location	Action Description
S100_disable_java_gui	/opt/OV/bin/OpC/utils/disable_java_gui	Disables Java GUI
S400_oracle	/opt/OV/bin/OpC/utils/ha/ha_start_oracle	Starts Oracle
S500_cb	/opt/OV/bin/OpC/utils/ha/ha_start_cb	Starts the BBC communication broker
S600_ov_server	/opt/OV/bin/OpC/utils/ha/ha_start_ovserver	Starts the OVO management server
S700_enable_java_gui	/opt/OV/bin/OpC/utils/enable_java_gui	Enables Java GUI

Table 12-3 Stop Links

Link Name	Script Location	Action Description
K100_disable_java_gui	/opt/OV/bin/OpC/utils/disable_java_gui	Disables java GUI
K400_ov_server	/opt/OV/bin/OpC/utils/ha/ha_stop_ovserver	Dtops the OVO management server
K500_cb	/opt/OV/bin/OpC/utils/ha/ha_stop_cb	Stops the BBC communication broker
K600_oracle	/opt/OV/bin/OpC/utils/ha/ha_stop_oracle	Stops Oracle

Table 12-4 Monitor Links

Link Name	Script Location	Action Description
M100_oracle	/opt/OV/bin/OpC/utils/ha/ha_mon_oracle	Monitors Oracle
M200_cb	/opt/OV/bin/OpC/utils/ha/ha_mon_cb	Monitors the BBC communication broker
M300_ov_server	/opt/OV/bin/OpC/utils/ha/ha_mon_ovserver	Monitors the OVO management server

Monitored OVO Management Server Processes Cause an Unwanted Switchover of the OVO Management Server HA Resource Group

Changing the List of Monitored OVO Management Server Processes

If specific monitored processes abort and cause switchover of the OVO management server HA Resource Group, remove these processes from the list of monitored processes by performing the following procedure:

1. Open the /opt/OV/bin/OpC/utils/ha/ha_mon_ovserver file for editing.
2. At the end of the file, look for the list of monitored OVO management server processes and comment out all aborting processes. These processes will not be monitored anymore.

Preconfigured Elements

Templates and Template Groups

Template Group

`HA Management Server`

The template group `HA Management Server` contains the OVO management server templates for cluster environments and consists of the following template subgroups:

- ❏ `HA Virtual Management Server`

  This subgroup contains the following templates for the virtual management server node:

  - `SNMP 6.20 Traps`
  - `SNMP ECS Traps`

- ❏ `HA Physical Management Server`

  This subgroup contains the following templates for the physical management server:

  - `distrib_mon`
  - `opcmsg (1|3)`
  - `Cron`
  - `disk_util`
  - `proc_util`
  - `mondbfile`

Files

The OVO Management Server HA Files

- ❏ The OVO management server files

  The OVO management server HA files are located in the following directory:

/opt/OV/bin/OpC/utils/ha

- ha_mon_cb
- ha_mon_oracle
- ha_mon_ovserver
- ha_remove
- ha_start_cb
- ha_stop_oracle
- ha_stop_ovserver

OV HA scripts

- ❏ /opt/OV/lbin/ovharg
- ❏ /opt/OV/bin/ovharg_config

OV Cluster Specific HA Files

- ❏ MC/ServiceGuard Files

  MC/ServiceGuard specific files are located in the following directory:

  /opt/OV/lbin/clusterconfig/mcsg

  - ov_rg.cntl
  - ov_rg.conf
  - ov_rg.mon

- ❏ Sun Cluster Files

  The following Sun Cluster specific files are located in directory /opt/OV/lbin/clusterconfig/sc3:

  - monitor_start
  - monitor_stop
  - start
  - stop
  - probe
  - gettime

- `HP.OVApplication`

The following Sun Cluster specific files are located in directory `/opt/OV/lbin/clusterconfig/sc3/OVApplication`:

- `monitor`
- `online`
- `offline`

B

D

E

F

I

N

Q

R

S

X

Z

Master Index