# HP OpenView IT/Operations Administrator's Reference

## Management Server on HP-UX

**Edition 3**


**B6941-90001**
**HP OpenView IT/Operations**
**Version A.05.00**
**February 1999**

# Legal Notices

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

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

**Year 2000 Readiness**. Hewlett-Packard has made every effort to ensure the accuracy of our product testing. However, because each customer's environment is different from Hewlett-Packard's laboratory test environment, it is the customer's responsibility to validate the Year 2000 readiness of these products in their own environment. Therefore, information about the Year 2000 status of Hewlett-Packard products is provided “as is” without warranties of any kind and is subject to change without notice.

Hewlett-Packard makes no representation or warranty respecting the accuracy or reliability of information about non-Hewlett-Packard products. Such information, if any, was provided by the manufacturers of those products and customers are urged to contact the manufacturer directly to verify Year 2000 readiness.

The information provided here constitutes a Year 2000 Readiness Disclosure for purposes of the Year 2000 Information and Readiness Disclosure Act.

for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

HEWLETT-PACKARD COMPANY
3404 E. Harmony Road
Fort Collins, CO 80525 U.S.A.

Use of this manual and flexible disk(s), tape cartridge(s), or CD-ROM(s) supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and back-up purposes only. Resale of the programs in their present form or with alterations, is expressly prohibited.

# Printing History

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

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

First Edition: June 1996

Second Edition: August 1997

Third Edition: February 1999

# In This Book

This guide is for the person who installs ITO on the managed nodes, and is responsible for administering and troubleshooting the ITO system. It covers agent installation, first-time configuration, agent de-installation, tuning, and troubleshooting. The guide assumes that the reader has a sound knowledge of HP-UX system and network administration and troubleshooting. The reader should be able to:

- update the system with new software
- perform remote logins to other systems
- search, locate and edit ASCII files

The reader should be thoroughly familiar with:

- file system organization
- X applications
- HP OpenView NNM platform user interface and services
- Database administration
- ITO concepts

For information on how to install ITO on the management server, see the *HP OpenView IT/Operations Installation Guide for the Management Server*.

For information about upgrading an earlier version of ITO , see the *HP OpenView IT/Operations Software Release Notes*.

For information about ITO concepts, see the *HP OpenView IT/Operations Concepts Guide*.

# Conventions

The following typographical conventions are used in this manual.

| Font Type | What the Font Type Represents | Example |
|---|---|---|
| *Italic* | Book or manual titles, and man page names | Refer to the *HP OpenView IT/ Operations Administrator's Reference* and the *opc(1M)* manpage for more information. |
| | Provides emphasis | You *must* follow these steps. |
| | Specifies a variable that you must supply when entering a command | At the prompt type: `rlogin` *your_name* where you supply your login name. |
| | Parameters to a function | The *oper_name* parameter returns an integer response. |
| **Bold** | New terms | The **monitor agent** observes... |
| `Computer` | Text and items on the computer screen | The system replies: `Press Enter` |
| | 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... |
| **`Computer Bold`** | Text that you must enter | At the prompt, type: **`ls -l`** |

| Font Type | What the Font Type Represents | Example |
|---|---|---|
| **Keycap** | Keyboard keys | Press **Return.** |
| `[Button]` | Buttons on the user interface. | Click `[Operator]`.<br>Click on the `[Apply]` button. |
| `Menu Items` | A 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:Utilities-> Reports...` |

# The IT/Operations Documentation Map

ITO provides a set of manuals and online help which aim to assist you in using ITO and improve your understanding of the underlying concepts. This section illustrates what information is available and where you can find it.

### HP OpenView IT/Operations Printed Manuals

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

The *HP OpenView IT/Operations Concepts Guide*

provides you with an understanding of ITO on two levels. As an operator, you can learn about ITO's basic structure; as an administrator, you can use this book to gain an insight into the setup and configuration of ITO in your own environment.

The *HP OpenView IT/Operations Installation Guide for the Management Server*

is for administrators who install ITO software on the management server and perform initial configuration. It includes:

- verification of software and hardware requirements
- software installation and de-installation instructions
- configuration instructions using defaults

The *HP OpenView IT/Operations Administrator's Reference*

is for people who install ITO on the managed nodes and are responsible for the administration and troubleshooting of ITO in general.

The *HP OpenView IT/Operations Error Message Reference*

is for administrators involved in ITO problem solving. It provides a copy of all ITO error messages that have additional instructional text available. This book contains no information that is not also available from the user interface.

*Managing Your Networks with HP OpenView Network Node Manager*
is for administrators and operators. It describes the basic functionality of HP OpenView Network Node Manager which is an embedded part of ITO.

The *HP OpenView ServiceNavigator Concepts and Configuration Guide*
provides information for administrators who are responsible for installing, configuring, maintaining, and troubleshooting the HP OpenView ServiceNavigator. It also contains a high-level overview of the concepts behind service management.

The *HP OpenView IT/Operations Reporting and Database Schema*
contains a detailed description of the ITO database tables and provides examples for generating reports from the ITO database.

The *HP OpenView IT/Operations Software Release Notes*
give a description of new features. In addition, they provide information to help you:

- compare the current software's features with those available in previous versions of the software
- determine system and software compatibility
- solve known problems

#### ITO Online Information

The following information is available online:

The HP ITO Administrator's Guide to Online Information
is a context-sensistive help system and contains detailed help for each window of the ITO administrator GUI as well as step-by-step instructions for performing administrative tasks.

The HP ITO Operator's Guide to Online Information
is a context-sensitive help system and contains detailed help for each window of the ITO operator Motif GUI as well as step-by-step instructions for operator tasks.

The HP ITO Java-based GUI Online Documentation
is available in HTML-format for the ITO Java-based operator GUI and the ServiceNavigator, and contains detailed information about general ITO and

ServiceNavigator concepts and tasks for the ITO operator, as well as reference and troubleshooting information.

The HP OpenView IT/Operations Man Pages
: are available online for ITO.

#### HP OpenView IT/Operations Developer's Toolkit

If you purchase the HP OpenView IT/Operations Developer's Toolkit, you receive the full ITO documentation set, as well as the following manuals:

The *HP OpenView IT/Operations Application Integration Guide*
: suggests several ways in which external applications can be integrated into ITO.

The *HP OpenView IT/Operations Developer's Reference*
: provides an overview of all available application programming interfaces (APIs).

#### HP OpenView ECS Designer for NNM and ITO

If you purchase the HP OpenView Event Correlation Services (ECS) Designer for NNM and ITO, you receive the full ECS Designer documentation set including the title:

*HP OpenView ECS Configuring Circuits for NNM and ITO*
: which contains information you need to use the ECS Designer product in the NNM and ITO environments.

#### Advanced Network Security for HP OpenView IT/Operations

If you purchase the Advanced Network Security (ANS) extension for HP OpenView IT/Operations , you receive the following additional documentation:

*Advanced Network Security for HP OpenView IT/Operations*
: provides information for administrators who are responsible for installing, configuring, maintaining, and troubleshooting ANS.

#### Electronic Version of the Manuals

All manuals except the *HP OpenView IT/Operations Software Release Notes* are also included as Portable Document Format (PDF) files in the appropriate documentation software bundle. See the *HP OpenView*

*IT/Operations Installation Guide for the Management Server* for general installation instructions using `swinstall`. The manuals are installed into the following directory on the management server:

`/opt/OV/doc/<LANG>/OpC/`

Alternatively, you can download the manuals from the following web site:

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

Or, view them in HTML format at:

`http://docs.hp.com`

#### ITO DynaText Library

The ITO DynaText Library is a collection of ITO manuals in online format based on DynaText. DynaText is an application for viewing, searching, printing, and annotating your online library. The browser and the manuals are available in the appropriate ITO documentation software bundle. See the *HP OpenView IT/Operations Installation Guide for the Management Server* for general installation instructions using `swinstall`. Once the bundle is installed, you can open the library by selecting `Online Manuals` from the `Help` menu of any primary ITO window.

# Using the Online Help System

### The ITO Motif GUI Online Help System

ITO's Motif GUI online information consists of two separate volumes, one for operators and one for administrators. In the operator's volume, you will find the HP OpenView IT/Operations Quick Start describing the main operator windows. Both volumes include:

- ❏ information you need to perform tasks, whether you are an operator or an administrator
- ❏ popup menus, reference information about ITO icons, accessible with just a point and click on the right mouse button
- ❏ information about errors displayed in the ITO-Error Information window. You can get help either when the error occurs or by using the message number provided to perform a keyword search within the help system
- ❏ an index search utility that leads you directly to the desired topic
- ❏ a glossary of terms that are important to users of ITO
- ❏ help on help for users just getting started with online information systems
- ❏ a printing facility, which allows you to print any or all topics in the help system (a HP LaserJet printer is required to print graphics)

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

- ❏ in any active text field or on any active button, press the **F1** key,
- ❏ click the `Help` button in the bottom of any window
- ❏ open the drop-down `Help` menu from the menu bar
- ❏ click a symbol and use the right-hand 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 get 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 on which you want help. When you click the mouse button, the required help page is displayed in its help window.

#### The ITO Java-based GUI and OV ServiceNavigator Online Documentation

The ITO Java-based GUI online documentation helps operators to become familiar with and use the ITO product. The following information is included:

- Tasks—Step-by-step instructions for using ITO and the OV ServiceNavigator
- Concepts—An introduction to the key concepts and features of ITO and the OV ServiceNavigator.
- References—Detailed information to help operators maximize their use of ITO and the OV ServiceNavigator.
- Troubleshooting—Solutions to common problems you may encounter while using ITO or the OV ServiceNavigator.
- Index—An index to help operators quickly find the information they need.

To view any topic, open the appropriate folders in the frame on the left and click on the topic title. Hyperlinks provide related information on other help topics.

Access the help system by selecting `Help: Contents` from the main menu of the Java GUI. A web browser opens and displays the help contents. Note that you must first configure ITO to use your preferred browser, see the *HP OpenView IT/Operations Installation Guide for the Management Server* for more information.

# Contents

# Contents

# Contents

# Contents

# Contents

# Contents

# Contents

# Contents

# Contents

# 1 Prerequisites for Installing ITO Agent Software

This chapter lists all supported agents and describes the hardware and software prerequisites for each type of supported agent. This information is provided in order to help you select the correct agent platforms to use as ITO managed nodes. Check the minimum requirements thoroughly for each agent platform that you expect to install as a managed node.

**NOTE** In this section, ITO managed nodes are also referred to as ITO agents.

# Managed Node Requirements

To prepare for the installation of ITO on the managed nodes, make sure that the chosen managed nodes satisfy the following hardware and software requirements. This section is split into the following sections:

- Hardware requirements
- Software requirements

## Hardware Requirements

This section explains what hardware requirements exist for given agent platforms.

### Novell NetWare Hardware Requirements

The Novell NetWare systems you select as managed nodes must meet the following hardware requirements:

- Novell NetWare 4.1 Server or higher (Novell SMP is not supported)
- 10 MB disk space on each NetWare server in the SYS: volume
- 20 MB disk space for the software depot on the NetWare depot server in the SYS:volume
- 7 MB additional free RAM on the NetWare server (4 MB for the ITO agent, 1 MB for TI-RPC, and 0.5 to 2 MB for the NetWare Management Agent and XCONSOLE). At least 32 MB of server RAM is suggested for fair performance.
- 16 MB additional free RAM for the ITO agent if you are using NetWare SFT III file servers

### OS/2 Hardware Requirements

The OS/2 systems you select as managed nodes must meet the following hardware requirements:

❑ 10 MB disk space free

(About 20 MB required during software installation.)

- ❏ The ITO agent must be installed on an HPFS partition: FAT partitions are not supported for ITO Agent installation and operation.
- ❏ Additional swap space: none
- ❏ Additional RAM: 4MB

### UNIX Hardware Requirements

The UNIX systems you select as managed nodes must meet the following hardware requirements:

- ❏ 10 MB disk space free

  (About 20 MB is required during software installation.)
- ❏ Additional swap space: none
- ❏ Additional RAM: none

**NOTE** Only PA-RISC version 1.1 is supported on HP-UX 10.x managed nodes.

### Windows NT Hardware Requirements

The Windows NT systems you select as managed nodes must meet the following minimum hardware requirements:

- ❏ Windows NT 4.0 Workstation or Server
  - Windows NT 4.0 Server: 16 MB Memory
  - Windows NT 4.0 Workstation: 12 MB Memory
- ❏ 10 MB disk space on local NTFS disk
- ❏ During installation, an additional 10 MB of disk space is required on the local `C:` drive

## Software Requirements

This section lists the specific versions of the various agent operating systems that are supported by ITO and also provides information concerning how the software requirements for agents vary according to the specific operating system. In addition, this section explains what requirements exist for communication software (DCE and NCS) for each agent platform.

## ITO Supported Agent Platforms and Operating System (OS) Versions

Table 1-1 on page 31 lists the specific versions of the various agent operating systems that are supported by ITO.

**Table 1-1 Supported ITO-Agent Operating System Versions**

| Operating System | Platform | Supported OS Versions | Supported Communication Type [a] |
|---|---|---|---|
| AIX | IBM RS/6000<br>BULL DPX/20 | 4.1, 4.2, 4.3 | DCE |
| DataCenter/OSx SVR4 | Pyramid | 1.1 | NCS |
| Digital UNIX | DEC Alpha | 4.0 | DCE |
| DYNIX/ptx | Intel 486 or higher | 4.1.2, 4.1.3, 4.2.0, 4.4.0, 4.4.1, 4.4.2 | NCS |
| HP-UX | HP 9000 Technical Workstations [b] | 10.01, 10.10, 10.20<br>11.0 | DCE<br>DCE |
| HP-UX | HP 9000 Enterprise Servers [c,d] | 10.01, 10.10, 10.20<br>11.0 | DCE<br>DCE |
| IRIX | Silicon Graphics | 5.3, 6.2, 6.4, 6.5 | NCS |
| MPE/iX | HP 3000/900 | 5.5, 6.0 | NCS |
| NCR UNIX SVR4 | NCR System 3xxx/4xxx/5xxx (Intel 486 or higher) [e] | R.03.02 | NCS |
| Novell NetWare | Intel 486 or higher | 4.1, 4.11, 4.11 SFT III, | EZRPC [f] |
| Olivetti UNIX SVR4.2 | Olivetti (INTEL PCs) | 2.4.2 | NCS |

| Operating System | Platform | Supported OS Versions | Supported Communication Type [a] |
|---|---|---|---|
| OS/2 Warp | Intel 486 or higher | 3.0, 4.0 | DCE |
| SCO OpenServer | Intel 486 or higher | 3.2 (v4.0, v4.2, v5.0.0, v5.0.1, v5.0.2, v5.0.3, v5.0.4, v5.0.5) | NCS |
| SCO UnixWare | Intel 486 or higher | 2.1 | DCE |
| SINIX/Reliant | Siemens-Nixdorf | 5.43, 5.44 | NCS/DCE |
| Solaris | Sun SPARCstation | 2.5, 2.51, 2.6, 7 | NCS |
| Windows NT | Intel 486 or higher | 3.51, 4.0 (NT server and workstation)[g] | DCE [h] |
| | DEC Alpha | | |

a. DCE can be purchased at additional cost for some of these agent platforms, either from the platform vendor, or from a third-party supplier.
b. HP 9000/700 workstations are now referred to as HP 9000 Technical Workstations.
c. HP 9000/800 servers are now referred to as HP 9000 Enterprise Servers.
d. ITO uses the same binaries as for HP 9000 Technical Workstations.
e. NCR hardware types: 4700, 5100, and 5150 are supported only if the installed version of the standard NCR UNIX operating system is supported by ITO and any additional software which is installed does not change the IP address of the NCR node under *any* circumstances (takeover, etc).
f. Transport Independent Remote Procedure Call
g. ITO does not yet support special editions of the Windows NT Server operating system; for example, Windows NT Server Enterprise Edition or Windows NT Server Terminal Server Edition; nor does it support any software products extending these editions; for example, WinFrame or MetaFrame from Citrix Systems, Inc.. Contact your local HP Sales Representative for the latest information about support for these products.
h. ITO supports the remote protocol calls (RPCs) but not the security features.

Additional agent platforms may also be supported by HP partners, or directly by HP, either currently or in the near future. For a current list of supported agent platforms, contact your HP representative.

## Communication Software

ITO can use two mechanisms to communicate between the management server and the client nodes, these are the Distributed Computing Environment (DCE) and Network Computing System (NCS). Processes running on the ITO management server communicate using DCE by default, however, processes on the agents can communicate with the management server using either DCE or NCS. DCE is the recommended communication mechanism wherever possible. Table 1-2 on page 33 shows which version of DCE is required for a given agent operating system.

**Table 1-2 DCE version for ITO-Agent Operating Systems**

| Agent OS | Required DCE version |
|---|---|
| AIX | 1.2.1/1.4.1 or higher |
| Digital UNIX | 2.0 |
| HP-UX | 1.2.1/1.4.1 or higher |
| OS/2 | 1.0.2 or 2.1 |
| SINIX/Reliant | 2.0 |
| SCO UnixWare | 1.1 |
| Windows NT | 1.2.1/1.4.1 or higher |

If DCE runtime is not available with your other agent platforms, you will need to use NCS 1.5.1, with the Local Location Broker Daemon (`llbd`) instead of `dced`/`rpcd` running on the managed node.

**NOTE** Starting with DCE version 1.4.1, the DCE daemon (`dced`) replaces the RPC daemon (`rpcd`).

For platforms which support the NCS communication type, the following configuration step applies. If DCE or NCS runtime is not found on the managed node during installation, ITO automatically installs the appropriate NCS components (the `llbd` and `lb_admin` programs) on NCS nodes.

## Software Requirements for IBM AIX Managed Nodes

The following software must be installed on AIX managed nodes:

- ❏ Operating system. For the supported OS versions, see Table 1-1 on page 31.
- ❏ DCE RPC:
  - DCE RPC.
  - For AIX 4.1, it is recommended you install the `libc_r.a` patch. It can be found on CD-ROM 5765-393, (titled, *AIX V4 Update CD-ROM*). To install, login as root and run: `smitty update_all`.
  - The following filesets must be installed on the AIX 4.1 or 4.2 DCE RPC managed node:

```
dce.client.core.rte 2.1.0.6
dce.client.core.rte.rpc 2.1.0.0
dce.client.core.rte.cds 2.1.0.1
dce.client.core.rte.security 2.1.0.5
dce.client.core.rte.time 2.1.0.4
dce.client.core.rte.zones 2.1.0.0
dce.client.core.rte.admin 2.1.0.5
dce.client.core.rte.config 2.1.0.2
dce.client.dfs.rte 2.1.0.6
```

  - The following filesets must be installed on the AIX 4.3 DCE RPC managed node:

```
dce.client.core.rte 2.1
```

- ❏ ARPA/Berkeley Services.
- ❏ The MIB monitoring functionality of ITO requires SNMP-based, MIB-I (RFC 1156) or MIB-II (RFC 1158) compliant agent software.

## Software Requirements for DEC Alpha NT Managed Nodes

See “Software Requirements for Windows NT Managed Nodes” on page 42 for information regarding the software which has to be installed and running on managed nodes running DEC Alpha NT:

## Software Requirements for Digital UNIX (OSF/1) Managed Nodes

The following software must be installed on Digital UNIX (OSF/1) managed nodes:

- ❏ Operating System. For the supported OS versions, see Table 1-1 on page 31.
- ❏ Basic networking services
  - OSFCLINET4xx Basic Networking Services
- ❏ DCE Runtime Kit
  - DCERTS20x DCE Runtime Services V2.0

**NOTE** ITO supports DCE versions supplied with the Digital Unix operating system. However, although the Digital Unix operating system includes DCE, DCE has to be installed separately as an optional product.

- ❏ Japanese base system (only for managed nodes running Digital Unix in a Japanese environment)
  - IOSJPBASE4xx Japanese Base System

### Software Requirements for HP-UX 10.x Managed Nodes

The following software must be installed on HP-UX 10.x managed nodes:

- ❏ Operating system. For the supported OS versions, see Table 1-1 on page 31.
- ❏ DCE RPC version 1.2.1 or higher on HP-UX 10.x

  (SD-package: DCE-Core.DCE-CORE-RUN)
- ❏ Internet Services

  (SD-package: InternetSrvcs.INETSRVCS-RUN)
- ❏ LAN/9000

  (SD-package: Networking.NET-RUN)
- ❏ SNMP agent for MIB monitoring.

  SD-Package for HP-UX 10.20 and lower: NetworkingSnmpAgent

  SD-Package for HP-UX 10.30 and higher: OVSNMPAgent
- ❏ Native Language Support (NLS) Package

  (SD-package: OS-Core.NLS-AUX)

## Software Requirements for HP-UX 11.x Managed Nodes

The following software must be installed on HP-UX 11.x managed nodes:

- ❏ Operating system. For the supported OS versions, see Table 1-1 on page 31.
- ❏ DCE RPC version 1.7 or higher on HP-UX 11.x managed nodes.

  (SD-package: DCE-Core.DCE-CORE-RUN)
- ❏ DCE/9000 Kernel Thread Support

  (SD-package for HP-UX 11.x DCE-KT-Tools)
- ❏ 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 lower: NetworkingSnmpAgent)

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

  (SD-package: OS-Core.NLS-AUX)

## Software Requirements for MPE/iX Managed Nodes

The following software must be installed on MPE/iX managed nodes:

- ❏ Operating System. For the supported OS versions, see Table 1-1 on page 31.
- ❏ NCS version 1.5.1 or DCE RPC.
- ❏ NS services.

## Software Requirements for NCR UNIX SVR4 Managed Nodes

The following software must be installed on NCR UNIX SVR4 managed nodes:

- ❏ Operating System. For the supported OS versions, see Table 1-1 on page 31.
- ❏ If only the Multi-User operating environment is installed, then the networking package, WIN-TCP, must also be installed.
- ❏ NCS Version 1.5.1 (package NckNidl) or StarPRO DCE Executive from NCR UNIX SVR4.

  If neither NCS nor StarPRO DCE are found on the managed node, ITO installs `llbd` and `lb_admin` during the ITO agent software installation.
- ❏ The MIB monitoring functionality of ITO requires SNMP-based, MIB-I (RFC 1156) or MIB-II (RFC 1158) compliant agent software.

## Software Requirements for Novell NetWare Managed Nodes

The following software must be installed on Novell NetWare managed node:

- ❏ Operating System. For the supported OS versions, see Table 1-1 on page 31.
- ❏ TCP/IP services configured, running and automatically started
- ❏ Network FRAMING types must be configured (Ethernet II frame type is required)
- ❏ CLIB.NLM version 4.10 or higher
- ❏ Novell TIRPC (If this product is missing ITO copies the required files during the installation process.)
- ❏ SNMP daemon configured, running and automatically started
- ❏ XCONSOLE configured and running: remote console access (via telnet) must be allowed

  XCONSOLE.NLM must be installed and configured on each server. XCONSOLE is part of Novell products like Flex-IP or NetWare/IP.
- ❏ Novell NMA 2.1 installed and configured

  Novell NMA 2.1 is a NetWare add-on product and can be purchased from Novell. Note that almost all ITO NetWare agent instrumentation is based on NMA. NetWare servers which do not run NMA can, therefore, only be managed in a very limited way by ITO.

- ❏ NetBasic must be installed on NetWare depot servers

  NetBasic runtime version 6.00j - Build 4.127 or higher is required for NetWare depot server(s) (the systems which are used for the ITO agent software installation). See “Installation Tips for Novell NetWare Managed Nodes” on page 75 for details on how to get and install NetBasic.The valid runtime serial number to be used with NetBasic is delivered together with the ITO NetWare agent at no additional cost.

## Software Requirements for Olivetti UNIX Managed Nodes

The following software must be installed on Olivetti UNIX managed nodes:

- ❏ Operating System. For the supported OS versions, see Table 1-1 on page 31.
- ❏ Olivetti networking support utilities: nsu 2.4
- ❏ Olivetti internet utilities software: inet 2.4
- ❏ Gradient NCS 1.5.1 package SVR4 for x86: NckNidl GR 1.3.1

  If NCS is not yet installed on the managed node, ITO installs `llbd` and `lb_admin` during ITO software installation.
- ❏ For use in NFS cluster-client operations, the Olivetti NFS product (nfs 2.2) must be installed on the managed node.

## Software Requirements for OS/2 Managed Nodes

The following software must be installed on managed nodes running OS/2:

- ❏ Operating system: for the supported OS versions, see Table 1-1 on page 31.
- ❏ Networking packages for OS/2 Warp 3.0 or OS/2 Warp 4.0
  - TCP/IP 3.0 (requires MPTS - included in OS/2 Warp 3.0 Connect and OS/2 Warp 4.0)

    To get the SNMP daemons on OS.2 Warp 4.0, install System View Agent.

TCP/IP (or System View Agent on OS/2 Warp 4.0) includes two SNMP deamons, `snmpd` and `mib_2`. Both must be running when you install the agent software. They ensure that the management server is able to determine the node type of the managed node. If you want to use MIB variable monitoring, both deamonns must continue to run after the installation.

- DCE Runtime 1.0.2 or 2.1 (part of DSS/DCE for OS/2)
- TME NetFinity required for monitoring of some MIB variables

  TME NetFinity is pre-installed on OS/2 Warp 4.0 managed nodes, but must be installed separately on OS/2 Warp 3.0 managed nodes. The monitor template `os2_cpu_util` does not work on nodes without TME NetFinity installed.

## Software Requirements for Pyramid DataCenter/OSx Managed Nodes

The following software must be installed on Pyramid DataCenter/OSx managed nodes:

- ❏ Operating System. For the supported OS versions, see Table 1-1 on page 31.
- ❏ Pyramid TCP/IP software: OpenNet TCP/IP 1.0
- ❏ Gradient NCS 1.5.1 package SVR4 for MIPS: NckNidl GR1.3.0

  If NCS is not yet installed on the managed node, ITO installs `llbd` and `lb_admin` during ITO software installation.
- ❏ For use in NFS cluster-client operations, the Pyramid NFS product (OpenNet NFS 1.1) must be installed on the managed node.

## Software Requirements for SCO OpenServer Managed Nodes

The following software must be installed on SCO OpenServer managed nodes:

- ❏ Operating System. For the supported OS versions, see Table 1-1 on page 31.
- ❏ NCS 1.5.1 package or SCO DCE (DCE Executive).

  If neither NCS nor DCE are found on the managed node, ITO installs `llbd` and `lb_admin` during the ITO agent software installation.

## Software Requirements for SCO UnixWare Managed Nodes

The following software must be installed on SCO UnixWare managed nodes:

- ❑ Operating System. For the supported OS versions, see Table 1-1 on page 31.
- ❑ UnixWare Networking Support Utilities:
  - nsu 2.1
- ❑ UnixWare internet utilities software:
  - inet 2.1
- ❑ DCEcore 1.1
- ❑ For use in NFS cluster-client operations, the following version of the UnixWare NFS product must be installed on the managed node:
  - nfs 2.1

## Software Requirements for Sequent DYNIX/ptx Managed Nodes

The following software must be installed on Sequent managed nodes:

- ❑ Operating System. For the supported OS versions, see Table 1-1 on page 31.
- ❑ Sequent local area network product: ptx/LAN version 4.0.1. or higher
- ❑ Sequent TCP/IP product: ptx/TCP/IP version 4.0.3 or higher
- ❑ Gradient NCS 1.5.1 package NckNidl.

  If NCS is not found on the managed node, ITO installs `llbd` and `lb_admin` during the ITO agent software installation.

## Software Requirements for SGI IRIX Managed Nodes

The following software must be installed on IRIX managed nodes:

- ❑ Operating System. For the supported OS versions, see Table 1-1 on page 31.

- ❏ On IRIX 5.3, NCS 1.5.1 package netls_eoe.sw or gr_ncs.sw. On IRIX 6.2, NCS 1.5.1 package license_eoe.sw.netls.server. If neither NCS nor DCE are found on the managed node, ITO installs `llbd` and `lb_admin` during ITO software installation.
- ❏ On IRIX 5.3, package `eoe1.sw.svr4net` with System V compatible networking must be installed. On IRIX 6.2, package `eoe.sw.svr4net` with System V compatible networking must be installed.
- ❏ For diskless operations IRIX NFS must be installed on a cluster server.

## Software Requirements for Siemens-Nixdorf SINIX/Reliant Managed Nodes

The following software must be installed on SINIX/Reliant managed nodes:

- ❏ Operating System. For the supported OS versions, see Table 1-1 on page 31.
- ❏ Siemens-Nixdorf networking packages (5.43):
  - tcp
  - SImac596
- ❏ NCS 1.5.1

  If NCS is chosen as the `Node Type` in the ITO GUI, and NCS 1.5.1 is not found on the managed node, ITO installs `llbd` and `lb_admin` during the ITO agent software installation.
- ❏ DCE DCE-CLNT 2.0

  If the chosen communication type for the managed node is NCS RPC and NCS is not installed on the managed node, ITO installs llbd and lb_admin during the ITO agent software installation. If the communciation type is set to DCE RPCS (TCP or UDP), CDE-CLNT must be installed on the managed node
- ❏ Package: attcmd

## Software Requirements for Sun Solaris Managed Nodes

The following software must be installed on Solaris managed nodes:

- ❏ Operating System. For the supported OS versions, see Table 1-1 on page 31.
- ❏ NCS version 1.5.1 or DCE RPC. If neither NCS nor DCE are found on the managed node, ITO installs `llbd` and `lb_admin` during the ITO agent software installation.
- ❏ ARPA/Berkeley Services.
- ❏ The MIB monitoring functionality of ITO requires the snmpd of the HP OpenView platform, or SNMP-based, MIB-I (RFC 1156) or MIB-II (RFC1158) compliant agent software.

## Software Requirements for Windows NT Managed Nodes

The following software must be installed on Windows NT managed nodes:

- ❏ Required Service Packs:
  - Windows NT 3.51: Service Pack 5
  - Windows NT 4.0: Service Pack 3 or 4
- ❏ Operating system: for the supported OS versions, see Table 1-1 on page 31.
- ❏ FTP Service running (required during “ftp Agent Package” type installation)
- ❏ Schedule Service must not be disabled (required during installation)
- ❏ TCP/IP services running and automatically started
- ❏ RPC Services running (Server, Remote Procedure Call Service) and automatically started
- ❏ Event Log and SNMP Services (if discovery and other SNMP features of ITO should be used)
- ❏ The DHCP (dynamic address service for Windows NT clients) must not be used, since ITO relies on the IP address to identify the managed nodes.

# 2 Installing ITO Agents on the Managed Nodes

This chapter describes how to install the ITO agent software on the various supported managed nodes, and includes numerous tips for different operating systems.

The installation procedures assume that you have already installed and configured the database and ITO on the management server, as described in the *HP OpenView IT/Operations Installation Guide for the Management Server*.

# Overview

This section contains important information about installing and de-installing ITO agent software on managed nodes with various operating systems. This section includes:

- ❏ installation tips
- ❏ steps for installing the ITO agent software on managed nodes
- ❏ automatic installation or update procedures
- ❏ automatic de-installation procedures for managed nodes

Make sure that the kernel parameters are set correctly on UNIX systems. Although system default values are normally sufficient, the logfile encapsulator sometimes requires that the number of open files be increased. You can check and change the system parameters using the tools listed in Table 2-1 on page 45.

**Table 2-1 System Administration Tools**

| Operating System | Tool |
|---|---|
| AIX | SMIT |
| Digital UNIX | setup |
| DYNIX/ptx | menu |
| HP-UX | SAM |
| IRIX | sysmgr |
| NCR UNIX | sysadm |
| Olivetti UNIX | sysadm |
| Pyramid DataCenter/OSx | sysadm |
| SCO OpenServer | 3.2v4*: sysadmsh |
| | 3.2v5.0.x: scoadmin |

| Operating System | Tool |
|---|---|
| SCO UnixWare | sysadm |
| SINIX | sysadm |
| Solaris | admintool |

NCR UNIX SVR4 and SGI have no automated tools. Windows NT system parameters cannot be changed.

Table 2-2 on page 46 gives values for kernel parameters on HP-UX managed nodes. Other agent platforms generally require similar values.

**Table 2-2 Important Kernel Parameters for Managed Nodes**

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

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

# General Installation Tips for Managed Nodes

- When possible, install the latest ITO agent software version on all managed nodes. This will enable the latest ITO features to be used on those nodes.
- The names bin, conf, distrib, unknown and mgmt_sv may not be used for managed nodes. These names are used internally by ITO, and therefore must not be used as the name of any system.
- Avoid using host aliases, as this will cause problems in the event that two aliases are identical.
- 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: `/etc/hosts` (UNIX systems), or `HOSTS.NET.SYS` (MPE/iX systems). On HP-UX, Solaris, AIX, and other UNIX SVR4 systems, you can verify this by using the `nslookup` command. On systems running; Windows NT, OS/2, or NetWare use the `ping` command or NLM.
- The DCE RPC daemon (dced or rpcd) must be running when installing or updating the ITO Software on the management server. Either the DCE RPC daemon (dced or rpcd) or NCS Local Location Broker daemon (llbd) must be running when installing or updating the ITO Software on the management server and/or managed node. If they are not, the ITO services cannot be started. Automatic startup and integration of the startup functionality in the appropriate boot procedure is done by ITO only for the `dced/rpcd` or `llbd`, and only if you have selected the `Automatic Update of System Resource Files` option, see the `Add/Modify Node` window in the ITO administrator GUI.

  System resource files are, for example, `/etc/rc.config.d` (HP-UX 10.x and 11.x), `/etc/inittab` (AIX), and `SYSSTART.PUB.SYS` (MPE/iX)

  On HP-UX systems, see the appropriate man pages, for example: *dced(1M)*, *rpcd(1M)*, or *llbd(1M)*. On MPE/iX systems, see the NCS online documentation located at: `ncsman.pub.hpncs` and `manual.pub.hpncs`.

- Identify managed nodes having more than one IP address, and specify the most appropriate address (for example, the IP address of a fast network connection) in the ITO configuration. Verify that all other IP addresses of that managed node are also known at the management server. Otherwise, the messages from the multiple IP address systems might not be forwarded by ITO.
- During installation on managed nodes, twice the amount of disk space actually required by ITO is necessary, because the tape image is transferred to the managed node before uncompressing and unpacking it.
- For MPE/ix managed nodes, use only fully qualified ARPA host names. It is also recommended that you set the environment variable *HPSYSNAME* to the name of your MPE/iX system. The best way to do this is to insert the setting in a system-wide logon-UDC in the format:

  **:HPSYSNAME=<full_qualified_hostname>**

  Use long host names in your templates only when performing automatic and/or operator initiated actions.
- Do not up or downgrade the OS version of the management server or managed node to a level not supported by ITO. For a list of supported OS versions on the management server, see the *HP OpenView IT/Operations Installation Guide for the Management Server*, and on the managed nodes, see Table 1-1, “Supported ITO-Agent Operating System Versions,” on page 31. You can also get this information by running the following script on the management server:

  **/opt/OV/bin/OpC/agtinstall/opcversion**
- Check that the system times of the management server and the managed nodes are synchronized—as far as possible—to guarantee that the time received on the management server is always later than the time the message has been generated on the managed node.
- Make sure you know all the root passwords of all the managed nodes when you install the ITO agent software.

  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 10.x/11.x).
- If you don’t have enough disk space in your UNIX file system for ITO, apply one or more of the following solutions:

- Use a symbolic link. For example, for HP-UX 10.x:

  ```
  ln -s /mt1/OV /opt/OV
  ```

- Mount a dedicated volume. For example, for AIX:

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

Note that for HP-UX systems (versions below 10.00), `/etc/update(1M)` does not support installation on NFS-mounted file systems. You can also set the following `swinstall` option:

```
write_remote_files=true
```

❏ If you wish to move the management server to some other system, you must first de-install the ITO managed node software from all managed nodes, or change the management server entry in the related ITO information file. For the location of this file, see Table 10-3 on page 399.

❏ If you do not need the functionality of the ITO default operator on your managed nodes (except on the management server), you can purge the related information:

UNIX:

- erase the home directory of the user **`opc_op`**
- remove the **`opc_op`** entry from `/etc/passwd`
- remove the **`opcgrp`** entry from `/etc/group`

MPE/iX:

- purge the account `OVOPR`

**NOTE**

The ITO default operator may not be removed from Windows NT managed nodes because the agents run under the operator's account.

❏ When you upgrade or reinstall ITO software on managed nodes, make sure that all programs and applications which use the `opcmsg(3)` or `opcmon(3)` API are stopped.

This is important because these and other APIs are stored in the ITO shared library, which is over-written during ITO software upgrade or reinstallation. For more information, see the *HP OpenView IT/Operations Developer's Reference*.

## Installation Tips to be Performed on the Management Server

- If you want to stop the configuration and script/program distribution, for example, if the configuration is invalid, clean the `/distrib` directory. This should only be done in an emergency and only after the ITO management server processes have been stopped.

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

- Avoid interrupting the software installation or de-installation process on managed nodes. Doing so will cause a semaphore file to be left on the management server, and you will not be able to re-invoke the installation. In this case, remove the file manually.

  **`/var/opt/OV/share/tmp/OpC/mgmt_sv/inst.lock`**

  If you interrupt the software installation or de-installation on the managed nodes at the time you are asked for a password, your terminal settings will be corrupted and any commands that you type will not be echoed in the terminal. If this happens, you can reset the terminal by typing the following:

  **`stty echo`**

- Do not de-install any of the management server bits, for example `OVOPC-ORA` or `OVOPC`, if any managed node is still configured and has the appropriate ITO bits.

- Do not de-install the managed node tape images (for example `OVOPC-CLT-ENG/JPN`) from the management server, if any managed node of this type is still configured and has the ITO bits installed on it. If you do, you will be unable to de- install the ITO agent software using the ITO GUI.

## Installation Tips for UNIX Managed Nodes

### General Tips

- Make sure that `uname(1M)` returns the short system name.

- The nameservice (`/etc/hosts` and/or DNS) needs to be set up so that *all* name-service operations (like `nslookup`) are consistently resolved to the fully-qualified system name. For example, `hostname` is not name-service related and may return the short hostname.

- ❏ The non-default log directory on UNIX systems is erased during de-installation of ITO. Note the following rules about this directory:
  - Do not use the same directory for more than one managed node, this could be a potential problem in cluster environments, or in cases where the directory is NFS-mounted across several systems.
  - Do not use the same log directory for ITO and other applications.
  - Do not create subdirectories beyond ITO's log directory for use by other applications or other managed nodes.
- ❏ Make sure that `inetd`'s security file on the managed nodes allows `remshd` or `ftpd` for the management server. For example:

  HP-UX 10.x `/var/adm/inetd.sec`
- ❏ Make sure that root is not registered in `/etc/ftpusers` on the managed node, if no .rhosts entry for root and no `/etc/hosts.equiv` entry for the management server is available.
- ❏ By default, ITO registers the default operator opc_op with user-ID 777 and group-ID 77, if available, for AIX, and user-ID 777 and group-ID 177, if available, for SINIX, Olivetti, Pyramid, and SCO UnixWare. For consistency, make sure that the user-ID and group-ID are identical on all your managed nodes.

**NOTE**

If you wish to install or re-install the ITO agent manually on nodes with the ITO Advanced Network Security (ANS) extension, you need to copy the file `nsp_pkg.Z`, too. For more information on which platforms are supported, see the *Advanced Network Security Extension for HP OpenView IT/Operations* guide.

## Tips for NFS Cluster Client Specials

The ITO software maintenance process for managed nodes makes the following assumptions about NFS cluster configurations:

- ❏ If the file system containing the ITO agent binaries of a managed node is NFS-mounted to a file system on another computer, then this managed node is considered an ITO **cluster client**. The system that exports the file system that is mounted by the managed node is called the **cluster server**.

  ```
  CLUSTER SERVER <server>: CLUSTER CLIENT <client>:

  exported /opt <-------     server:/opt on /opt
  ```

This assumption is valid for all platforms that support NFS operations, regardless of special support for diskless nodes. For example, NCR UNIX does not support diskless configurations but you can make a cluster of NCR workstations that share common ITO agent code.

For platforms belonging to the UNIX family that support diskless or disk- poor cluster nodes:

- ❏ Systems belonging to the same cluster cannot belong to different ITO environments.
- ❏ Make sure that all ITO agent processes on any cluster node are completely stopped when installing a new ITO version on the cluster or when de-installing the ITO software from the cluster; use:

  ```
  opcagt -kill
  ```

- ❏ The agent software component must also be selected for cluster clients, even if the software is already installed on the cluster server because node-specific directories, symbolic links, mounts etc. are established for each cluster node. You can, however, respond with “n” to the question, “Do you want to force update?”.
- ❏ The ITO agent software package is only installed on the cluster server when the first cluster member (cluster client or cluster server) is installed with ITO. The installation process for other cluster clients only establishes local directories, updates local client resources, and starts local ITO agents.

## Installation Tips for AIX Managed Nodes

- ❏ Verify that at least `rshd` or `ftpd` is available if `securetcpip` is enabled.
- ❏ Check that the limits specified in `/etc/security/limits` fit your requirements. The **default**, **root**, and **opc_op** entries are of special interest.
- ❏ Verify that one of the following DCE software packages is installed:
  - dcebase.base.obj
  - dce.client.core.rte.admin
- ❏ The ITO agent software is installed on the `/usr/lpp` file tree.

If the file system which hosts the `/usr/lpp` file tree is too small to install ITO Agents, create a symbolic link before installing ITO. For example: if `/bigdisk` is a local file system with enough free space:

```
mkdir -p /bigdisk/OV

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

In a cluster environment, you must check that `/bigdisk` 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.

- In ITO version A.02.00 and later, agent software is installed under the `/usr/lpp/OV` path name instead of under `/export/lpp/OV/rs6000/aix` as it was in earlier versions. Since `/usr` (or `/usr/lpp`) and `/export` normally belong to different file systems, this means that enough disk space must exist on `/usr` (or `/usr/lpp`) file system before an upgrade to A.02.10 can be successfully installed. This differs from other upgrades where software is installed in the same directories as the previous version. Disk space occupied by previous versions of ITO agents under `/export/lpp/OV/rs6000/aix` will be freed.
- AIX diskless nodes may initially be created so that root password is not required. It is possible to remote login on these systems but command execution with remsh will not be possible because .rhosts is initially not present on the diskless client. FTP to this type of node will also not be possible because the root password is empty. It is, therefore, not possible to install ITO automatically on a diskless node before either the root password is assigned or the `.rhosts` file is set up properly. Note that initially the /etc/hosts file on the diskless node also does not include the ITO management server.

## Manual AIX Agent Installation

In some situations, it may be desirable to install the AIX agent software without using the management server. This *manual installation* makes it possible to prepare the workstation, so that it is ready to become an ITO managed node when it is later connected to the network. This may be useful if many workstations are prepared in some central location, or if one wants to avoid the root connection over the network that is necessary for a standard agent installation.

#### Install the Agent on the Managed Node:

Use the following instructions to install the ITO AIX agent on an AIX system that will become an ITO managed node:

1. Copy the ITO agent package to a temporary directory on the managed node. On the management server, this agent package is located in:

   ```
   /var/opt/OV/share/databases/OpC/mgd_node/vendor/ibm/\
   rs6000/aix/A.05.00/RPC_DCE_[TCP|UDP]/opc_pkg.Z
   ```

   If you intend to run ITO Advanced Network Security (ANS) on this node, you also need to copy the file:

   ```
   /var/opt/OV/share/databases/OpC/mgd_node/vendor/ibm/\
   rs6000/aix/A.05.00/RPC_DCE_[TCP|UDP]/nsp_pkg.Z
   ```

2. Uncompress the agent package:

   **`uncompress opc_pkg.Z`**

   If appropriate, uncompress the ANS package, too:

   **`uncompress nsp_pkg.Z`**

3. Install the agent on the node:

   **`installp -ac -I -X -F -d<`*`directory`*`>/opc_pkg all`**

   If appropriate, install ANS on the node, too:

   **`installp -ac -I -X -F -d<`*`directory`*`>/nsp_pkg all`**

#### Activate the Node Using the Command Line:

You can activate the agent on the node over the net (without the GUI and without root access) by using the following command-line steps:

1. After manually installing the agent on the node, enter:

   **`/opt/OV/bin/OpC/install/opcactivate <`*`ITO_mgt_server`*`>\`**

   **`-cs <server_codeset> -cn <agent_codeset>`**

   This will activate the agent, which will then attempt to send messages to the management server. For more information about codesets, see Chapter 8, “ITO Language Support,” on page 333.

**NOTE**

Use the `opcactivate` command with the **`-mode`** option to activate:

| | |
|---|---|
| hacmp | for ITO agents on AIX HACMP systems. See also "Installation Prerequisites for AIX HACMP Agents" on page 58 |
| cluster server/client | for ITO agents on AIX Cluster-Client systems after the ITO agent software package has been installed on the AIX Cluster Server system. For more information, see "Manually Activating the ITO Agent on NFS Cluster Clients" on page 169. |

See the man page *opcactivate(1m)* for more information.

2. After the node is connected to the network execute the following two commands on the management server:

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

   b. **`/opt/OV/bin/OpC/opchbp -start <node>`**

   This will update the database and start heartbeat polling for the node. The templates, monitors, commands, and actions must still be installed using the ITO administrator GUI.

#### Activate the Node Using the ITO GUI:

After the node with the pre-installed agent is connected to the network, use this procedure to activate and register the managed node.

1. Add the pre-installed node(s) to the `ITO Node Bank` using the menu sequence `Actions:Node->Add`.
2. Add the node to an ITO node group. The easiest way to do this is to drag and drop it onto a node group in the `ITO Node Group Bank window`.
3. Distribute the ITO configuration to the node:

   a. Select `Actions:Agents->Install` from the menubar of the `ITO Node Bank`. The `Install /Update ITO Software and Configuration` window opens.

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

**NOTE** Do not check `[Force Update]` otherwise 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.

Note that if the agent software is *not* pre-installed, this action will install the agent.

4. Execute the following command to verify that the Control, Message, and Action Agents are all running on the managed node:

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

### Tips for DCE on AIX 4.1 and 4.2

- To run `snmpd` at boot time, uncomment the line:
  `#start /usr/sbin/snmpd "$src_running"`
  in the file /etc/rc.tcpip.
- Even though the `rpcd` daemon does not exist on AIX 4, the SMIT utility erroneously tries to run it in the option entitled *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*.

### Problems Caused by Missing OS Patches for AIX

- Sometimes the ITO agent de-installation procedure on AIX 4.1 systems does not return freed disk space when ITO is removed from the systems. If the `'df'` output does not reflect the freed disk space, reboot the machine and check free disk space on `/usr` with **`'df -k /usr'`**.

## Installation Tips for AIX Managed Nodes Running SP2/HACMP

This section includes important information about installing ITO agents on nodes running HACMP. General installation tips for AIX also apply to AIX nodes running HACMP. This section is organized as follows:

- ITO Agents in the HACMP environment
- Installation Prerequisites for AIX HACMP Agents

- Pre-installation tasks
- Problems with IP aliases in AIX OS
- Installing AIX HACMP agents

## ITO Agents in the HACMP Environment

Each node in an HACMP cluster has its own ITO agent and must be accessible on a fixed IP address, which represents the node in the ITO Node Bank. This IP address must always remain bound to the same node. Consequently, IP addresses which are subject to change cannot be used to install and run an ITO agent running HACMP.

If an additional adapter (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, it can be used for ITO Agent installation. However, communication with the ITO server *must* be possible via this additional adapter. There is no need to set up IP aliases or modify shell scripts in this case, and all pre-installation tasks can be skipped. But it is important that the IP address on this adapter does not change.

If no such adapter is available, each node should be assigned an IP alias in the same network in which the boot and service IP addresses reside. In addition, the node must be configured 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 ITO agent on the node. After successful installation of the ITO agent, the IP alias is present in the `/var/lpp/OV/conf/OpC/nodeinfo` file in the field `OPC_IP_ADDRESS`.

To avoid confusion with any other IP addresses that may be set on the interface or with messages in the Message Browser originating from addresses other than the service address of the node, the following naming scheme is recommended in your HACMP environment:

| | |
|---|---|
| `<nodename>_boot` | for the node's boot address |
| `<nodename>_svc` | for node's service address |
| `<nodename>_stdby` | for node's standby address |
| `<nodename>_ito` | for the node's IP alias |

Where <nodename> is the name of the node as defined in the HACMP configuration.

Note that the status of the icon representing the node in `Node Bank` window does not change color immediately when the node in the HACMP cluster goes down: it will change color only after ITO has determined that it cannot contact the control agent on that node.

## Installation Prerequisites for AIX HACMP Agents

The following software versions are supported:

- AIX 4.2 / 4.3 (DCE agents)
- HACMP 4.2.2

## AIX HACMP Agents: General Pre-installation Tasks

You *must* set the IP alias that is used by the ITO agents during and after the installation process on each node on which you wish to run the ITO agent. To set the IP alias:

on AIX v4.3

1. Use the `smit` menus.
2. In a shell, enter the following command:

   **`smit tcpip`**

   Then select from the menu bar:

   `Further Configuration -> Network Interface Selection -> Configure Aliases -> Add an IPV4 Network Alias`
3. Select the desired interface, eg: `en0`
4. Enter values for the IP address and network mask

on AIX v<4.3

1. Use the following command:

   **`/usr/sbin/ifconfig en0 <IP_Adress> alias`**

   where <IP_Address> is the IP address of the node on which you want to install the ITO agent for AIX HACMP.
2. This command can also be included in the file `/etc/rc.net` so that the IP alias is set automatically when the OS is booted.

## Problems with IP Aliases in AIX OS

One very important consequence of setting the IP alias on the interface is that HACMP no longer works correctly. This is true for *all* events that deal with IP addresses, such as; `acquire service address`, `acquire takeover address`, `swap adapter`, and so on. The problem is due to a flaw in the AIX OS, and may be addressed in the following way:

- download and install the appropriate fix(es) for the AIX OS

For managed nodes where AIX OS fixes have already been installed, refer to "Pre-Installation Instructions for Managed Nodes with the AIX OS Patch for IP Aliases" on page 59.

It is highly recommended that the appropriate fixes for the AIX OS are installed to overcome the problems with IP aliases and HACMP. The fixes may be obtained using IBM's FixDist package or from their web site. The following APARs can be used to obtain the fixed versions of related packages:

- AIX 4.2 IX75987
- AIX 4.3 IX78397

Only after the fixes for the AIX OS have been installed will HACMP function properly: some HACMP functionality does not work on managed nodes without the AIX OS fixes installed (e.g. swap adapter event).

## Pre-Installation Instructions for Managed Nodes with the AIX OS Patch for IP Aliases

All HACMP events work once the AIX OS fixes are installed and the IP alias is set on the interface. However, due to a minor problem with the IP alias address itself, you *do* have to reset the IP alias on the interface after each change of the IP address - the IP alias address no longer works after the `ifconfig` command is used to change the main IP address on the interface. Note that you have to reset the IP alias on all cluster nodes where the ITO agent is to be installed. The following shell script may be used to set the IP alias on the interface where the service or boot IP address is set:

```
#!/bin/sh
ALIAS_IP="192.168.1.54"
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 that was used for the installation of the ITO agent. Remember to change the *ALIAS_IP* variable if you copy the shell script to other nodes in the cluster. This 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, the script can be used as the post-event script for the following HACMP events:

- acquire service address
- release service address
- swap adapter

Use the SMIT screens by entering the following command in a shell: **`smit hacmp`**. Then select `Cluster Configuration -> Cluster Resources -> Change/Show Cluster Events`. Next, select the appropriate 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`.

Note that from time to time entries like this will appear in the file: `/var/lpp/OV/log/OpC/opcerror`:

```
WARNING opcmsga (Message Agent)(8028) [genmsga.c:535]:
Communication failure to message receiver: Connection
request rejected (dce/rpc).Buffering messages.(OpC30-3)
```

These entries may safely be ignored. Messages are not lost: they are sent to the ITO server after communication is re-established. This usually takes no more than a few seconds.

## Installing AIX HACMP Agents

The installation process is straightforward and does not differ from the installation of the ITO agents on any other computer running AIX, with the exception of the following:

- the IP *alias* address must be used as the IP address for the host on which the ITO agent is to be installed.

- The installation script checks if the IP address which is used for the ITO installation is tied to the boot, service, or standby interfaces, and issues a warning if this is the case. However, the installation proceeds nonetheless.
- If you select automatic start of ITO agents, the file `/etc/inittab` is also updated so that the `clinit` entry remains the last one - as is required by HACMP.
- After successful installation of the ITO agent, the IP alias appears in the `/var/lpp/OV/conf/OpC/nodeinfo` file in the field `OPC_IP_ADDRESS`.
- The following line is added to the `opcinfo` file during installation process:

  `OPC_NAMESRV_LOCAL_NAME <hostname>`

  where `<hostname>` is the name of the host configured with the IP address used for the installation of the ITO agent. If this IP address changes, this line should be changed accordingly. Note that this line *must* be present in order to ensure that the IP address is the same in the context of both ITO *and* ANS (ITO's Advanced Network Security extension). This ensures that the same hostname is used by all security functions that require `<hostname>` as their argument (e.g. secret key generation). If this keyword is *not* present, ANSE functions retrieve hostname from the RPC runtime, which is often different from the hostname used for ITO installation, and the ANSE functions will fail.

## Installation Tips for DEC Alpha NT Managed Nodes

For general information, see "Installation Tips for Windows NT Systems" on page 99. Note the following important points:

- ❏ path names differ only in the architecture name, for example:
  - `...ms/intel/nt`
  - `...ms/alpha/nt`
- ❏ Fileset is: OVOPC-CLT-ENG.OVOPC-ANT-CLT
- ❏ After entering `Label` and `Hostname` in the `Add Node` window, ITO looks up and retrieves the following values:

- Machine Type: **DEC Alpha**
- OS name: **Windows NT**

If SNMP services are not running on the Windows NT node ITO cannot detect the Machine Type and OS Name. In this case, enter the appropriate values and continue with the installation.

### Manual Installation: DEC Alpha NT Agent

For instructions on manually installing the DEC Alpha NT agent, see "Manual Installation: Windows NT Agent" on page 111. Note however that the location on the ITO management server of the opc_pkg.Z, opc_inst.bat, opc_pre.bat, opcsetup.inf, unzip.exe and unzip.txt files for the DEC Alpha NT platform is:

```
/var/opt/OV/share/databases/OpC/mgd_node/vendor/ms/\
alpha/nt/A.05.00/RPC_DCE_TCP
```

**NOTE** If you are installing the DEC Alpha NT agent using the instructions in "Manual Installation: Windows NT Agent" on page 111, all references to intel in the path name should be replaced with alpha. For example:

/ms/*intel*/nt should be changed to;/ms/*alpha*/nt

## Installation Tips for Digital UNIX Managed Nodes

- The ITO Agent software is installed on the /usr/opt file tree. If there is not enough space for installation of the ITO agents, create a symbolic link *before* installing ITO. For example: if /bigdisk is a local file system with enough free space:

  ```
  mkdir -p /bigdisk/OV
  ln -s /bigdisk/OV /usr/opt/OV
  ```

  In a cluster environment, you must check that /bigdisk 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.

- Some logfiles monitored by the logfile encapsulator are not present on Digital UNIX managed nodes by default. 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 lines 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:

```
touch /var/adm/sialogr
```

## Installation Tips for DYNIX/ptx Managed Nodes

- The ITO Agent software is installed on the `/opt` file tree. An empty `/opt` file tree is created during installation of the DYNIX/ptx operating system. By default, this file tree is positioned on the root file system. If the root file system is too small for the installation of ITO agents, create a symbolic link before installing ITO. For example: if `/bigdisk` is a local file system with enough free space:

  ```
  mkdir -p /bigdisk/OV
  ln -s /bigdisk/OV /opt/OV
  ```

  In a cluster environment, you must check that `/bigdisk` 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.

## Installation Tips for HP-UX 10.x and 11.x Managed Nodes

You can install ITO on HP-UX 10.x and 11.x platforms using the advanced features of HP Software Distributor (HP SD-UX) to help reduce installation costs and time. You can use this method to install the ITO agent software package from a software depot on a node other than the ITO management server.

This feature is especially useful in an environment where a LAN of managed nodes is managed by the management server over a WAN. Instead of transferring “x” number of agent packages over the WAN line,

the package is installed once on a **depot node** in the remote LAN. Subsequent agent installations then get the package from the local depot.

**Figure 2-1 Standard ITO Agent Installation Method**

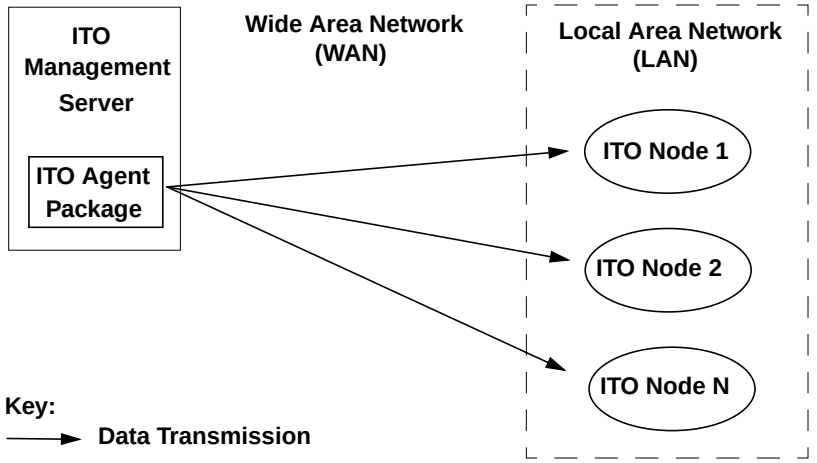
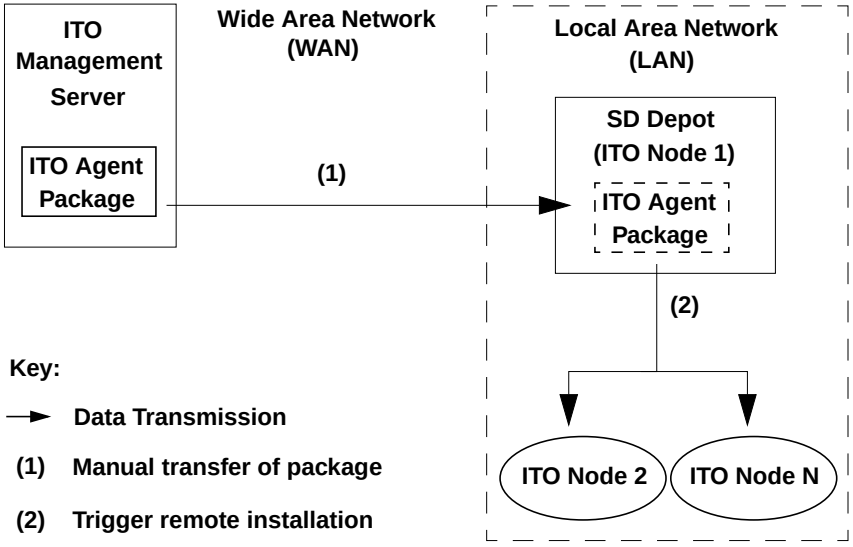


**Figure 2-2** **Using HP SD-UX Remote Software Depot to Install ITO on HP-UX 10.x and 11.x Managed Nodes**




## Creating a Software Depot on a Remote Node

To create an HP-UX 10.x or 11.x Software Distributor (SD) Depot for the installation of ITO managed nodes:

- If you don't have additional licenses, you can only copy the package locally. If this is the case on the depot node, transfer the ITO software package from the management server over the WAN to the depot node using FTP. The ITO software package (`opc_pkg.Z`) is located in the following directory on the management server:

  for HP-UX 10.x managed nodes:
  `/var/opt/OV/share/databases/OpC/mgd_node/vendor/hp/\`
  `s[7|8]00/hp-ux10/<`*`ito_version`*`>/RPC_DCE_[TCP|UDP]/\`
  `opc_pkg.Z`

  for HP-UX 11.x managed nodes:
  `/var/opt/OV/share/databases/OpC/mgd_node/vendor/hp/\`
  `pa-risc/hp-ux11/<ito_version>/RPC_DCE_[TCP|UDP]/\`
  `opc_pkg.Z`

- Copy an *uncompressed* package into the `/tmp` directory and execute as follows:

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

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

- To obtain a *compressed* depot, you must first create a temporary, uncompressed depot. You can then copy the depot to another depot, and specify the options **`-x compress_files=true`** in the `swcopy` command:

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

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

- To remove the product from the SD depot on the depot node, enter (on the depot node):

  ```
  swremove -d OVOPC-AGT @ depot2
  ```

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

## Using the Software Depot

Once the SD depot is established, all ITO agents within the LAN can retrieve the ITO binary package from the SD depot instead of from the management server, see Figure 2-1 and Figure 2-2. This part of the installation process is performed automatically.

The install operation is initiated from the administrator's GUI on the ITO 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 package from the SD depot using the `swinstall` command, for more information, see the `swinstall(1M)` man page.

To enable the SD, configure the node name for the SD depot using the `Add/Modify Node: Advanced Options` window in the ITO administrator's GUI. You can choose between the traditional installation method (default) or use an SD depot.

## Manual HP-UX Agent Installation

In some situations, it may be desirable to install the ITO HP-UX agent software without using the management server. This *manual installation* makes it possible to prepare the workstation, so that it is

ready to become an ITO managed node when it is later connected to the network. This may be useful if many workstations are prepared in some central location, or if one wants to avoid the root connection over the network that is necessary for a standard agent installation.

#### Install the Agent on the Managed Node:

Use the following instructions to install the HP-UX agent on an HP-UX workstation that will become an ITO managed node:

1. Install the agent package files from the ITO management server to the managed node. You can do this either by copying an SD tape file to the node, or by using an SD depot. Using an SD tape file allows you to install the agent without a depot, and without any network connection. However, if you plan to pre-install many agents, you may find it more convenient to create and use a depot (see "Creating a Software Depot on a Remote Node" on page 65).

   - Using an **SD tape file**:

     a. Copy the ITO agent package to a temporary directory on the managed node. On the management server, this agent package is located in:

        for HP-UX 10.x managed nodes:
        `/var/opt/OV/share/databases/OpC/mgd_node/\`
        `vendor/hp/s[7|8]00/hp-ux10/<`*`ito_version`*`>/\`
        `RPC_DCE_[TCP|UDP]/opc_pkg.Z`

        for HP-UX 11.x managed nodes:
        `/var/opt/OV/share/databases/OpC/mgd_node/\`
        `vendor/hp/pa-risc/hp-ux11/<ito_version>/\`
        `RPC_DCE_[TCP|UDP]/opc_pkg.Z`

**NOTE**

If you intend to run ITO Advanced Network Security (ANS) on this node, you also need to copy the following file from the same directory (HP-UX 10.x/11.x, as appropriate):

`nsp_pkg.Z`

     b. Uncompress the agent package:

        **`uncompress opc_pkg.Z`**

        If appropriate, uncompress the ANS package, too:

        **`uncompress nsp_pkg.Z`**

c. Install the agent on the node:

```
swinstall -x source_type=tape -s\
/<full_path>/opc_pkg OVOPC-AGT
```

If appropriate, install the ANS package on the node, too:

```
swinstall -x source_type=tape -s\
/<full_path>/nsp_pkg ITOAgentNSP
```

**NOTE** For cluster nodes, use `swcluster`, instead of `swinstall`, on the cluster server.

d. Examine the node's logfile `/var/adm/sw/swagent.log`. If any errors occurred during installation, correct the problems and reinstall.

- Using an **existing SD depot**:

a. Install the agent on the node:
**`swinstall -s <`*`depot_host`*`:`*`depot_path`*`> OVOPC-AGT`**

If appropriate, install the ANS agent package on the node, too:

**`swinstall -s <`*`depot_host`*`:`*`depot_path`*`>\`**
**`ITOAgentNSP`**

b. Examine the node's logfile `/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 with the SD GUI, but it has the disadvantage that it does not notify you of any warnings found in the analysis phase unless you run it twice and set the **`-p`** option in the first run. If you would like to use the GUI, simply omit the name of the agent package (`OVOPC-AGT`) when you enter the `swinstall` command.

Installing the agent package will produce dependency errors, because the package does not hold all the files necessary for the agent to run. If you want to be certain that all these files exist, you can use the command **`/usr/sbin/swlist -l product`** to get a list of all software that is installed on the node.

#### Activate the Node Using the Command Line

You can activate the agent on the node over the net (without the GUI and without root access) by using the following command-line steps:

1. After manually installing the agent on the node, enter:

   ```
   opcactivate <ITO_mgt_server> -cs <server.codeset> \
   -cn <agent.codeset>
   ```

   See also Chapter 8, “ITO Language Support,” on page 333 for more information about codesets.

   This will activate the agent, which will then attempt to send messages to the management server.

2. After the node is connected to the network execute the following two commands on the management server:

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

   b. **`/opt/OV/bin/OpC/opchbp -start <node>`**

   This will update the database and start heartbeat polling for the node. The templates, monitors, commands, etc. must still be installed using the management server GUI.

#### Activate the Node Using the ITO GUI

After the node with the pre-installed agent is connected to the network, use this procedure to activate and register the managed node.

1. Add the pre-installed node(s) to the ITO Node Bank using the menu sequence: `Actions-> Node-> Add`.
2. Add the node to an ITO node group. The easiest way to do this is to drag and drop it onto a node group in the `ITO Node Group Bank window`.
3. Select: `Actions-> Agents-> Install` to bring up the `Install /Update ITO Software and Configuration` window. Select all components (but do not check `[Force Update]` otherwise the management server will re-install the agent), then click `[OK]`. If the agent is pre-installed on the node, the management server will activate the node, and install the selected components. Note that if the agent software is *not* pre-installed, this action will install the agent.

4. Use the command **`/opt/OV/bin/OpC/opcragt -status <node>`** to verify that the Control, Message, and Action Agents are all running on the managed node.

## Installation Tips for IRIX Managed Nodes

- The ITO agent software is installed on the `/opt` file tree. If the file system that hosts the `/opt` file tree is too small for the installation of ITO Agents, create a symbolic link before installing ITO. For example: if `/bigdisk` is a local file system with enough free space:

  ```
  mkdir -p /bigdisk/OV
  ln -s /bigdisk/OV /opt/OV
  ```

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

## Installation Tips for MPE/iX Managed Nodes

**NOTE** Interactive log on and log off UDCs are not supported by ITO. For this reason, logon and logoff UDCs must be disabled during both software installation and application starts using the vt3k connection.

- For software installation, disable the logon/logoff UDCs for `manager.sys`, `mrg.ovopc` and `agent.ovopc` if these are present.
- Always set LANG to C before starting the ITO agent software installation.
- Use ncktest.pub.hpncs to check IP addresses. For more information, see the section “RPC Daemon or Local Location Broker Problems and Solutions” on page 422.

  On MPE/iX 6.0 use NSLOOKUP.HPDCE.SYS to check IP addresses.
- On HP-UX 10.x management servers, ftp is used to install the MPE/iX agent.
- In its current release, ITO only supports 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 via Network Directory (NSDIR.NET.SYS) or Probe (and Probe Proxy) is not supported.

- If the lanconfig(1M) statement on the management server in /etc/netlinkrc does not have the ieee parameter, the commands vt3k(1) and dscopy(1) which are required for ITO software maintenance and application starts will not work.
- The logging group on MPE/iX (where the files opcmsglg (local message logfile), and opcerror reside), must belong to the account OVOPC; if it does not, ITO services cannot write or create files in that group. For more information, see the section "System Maintenance" on page 460.
- ITO agents run in the job, **OPCAGTJ,AGENT.OVOPC;** for this reason, the **HPJOBLIMIT** must probably be adapted to guarantee that all jobs, including ITO agents, can be started (as when not running ITO's intelligent agents).

  The ITO action agent also streams separate jobs for application startup and command broadcasting. Adapt the **HPJOBLIMIT** accordingly.
- The system boot file SYSSTART.PUB.SYS can be used to set up a normal user environment automatically when ITO is started. The contents of this file should include command parameters appropriate for your environment, such as:
  - standard limits for job sessions
  - spooler start commands
  - stream device identification
  - outfence priorities
  - event logging, and so on.

  A SYSSTART file can contain selected MPE/iX commands (and their parameters) that the system manager is allowed to execute. Note that networking commands are excluded and should be executed from a job that is streamed from SYSSTART, or from a logon UDC for OPERATOR.SYS.

- If the Add/Modify Node window has been used to select the **Automatic Update of System Resource Files** option for the managed node, SYSSTART.PUB.SYS is created or updated, (unless it already contains a pre-existing ITO entry). It contains the start sequence for the job *stream* OPCSTRTJ.BIN.OVOPC, used for starting the Local Location Broker (llbd) and the ITO agents. (*stream* refers to the standard **STREAM** commands, or to the node-specific *stream* utility configured in the administrator's GUI, using the Advanced Options window, accessed from the Add/Modify Node window.) Before ITO agents start up, the administrator must first ensure that the network services are running. For an example of this streamed job, see the file:

  ```
  /var/opt/OV/share/databases/OpC/mgd_node/\
  vendor/hps 900/mpe-ix/A.02.10/sysstrtj.
  ```

- You can set your own *stream* facility in order to improve security by avoiding hard-coded passwords. See the Node Advanced Options window, accessed from the Add/Modify Node or Node Defaults window. If you do this, there are no passwords placed in the ITO job files, and control over the job is given to your own *stream* facility. Alternatively, you may leave the ITO default. If you leave the default, passwords remain unencrypted and the file OPCSTRTJ.BIN.OVOPC contains the AGENT.OVOPC password.

- The job OPCSTRTJ.BIN.OVOPC for starting the Local Location Broker and ITO services requires that the network be up and running. If you have time constraints, increase the PAUSE value before starting the **llbd** in OPCSTRTJ.BIN.OVOPC.

- If you want to use a customer-defined job-stream facility, check the MPE/iX startup file SYSSTART.PUB.SYS before installation of ITO A.02.00/01 software. If there is an entry for ITO (the installation process checks for the keyword '**OperationsCenter**'), that entry won't be modified.

  You can modify the line that streams the ITO startup job OPCSTRTJ.BIN.OVOPC manually so that it won't be changed by later software installation.

  For example, change the line:

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

  to

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

where <my job-stream facility> for example, is Maestro's **mstream**.

If there is no entry for ITO in SYSSTART.PUB.SYS, the automatic software installation will insert an entry for ITO in SYSSTART.PUB.SYS where the major parts look like this:

```
comment   ...    OperationsCenter

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

- The executable library, SNMPXL.NET.SYS, must be available, and ITO must have execution rights; if not, the ITO Monitoring Agent will not operate.
- The **TIMEZONE** variable must be set to correct differences between the different time resources used by ITO's C-routines and MPE's intrinsics and commands; if not, messages and error and trace logfiles receive the wrong creation time stamp. This can cause problems when working with multiple management servers.

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

  **call: setvar TZ,"TIMEZONE"**

## Required MPE/iX Patches

- Patch MPEKXE5A must be installed on all MPE/iX 5.5 systems. This patch adds routines to the system SL.PUB.SYS that the console interceptor requires to operate. This patch may be incorporated into future MPE Power Patch releases.
- Patch MPEKXE5B must be installed on all MPE/iX 6.0 systems. This patch adds routines to the system SL.PUB.SYS that the console interceptor requires to operate. This patch may be incorporated into future MPE Power Patch releases.
- Patch ITOED07A must be installed on all MPE/iX 6.0 systems. This patch provides routines to the XL.PUB.SYS to allow the ITO agent to call various NCS routines. This patch may become unnecessary for future MPE agent versions.

# Installation Tips for NCR UNIX SVR4 Managed Nodes

- The system name `uname -s` must *not* be set to any of the names `AIX`, `Solaris`, `HP-UX`, `SCO`, `DYNIX/ptx`, `OSF/1`, `Digital UNIX`, `Reliant UNIX`, `SINIX`, `IRIX`, `Olivetti`, or `UnixWare`.
- If the Multi-User version of UNIX is installed, ITO can be installed only after networking package `WIN-TCP` from NCR UNIX SVR4 is first installed.
- If bad login attempts are to be monitored by ITO, file `/var/adm/loginlog` must first be manually created. By default, `loginlog` does not exist, so no logging is done. To enable logging, the log file must be created with read and write permission for the owner **root** and the group **sys**. After doing the above, you may configure the logfile template **Bad Logs (NCR UNIX SVR4)** for the node.
- The ITO agent software is installed on the `/opt` file tree. If the file system that hosts the `/opt` file tree is too small for the installation of ITO Agents, create a symbolic link before installing ITO. For example: if `/bigdisk` is a local file system with enough free space:

  ```
  mkdir -p /bigdisk/OV
  ln -s /bigdisk/OV /opt/OV
  ```

  In a cluster environment, you must check that `/bigdisk` 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.

## Manual NCR UNIX SVR4 Agent Installation

For instructions on how to manually install the NCR Agent, use the instructions in “Manual Solaris Agent Installation” on page 96. However, note that the location of the agent package `opc_pkg.Z` on the ITO management server for the NCR platform is:

```
/var/opt/OV/share/databases/OpC/mgd_node/vendor/ncr\
3000/unix/A.05.00/RPC_NCS/opc_pkg.Z
```

# Installation Tips for Novell NetWare Managed Nodes

The process for installing the ITO 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 NetWare-server-based. It can be separated into the following phases:

**ITO GUI phase**

- ❏ Adding the managed nodes to the `ITO Node Bank`
- ❏ Transferring the ITO agent package to the managed nodes

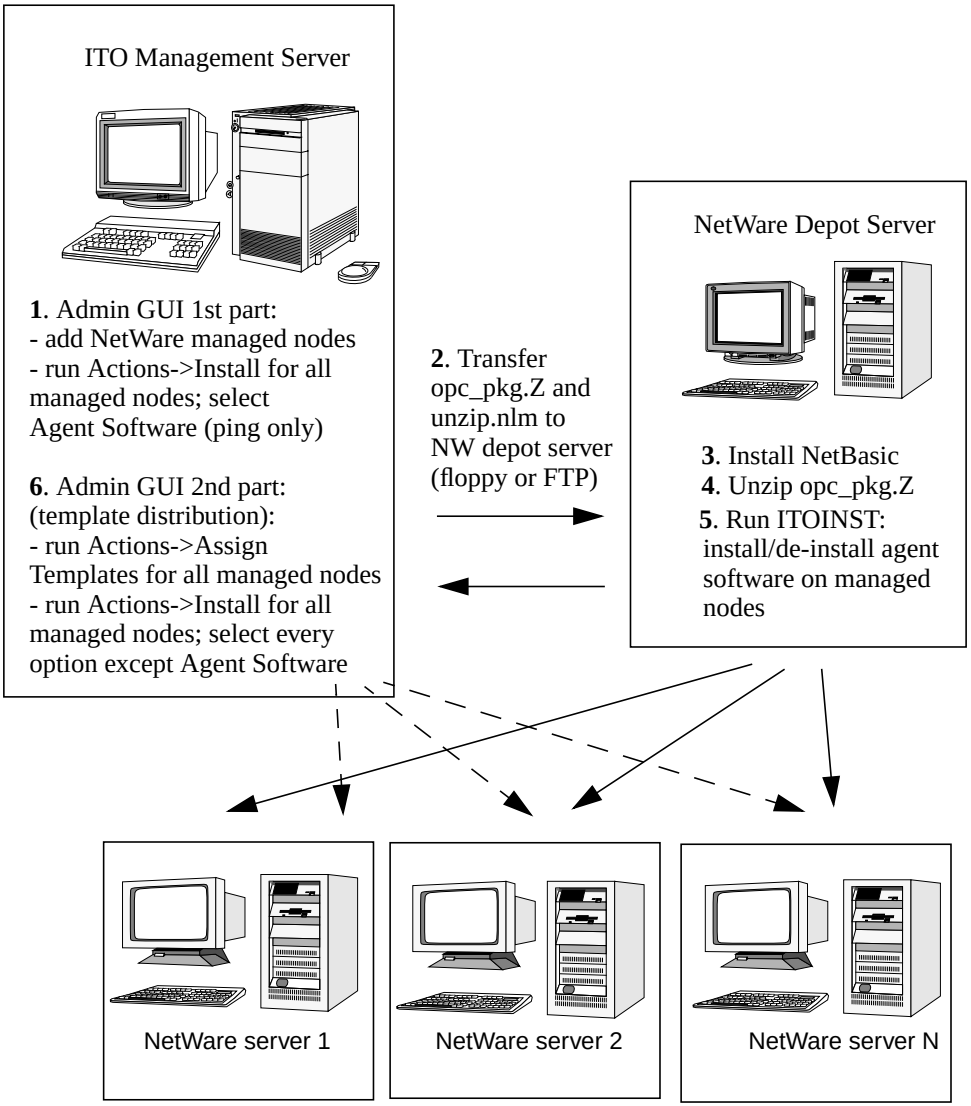
**NetWare Depot Server phase**

- ❏ Installing NetBasic on the NetWare depot server
- ❏ Unzipping the ITO agent package
- ❏ Installing the ITO agent software on the managed nodes
  - Installing the ITO agent software – ping only
  - Assigning and transferring templates to the managed nodes

Note that installing the ITO agent on Novell NetWare SFT III does not differ from the standard agent installation on Novell NetWare. Differences are noted in the following sections where they occur during the installation.

Figure 2-3 on page 76 shows all installation steps made on the ITO management server and on the Novell NetWare depot server. Note that the numbers in the installation steps correspond to numbers of the following instructions.

**Figure 2-3 Installing the ITO Novell NetWare Agent Package**




## The ITO GUI Phase

1. Ensure that the Novell NetWare nodes are known to ITO and are accessible:

a. Add your Novell NetWare managed nodes to the `ITO Node Bank`.

b. Open the `Install / Update ITO Software and Configuration` window, and add the Novell NetWare managed nodes where you want to install the ITO agent software. Select `[Agent Software]` and click on `[OK]`.

   This sends the `ping` command to the nodes.

   Note that 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 Novell NetWare agent software from the ITO management server to a temporary directory on the Novell NetWare Depot Server. The installation package is located in the following directory on the management server:

   ```
   /var/opt/OV/share/databases/OpC/mgd_node/vendor/\
   novell/intel/nw/A.05.00/RPC_SUN_TCP/opc_pkg.Z
   ```

   The above directory also contains the files `unzip.nlm` and `unzip.txt` which are used to unzip the `opc_pkg.Z` file on the NetWare depot server. Copy the files to the `sys:/system` directory on the NetWare depot server.

## The NetWare Depot Server Phase

The NetWare depot server is a NetWare server which installs the ITO agent software on other NetWare servers. It stores the ITO agent depot which contains the installation package `opc_pkg`. All ITO agents are installed from the depot server.

### Prerequisites of the NetWare Depot Server

The selection criteria for determining the depot server are as follows:

- The depot server must have NetWare connectivity to all NetWare servers where the ITO agent is to be installed. This means that each NetWare server must be accessible from the depot server by way of the IPX transport layer.
- IP connectivity must be established throughout the network. You can use NetWare `PING.NLM` to check that all NetWare servers are accessible from the depot server.

- It is recommended that the depot server runs ftp so that the ITO agent package can be easily transferred from the ITO management server to the depot server.
- NetBasic, from the HiTecSoft company, must be installed on the NetWare depot server. Note that the NetBasic components bundled with NetWare 4.11 are not sufficient because some .NLMs (such as `NETMODUL.NLM`) which are required for installation are missing.

  You do not need to install NetBasic if you already have at least the runtime version of NetBasic installed on the depot server. Issue the following command from the DOS workstation command prompt to check for the correct version:

  ```
  ndir f:\system\NetBasic.nlm /ver
  ```

  where f: is the drive letter mapped to SYS:/

  If the version you have is 6.00j – Build 4.127 or above you do *not* need to install NetBasic.

  You also need a Windows 95 or Windows NT version 4.0 system acting as a NetWare client to perform the NetBasic installation.

3. Install NetBasic on the NetWare depot server.

   a. NetBasic is located in the following directory on the ITO management server:

   ```
   /var/opt/OV/share/databases/OpC/mgd_node/vendor/\
   novell/intel/nw/A.05.00/RPC_SUN_TCP/nbv6.exe
   ```

   Alternatively, you can obtain NetBasic from the following address:

   ```
   ftp://ovweb.external.hp.com/pub/NetBasic/nbv6.exe
   ```

**NOTE** HP OpenView can change the location and/or name of the NetBasic installation file without notice.

   b. Run `NBV6.EXE` on the Windows 95 or Windows NT version 4.0, and follow the instructions provided during the NetBasic installation.

   c. Select a NetWare server as the depot server to which all `.NLM`s are copied.

   d. Enter the runtime license number 300-3193-40100022; it is part of the ITO agent for NetWare.

This number does not allow you to use the NetBasic Integrated Developer Environment. You can not develop or compile your own NetBasic script programs.

e. After all required NetBasic `.NLM`s have been successfully installed on the depot server, the Windows 95 or Windows NT 4.0 system is no longer needed.

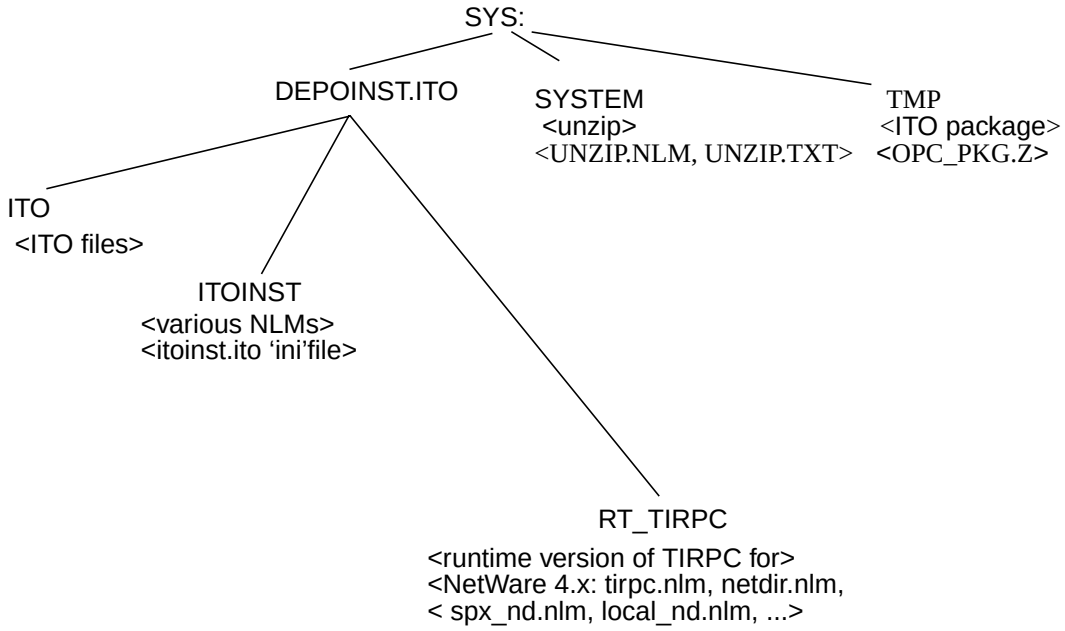
4. Unzip `opc_pkg.z`, enter:

   **`load unzip sys:/tmp/opc_pkg.Z`**

   Note that this assumes that `opc_pkg.Z` has been copied to the directory `sys:/tmp`.

   Figure 2-4 on page 79 shows the file tree layout of the directory `SYS:/ volume:` after `opc_pkg.Z` has been unzipped.

**Figure 2-4 File Tree Layout of the ITO NetWare Depot Server**



#### Prerequisites for Installing the ITO Agent Software

The ITO agent software can be installed using bindery mode or NetWare Directory Services (NDS). It is recommended to use NDS because bindery mode may become obsolete with future releases of Novell NetWare.

Before beginning with the installation, make sure that the following information is known and all requirements are met:

- ❏ name and IP address of the ITO management server
- ❏ names and IP addresses of the NetWare managed nodes

  If you use bindery mode:

  - `ADMIN` usernames and passwords of the NetWare managed nodes
  - `SET BINDERY CONTEXT =` `ou=<`*organizational_unit*`>.o=<`*organization*`>` must be present in `SYS:SYSTEM/AUTOEXEC.NCF` on each NetWare server. This is the default Novell setting.

  If you use NDS:

  - `ADMIN` login name and password for the directory tree
- ❏ the software described in "Software Requirements for Novell NetWare Managed Nodes" on page 37 is installed and running on each NetWare managed node.

5. Install the ITO agent software on the Novell NetWare managed nodes.

   Do not stop the ITO mangement server processes when installing the ITO agent software.

   a. On the depot server, execute the command `itoinst`.

      The following menu options are displayed:

      - `Install HP IT/Operations Agent for NetWare 4.x` installs the ITO agent.
      - `Deinstall HP IT/Operations Agent for NetWare 4.x` de-installs the ITO agent.
      - `View 'READ.ME' file` displays the content of `README.ITO` file from `SYS:/DEPOINST.ITO/ITOINST` directory.

- `Exit Installation` immediately exits the procedure.

b. Select the `Install HP IT/Operation Agent for NetWare 4.x` option and respond to the prompts.

c. Enter the name of the ITO management server.

d. Enter the IP address of the ITO management server.

e. Specify whether you want the name and IP address of the management server added to the `SYS:/ETC/HOSTS`.

f. Decide whether you want to use NDS or proceed in bindery mode.

If you answer **`No`**, the installation proceeds in bindery mode.

If you answer **`Yes`**, you are prompted to log into NDS. Enter the distinguished login name in the format:

**`.cn=admin.ou=<organizational_unit>.o=<organization>`**

For example: **`.cn=admin.ou=ITO.o=hp`**

The distinguished login name is made up of the full path from the root of the directory tree.

g. Schedule a shutdown of the NetWare servers to take place after the installation. This is optional.

If you have selected this option, the installation procedure asks for the date and time of the shutdown; the format of the date and time string is MM–DD–YYYY hh:mm:ss.

Note that you can choose to shut down NetWare SFT III servers. The systems will be shut down, but cannot be restarted automatically.

h. Log into NDS or bindery mode depending on what you have chosen above.

i. A list of all available NetWare servers is displayed; this list has the following additional options:

- `Select all NetWare servers`
- `Unselect all NetWare servers`

You can browse the list, select all, deselect all, or individually select some NetWare servers; the selected servers in the list are indicated by a checkmark.

Systems running Novell NetWare 3.x or Novell NetWare 5.x are also listed but cannot be selected. If a Novell NetWare 5.x file server is accidentally selected, the installation procedure reports the NetWare version as 3.x and does not allow selection. The NetWare depot server is listed; note that it can also be an ITO agent for the NetWare server.

Any NetWare SFT III systems are also on the list and can be selected in the same way as other Novell NetWare systems.

For each selected server the installation process does the following:

- If you are using bindery mode, the installation process asks for the password of the NetWare superuser `ADMIN`. The installation procedure tries to log in to the selected NetWare server. If the login is unsuccessful the installation procedure displays an error message, and proceeds to the next selected NetWare server.

  If you are using NDS, the superuser `ADMIN` is already logged in, and the installation proceeds with the following step.

- Checks that ITO agent processes are not running already.

  If `OPCAGT.NLM` is running on the selected NetWare server, currently active `ITO.NLM`s must be stopped manually on the NetWare server in order to (re-)install the ITO agent.

- Checks for `OPCINFO` file

  If the file exists, the ITO agent is already installed on this system. If the ITO management server name from the line `OPC_MGMT_SERVER` in the file `OPCINFO` differs from the ITO management server name entered above, an error reports that the previous ITO agent is connected to a different ITO management server. De-install the old ITO agent software and retry the installation.

- Checks for TCP/IP

  TCP/IP must be configured and running on the NetWare server; this is checked by scanning the list of active `.NLM` modules in NetWare server's memory. If there is no active `TCPIP.NLM`, `SYS:SYSTEM/AUTOEXEC.NCF` is checked for the string TCPIP so that TCPIP will be loaded with the next server

reboot. If the string is found you are notified that in order to run the ITO agent for the NetWare server, TCP/IP must be invoked.

If there is no such string the NetWare server may use the configurator, `INETCFG.NLM`, to set network parameters. Inspect the `AUTOEXEC.NCF` file for inclusion of the string `INITSYS` on a separate line to determine if this method is used.

If this is the case the file `SYS:ETC/NETINFO.CFG` is checked for the string TCPIP. If the string is found you are warned that in order to run ITO server, TCP/IP should be invoked and it is suggested that you also run `INETCFG.NLM`.

If the presence of TCPIP cannot be determined the procedure exits. The installation procedure does not try to invoke TCPIP because of its complexity and the problems that this may cause.

- Checks for TIRPC

  The ITO management server requires the TIRPC module. If the installation process does not find the module and it is not located in `SYS:SYSTEM`, a warning is displayed. You can safely ignore this warning message because the TIRPC module was already copied when unzipping the package.

- Checks for `XCONSOLE`

  The active modules list and the `AUTOEXEC.NCF` and/or `NETINFO.CFG` are scanned for `XCONSOLE`. `XCONSOLE` requires `REMOTE.NLM`. If the strings `REMOTE` and/or `XCONSOLE` do not exist in either of the two configuration files, the installation procedure updates `AUTOEXEC.NCF` by inserting the appropriate command(s) at the end of the file:

  either: `load remote <remote console password>`

  or: `load xconsole`

  or both.

  If the string `REMOTE` is not present, the installation procedure prompts you for the remote console password.

  On NetWare SFT III servers, the installation procedure cannot check whether `REMOTE.NLM` is running. If it isn't, you are not prompted for the remote console password. `XCONSOLE.NLM` is

also checked to make sure that it is running. If it isn't, all standard locations are checked for the `load xconsole` command. The configuration file of the primary IO Engine is not searched.

- Checks for NetWare Management Agent (NMA)

  The NMA agent is supported by the ITO agent for NetWare server but this functionality requires NMA to be installed on the selected NetWare servers; currently NMA installation is not provided as part of the ITO agent for NetWare server installation

- Checks for CLIB

  The `CLIB.NLM` version is checked; version 4.10 or higher is supported.

- Checks the disk space

- Checks the memory

  The installation procedure knows how much memory in KB is needed; this figure is subtracted from the NetWare server parameter cache buffers. If the calculated amount is more than 30% of NetWare parameter total server work memory the installation proceeds, otherwise the installation for the current NetWare server is aborted, and the next selected NetWare server is processed.

- Copies files

  If the source file is a `.NLM` file, the installation checks if `.NLM` already exists on the target NetWare system. If it does, the NetWare depot server is checked to see what version is available there. Later versions of `.NLM` are always copied from the NetWare depot server to the target. Older versions of `.NLM` are only copied to the target if you agreed to overwrite the `.NLM`. It is recommended to use the default option, that is; not to overwrite previous versions.

- Flags directories as 'purgable'

  Deleted files occupy space although Novell NetWare can re-use the space in a low disk quota situation. Deleted files can be completely removed with the command-line utility `PURGE`. If a directory is marked 'purgable' then each deleted file is no longer kept by Novell.

- Updates system configuration files

  The Installation procedure updates the `OPCINFO` file and writes the ITO start command (`OPCAGT.NCF`) to the `AUTOEXEC.NCF`. On NetWare SFT III systems, `OPCAGT.NCF` is added to `SYS:SYSTEM/MSAUTO.NCF`.

  The `SYS:/ETC/HOSTS` file is updated with the IP address of the ITO management server if you agreed to add the ITO management server to the `SYS:/ETC/HOSTS` file.

  The internet name and IP address of the target NetWare server that is currently processed are also required and must be entered now. Both are added to the `SYS:/ETC/HOSTS` file. If you are installing a NetWare SFT III managed node, enter the name and IP address of the MS Engine.

- Creates ITO Operator and Group

  The NetWare group OPCGRP is created, and the NetWare user OPC_OP is added to the OPCGRP group; OPC_OP has the same security level as the user ADMIN. All these actions are performed in bindery or NDS mode.

**CAUTION** Do not forget to manually change the password for the user OPC_OP.

j. When all selected servers have been processed a special `.NLM` is invoked at the depot server to perform a shutdown at the time you previously scheduled. The shutdown is only performed if no files are opened on the NetWare server. There is no forced shutdown.

6. Inform the management server that the agent software has been successfully installed on the new ITO managed nodes. Enter:

   **`/opt/OV/bin/OpC/opcsw -installed <`*`node_name`*`>`**

7. Assign your templates to the NetWare managed nodes and distribute the templates, actions, monitors, and commands. See the HP ITO Administrator's Guide to Online Information for more information about assigning and distributing templates.

## General Installation Notes for NetWare Nodes

❑ Each step of the installation is recorded in the logfile `SYS:DEPOINST.ITO/ITOINST`. If you encounter problems during the installation, check this logfile for warnings and errors, and retry the installation if necessary.

- NetWare Directory Services (NDS)

  If you use NDS to install the ITO agent software, the installation process creates the file `SYS:/OPT/OV/BIN/OPC/INSTALL/NDSINFO` on each managed node. This file contains information about the position of the managed node in the NDS directory tree so that the ITO agent .NLMs can log in to NDS when they are started. The ITO default operator opc_op is also inserted.

  If you use bindery mode `NDSINFO` is not created and the default context is used.

- Changed Configuration Files

  Each configuration file on the NetWare server that is changed by the ITO installation process (like `AUTOEXEC.NCF`) is stored in the same directory with the extension `.ITO`; this is in case you need to restore the old system.

- `SNMPLOG.NLM` and the ITO Event Interceptor

  The ITO event interceptor and Novell's `SNMPLOG.NLM` *cannot* be used together. If you experience problems with the ITO event interceptor check that `SNMPLOG.NLM` is not loaded. If you need `SNMPLOG.NLM` to report traps, disable the ITO event interceptor.

- Setting `/usr/adm/inetd.sec` on the Management Server

  The ITO agent monitors the connection from the NetWare server to ITO management server by sending the UDP echo packages. The UDP echo service must, therefore, be enabled on the ITO management server. Verify that the echo service is not disabled in the `/usr/adm/inetd.sec` file. Note that the echo service is enabled if it is not listed in the `inetd.sec` file.

- Using the ITO NetWare Integration Package

  Before installing the ITO Agent Package all users of the NetWare Integration package must either delete or rename the maps `NetWare Config`, `NetWare Tools` and `NetWare Performance`. These maps can be found in the `ITO Application Bank` window.

- If you use UDP protocol for agent-server communication, set the data array size to 2048 bytes or less, otherwise the communication fails for larger messages. To set the size of data array, use `OPC_RPC_ARRAY_SIZE` in `opcinfo` file. The default value for data array size when using the UDP protocol is 2048 bytes.

- Note that PATH cannot be changed during runtime on Novell NetWare managed nodes. All actions, montiors, and commands must be either fully qualified or must reside in PATH. PATH must be set before the ITO agents are started.
- Unsupported ITO Agent Functionality

  Due to specifics of the NetWare platform a subset of the ITO agent functionality is not supported or is implemented in a slightly different way.

  - The `opcmsg(1)` command and `opcmsg(3)` API are not implemented.
  - The `opcmon(1)` command is not implemented. The `opcmon(3)` API is implemented.
  - MSI on the managed node is not implemented.
  - The message interceptor is not implemented.
  - Only the regular level of security is implemented.
  - The subagent registration file `SYS:/VAR/OPT/OV/CONF/OPC/AGTREG` is not encrypted.
  - Tracing cannot be switched on/off during agent operation.
  - 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 ITO 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 ITO agent opens a separate virtual screen on NetWare server console when started. By selecting the options in the menu of the ITO agent screen the operator is able to start/stop the ITO agents and query the agents status.

    The following actions can be executed by the ITO agent service:

    `DISPLAY`: Prints status of ITO agents to the console

    `START`: Starts or re-initializes the other ITO Agent processes (equivalent to `opcagt -start`)

    `STOP`: Stops all ITO agent processes except for the message agent and the control agent functionality (equivalent to `opcagt -stop`)

`KILL`: Stops all ITO 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.

## Installation Tips for Olivetti UNIX Managed Nodes

- The ITO Agent software is installed on the /opt file tree. If the root file system is too small for the installation of ITO Agents, create a symbolic link before installing ITO. For example: if `/bigdisk` is a local file system with enough free space:

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

  **`ln -s /bigdisk/OV /opt/OV`**

  In a cluster environment, you must check that `/bigdisk` 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.

- Some of the logfiles checked by the logfile encapsulator are not, by default, present on Olivetti managed nodes, for example `/var/adm/messages`. It is important that all logfiles that are checked by the logfile encapsulator agent are present on the managed node. To add the logfile `/var/adm/messages` to the managed node, edit the `/etc/syslog.conf` file by adding the following lines:

  ```
  kern,mark.debug                 /var/adm/messages
  ```

  To create the /var/adm/messages file on the managed node, enter:

  **`touch /var/adm/messages`**

  Then restart the syslog daemon, see the manpage syslog(1m).

- Make sure that the entry root is not contained in the `/etc/ftpusers` file; Otherwise the installation of ITO agents to the managed nodes will fail.

# Installation Tips for OS/2 Managed Nodes

Both standard and manual agent installation are supported on OS/2 managed nodes.

## Standard OS/2 Agent Installation

- During the installation, the installation script checks that sufficient disk space is available on the disk entered in the `[Install Onto Drive]` field of the `Node Advanced Options` window in the ITO GUI. If there is not enough space available, or, if no disk drive was specified, the installation script selects the first disk with sufficient disk space and installs the agent software. The directories `\opt\OV` and `\var\opt\OV` are created for the agent software.

  `ftp` and `remsh` (rsh) services must be enabled. The installation requires the following setup:

  - On the management server, check `[Automatic (De-)Installation]` in the `Node Advanced Options` window; a username must be provided for the installation.
  - FTP must be enabled for the user who is installing the agent software, and `ftpd` must be running. FTP access can be configured in the TCP/IP Configuration notebook (Security tab), or by hand, by adding a new user in the `\MPTN\ETC\TRUSERS` file.
  - The user must be allowed to execute commands remotely from the management server via `remsh` without supplying a password. Access can be configured in TCP/IP Configuration notebook (Security tab, page 2), or by adding a user and host to `\MPTN\ETC\RHOSTS`. Also `rshd` must be started either as a separate process or by Inetd.

- If Domain Name Service (DNS) is not present on the managed node, it is necessary to add at least the management server and the managed node to the hosts file. This file is located in the directory to which the environment variable `ETC` is pointing. The variable ETC is set in `CONFIG.SYS`.

- The DCE daemon must be running before the ITO agents are started. On DCE 1.0.2, the DCE daemon process can be started through `RPCD.EXE`; `DCED.EXE` on DCE 2.x. If they are not running during the installation, a warning will be issued.

- ❑ Note that PATH cannot be changed during runtime on OS/2 managed nodes. All actions, montiors, and commands must be either fully qualified or must reside in PATH. PATH must be set before the ITO agents are started.

## Manual OS/2 Agent Installation

In some situations, it may be desirable to install the OS/2 agent software without using the management server. A *manual installation* prepares the system so that it is ready to become an ITO managed node when it is later connected to the network. This may be useful if many systems are prepared in a central location, or if you want to avoid the root connection over the network that is necessary for a standard agent installation.

Note that RPCD/DCED must be running if the ITO agent software is installed manually, so that the management server may be informed about a successful installation. If it is not running, a warning is displayed along with instructions concerning how to inform the management server manually.

1. Copy the following files from the management server to a temporary directory on the OS/2 managed node:

   - installation script `opcinst.cmd`

     ```
     /var/opt/OV/share/databases/OpC/mgd_node/vendor/\
     ibm/intel/os2/A.05.00/RPC_DCE_TCP/install/\
     opcinst.cmd
     ```

   - package `opc_pkg.z`

     ```
     /var/opt/OV/share/databases/OpC/mgd_node/vendor/\
     ibm/intel/os2/A.05.00/RPC_DCE_TCP/opc_pkg.z
     ```

     `opc_pkg.z` can be unpacked by running the OS/2 utility `unpack`.

2. Add the managed node to the `ITO Node Bank`.

   Note: if you do *not* do this step now, the installation script will issue a warning, and tell you how to notify the management server of the new managed node using the command `itonotfy.exe`.

3. Run the installation script `opcinst.cmd` in *one* of the following ways on the managed node:

   - using the command line options:

```
opcinst.cmd /TAPEDIR:<tape_dir>
/DRIVE:<install_drive>
/MGMT_SERVER:<management_server>
```

See Table 2-3 on page 91 for a list of available command line options or type **`opcinst.cmd /help`** for help.

- using a response file (a text file that contains default answers): **`opcinst.cmd <response_file>`**

  See Table 2-3 on page 91 for a list of available response file tokens. The following is an example of a typical response file:

```
INSTALLATION_TMP_DIR C:\TMP
OPC_INSTALLATION_DRIVE C:
MANAGEMENT_SERVER management.server.com
```

- interactively, by calling the `opcinst.cmd` command and responding directly to the prompts of the installation script:

  **`opcinst.cmd`**

**Table 2-3 Command Options for the OS/2 Agent Installation**

| Option | Response File Token | Possible Values | Value Type |
|---|---|---|---|
| /DRIVE: | OPC_INSTALLATION_DRIVE | | drive: |
| /INSTSIZE:[a] | N/A | any | bytes |
| /LOGDIR: | INSTALLATION_LOG_DIR | /var/opt/ov/log/opc (default) | [drive:]dir |
| /MGMT_SERVER: | MANAGEMENT_SERVER | | hostname |
| /MODE: | INSTALL_MODE | INSTALL (default)<br>REMOVE<br>CHECK<br>RCHECK | const |
| /REMOTE:[a] | N/A | N/A | N/A |
| /START: | OPC_START | YES<br>NO (default) | const |

| Option | Response File Token | Possible Values | Value Type |
|---|---|---|---|
| /UPDATE: | UPDATE_CONFIG | YES<br>NO (default) | const |
| /TAPEDIR: | INSTALLATION_TMP_DIR | any | drive:dir |
| /TAPESIZE:[a] | N/A | any | bytes |

a. Used for remote installation only.

## Installation Tips for Pyramid DataCenter/OSx Managed Nodes

- The ITO Agent software is installed on the `/opt` file tree. If the root file system is too small for the installation of ITO Agents, create a symbolic link before installing ITO. For example: if `/bigdisk` is a local file system with enough free space:

  ```
  mkdir -p /bigdisk/OV
  ln -s /bigdisk/OV /opt/OV
  ```

  In a cluster environment, you must check that `/bigdisk` 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.

- Some of the logfiles checked by the logfile encapsulator are not, by default, present on Pyramid managed nodes, for example `/var/adm/badlog`. It is important that all logfiles that are checked by the logfile encapsulator agent are present on the managed node. To add the logfile `/var/adm/badlog` to the managed node, edit the `/etc/syslog.conf` file by adding the following lines:

  ```
  auth.warning          /var/adm/badlog
  ```

  To add /var/adm/badlog file to the managed node, enter:

  ```
  touch /var/adm/badlog
  ```

  Then restart the syslog daemon, see the manpage syslog(1m).

- Make sure that the entry root is not contained in the `/etc/ftpusers` file; Otherwise the installation of ITO agents to the managed nodes will fail.

## Installation Tips for SCO OpenServer Managed Nodes

- The ITO agent software is installed on the `/opt` file tree. An empty `/opt` file tree is created during installation of the SCO OpenServer operating system. By default, this file tree is positioned on the root file system. If the root file system is too small for the installation of ITO agents, create a symbolic link before installing ITO. For example: if `/bigdisk` is a local file system with enough free space:

  ```
  mkdir -p /bigdisk/OV
  ln -s /bigdisk/OV /opt/OV
  ```

  In a cluster environment, you must check that `/bigdisk` 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.

## Installation Tips for SCO UnixWare Managed Nodes

- The ITO agent software is installed on the `/opt` file tree. If there is not enough space for the installation of the ITO agents, create a symbolic link before installing ITO. For example: `/bigdisk` is a local file system with enough free space:

  ```
  mkdir -p /bigdisk/OV
  ln -s /bigdisk/OV /opt/OV
  ```

  In cluster environment you must check that /bigdisk is also accessible from all cluster clients; that it is mounted from all client nodes also. For example, local file system /bigdisk on cluster client must be mounted to exported file system /bigdisk on cluster server.

- Some of the logfiles that are observed by the ITO logfile encapsulator are not present by default on UnixWare managed nodes, for example the logfile `/var/adm/messages`.

To add the logfile, edit the file `/etc/syslog.co` and add the following lines:

```
kern,mark.debug        /var/adm/messages
```

To activate your changes, enter:

```
touch /var/adm/messages
```

Then restart the syslog daemon, see the man page *syslog(1m)* for details.

- An entry for the user root must not be present in the file `/etc/ftpusers`. Otherwise the installation of ITO agents will fail.

## Installation Tips for SINIX Managed Nodes

- The ITO Agent software is installed on the `/opt` file tree. If the root file system is too small for the installation of ITO Agents, create a symbolic link before installing ITO. For example: if `/bigdisk` is a local file system with enough free space:

  ```
  mkdir -p /bigdisk/OV
  ln -s /bigdisk/OV /opt/OV
  ```

  In a cluster environment, you must check that `/bigdisk` 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.

- Some of the logfiles checked by the logfile encapsulator are not, by default, present on SINIX 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 ITO, 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.

- If you want to configure the Domain Name Server (DNS) on a SINIX managed node, in addition to editing the /etc/resolv.conf file, you will need to add the line: <nodename> (uname -n)

  to the following files:

  - /etc/net/ticlts/hosts
  - /etc/net/ticots/hosts
  - /etc/net/ticotsord/hosts

  If the <nodename> is not defined in these three files the ITO installation will fail because the opcnsl program will be unable to determine the management server.

### Manual SINIX Agent Installation

For instructions on how to manually install the SINIX agent, use the instructions in "Manual Solaris Agent Installation" on page 96. However, note that the location of the agent package opc_pkg.Z on the ITO Management Server for the SINIX platform is:

```
/var/opt/OV/share/databases/OpC/mgd_node/vendor/ncr\
3000/sinix/A.05.00/RPC_[NCS|DCE_TCP|DCE_UDP]/opc_pkg.Z
```

## Installation Tips for Solaris Managed Nodes

- Package SUNWaccu MUST be installed on the system if process table and CPU utilization are to be monitored by ITO. If this package is not installed, and monitoring templates proc_util and cpu_util are configured, warning messages will appear in the Message Browser stating that the corresponding shell scripts failed to execute.
- If bad login attempts are to be monitored by ITO, 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 log file 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.
- The ITO agent software is installed on the /opt file tree. If the file system that hosts the /opt file tree is too small to install ITO Agents, create a symbolic link before installing ITO.

  For example: if /bigdisk is a local file system with enough free space:

```
mkdir -p /bigdisk/OV
ln -s /bigdisk/OV /opt/OV
```

In a cluster environment, you must check that `/bigdisk` is also accessible from all cluster clients, and that it is also 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.

## Manual Solaris Agent Installation

In some situations, it may be desirable to install the Sun Solaris agent software without using the management server. Manual installation prepares the workstation to become an ITO managed node when it is later connected to the network. This is useful if many workstations 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.

#### Install the Agent on the Managed Node:

Use the following instructions to install the ITO Solaris agent on a Solaris workstation that will become an ITO managed node:

1. Copy the ITO appropriate agent package (NCS, DCE TCP/UDP) to a temporary directory on the managed node. On the management server, the agent packages are located in:

   ```
   /var/opt/OV/share/databases/OpC/mgd_node/vendor/sun/\
   sparc/solaris/A.05.00/RPC_[NCS|DCE_TCP|DCE_UDP]/\
   opc_pkg.Z
   ```

**NOTE**

If you intend to run ITO Advanced Network Security (ANS) on this node, you also need to copy the following file from the same directory:

```
nsp_pkg.Z
```

2. Uncompress and untar the agent package:

   ```
   uncompress opc_pkg.Z
   tar xvf opc_pkg
   ```

   If appropriate, uncompress and untar the ANS package, too:

   ```
   uncompress nsp_pkg.Z
   ```

```
tar xvf nsp_pkg
```

3. Install the agent on the node:

   ```
   pkgadd -d <directory> -a <directory>/OPC/install/admin \
   OPC
   ```

   If appropriate, install ANS on the node, too:

   ```
   pkgadd -d <directory> -a <directory>/OPC/install/admin \
   ITOAgentNSP
   ```

#### Activate the Node Using the Command Line:

You can activate the agent on the node over the net (without the GUI and without root access) by using the following command-line steps:

#### Activate the Node Using the ITO GUI:

After the node with the pre-installed agent is connected to the network, use this procedure to activate and register the managed node.

1. Add the pre-installed node(s) to the `ITO Node Bank` using the menu sequence: `Actions:Node->Add`.
2. Add the node to an ITO node group. The easiest way to do this is to drag and drop it onto a node group in the `ITO Node Group Bank window`.
3. Distribute the ITO configuration to the node:

   a. Select `Actions:Agents->Install` from the menu bar of the `ITO Node Bank`. The `Install /Update ITO Software and Configuration` window opens.

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

**NOTE**

Do not check `[Force Update]` otherwise 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. Note that if the agent software is *not* pre-installed, this action will install the agent.

4. Execute the following command to verify that the control, message, and action agents are all running on the managed node:

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

Activate the agent on the managed node:

1. After manually installing the agent on the node, enter:

   **`/opt/OV/bin/OpC/install/opcactivate <ITO_mgt_server>\ -cs <server_codeset> -cn <agent_codeset>`**

   The agent then attempts to send messages to the management server. For more information about codesets, see Chapter 8, "ITO Language Support," on page 333.

**NOTE**

Use the `opcactivate` command with the **`-mode`** option to activate:

| | |
|---|---|
| hacmp | for ITO agents on AIX HACMP systems. See also "Installation Prerequisites for AIX HACMP Agents" on page 58 |
| cluster server/client | for ITO agents on AIX Cluster-Client systems after the ITO agent software package has been installed on the AIX Cluster Server system. For more information, see "Manually Activating the ITO Agent on NFS Cluster Clients" on page 169. |

See the man page *opcactivate(1m)* for more information.

2. After the node is connected to the network execute the following two commands on the management server:

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

   b. **`/opt/OV/bin/OpC/opchbp -start <node>`**

## Problems Caused by Missing OS Patches for Solaris

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

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

To solve this problem, either:

- Install patch version -06 (or later).
- De-install the old patch.

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

```
showrev -p
```

## Installation Tips for Windows NT Systems

This section explains how to install the ITO agent package on Windows NT systems. There are four installation procedures that you can use depending on the network configuration as described in Table 2-4 on page 99:

**NOTE**

In this manual, a Windows NT **installation server** is a primary or backup domain controller with the ITO agent package installed.

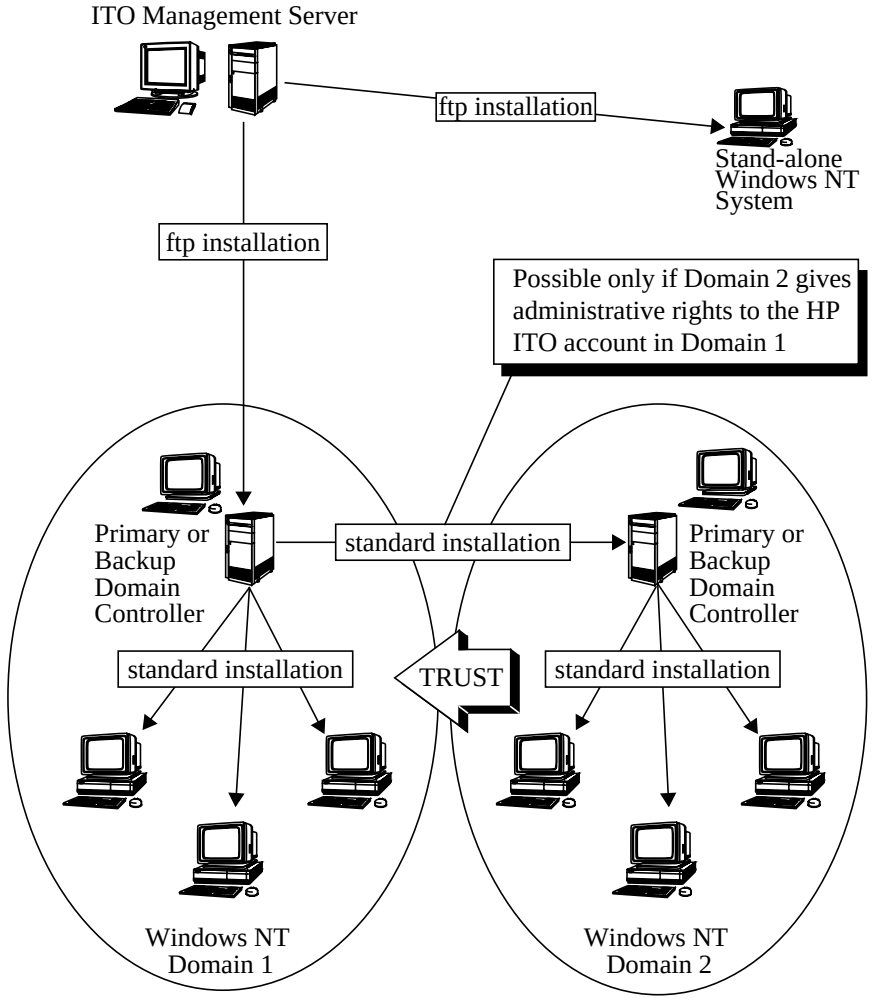
**Table 2-4 NT-Agent Installation Options**

| Use the... | described on... | to install or upgrade the NT agent package on... |
|---|---|---|
| ftp installation | page 103 | • a primary or backup domain controller<br>• a primary or backup domain controller that does not give administrative rights[a] to the HP ITO account on an installation server in another domain<br>• a stand-alone system |
| standard installation | page 106 | • a system that has an installation server in its domain<br>• a system in a domain that gives administrative rights[a] to the HP ITO account on an installation server in another domain |

| Use the... | described on... | to install or upgrade the NT agent package on... |
|---|---|---|
| ftp re-installation | page 109 | • a primary or backup domain controller for the second time<br>• a primary or backup domain controller that does not give administrative rights to the HP ITO account of a domain with an installation server<br>• a stand alone system |
| manual installation | page 111 | • an NT system that is not yet connected to the network.<br>• an NT system that is connected to a network where an ftp connection with write permission is either impossible or inadvisable |

a. A standard installation procedure requires the HP ITO account on the installation server in a **trusted** domain to have administrative rights in the **trusting** domain. Trust refers to a relationship between Windows NT domains, in which one domain is aware of the users in another domain, and can assign rights to those users. The trust relationship is established by using the **User Manager for Domains**, on the primary domain controller of the trusted and trusting domains.

**Figure 2-5 Installing the ITO Windows NT Agent Package**




## Installation Requirements

❑ Requirements for all Windows NT nodes

- Ten MB of space must be free on an NTFS-formatted local disk that is available to the node.
- Ten MB free disk space must be temporarily available on local `C:` drive during installation via the installation server.

- Schedule services must not be disabled.
- SNMP services must be running for ITO to automatically identify the node as an NT system. This is helpful, but not absolutely necessary for a successful installation.

❑ Requirements for a Windows NT Installation Server

- All Windows NT node requirements as listed above.
- Additional four MB of space must be free on an NTFS-formatted local disk that is available to the node.
- Ten MB free disk space must be temporarily available on the drive that contains the ftp directory during installation.
- An installation server must be a primary domain controller or a backup domain controller.
- ftp services must be running on the primary or backup domain controller if the agent package is being installed from the ITO management server (this will always be true for the first installation).
- The ftp service must have read/write permission for drive that contains the ftp home directory.

❑ Requirements for the ITO Management Server

- The ITO management server must be installed with the client software bundle OVOPC-NT-CLT. You can verify that the bundle has been installed with the command:

  **`swlist -l fileset OVOPC-CLT.OVOPC-NT-CLT`**

- If your installation includes 35 or less NT managed nodes, use the setting for the kernel parameter maxfiles given in the *HP OpenView IT/Operations Installation Guide for the Management Server*. If your installation includes more than 35 NT managed nodes, increase the setting of maxfiles by:

  3*Number_of_additional_NT_nodes + 15

## ftp Agent Package Installation

This procedure uses ftp to install the agent package from the ITO management server to a Windows NT primary or backup domain controller that does not currently have the agent running. This type of installation must be done at least once; it requires ftp services and one manual step on the NT system.

Use these instructions for your first Windows NT 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.

If an installation server is already available, and you want to install ITO agent software on additional Windows NT nodes, see "Standard Agent Package Installation" on page 106.

1. Check the "Installation Requirements" on page 101. Make sure that your systems meet all the listed requirements.
2. Select `Window: Node Bank` from any submap to display the `ITO Node Bank` window.
3. Select `Actions: Node: Add...` to display the `Add Node` window.
4. Fill in the following fields of the `Add Node` window:
   - `Label`: enter the name of the node as it will appear in the ITO Node bank. In this example **`ntserver`** is used.
   - `Hostname`: enter the complete hostname of the Windows NT domain controller that you want to set up as the Windows NT installation server. This example will use the hostname: **`ntserver.com`**. After entering this name and pressing return, ITO will look up and verify the IP Address, as well as the Net Type, Machine Type and OS name. Look at this information to ensure that the OS name is Windows NT.
   - `As User`: This can be the administrator, or even anonymous if the ftp server allows it

**NOTE** If SNMP services are not running on the Windows NT node, ITO cannot detect the OS name, Net type, etc. In this case, select Windows NT and continue with the installation.

5. Click `[Advanced Options]` to display the `Node Advanced Options` window; the fields below are unique to Windows NT nodes:

- `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, ITO will search the available local drives for an NTFS drive that has enough free space.
- `Installation Server`: leave this field blank. An installation server is not available for this domain (you are creating one with this procedure), and any entry here will create an error message when the installation script runs.
- If Service Pack 1 or 2 is installed on your Windows NT version 3.51 or 4.0 managed node, change the communication type from `DCE RPC (UDP)` to `DCE RPC (TCP)`.

6. Click `[Close]` to dismiss the `Advanced Options` window, then `[OK]` to dismiss the `Modify Node` window.

   The `ITO Node Bank` window now shows a new symbol with the label you entered in the `Label` field, in this example **`ntserver`**.

7. Add the new node to a node group so that it can be managed by an ITO operator:

   a. Open the `ITO Node Group Bank` window and 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 ITO default node groups. Remember to assign any new node groups to an operator.

   b. Drag the node from the `ITO Node Bank` window and drop it into the submap of the node group.

8. You can monitor the rest of the installation by looking at messages received in the message browser. If you added a new group, configure the message browser to receive messages from this new group. If the message browser is open, it will prompt you for a restart when you finish the step above. If it is not open, add the new node group and open the message browser now.

9. Click the new icon to highlight it, then choose `Actions: Agents: Install/ Update SW & Config...` to display the `Install/Update ITO Software and Configuration` window.

10. Under `Target Nodes`, Select `Nodes in list requiring update`, then click `[Get Map Selection]`; the node name will appear in the window.
11. Under components, select `[Agent Software]`, then click `[OK]`.

    The installation will begin. A new shell will open and start the installation script. When prompted for the "as user" password, give the password of the NT system administrator. When prompted for the HP_ITO password you can either specify a password, or simply press **Enter** and ITO will create a password for you.

**NOTE** If you are installing the ITO agent software on a **domain controller**, do not let ITO create a password for you, but specify your own. You will need this password again when installing on another domain controller.

    The installation script will then install the agent package on the NT node.

**NOTE** The agent can also be installed via anonymous ftp if you have read/write access to the ftp home directory drive. Use user **ftp** and password **ftp**

**NOTE** The next five steps must be performed on the NT machine. If the NT system is not physically near you, you can ask someone near the machine to perform these steps.

12. At the NT machine, log in as the administrator and open a MS-DOS command prompt.
13. Switch to the ftp home directory and drive
14. Change directory to `temp`.
15. Type **`opc_inst`**. This invokes a script that takes about two minutes to execute. The script will set up the domain controller as the Windows NT managed node that can also function as the installation server for all other NT nodes.
16. The installation is complete when you see the line `Installation program successfully finished`. If the installation fails, check the contents of the installation log file, located in `C:\temp\inst.log`. Examine the log file for lines that begin with `E->` to find the cause of the terminated installation.

You can also verify the installation by checking the NT services window and looking for the entry **HP ITO Agent**, which should be running, and the **HP ITO installation service**, which will not be running. (This service runs only when you want to install the agent on another NT system.)

**NOTE** The next steps must be performed at the ITO management server.

17. At the ITO management server, verify that the agent is running on the NT node by highlighting the node icon and double-clicking on the `ITO Status` application (in the `ITO Application Bank` window).

    This application returns the status of the ITO agent processes. If they are running, you know that the NT agent is installed and that the NT domain controller is functioning as the NT installation server.

## Standard Agent Package Installation

This procedure uses a Windows NT installation server to install or upgrade the agent package on Windows NT systems. To use this procedure, a Windows NT installation server must be available either:

- ❏ in the domain of the system you are installing, or
- ❏ in some other domain where the HP ITO account has administrative rights on the system where you want to install the agent.

**NOTE** Ensure that the latest version of the ITO agent software is installed on the installation server. See “ftp Agent Package Installation” on page 103 for instructions on how to prepare the installation server.

If an installation server that meets these requirements is not available, create one by using the procedure explained in “ftp Agent Package Installation” on page 103.

This type of installation does not require ftp services, and can be performed on any NT system within the installation server's domain. This procedure can also be performed on the primary or backup domain controller of any domain that grants administrative rights to the HP ITO account of another installation server, and can thus be used to create other installation servers in other domains.

**NOTE** Although an installation server *can* install the agent package on workstations in other domains, it is recommended to install the agent package on workstations *only* from the installation server in that

workstation's domain. This is recommended because the process of creating an installation server automatically installs the HP ITO account on the domain controller, where it will have the necessary rights throughout the domain. (If the HP ITO account does not have administrative rights throughout the domain, you will have to manually assign them on each workstation where you install the agent.) For more information on rights and permissions for the HP ITO account, see "The HP ITO Account" on page 114.

1. Check the "Installation Requirements" on page 101. Make sure that your systems meet all the listed requirements.
2. Select `Window: Node Bank` from any submap to display the `ITO Node Bank` window.
3. Select `Actions: Node->Add...` to display the `Add Node` window.
4. Fill in the following fields of the `Add Node` window:
   - `Label`: enter the name of the node as it will appear in the `ITO Node Bank`. In this example **`ntworkstation`** is used.
   - `Hostname`: enter the complete hostname of the Windows NT system where you want to install the agent. This example will use the hostname: **`ntworkstation.com`**. After entering this name and pressing return, ITO will look up and verify the IP Address, as well as the Net Type, Machine Type and OS name. Look at this information to ensure that the OS name is Windows NT.

**NOTE** If SNMP services are not running on the Windows NT node, ITO cannot detect the OS name, Net type, etc. In this case, select Windows NT and continue with the installation.

5. Click `[Advanced Options]` to display the `Node Advanced Options` window and 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, ITO will search the available drives for an NTFS drive that has enough free space.

- `Installation Server`: enter the name of a Windows NT 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). This example uses the system **`ntserver.com`**.
- If Service Pack 1 or 2 is installed on your Windows NT version 3.51 or 4.0 managed node, change the communication type from `DCE RPC (UDP)` to `DCE RPC (TCP)`.

6. Click `[Close]` to dismiss the `Advanced Options` window, then `[OK]` in the `Add Node` window.
7. Add the new node to a node group so that it can be managed by an ITO operator:

   a. Open the `ITO Node Group Bank` window and 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 ITO default node groups. Remember to assign any new node groups to an operator.

   b. Drag the node from the `ITO Node Bank` window and drop it into the submap of the node group.
8. You can monitor the rest of the installation by looking at messages received in the message browser. If you added a new group, configure the message browser to receive messages from this new group. If the message browser is open, it will prompt you for a restart when you finish the step above. If it is not open, add the new node group and open the message browser now.
9. Click the new icon to highlight it, then choose `Actions:Agents->Install/ Update SW & Config...` to display the `Install/Update ITO Software and Configuration` window.
10. Under `Target Nodes`, select `[Nodes in list requiring update]`, then click `[Get Map Selection]`, the node name will appear in the window.
11. Under components, select `[Agent Software]`, then click `[OK]`.

    The installation will begin. A new shell will open and start the installation script. When prompted for the HP_ITO password you can either specify a password, or simply press **Enter** and ITO will create a password for you.

**NOTE**

If you are installing the ITO agent software on a **domain controller**, do not let ITO create a password for you, but specify your own. 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 will then install the agent package on the NT workstation.

12. Verify that the agent is running on the NT node by highlighting the node icon and double-clicking on the `ITO Status` application (in the `ITO Application Bank` Window). This application returns the status of the ITO agent processes. If they are running, you know that the NT agent is installed and that the NT domain controller is functioning as the NT installation server.

    If you wish to examine the installation log, use the ITO `Install Log` application in the ITO `Application Group: NT Tools` Window.

## ftp Agent Package Re-installation

This procedure uses a Windows NT installation server to re-install or upgrade the agent package that were originally installed on Windows NT systems using the ftp-installation method.

**NOTE**

If the installation program aborts during the (re)installation of a new version of the Windows NT agent, check that there are no monitor scripts running on the managed node. Monitor scripts that are not stopped during the agent shutdown and which are still running during the subsequent install process can lead to a situation where the message catalog is locked, which causes any subsequent installation to fail.

Use the following instructions to re-install or upgrade the agent package on the first Windows NT primary or backup domain controller. You can also use these instructions if you need to 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.

If an installation server is already available, and you want to re-install or upgrade ITO agent software on additional Windows NT nodes, see "Standard Agent Package Installation" on page 106.

1. Check the "Installation Requirements" on page 101. Make sure that your systems meet all the listed requirements.
2. Select `Window:NodeBank` from any sub-map to display the `ITO Node Bank` window.
3. Select `Actions:Node:Modify…` to display the `Modify Node` window.
4. Click `[Advanced Options]` to display the `Node Advanced Options` window; the fields below are unique to Windows NT nodes:
   - `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, ITO will search the available local drives for a disk that has enough free space.

     If you are re-installing the ITO agent software, enter the letter of the NTFS drive where the agent software was installed.

**NOTE** If you want to re-install on a different NTFS drive, de-install the ITO agent software first, and then proceed with the ftp installation.

   - `Installation Server`: enter the complete hostname of the Windows NT system where you want to install the agent. This example will use the hostname: **`ntsystem.com`**.
   - If Service Pack 1 or 2 is installed on your Windows NT version 3.51 or 4.0 managed node, change the communication type from `DCE RPC (UDP)` to `DCE RPC (TCP)`.
5. Click `[Close]` to dismiss the `Advanced Options` window, then `[OK]` to dismiss the `Modify Node` window.
6. Click the new icon to highlight it, then choose `Actions:Agents->Install/ Update SW & Config…` to display the `Install/Update ITO Software and Configuration` window.
7. Under `Target Nodes`, select `[Nodes in list requiring update]`, then click `[Get Map Selection]`; the node name will appear in the window.

8. Under components, select [`Agent Software`], then click [`OK`].

   The installation will begin. A new shell will open and start the installation script. When prompted for the Administrator password, give the password of the NT system administrator. When prompted for the HP_ITO password you can either specify a password, or simply press **Enter** and ITO will create a password for you.

**NOTE**

If you are installing the ITO agent software on a **domain controller**, do not let ITO create a password for you, but specify your own. You will need this password again when installing on another domain controller.

   The installation script will then install the agent package on the NT node. You will not receive any installation messages in the message browser until the installation is complete.

9. Verify that the agent is running on the NT node by highlighting the node icon and double-clicking the ITO `Status` application (in the `ITO Application Bank` Window).

   This application returns the status of the ITO agent processes. If they are running, you know that the NT agent is installed and that the NT domain controller is functioning as the NT installation server.

   If you wish to examine the installation log, use the `ITO Install Log` application (in the `ITO Application Group: NT Tools` Window).

## Manual Installation: Windows NT Agent

In some situations, it may be desirable to install the ITO NT agent software on an NT PC without using the management server. This *pre-installation* makes it possible to prepare the PC, so that it is ready to become an ITO managed node when it is later connected to the network. This 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.

**NOTE**

If you are using this section to install the DEC Alpha NT agent, all references to `intel` in the path name should be replaced with `alpha`. For example:

`/ms/`*`intel`*`/nt` should be changed to;`/ms/`*`alpha`*`/nt`

To install the NT agent on an NT PC that will become an ITO managed node:

1. Copy the files listed below from:

   `/var/opt/OV/share/databases/OpC/mgd_node/vendor/ms/\`
   `[intel | alpha]/nt/A.05.00/RPC_DCE_TCP/`

   on the ITO management server, to the `C:\temp` directory of the managed node:

   - `opc_pkg.Z` *(rename this file to* `opc_pkg.zip`*)*
   - `opc_pre.bat`
   - `unzip.exe`
   - `unzip.txt`
   - `opcsetup.inf`
   - `opc_inst.bat`
   - `nsp_pkg.Z` (Only for nodes with ITO Advanced Network Security (ANS) installed. Note that you wil have to rename this file manually to `nsp_pkg.zip` ).

   Always use `RPC_DCE_TCP` as communication type, if Service Pack 1 or 2 is installed on your Windows NT version 3.51 or 4.0 managed node. Using `RPC_DCE_UDP` may cause problems with the operating system.

2. Edit the `opcsetup.inf` file, changing the entries for `setup drive` and `management server` as appropriate:

```
[Setup Drive]
 C:
[Management Server]
 management_server.domain.com
[Account Password]
(empty by default)
[HP ITO Version]
 A.05.00
[Agent Architecture]
ms/intel/nt[1]
```

1. [intel | alpha] as appropriate

**NOTE**

If the password line is left in its default state (empty) a random password is generated. If you want to use a specific password, it needs to be encrypted on the ITO management server with the `opcpwcrpt` tool, which resides in `/opt/OV/bin/OpC/install`.

If you are installing the ITO agent software on a **domain controller**, do not let ITO create a password for you, but specify your own. You will need this password again when installing on another domain controller.

3. Create the following file in the `C:\temp` directory of the NT managed node:

   - File: `nodeinfo`

```
OPC_NODE_TYPE CONTROLLED
OPC_MGMTSV_CHARSET iso88591 (or sjis for Japanese)
OPC_NODE_CHARSET acp1252 (or acp932 for Japanese)
OPC_COMM_TYPE RPC_DCE_TCP
OPC_NSP_TYPE [NONE | SECRET][1] (for ANS only)
OPC_NSP_VERSION 0 (for ANS only)
```

**NOTE**

If the ITO agent version A.04.x or lower is already installed on the managed node, run the following commands to stop the ITO agent on the node and remove the *old* `nodeinfo` file, which is incompatible with ITO A.05.00 agent, before you continue with the re-installation:

a. **`\usr\OV\bin\OpC\[intel | alpha]\opcagt -kill`**

b. **`del \usr\OV\conf\OpC\<node>\nodeinfo`**

4. Run the setup batch file on the NT PC from a command prompt:

   **`C:`**

   **`cd \temp`**

   **`opc_pre.bat`**

5. On the management server, add the NT node to the appropriate node group.

6. When the NT PC is connected to the ITO management server, update the database and start heartbeat polling for the NT node manually, from the management server, as follows:

1. One or the other depending on your ANS setting requirements

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

b. **`/opt/OV/bin/OpC/opchbp -start <node>`**

## The HP ITO Account

The standard installation of the ITO agent package on a Windows NT managed node installs the HP ITO account by default as a member of the `administrators` group and consequently gives the account all those user rights that are available under Windows NT. Although it is essential that the HP ITO account be a member of the `administrators` group, only those user rights listed in Table 2-5 on page 114 are required by the account to function correctly. All other user rights associated by default with the HP ITO account may be removed or granted as required.

**Table 2-5 Required User Rights for the HP ITO Account**

| User Right... | is required in ITO... |
|---|---|
| Access this computer from the network | by the NT installation server |
| Act as part of the operating system | by the `ITO action agent` to switch user |
| Log on as a service | by the ITO 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 |

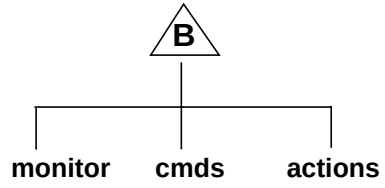
# 3 File Tree Layouts on the Managed-Node Platforms

This chapter provides file trees to show the directory structures on all Managed Node platforms supported by ITO. These are as follows:

- AIX
- DEC Alpha NT
- Digital UNIX (OSF/1)
- HP-UX 10.x/11.x
- MPE/iX
- NCR UNIX SVR4
- Novell NetWare
- Olivetti UNIX
- OS/2
- Pyramid DataCenter/OSx
- SCO OpenServer/UnixWare
- Sequent DYNIX/ptx
- Siemens Nixdorf SINIX/Reliant UNIX
- SGI IRIX
- Solaris
- Windows NT

The diagrams showing the file-tree layouts of the various operating systems in this section use the symbol B to represent the directory structure indicated in the following diagram:

**Key:**




For each platform, information is provided about the:

- ITO default operator
- system resources that are automatically adapted by ITO

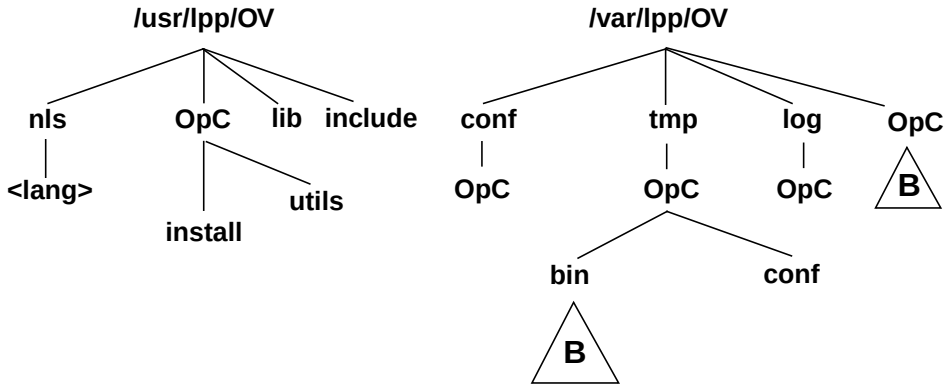
- NFS cluster clients and server systems, where appropriate

For detailed information about the directory contents, see the *opc(5)* page. Note that all man pages reside on the management server.

# File Tree Layout on AIX Managed Nodes

The ITO Software on AIX managed nodes is organized in the following way:

**Figure 3-1 ITO Software on AIX Managed Nodes**




`/usr/lpp/OPC` and `/lpp/OpC` are used by the **installp** utility for software maintenance

## Standalone System or NFS Cluster Server on AIX

The cluster server exports the `/usr` file system with read-only permissions. The ITO software is located in `/usr/lpp/OV` with the same logical and physical path names. This is a different location from previous releases (`/export/lpp/OV/rs6000/aix`). This simplification was possible because ITO software can now operate from the read-only `/usr` file system on cluster clients.

## NFS Cluster Client on AIX

AIX cluster clients (both diskless, dataless, and diskpoor) are those AIX systems that have `/usr` file system NFS mounted. Their cluster server is the system to which `/usr` is mounted. No additional mounts are required on cluster clients on AIX by ITO version A.02.00 and later.

## ITO Default Operator on AIX

The ITO default operator, **opc_op**, owns `/home/opc_op` as home directory. By default, the operator uses the Korn Shell (`/bin/ksh`) and is not allowed to log into the system directly (* entry in `/etc/passwd`).

## System Resources Adapted by ITO on AIX

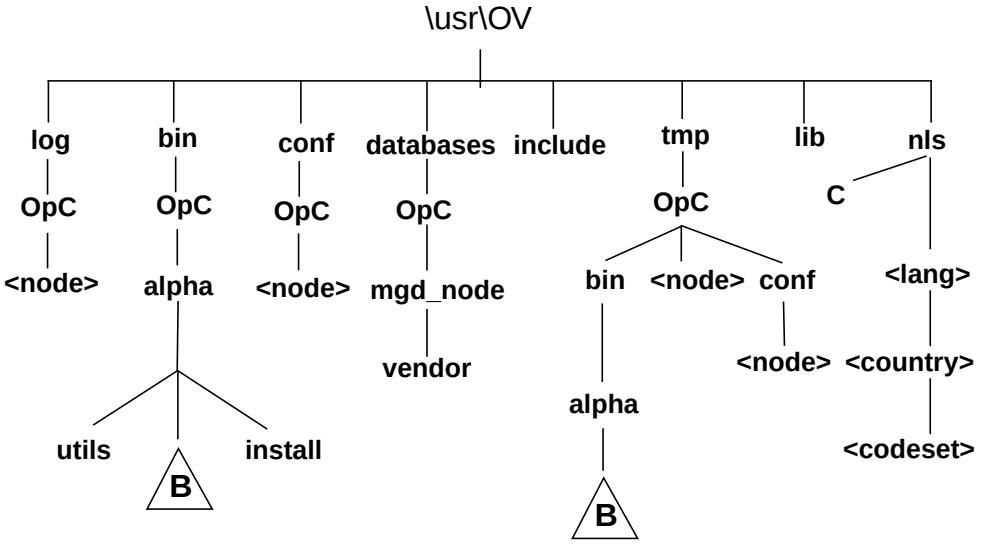
ITO applies changes in the following system resource files:

- `/etc/passwd` and `/etc/security/passwd` - entry for ITO default operator
- `/etc/group` and `/etc/security/group` - group entry for ITO default operator
- `/etc/inittab` - ITO Agent startup entry; only done, if the **Automatic Update of System Resource Files** option has been set
- `/etc/rc.opc` - ITO startup file; called by `/etc/inittab`

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

# File Tree Layout on DEC Alpha NT Manged Nodes

**Figure 3-2** **ITO Software on DEC Alpha NT Managed Nodes**




## ITO Default Operator on DEC Alpha NT Managed Nodes

Information concerning default ITO operators for DEC Alpha NT is the same as the information concerning default ITO operators for Windows NT on intel and is described in “ITO Default Operator on Windows NT” on page 161.

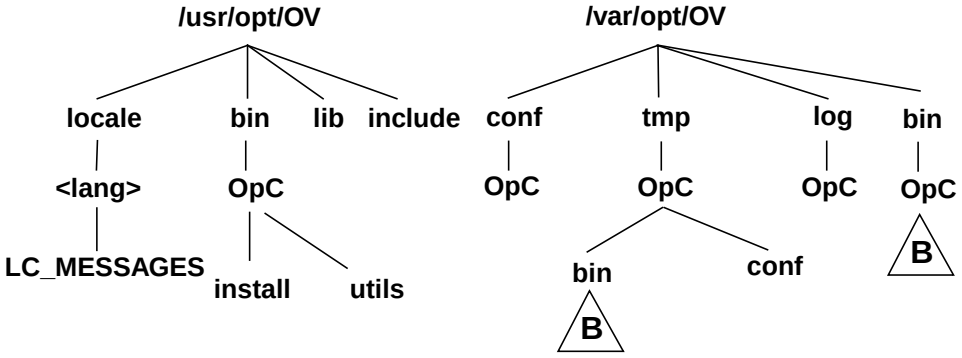
## System Resources Adapted by ITO on DEC Alpha NT Managed Nodes

Information concerning adapted system resources for DEC Alpha NT is the same as the information concerning adapted system resources for Windows NT on intel and is described in “System Resources Adapted by ITO on Windows NT” on page 161.

# File Tree Layout on Digital UNIX Managed Nodes

The ITO software on Digital UNIX managed nodes is arranged as follows:

**Figure 3-3 ITO Software on Digital UNIX Managed Nodes**




## Standalone Systems or NFS Cluster Servers on Digital UNIX

In general, standalone systems are treated as cluster servers.

The cluster server exports the `/usr/opt` or `/usr` file system with read-only permissions. ITO software is located on the `/usr/opt/OV` path, with the logical path name the same as the physical path-name.

**NOTE**

By default, Digital UNIX does not export the `/usr/opt` or the `/usr` file system. You can enable ITO cluster operations manually by exporting the `/usr/opt` or `/usr` file system to one Digital UNIX system, and then mount it from other Digital UNIX systems. You must set up the cluster manually before the ITO installation process, so that it is available for the ITO installation.

## NFS Clients on Digital UNIX

Digital UNIX cluster clients are those Digital UNIX systems that have the `/usr/opt` or `/usr` file system NFS mounted. Their cluster server is the system to which `/usr/opt` or `/usr` is mounted and must also be a system running Digital UNIX.

## The ITO Default Operator on Digital UNIX

The ITO default operator **opc_op** and the group **opcgrp** are created as the ITO default operator if they don't already exist.

**Table 3-1 ITO Entry in /etc/passwd on Digital UNIX Managed Nodes**

| Field | Entry |
|---|---|
| **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** | ITO default operator |
| **Home Directory** | `/usr/users/opc_op` |
| **Login Shell** | `/bin/sh` |

**Table 3-2 ITO Entry in /etc/group on Digital UNIX Managed Nodes**

| Field | Entry |
|---|---|
| **Group Name** | opcgrp |
| **Encrypted Password** | empty |
| **Group-ID** | 77 or higher |
| **Users** | opc_op |
| **Description** | ITO default operator group |

## System Resources Adapted by ITO on Digital UNIX

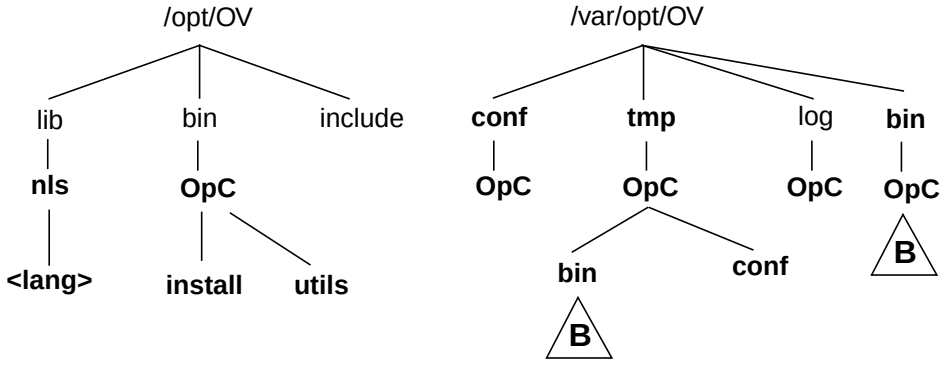
ITO makes changes in the following system resource files during installation:

- `/etc/passwd` and `/etc/shadow` (if present), Protected Password Database (if present) - entry for the default ITO operator
- `/etc/group` - group entry for the default ITO operator
- `/sbin/init.d/opcagt` - ITO startup/shutdown script
- `/sbin/rc0.d` - file K01opcagt created
- `/sbin/rc2.d` - file K01opcagt created
- `/sbin/rc3.d` - file S97opcagt created

# File Tree Layout on HP-UX 10.x and 11.x Managed Nodes

The ITO software on HP-UX 10.x and 11.x managed nodes is organized in the following way:

**Figure 3-4** **ITO Software on HP-UX 10.x and 11.x Managed Nodes**




If HP OpenView NNM is also installed on the managed node, only those directories displayed in **bold-face** type are created by ITO.

On the management server (which also acts as a managed node) the software trees shown above is combined with the management server file tree at installation. For a diagram of the management server file tree, see the *HP OpenView IT/Operations Installation Guide for the Management Server*.

## NFS Cluster Servers on HP-UX 10.x

In an NFS diskless environment, each cluster client has its own **private root directory** containing files and directories that are private to that client. The cluster client can access its operating system components on the cluster server using direct NFS mounts to the shared root directory.

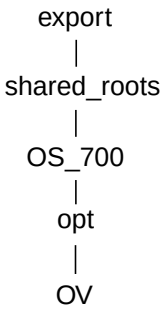
**NOTE** NFS diskless clusters are not supported on HP-UX 11.x

The file system on the NFS cluster server consists of a private root directory, and one or more **shared root directories** that are used by the cluster clients. Each of the shared roots contains the part of the operating system that can be shared by the cluster clients.

The cluster server exports the file system shown in Figure 3-5 to the cluster clients.

**NOTE** You can configure cluster clients for HP-UX 10.01 and above using SAM.

**Figure 3-5 Exported File System From HP-UX 10.x Cluster Server to Cluster Clients**




**NOTE** The cluster server must also be configured as an ITO managed node if you are monitoring cluster clients, as the tree is only writable for the cluster server.

## NFS Cluster Client on HP-UX 10.x

In general, cluster clients mount directories and swap space from the cluster server directories.

Each cluster client that is also a managed node, mounts the following directory with read permissions:
`<cluster_server>:/export/shared_roots/os_700/opt`

**NOTE** You can configure cluster clients for HP-UX 10.01 and above using SAM.

## The ITO Default Operator on HP-UX 10.x and 11.x

The ITO default operator, **opc_op**, owns /home/opc_op as home directory. By default, the operator uses the Korn Shell (/usr/bin/ksh) and is not allowed to log into the system directory (a * entry is made for the password in /etc/passwd).

If the managed node is a Network-Information-Service (NIS or NIS+) client, you must add the ITO default operator **opc_op** on the NIS server before installing the ITO software on a managed node. This ensures that the ITO default operator **opc_op** is used by ITO and is consistent on all systems.

## System Resources Adapted by ITO on HP-UX 10.x and 11.x

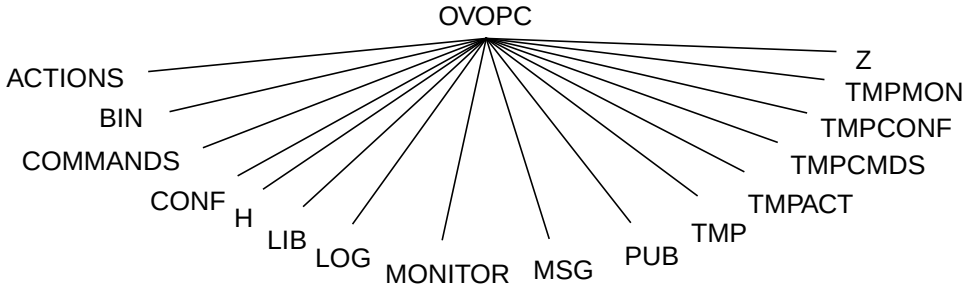
ITO makes changes in the following system resource files:

- /etc/passwd - entry for the default ITO operator
- /etc/group - entry for the default ITO operator
- /sbin/init.d/opcagt - ITO startup/shutdown script
- /etc/rc.config.d/opcagt - ITO startup/shutdown configuration script
- /sbin/rc3.d - file S941opcagt created
- /sbin/rc2.d - file K59opcagt created

Note that if you are working with Network Information Services (NIS or NIS+) you should adapt the user registration accordingly.

# File Tree Layout on MPE/iX Managed Nodes

**Figure 3-6 ITO Software on MPE/iX Managed Nodes**




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

## ITO Default Operator on MPE/iX

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

## System Resources Adapted by ITO on MPE/iX

ITO makes changes to the following system resource files:

- SYSSTART.PUB.SYS

  ITO agent startup; modification is only done if the **Automatic Update of System Resource Files** option has been set.

## ARPA-to-NS Node-Name Mapping for MPE/iX

ITO uses the **vt3k** operation for software (de-)installation purposes and for a virtual terminal connection from the operator's Application Desktop or the administrator's 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, a selected node's ARPA

hostname is truncated after the first dot (.), and 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, since a fully-qualified NS node name is unavailable.

If the truncated ARPA host name differs from the NS node name or the MPE/iX managed node belongs to a different NS domain, ITO supports the mapping file below to avoid this problem:

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

This file can be a symbolic link to /etc/xnmvt3k.conf or the file below, used by ITO for remote logins on HP 3000 systems via vt3k:

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

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

1. It searches for the first line in the `vt3k.conf` file that begins with a matching ARPA hostname. If a matching name is found, the NS node name in the second column is input to the **vt3k** operation.
2. If no matching ARPA hostname is found in the `vt3k.conf` file, the search is repeated with only the first part of the ARPA host name (the part preceding the first dot). If a matching name is found, the NS node name in the second column is input to the **vt3k** operation.
3. If no matching name is found in the `/vt3k.conf` file or the mapping file does not exist (the default case), the truncated hostname is input to the **vt3k** operation. This case assumes that the name identifies a node in the same NS domain as the management server, since a fully-qualified NS node name is missing.

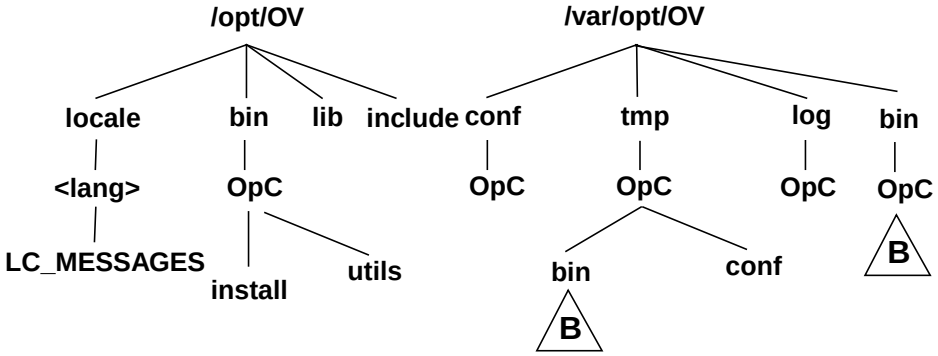
You can configure the `vt3k.conf` file at any time; you do not have to exit the ITO GUI or restart any ITO services.

**Figure 3-7** ARPA to NS Node Name Mapping

```
#ARPA                 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 as
                                            #management server
topaz.sgp.hp.com      nstopaz.mis.hpsg      #node names and domains differ
```

# File Tree Layout on NCR UNIX SVR4 Managed Nodes

**Figure 3-8** **ITO Software on NCR UNIX SVR4 Stand-alone Systems**




The directory `/var/sadm/pkg/OPC` is used by the `pkgadd` utility for software maintenance.

## Standalone System or NFS Cluster Server on NCR UNIX SVR4

In general, stand-alone systems are treated as cluster servers. The cluster server exports the `/opt` file system with read-only permissions. ITO software is located on `/opt/OV` path, with the same logical and physical path names.

**NOTE**

By default NCR UNIX does not export the `/opt` file system. ITO cluster operations can only be enabled by manually exporting the `/opt` file system on one NCR system and then mounting it from one or more NCR systems. This manual cluster setup must be done before the ITO installation process in order to have an impact on the ITO installation.

## NFS Cluster Client on NCR UNIX SVR4

NCR UNIX cluster clients are those NCR UNIX systems that have `/opt` file system NFS mounted. Their cluster server is the system to which `/opt` is mounted and must also be a system running NCR UNIX.

## The ITO Default Operator on NCR UNIX SVR4

The ITO default operator, **opc_op**, owns /home/opc_op as home directory. By default, the operator uses the Bourne Shell (/bin/sh) and is locked until the passwd(1M) command is executed. User opc_op belongs to the group opcgrp.

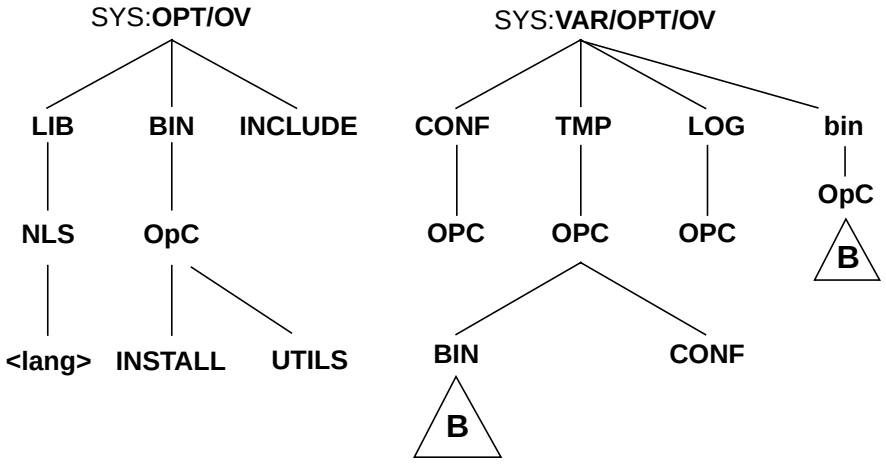
## System Resources Adapted by ITO on NCR UNIX SVR4

ITO makes changes to the following system resource files:

- /etc/passwd and /etc/shadow - entry for the default ITO operator
- /etc/group - group entry for the default ITO operator
- /etc/init.d/opc - ITO startup script
- /etc/rc2.d - file S93opc is created
- /etc/rc0.d - file K07opc is created
- /etc/rc1.d - file K07opc is created
- /etc/init.d/ncs - NCS startup script, if not already present
- /etc/rc2.d: file S76ncs is created, if not already present
- /etc/rc0.d: file K52ncs is created, if not already present
- /etc/rc1.d: file K52ncs is created, if not already present

# File Tree Layout on Novell NetWare Managed Nodes

**Figure 3-9** **ITO Software on Novell NetWare Managed Nodes**




During installation, ITO creates the opc_op account which has the same security level as the user ADMIN. This account is a normal user account and is used to execute applications.

## ITO Default Operator on Novell NetWare

**Table 3-3** **ITO Entry in the User Manager for Domains on Novell NetWare Managed Nodes**

| Field | Entry |
|---|---|
| **User Name** | OPC_OP |
| **Encrypted Password** | Must be entered manually. Use NETADMIN or NWADMIN |
| **User-ID** | N/A |
| **Group-ID** | N/A |

| Field | Entry |
|---|---|
| **Description** | OPC_OP is a special user with rights equivalent to NetWare system administrator ADMIN |
| **Home Directory** | Not set |
| **Login Shell** | NetWare deals with login scripts; user OPC_OP does not have any login script assigned |

## System Resources adapted by ITO on Novell NetWare

During agent software installation, ITO modifies the AUTOEXEC.NCF file. ITO agent start up command OPCAGT.NCF is added.

The following resources are changed during the ITO agent for NetWare installation:

SYS:/SYSTEM/AUTOEXEC.NCF

- OPCAGT.NFC is added to invoke the ITO agent for NetWare software if this command is not already present in this file
- LOAD REMOTE <remote_console_password> is added to invoke the remote console if the user does not yet have a correctly installed remote console
- LOAD XCONSOLE is added to invoke the X-windows console if you have not yet correctly installed this product

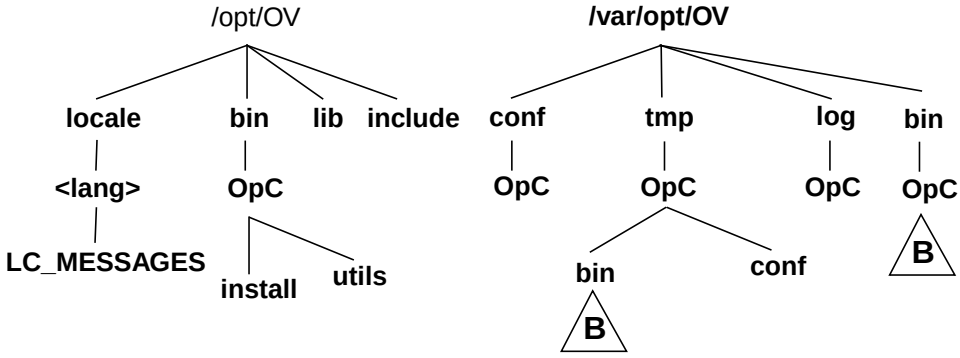
SYS:/ETC/HOSTS

- <server_name> <IP_address> is added for the NetWare server that is currently installed with ITO agent software if this line is not already present in this file
- <mng_server_name> <IP_address> is added when you answer (Y)es to the question “Do you want to add the ITO management server to SYS:ETC/HOSTS file?” if this line is not already present in the HOSTS file

# File Tree Layout on Olivetti UNIX Managed Nodes

The ITO software on Olivetti UNIX managed nodes is based on the typical SVR4 platforms as follows:

**Figure 3-10 ITO Software on Olivetti UNIX Managed Nodes**




## Standalone Systems or NFS Cluster Servers on Olivetti UNIX

In general, standalone systems are treated as cluster servers.

The cluster server exports the `/opt` file system with read-only permissions. ITO software is located on the `/opt/OV` path, with the same logical and physical path names.

**NOTE** By default, Olivetti UNIX does not export the `/opt` file system. You can enable ITO cluster operations manually by exporting the `/opt` file system to one Olivetti UNIX system, and then mount it from other Olivetti UNIX systems. You must set up the cluster manually before the ITO installation process, so that it is available for the ITO installation.

## NFS Cluster Clients on Olivetti UNIX

Olivetti UNIX cluster clients are those Olivetti UNIX systems that have the `/opt` file system NFS mounted. Their cluster server is the system to which `/opt` is mounted and must also be a system running Olivetti UNIX.

## The ITO Default Operator on Olivetti UNIX

The ITO default operator **opc_op** and the group **opcgrp** are created as the ITO default operator if they don't already exist.

**Table 3-4 ITO Entry in /etc/passwd on Olivetti UNIX Managed Nodes**

| Field | Entry |
|---|---|
| **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** | ITO default operator |
| **Home Directory** | `/usr/opc_op` |
| **Login Shell** | `/bin/sh` |

**Table 3-5 ITO Entry in /etc/group on Olivetti UNIX Managed Nodes**

| Field | Entry |
|---|---|
| **Group Name** | opcgrp |
| **Encrypted Password** | empty |
| **Group-ID** | 177 or higher |
| **Users** | opc_op |
| **Description** | ITO default operator group |

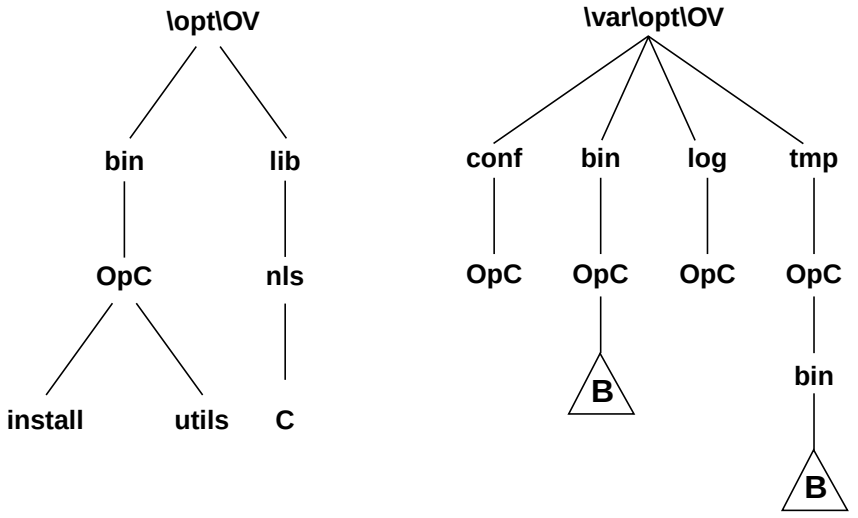
## System Resources Adapted by ITO on Olivetti UNIX

ITO makes changes in the following system resource files during installation:

- `/etc/passwd` and `/etc/shadow` (if present), Protected Password Database (if present) - entry for the default ITO operator
- `/etc/group` - group entry for the default ITO operator
- `/etc/init.d/opcagt` - ITO startup/shutdown script
- `/etc/rc0.d` - file `K09opcagt` created
- `/etc/rc1.d` - file `K09opcagt` created
- `/etc/rc2.d` - file `S99opcagt` created
- `/etc/init.d/ncs` - NCS startup/shutdown script (if not already present)
- `/etc/rc0.d` - file `K52ncs` created (if not already present)
- `/etc/rc1.d` - file `K52ncs` created (if not already present)
- `/etc/rc2.d` - file `S76ncs` created (if not already present)

# File Tree Layout on OS/2 Manged Nodes

**Figure 3-11** **ITO Software on OS/2 Managed Nodes**




## ITO Default Operator on OS/2 Managed Nodes

OS/2 does not support a user concept so that no ITO default operator exists on OS/2 managed nodes.

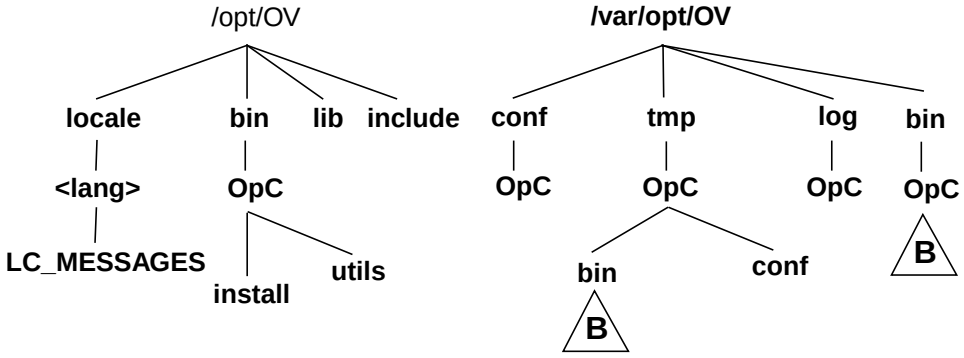
## System Resources adapted by ITO on OS/2 Managed Nodes

During agent software installation, ITO modifies the `STARTUP.CMD` file, if the box `[Automatic Update of System Resource Files]` is checked in the ITO GUI.

# File Tree Layout on Pyramid DataCenter/OSx Managed Nodes

The ITO software on Pyramid DataCenter/OSx managed nodes is based on the typical SVR4 platforms as follows:

**Figure 3-12 ITO Software on Pyramid DataCenter/OSx Managed Nodes**




## Standalone Systems or NFS Cluster Servers on Pyramid DataCenter/OSx

In general, standalone systems are treated as cluster servers. The cluster server exports the `/opt` file system with read-only permissions. ITO software is located on the `/opt/OV` path, with the logical path name the same as the physical path name.

**NOTE** By default, Pyramid DataCenter/OSx does not export the `/opt` file system. You can enable ITO cluster operations manually by exporting the `/opt` file system to one Pyramid DataCenter/OSx system, and then mount it from other Pyramid DataCenter/OSx systems. You must set up the cluster manually before the ITO installation process, so that it is available for the ITO installation.

## NFS Cluster Clients on Pyramid DataCenter/OSx

Pyramid DataCenter/OSx cluster clients are those Pyramid DataCenter/OSx systems that have the `/opt` file system NFS mounted. Their cluster server is the system to which `/opt` is mounted and must also be a system running Pyramid DataCenter/OSx.

## The ITO Default Operator on Pyramid DataCenter/OSx

The ITO default operator **opc_op** and the group **opcgrp** are created as the ITO default operator if they don't already exist.

**Table 3-6 ITO Entry in /etc/passwd on Pyramid DataCenter/OSx Managed Nodes**

| Field | Entry |
|---|---|
| **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** | ITO default operator |
| **Home Directory** | `/home/opc_op` |
| **Login Shell** | `/bin/sh` |

**Table 3-7 ITO Entry in /etc/group on Pyramid DataCenter/OSx Managed Nodes**

| Field | Entry |
|---|---|
| **Group Name** | opcgrp |
| **Encrypted Password** | empty |

| Field | Entry |
|---|---|
| **Group-ID** | 177 or higher |
| **Users** | opc_op |
| **Description** | ITO default operator group |

## System Resources Adapted by ITO on Pyramid DataCenter/OSx

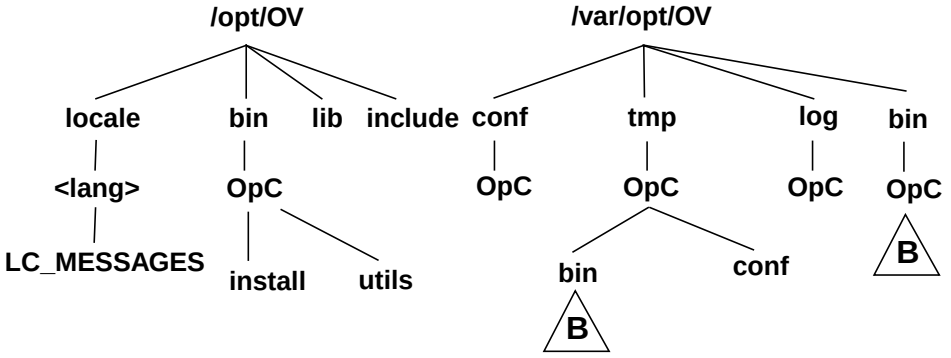
ITO makes changes in the following system resource files during installation:

- `/etc/passwd` and `/etc/shadow` (if present), Protected Password Database (if present) - entry for the default ITO operator
- `/etc/group` - group entry for the default ITO operator
- `/etc/init.d/opcagt` - ITO startup/shutdown script
- `/etc/rc0.d` - file `K09opcagt` created
- `/etc/rc1.d` - file `K09opcagt` created
- `/etc/rc2.d` - file `S89opcagt` created
- `/etc/init.d/ncs` - NCS startup/shutdown script (if not already present)
- `/etc/rc0.d` - file `K52ncs` created (if not already present)
- `/etc/rc1.d` - file `K52ncs` created (if not already present)
- `/etc/rc2.d` - file `S76ncs` created (if not already present)

# File Tree Layout on SCO OpenServer Managed Nodes

The ITO software on SCO OpenServer managed nodes is based on the typical SVR4 platforms as follows:

**Figure 3-13 ITO Software on SCO OpenServer Managed Nodes**




## Standalone Systems or NFS Cluster Servers on SCO OpenServer

In general, standalone systems are treated as cluster servers.

The cluster server exports the `/opt` file system with read-only permissions. The ITO software is located in the `/opt/OV` path, with the same logical and physical path names.

**NOTE** By default, SCO OpenServer does not export the `/opt` file system. You can enable ITO cluster operations manually by exporting the `/opt` file system on one SCO OpenServer system, then mount it from other SCO OpenServer systems. You must do cluster setup manually before the ITO installation process so that it has an effect on the ITO installation.

## NFS Cluster Clients on SCO OpenServer

SCO OpenServer cluster clients are those SCO OpenServer systems that have the `/opt` file system NFS mounted. Their cluster server is the system to which `/opt` is mounted and must also be a system running SCO OpenServer.

## The ITO Default Operator on SCO OpenServer

The ITO default operator **opc_op** and the group **opcgrp** are created as the ITO default operator if they don't already exist.

**Table 3-8 ITO Entry in /etc/passwd on SCO OpenServer Managed Nodes**

| Field | Entry |
|---|---|
| **User Name** | opc_op |
| **Encrypted Password** | * (no login) |
| **User-ID** | 778 if still available, or next possible free number |
| **Group-ID** | 77 if still available, or next possible free number |
| **Description** | ITO default operator |
| **Home Directory** | /HOME_DIR /opc_op [a] |
| **Login Shell** | `/bin/sh` (POSIX shell) |

a. HOME_DIR is set to the path name specified in `/etc/default/authsh` with the HOME_DIR. The HOME_DIR variable reflects the current settings on the system in question. If `/etc/default/authsh` is not present, or HOME_DIR is not set, then `/usr` is assumed.

**Table 3-9 ITO Entry in /etc/group on SCO OpenServer Managed Nodes**

| Field | Entry |
|---|---|
| **Group Name** | opcgrp |
| **Encrypted Password** | empty |

| Field | Entry |
|---|---|
| **Group-ID** | 77 or higher |
| **Users** | opc_op |
| **Description** | ITO default operator group |

## System Resources Adapted by ITO on SCO OpenServer

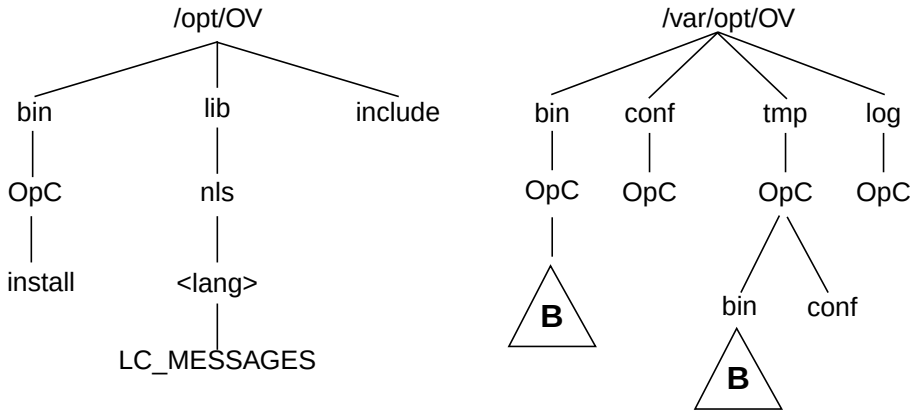
ITO makes changes in the following system resource files during installation:

- `/etc/passwd` and `/etc/shadow` (if present), Protected Password Database (if present) - entry for the default ITO operator
- `/etc/group` - group entry for the default ITO operator
- `/etc/init.d/opcagt` - ITO startup/shutdown script
- `/etc/rc0.d` - file `K09opcagt` created
- `/etc/rc2.d` - file `S94opcagt` created
- `/etc/init.d/ncs` - NCS startup/shutdown script
- `/etc/rc0.d` - file `K24ncs` created
- `/etc/rc2.d` - file `S93ncs` created

# File Tree Layout on SCO UnixWare Managed Nodes

The ITO software on SCO UnixWare managed nodes is based on the typical SVR4 platforms as follows:

**Figure 3-14 ITO Software on SCO UnixWare Managed Nodes**




## Standalone Systems or NFS Cluster Servers on SCO UnixWare

In general, standalone systems are treated as cluster servers.

The cluster server exports the `/opt` file system with read-only privileges. The ITO software is located in the `/opt/OV` path, with the same logical and physical path names.

**NOTE**

By default, SCO UnixWare does not export the `/opt` file system. You can enable ITO cluster operations manually by exporting the `/opt` file system on one SCO UnixWare system, then mount it from other SCO UnixWare systems. You must do cluster setup manually before the ITO installation process so that it has an effect on the ITO installation.

## NFS Cluster Clients on SCO UnixWare

SCO UnixWare cluster clients are those SCO UnixWare systems that have the `/opt` file system NFS mounted. Their cluster server is the system to which `/opt` is mounted and must also be a system running SCO UnixWare.

## The ITO Default Operator on SCO UnixWare

The ITO default operator **opc_op** and the group **opcgrp** are created as the ITO default operator if they don't already exist.

**Table 3-10 ITO Entry in /etc/passwd on SCO UnixWare Managed Nodes**

| Field | Entry |
|---|---|
| **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** | ITO default operator |
| **Home Directory** | /home /opc_op |
| **Login Shell** | `/bin/sh` (POSIX shell) |

**Table 3-11 ITO Entry in /etc/group on SCO UnixWare Managed Nodes**

| Field | Entry |
|---|---|
| **Group Name** | opcgrp |
| **Encrypted Password** | empty |
| **Group-ID** | 177 or higher |
| **Users** | opc_op |
| **Description** | ITO default operator group |

## System Resources Adapted by ITO on SCO UnixWare

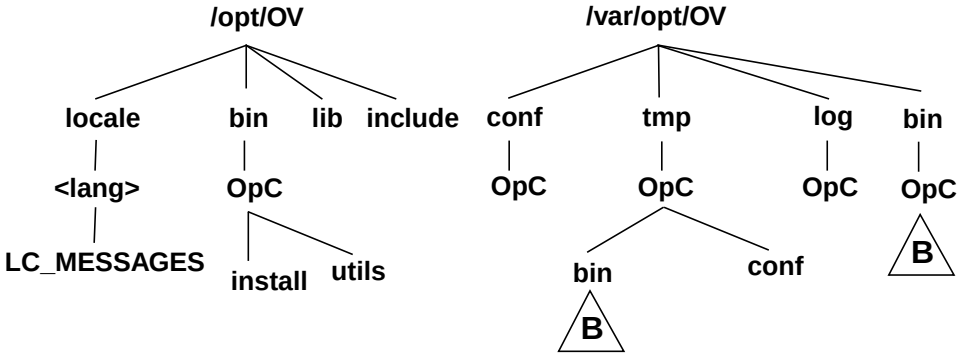
ITO makes changes in the following system resource files during installation:

- `/etc/passwd` and `/etc/shadow` (if present), Protected Password Database (if present) - entry for the default ITO operator
- `/etc/group` - group entry for the default ITO operator
- `/etc/init.d/opcagt` - ITO startup/shutdown script
- `/etc/rc0.d` - file `K09opcagt` created
- `/etc/rc1.d` - file `K09opcagt` created
- `/etc/rc2.d` - file `S95opcagt` created

# File Tree Layout on Sequent DYNIX/ptx Managed Nodes

The ITO software on Sequent DYNIX/ptx managed nodes is based on the typical SVR4 platforms as follows:

**Figure 3-15 ITO Software on Sequent DYNIX/ptx Managed Nodes**




## Standalone Systems or NFS Cluster Servers on Sequent DYNIX/ptx

In general, standalone systems are treated as cluster servers.

The cluster server exports the `/opt` file system with read-only permissions. ITO software is located on the `/opt/OV` path, with the logical path name the same as the physical path-name.

**NOTE** By default, Sequent DYNIX/ptx does not export the `/opt` file system. You can enable ITO cluster operations manually by exporting the `/opt` file system to one DYNIX/ptx system, and then mount it from other DYNIX/ptx systems. You must set up the cluster manually before the ITO installation process, so that it is available for the ITO installation.

## NFS Cluster Clients on DYNIX/ptx

Sequent DYNIX/ptx cluster clients are those DYNIX/ptx systems that have the `/opt` file system NFS mounted. Their cluster server is the system to which `/opt` is mounted and must also be a system running Sequent DYNIX/ptx.

## The ITO Default Operator on Sequent DYNIX/ptx

The ITO default operator **opc_op** and the group **opcgrp** are created as the ITO default operator if they don't already exist.

**Table 3-12 ITO Entry in /etc/passwd on Sequent DYNIX/ptx Managed Nodes**

| Field | Entry |
|---|---|
| **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** | ITO default operator |
| **Home Directory** | /home /opc_op |
| **Login Shell** | `/bin/sh` |

**Table 3-13 ITO Entry in /etc/group on Sequent DYNIX/ptx Managed Nodes**

| Field | Entry |
|---|---|
| **Group Name** | opcgrp |
| **Encrypted Password** | empty |
| **Group-ID** | 77 or higher |
| **Users** | opc_op |
| **Description** | ITO default operator group |

## System Resources Adapted by ITO on Sequent DYNIX/ptx

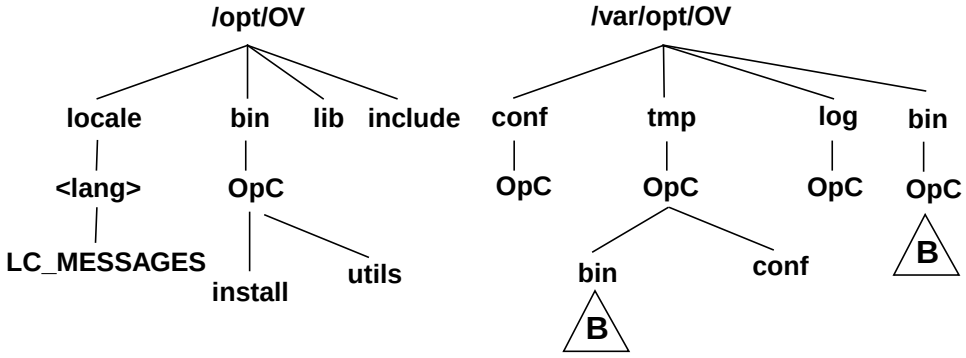
ITO makes changes in the following system resource files during installation:

- `/etc/passwd` and `/etc/shadow` (if present), Protected Password Database (if present) - entry for the default ITO operator
- `/etc/group` - group entry for the default ITO operator
- `/etc/init.d/opcagt` - ITO startup/shutdown script
- `/etc/rc0.d` - file `K07opcagt` created
- `/etc/rc2.d` - file `S93opcagt` created
- `/etc/init.d/ncs` - NCS startup/shutdown script
- `/etc/rc0.d` - file `K52ncs` created
- `/etc/rc2.d` - file `S76ncs` created

# File Tree Layout for Silicon Graphics IRIX

The file tree used by the ITO managed node software on IRIX is similar to other SVR4 platforms and organised in the following way:

**Figure 3-16 ITO Software on SGI IRIX Managed Nodes**




## Standalone Systems or NFS Cluster Servers on SGI IRIX

In general, stand-alone systems are treated as cluster servers. The cluster server exports the `/opt` file system with read-only permissions. ITO software is located in `/opt/OV`, with the same logical and physical path names.

## NFS Cluster Client on SGI IRIX

In addition to the general rule for determining cluster clients described in “Installation Tips for IRIX Managed Nodes” on page 70, there is also one specific rule for IRIX:

IRIX cluster clients (both diskless, and normal disks) are those IRIX systems that have either a `/usr` file system or `/opt` file system NFS mounted. Their cluster server is the system to which `/usr` or `/opt` is mounted. If the `/opt` file system is not already NFS mounted (only `/usr` NFS mounted), then ITO mounts `/opt` to `/opt` of the cluster server:

```
mount <cluster_server>:/opt /opt
```

## The ITO Default Operator on SGI IRIX

The ITO default operator **opc_op** and the group **opcgrp** are created as the ITO default operator if they don't already exist.

**Table 3-14 ITO Entry in /etc/passwd on SGI IRIX Managed Nodes**

| Field | Entry |
|---|---|
| **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** | ITO default operator |
| **Home Directory** | `/var/people/opc_op` |
| **Login Shell** | `/bin/sh` (POSIX shell) |

**Table 3-15 ITO Entry in /etc/group on SGI IRIX Managed Nodes**

| Field | Entry |
|---|---|
| **Group Name** | opcgrp |
| **Encrypted Password** | empty |
| **Group-ID** | 77 or higher |
| **Users** | opc_op |
| **Description** | ITO default operator group |

## System Resources Adapted by ITO on SGI IRIX

ITO makes changes in the following system resource files:

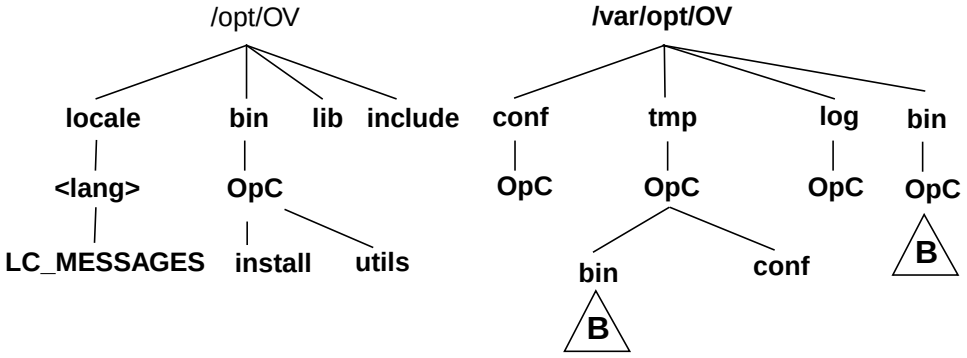
- `/etc/passwd` and `/etc/shadow` (if present) - entry for the default ITO operator

- `/etc/group` - group entry for the default ITO operator
- `/etc/init.d/opcagt` - ITO startup/shutdown script
- `/etc/rc0.d` - file `K09opcagt` created
- `/etc/rc2.d` - file `S89opcagt` is created
- `/etc/exports` - on cluster server only; entry for export of `/opt` directory
- `/etc/fstab` - on cluster client only; entry for mount `/opt` directory
- `/etc/init.d/grad_nck` - NCS startup/shutdown script
- `/etc/rc0.d` - file `K35nck` is created
- `/etc/rc2.d` - file `S40nck` is created

# File Tree Layout on SINIX Managed Nodes

The ITO software on SINIX managed nodes is based on the typical SVR4 platforms as follows:

**Figure 3-17 ITO Software on SINIX Managed Nodes**




## Standalone Systems or NFS Cluster Servers on SINIX

In general, standalone systems are treated as cluster servers.

The cluster server exports the `/opt` file system with read-only permissions. ITO software is located on the `/opt/OV` path, with the logical path name the same as the physical path name.

**NOTE** By default, SINIX does not export the `/opt` file system. You can enable ITO cluster operations manually by exporting the `/opt` file system to one SINIX system, and then mount it from other SINIX systems. You must set up the cluster manually before the ITO installation process, so that it is available for the ITO installation.

## NFS Cluster Clients on SINIX

SINIX cluster clients are those SINIX systems that have the `/opt` file system NFS mounted. Their cluster server is the system to which `/opt` is mounted and must also be a system running SINIX.

## The ITO Default Operator on SINIX

The ITO default operator **opc_op** and the group **opcgrp** are created as the ITO default operator if they don't already exist.

**Table 3-16 ITO Entry in /etc/passwd on SINIX Managed Nodes**

| Field | Entry |
|---|---|
| **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** | ITO default operator |
| **Home Directory** | `/home/opc_op` |
| **Login Shell** | `/bin/sh` |

**Table 3-17 ITO Entry in /etc/group on SINIX Managed Nodes**

| Field | Entry |
|---|---|
| **Group Name** | opcgrp |
| **Encrypted Password** | empty |
| **Group-ID** | 177 or higher |
| **Users** | opc_op |
| **Description** | ITO default operator group |

## System Resources Adapted by ITO on SINIX

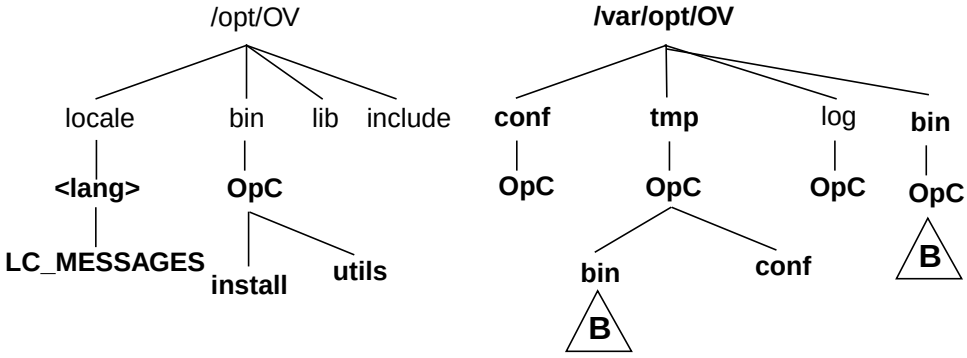
ITO makes changes in the following system resource files during installation:

- `/etc/passwd` and `/etc/shadow` (if present), Protected Password Database (if present) - entry for the default ITO operator
- `/etc/group` - group entry for the default ITO operator
- `/etc/init.d/opcagt` - ITO startup/shutdown script
- `/etc/rc0.d` - file `K09opcagt` created
- `/etc/rc1.d` - file `K09opcagt` created
- `/etc/rc2.d` - file `S89opcagt` created
- `/etc/init.d/ncs` - NCS startup/shutdown script (if not already present and communciation type is NCS RPC)
- `/etc/rc0.d` - file `K52ncs` created (if not already present and communciation type is NCS RPC)
- `/etc/rc1.d` - file `K52ncs` created (if not already present and communciation type is NCS RPC)
- `/etc/rc2.d` - file `S76ncs` created (if not already present and communciation type is NCS RPC)
- `/usr/lib/snmplib/libsnmpapi.so -> \ /opt/lib/snmpd/snmplib/libsnmpuser.so` - Symbolic link created if not already present

# File Tree Layout on Solaris Managed Nodes

The ITO software on Solaris managed nodes is organized in the following way:

**Figure 3-18 ITO Software on Solaris Managed Nodes**




The path `/var/sadm/pkg/OPC` is used by the `pkgadd` utility for software maintenance.

## Standalone Systems or NFS Cluster Servers on Solaris

In general, stand-alone systems are treated as cluster servers. The cluster server exports the `/opt` file system with read-only permissions. ITO software is located on `/opt/OV` path, with the same logical and physical path names. This simplification was possible because ITO software can now operate from the read-only `/opt` file system on cluster clients. By default, Solaris does not export the `/opt` file system; not even on the cluster server. During the ITO installation process on the cluster server, care is taken to export the `/opt` file system if it was not already exported.

## NFS Cluster Client on Solaris

In addition to the general rule for determining cluster clients described in the section "Installation Tips for UNIX Managed Nodes" on page 50 there is also one specific rule for Solaris:

Solaris cluster clients (both with and without disks) are those Solaris systems that have either a `/usr` or `/opt` file system NFS mounted. Their cluster server is the system to which `/usr` or `/opt` is mounted. If the `/opt` file system is not already NFS mounted (only `/usr` NFS mounted), then ITO mounts local `/opt` to `/opt` of the cluster server:

```
mount <cluster_server>:/opt /opt
```

## The ITO Default Operator on Solaris

The ITO default operator, **opc_op**, owns `/home/opc_op` as home directory. By default, the operator uses the Bourne Shell (`/bin/sh`) and is locked until the `passwd(1M)` command is executed. User **opc_op** belongs to the group **opcgrp**.

Currently, user **opc_op** and group **opcgrp** are only added locally on the managed node (**useradd** or **groupadd** are used). If the managed node is a Network-Information-Service (**NIS** or **NIS+)** client, the ITO installation checks if user opc_op is already in the NIS database. If so, no additional user is installed, otherwise, opc_op is added only locally on the managed node.

## Solaris System Resources Adapted by ITO

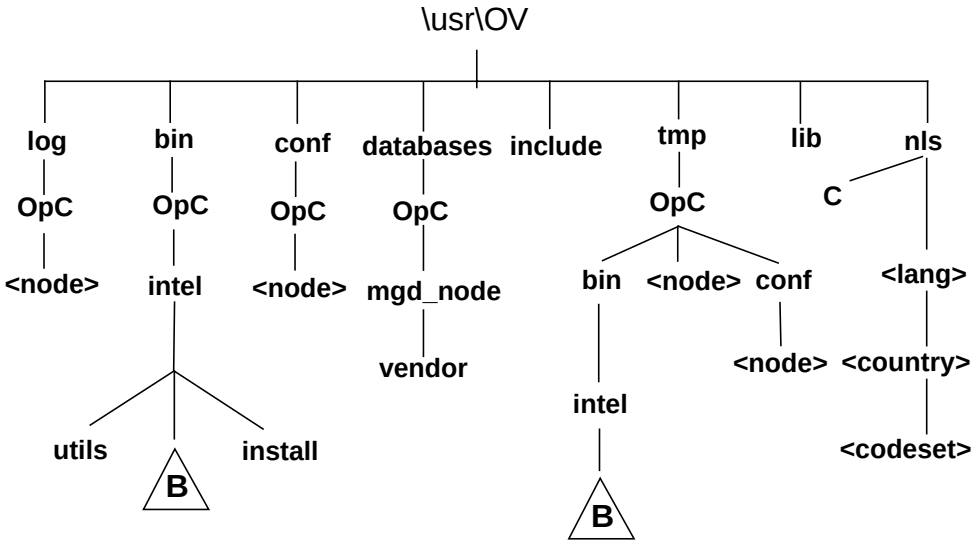
ITO makes changes in the following system resource files:

- `/etc/passwd` and `/etc/shadow` - entry for the default ITO operator
- `/etc/group` - group entry for the default ITO operator
- `/etc/init.d/opcagt` - ITO startup/shutdown script
- `/etc/rc3.d/S99opcagt` - file created
- `/etc/rc0.d/K09opcagt` - file created
- `/etc/rc1.d/K09opcagt` - file created
- `/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` - file created (if not already present)
- `/etc/rc0.d/K52ncs` - file created (if not already present)
- `/etc/rc2.d/K52ncs` - file created (if not already present)

# File Tree Layout on Windows NT Managed Nodes

**Figure 3-19** **ITO Software on Windows NT Managed Nodes**




During installation, ITO creates the HP ITO account which has all rights and privileges that are required for the ITO 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 3-19 by the letter **B** are created by the control agent if necessary

## ITO Default Operator on Windows NT

**Table 3-18 ITO User Accounts on Windows NT Managed Nodes**

| Field | Entry | |
|---|---|---|
| **User Name** | HP ITO account | opc_op |
| **Encrypted Password** | Defined during installation | Same as HP ITO account[a] |
| **Group** | administrator[b] or domain administrator[c] | users or domain users |
| **Description** | HP ITO *agent* account | HP ITO *operator* account |
| **Login Shell** | None | None |

a. All other properties assume the default value
b. NT Workstation
c. P/BDC: Primary/Backup Domain Controller

## System Resources Adapted by ITO on Windows NT

ITO inserts several keys in the Windows NT Registry. The keys and their associated values can be viewed with the Registry editor, using the following command **`%SystemRoot%\System32\regedt32.exe`**. The registry editor will show the following keys for ITO:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\ITO`
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0`
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HP ITO Agent`
- And if on a primary or backup domain controller: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HP ITO Installation Server`

# 4 Software Maintenance on Managed Nodes

This chapter provides important information about installing and de-installing ITO software on managed nodes with various operating systems. The installation, de-installation, and updating of ITO software is referred to as “software maintenance”. This chapter includes:

- ❏ Installing and upgrading the ITO agent software using the GUI.
- ❏ De-installation of the ITO agent software using the GUI.
- ❏ Checking installed agent software packages on the management server.
- ❏ Removing ITO agent software packages from the management server that are no longer required.

**NOTE**

For information about adding an additional ITO agent software package to the management server, see the *HP OpenView IT/Operations Installation Guide for the Management Server*.

# Overview

ITO software installation, update, and de-installation (software maintenance) uses functionality provided by the ITO administrator GUI and is performed using the `inst.sh(1M)` script. To avoid the verbose output of this script, you can set a shell variable for user **root**:

Bourne/Korn **`OPC_SILENT=1; export OPC_SILENT`**

C **`setenv OPC_SILENT`**

In order to be able to carry out software maintenance, you need to know either the root passwords of the managed nodes, or `.rhosts` entries must be available for user **root** (UNIX only). Failing that, make sure the local `/etc/hosts.equiv` (on the UNIX managed nodes) contains an entry for the management server.

Before installing ITO software on the managed nodes, or de-installing ITO software from the managed nodes, read the section “General Installation Tips for Managed Nodes” on page 47.

Before you can install ITO on a managed node, you must add the managed node to the `Node Bank` window using the `ITO Add Node` window, which is accessed by selecting `Actions:Node->Add...` from the menu bar of the `Node Bank` window see Figure 4-1. Alternatively, you can add nodes to the `Node Bank` by copying and pasting or dragging and dropping them from the IP submaps.

**Figure 4-1 Adding a Managed Node to the Node Bank Window**

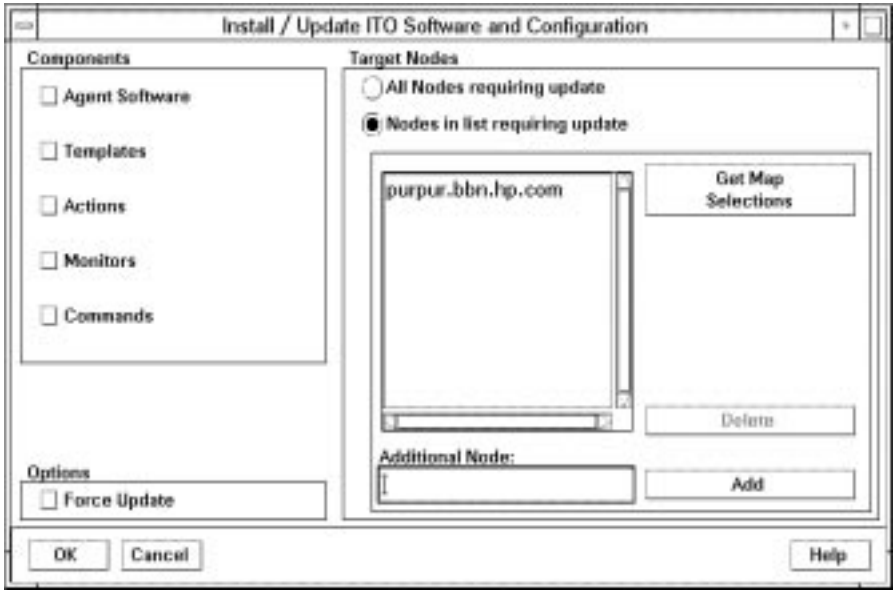

For detailed information about how to set the managed node attributes, refer to the online help.

Select the **Automatic (De-)Installation** option, and the ITO software is automatically installed onto the managed node when you invoke the installation for this system in the `Install/Update ITO Software and Configuration` window.

# Installing or Updating ITO Software Automatically

To install the ITO bits on the managed node automatically, use the `Install/Update ITO Software and Configuration` window and select the `Actions:Agents->Install/Update SW & Config...` item in the menu bar.

**Figure 4-2 Install/Update ITO Software and Configuration Window**




For detailed information about the `Install/Update ITO Software and Configuration` window, see the online help. To install or update the ITO software automatically:

1. Use the `Install/Update ITO Software and Configuration` window of the ITO administrator's GUI and select the appropriate options. For a software installation or update, the **Agent Software** component is the minimum selection.

With the Force Update checkbox unselected (default), only the differences between the previous configuration and the new configuration are distributed to the managed nodes. This reduces the amount of data being transferred, consequently reducing the load on the network.

2. After clicking on the `[OK]` button, an additional terminal window opens, running the installation script, `inst.sh(1M)`. Review the messages carefully, as the installation script might require your interaction (for example, if a root password is missing).

   First, the `inst.sh(1M)` script checks that all specified systems are reachable and accessible by the super user. (If a password is missing, you are asked to supply one before installation is done.)

   Watch the script execution carefully. Your interaction might be required if any errors or warnings occur.

   At the end of the script execution, when you have verified the overall result of the script run, close the terminal window by pressing **Return**.

3. Check the local (managed node) installation logfile for any problems:

| | |
|---|---|
| AIX | `/tmp/installp.log` |
| DEC Alpha NT | `c:\temp\inst.log` |
| Digital UNIX (OSF/1) | `/var/adm/smlogs/setld.log` |
| HP-UX 10.x and 11.x | `/var/adm/sw/swagent.log` and `/var/adm/sw/swinstall.log` |
| MPE/iX | No special logfile available. |
| NCR UNIX SVR4 | `/tmp/pkgadd.log` |
| Novell NetWare | `SYS:DEPOINST.ITO/ITOINST` on NetWare depot server |
| Olivetti UNIX | `/tmp/pkgadd.log` |
| OS/2 | No special logfile available. |
| Pyramid DataCenter/OSx | `/tmp/pkgadd.log` |
| SCO OpenServer | `/usr/lib/custom/history` |

This is the same logfile for both installation and removal operations. Only one record is written for each package.

| | |
|---|---|
| SCO UnixWare | `/tmp/pkgadd.log` |
| Sequent DYNIX/ptx | `/tmp/pkgadd.log` |
| SGI IRIX | `/tmp/inst.log` |
| SINIX | `/tmp/pkgadd.log` |
| Solaris | `/tmp/pkgadd.log` |
| Windows NT | `c:\temp\inst.log` |

If necessary, for example, if the installation process could not be reviewed in a terminal window, check the logfile below on the management server for errors or warnings.

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

Note that ITO agent software installation does not include configuration distribution.

## Manually Activating the ITO Agent on NFS Cluster Clients

You can manually activate the ITO agent on an NFS Cluster Client system. However, the ITO agent software must already be installed on the NFS Cluster Server system, and the ITO agent software bits must be available on the target node through an NFS mount of the ITO home directory (`/opt/OV` for HP-UX, Solaris, SINIX and NCR; `/usr/lpp/OV` for AIX).

The full path-name of `opcactivate` command is:

| | |
|---|---|
| AIX | `/usr/lpp/OV/OpC/install/opcactivate` |
| UNIX (other) | `/opt/OV/bin/OpC/install/opcactivate` |

For detailed information about the `opcactivate` command, see the *opcactivate(1m)* man page. All man pages reside on the management server.

**NOTE** Manual activation of the ITO agent software on NFS Cluster Client Nodes is only supported for HP-UX 10.x/11.x, AIX, Solaris, NCR and SINIX managed node with ITO version A.05.00 and higher. In addition, only homogeneous NFS Clusters are supported and the cluster server and cluster client systems must have the same OS.

To manually install the ITO agent on an NFS Cluster-Client managed node:

1. Install the ITO agent on NFS Cluster Server system (see Install the Agent on the Managed Node chapter for details).

**NOTE** This action should be executed only once to install the ITO agents on the NFS Cluster.

If the ITO agent software is to be re-installed, make sure that the ITO agents have been stopped on all NFS cluster nodes before starting the re-installation.

2. Execute the following command on the NFS Cluster Server system

   ```
   opcactivate -mode cluster_server <node>\
   <ITO_mgt_server>
   ```

3. Execute the following command on the NFS Cluster Client system:

   ```
   opcactivate -mode cluster_client
   ```

4. After the node is connected to the network execute the following two commands on the management server:

   ```
   opcsw -installed <node>
   ```

   ```
   opchbp -start <node>
   ```

   This updates the database and starts heartbeat polling for the node. The templates, monitors, commands, and actions must still be installed using the ITO administrator GUI.

## Changing the Communication Type

For the managed node platforms that support both NCS RPC and DCE RPC, you can choose between these communication types.

**NOTE** For Windows NT managed nodes running Service Pack 1 or 2, the communication type must be changed from DCE UDP to DCE TCP to avoid problems.

If you decide to change the communication type, you must update the ITO agent software:

1. Ensure that your managed nodes meet the software requirements described in Chapter 1 of the *HP OpenView IT/Operations Administrator's Reference*. In particular, ensure that the required DCE RPC software is installed and that the DCE daemon is running if you switch to DCE RPC.
2. Stop all ITO agent processes, enter:

   **`/opt/OV/bin/OpC/opcragt -stop`**
3. To change the communication type, you choose between the following methods depending on the number of managed nodes you want to modify:

   ❑ If you want to change the communication type for only a *small* number of nodes:

   a. In the ITO administrator GUI, select the managed node in the `ITO Node Bank` for which you want to change the communication type.

   b. Select `Actions: Node -> Modify...`. The `Modify Node` window opens.

   c. Click on `[Advanced Options]`, and change the communication type in the `Node Advanced Options` window. Select one of the following options:

   - `DCE RPC (UDP)` (recommended)
   - `DCE RPC (TCP)` (useful when communicating over a WAN)
   - `NCS RPC`

   d. Click on `[OK]` in the `Node Advanced Options` and the `Modify Node` window.

   ❑ If you want to change the communication type for a *large* number of managed nodes, you can use the ITO tool `opcnode`. The easiest way to do this is to add it as an ITO application to the `ITO Application Bank`:

a. In the ITO Application Bank window, select Actions: Add ITO Application.

b. Enter a name in the Application Name field, and enter the following in the Application Call field:

```
/opt/OV/bin/OpC/utils/opcnode -chg_commtype \
comm_type=COMM_DCE_UDP node_list="$OPC_NODES"
```

You can also choose COMM_DCE_TCP instead of COMM_DCE_UDP. Note, however, that COMM_DCE_UDP is recommended.

c. Select Start on Management Server, and specify user **root** to execute the application because opcnode must be called with root permissions. Click on [OK].

opcnode is added as an application to the ITO Application Bank.

d. Select the nodes for which you want to change the communication type in the ITO Node Bank or any other node hierarchy.

e. In the ITO Application Bank, double-click the opcnode symbol to execute the application.

The communication type changes for all selected nodes. Verify this by opening the Node Advanced Options window, or calling opcnode -list -nodes. See also the man page *opcnode(1M)* for more information.

4. Use the Install / Update ITO Software and Configuration window to update the ITO agent software.

   Depending on the communication type you have selected in the previous step, ITO automatically selects the appropriate agent fileset during the agent software installation.

# De-installing ITO Software from Managed Nodes

You can choose either of the following methods to de-install ITO software from the managed nodes:

- ❏ De-install only the ITO software from the managed node.
- ❏ Remove the node and de-install the ITO software.

ITO software is automatically de-installed from managed nodes if they are configured with the **Automatic (De-)Installation** option.

The following steps must be applied for automatic node software de-installation:

1. Delete the managed node symbol from the `Node Bank` window (for example, by selecting `Actions:Node->Delete` (or using the right-click popup menu) and confirming the following `ITO Question Dialog` window by clicking the `[Yes]` button).

   Another `ITO Question Dialog` window appears, asking about automatically de-installing software from the managed nodes. When leaving this window by clicking on the `Yes` button, the software de-installation script, `inst.sh(1M)`, is run in an additional terminal window.

   This script checks that all deleted managed nodes are accessible by root; if passwords are missing, you will be prompted for them.

   During script execution, errors or warnings requiring your attention or interaction may occur.

   At the end of the script run, verify the overall result of the script run and close the terminal window by pressing the **Return** key.

**NOTE**

If you are de-installing the ITO agent software from a Windows NT Primary or Backup Domain Controller, the accounts for the domain users `HP ITO account` and `opc_op` must be deleted manually after the de-installation of the ITO agent software.

2. Check the local (managed node) de-installation logfile for any problems:

   AIX — No special logfile available.

| | |
|---|---|
| DEC Alpha NT | `c:\temp\inst.log` |
| Digital UNIX (OSF/1) | `/var/adm/smlogs/setld.log` |
| HP-UX 10.x and 11.x | `/var/adm/sw/swagent.log` and `/var/adm/sw/swremove.log` |
| MPE/iX | No special logfile available. |
| NCR UNIX SVR4 | `/tmp/pkgrm.log` |
| Novell NetWare | `SYS:DEPOINST.ITO/ITOINST` on the NetWare depot server |
| Olivetti UNIX | `/tmp/pkgrm.log` |
| OS/2 | No special logfile available. |
| Pyramid DataCenter/OSx | `/tmp/pkgrm.log` |
| SCO OpenServer | `/usr/lib/custom/history`<br>This is the same logfile for both installation and removal operations. Only one record is written for each package. |
| SCO UnixWare | `/tmp/pkgrm.log` |
| Sequent DYNIX/ptx | `/tmp/pkgrm.log` |
| SGI IRIX | `/tmp/inst.log` |
| SINIX | `/tmp/pkgrm.log` |
| Solaris | `/tmp/pkgrm.log` |
| Windows NT | `c:\temp\inst.log` |

3. Systems running MPE/iX 5.0 or earlier could experience a problem using the `PURGEACCT` command, which leads to a possible de-installation error. If this occurs, reboot the system and purge the `OVOPC` account manually.

Note that you can also manually de-install the ITO agent software which is, however, only supported on selected managed node platforms. If you want to de-install the ITO agent software from NFS-cluster clients, you must use the command `opcdeactivate`, see the man page *opcactivate(1M)*. This is not necessary for the standard manual de-installation.

## Manually De-installing ITO Software from AIX Managed Nodes

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

   **`installp -ug OPC`**

**NOTE** Manually de-installing the ITO agent software from AIX managed nodes is only supported with ITO version A.05.00 and higher.

## Manually De-installing ITO Software from HP-UX Managed Nodes

## Manually De-installing ITO Software from OS/2 Managed Nodes

The installation script `opcinst.cmd` also de-installs the ITO agent software from OS/2 managed nodes.

1. On the managed node, change to the directory where `opcinst.cmd` is located.

   If `opcinst.cmd` has been removed after the installation, copy the script from the directory `\opt\OV\bin\OpC\install` on the managed node or from the management server to a temporary location, see “Manual OS/2 Agent Installation” on page 90.

**NOTE** `opcinst.cmd` must be executed in a temporary directory; do not run `opcinst.cmd` from the directories `\opt\OV` or `\var\opt\OV`.

2. To de-install the ITO agent software, enter:

   **`opcinst.cmd /MODE:REMOVE`**

   If you have changed the disk drive where you had previously installed the ITO agent, enter the new drive when prompted.

   Or enter:

   **`opcinst.cmd /MODE:REMOVE /DRIVE:<`*`install_drive`*`>`**

If the de-installation fails, stop all ITO agents and remove the directories `\var\opt` and `\opt\OV` from the managed nodes. Manually edit the startup command STARTUP. CMD to remove ITO-related information.

## Manually De-installing ITO Software from Solaris, NCR, and SINIX Managed Nodes

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

   **`pkgrm OPC`**

**NOTE**

Manually de-installing the ITO agent software from Solaris, NCR, and SINIX managed nodes is only supported with ITO version A.05.00 and higher.

## Manually De-installing ITO Software from Windows NT Managed Nodes

The installation script `opcsetup` also de-installs the ITO agent software from Windows NT managed nodes.

1. Stop all ITO agents running on the managed node
2. On Intel Windows NT, run the following command:

   **`\usr\OV\bin\OpC\intel\opcsetup -u`**

3. On DEC Alpha NT, run the following command:

   **`\usr\OV\bin\OpC\alpha\opcsetup -u`**

## Manually De-activating the ITO Agent on an NFS Cluster Client

You can manually de-activate the ITO agent on an NFS cluster client system. Manual de-activation removes the ITO agent from the NFS cluster client system. The full path-name of `opcdeactivate` command is:

AIX `/usr/lpp/OV/OpC/install/opcdeactivate`

UNIX (other) `/opt/OV/bin/OpC/install/opcdeactivate`

For detailed information about the `opcdeactivate` command, see the *opcactivate(1m)* man page. All man pages reside on the ITO management server.

**NOTE**

Manual de-activation of the ITO agent software on NFS Cluster Client Nodes is only supported for HP-UX 10.x/11.x, AIX, Solaris, NCR and SINIX managed node with ITO version A.05.00 and higher. In addition, only homogeneous NFS Clusters are supported and the cluster server and cluster client systems must have the same OS.

To de-activate the ITO agent from the NFS cluster client system manually:

1. Execute the following command on NFS Cluster Client system:

   **`opcdeactivate -mode cluster_client`**

2. Execute the following command on the NFS Cluster Server system

   **`opcdeactivate -mode cluster_server <node>`**

3. De-install ITO agent software from NFS Cluster Server system. For more information, see “De-installing ITO Software from Managed Nodes” on page 173.

**NOTE**

This action should be executed only once and after the ITO agent has been de-activated from *all* NFS Cluster Nodes.

# Managing ITO Agent Software

Frequently, managed nodes (even of the same architecture) do not run the same OS versions. This is because different systems are used for different purposes, for example:

- ❏ production systems running approved OS versions where all required applications are available
- ❏ development systems running approved or latest OS versions
- ❏ test systems running approved or latest OS versions

Consequently, ITO has to support a growing list of OS versions. Due to technical limitations and new technologies, future ITO versions might not always be able to support the entire spectrum of OS versions. Nonetheless, ITO does provide a way to control this problem by providing internal management of the ITO agent software version.

If you install a new ITO agent version (having the same fileset name) on a management server supporting the same (or a super) set of OS versions as the previously installed ITO agent version, the previous ITO agent version is erased. However, if you install a new ITO agent version on a management server supporting only some of the previously supported OS versions, then both ITO agent versions are kept on the management server.

Running the script below on the management server will display a summary of all installed ITO agent packages and the supported OS versions.

```
/opt/OV/bin/OpC/agtinstall/opcversion -a
```

The latest possible ITO agent version supporting the OS version of the managed node is always installed on that node. The related ITO software for each supported architecture is available in:

```
/var/opt/OV/share/databases/OpC/mgd_node/vendor/ \
<platform_selector>/<ito_version>/<package_type>
```

If an older ITO agent package is no longer required and is not installed on any managed node, you can remove it by running:

```
/opt/OV/bin/OpC/install/rm_opc.sh <platform_selector> \
<ito_version>
```

Where:

| | |
|---|---|
| <platform_selector> | Is one of the following values:<br>• dec/alpha/unix<br>• hp/s700/hp-ux<br>• hp/s700/hp-ux10<br>• hp/s800/hp-ux<br>• hp/s800/hp-ux10<br>• hp/pa-risc/hp-ux11<br>• hp/s900/mpe-ix<br>• ibm/intel/os2<br>• ibm/rs6000/aix<br>• ms/alpha/nt<br>• ms/intel/nt<br>• ncr/3000/unix<br>• novell/intel/nw<br>• olivetti/intel/unix<br>• pyramid/mips/unix<br>• sco/intel/unix<br>• sco/intel/uw<br>• sequent/intel/dynix<br>• sgi/mips/irix<br>• sni/mips/sinix<br>• sun/sparc/solaris |
| <ito_version> | Is the version of ITO that supports this agent platform, for example A.05.00 |
| <package_type> | Is the type of RPC communication used by that platform; either DCE or NCS or SUN. |

**NOTE**

Do not use `swremove` to de-install an ITO agent package that you no longer require. Running `swremove` is only useful if you wish to de-install *all* ITO agent packages of a particular architecture. In addition, remove the managed nodes from the `ITO Node Bank` *before* doing a complete de-installation of all managed nodes of a given architecture. Otherwise, the managed nodes can no longer be easily removed using the administrator GUI.

# Debugging Software (De-)Installation on Managed Nodes

ITO provides facilities for debugging the (de-)installation of the ITO software on the managed nodes. These tools help developers when testing ITO installation scripts for new platforms, and assist users in examining errors that occur during the installation of the ITO agent software.

The following facilities are available:

**Command tracing** prints shell commands and their arguments from installation programs into a file specified in the file `inst_debug.conf` as argument of the environment variable `OPC_DEBUG_FILE`.

**Event tracing** can be used in addition to command tracing to record important events of the installation process into the existing installation logfile `/var/opt/OV/log/OpC/mgmt_sv/install.log`

The (de-)installation process can be debugged both locally (on the management server) and remotely (on the managed node). A debug definition file `inst_debug.conf` is provided to force debugging and to specify debug options. The debug facility is, therefore, available regardless of whether the script `inst.sh` is invoked manually or called by the ITO GUI.

## Enabling (De-)Installation Debugging

The file `inst_debug.conf` must be edited before starting the installation process. It can only be edited by user root.

1. Copy the file `inst_debug.conf`, enter:

   ```
   cp /etc/opt/OV/share/tmp/OpC/mgmt_sv/inst_debug.conf
   \ /var/opt/OV/share/tmp/OpC/mgmt_sv/inst_debug.conf
   ```

2. Edit your copy of the file `inst_debug.conf` by uncommenting the desired environment variables and by changing the appropriate values.

**NOTE**

The syntax of the file `inst_debug.conf` is not checked. Be careful when editing this file because syntax errors will cause the installation process to abort.

To disable debugging remove the file `/var/opt/OV/share/tmp/OpC/mgmt_sv/inst_debug.conf`

For a detailed description of the (de-)installation debug facilities and examples of the file `inst_debug.conf`, see the man page *inst_debug(5M)*.

# 5 Configuring ITO

This chapter describes ITO's preconfigured elements. It also describes how to distribute the ITO configuration to managed nodes, and how to integrate applications into ITO. In addition to this chapter, you should also read the *HP OpenView IT/Operations Concepts Guide*, to gain a fuller understanding of the elements and the windows you can use to review or customize these preconfigured elements.

# Preconfigured Elements

This section describes all the preconfigured elements provided by ITO, including:

- ❏ applications
- ❏ database reports
- ❏ ITO message interception
- ❏ ITO users
- ❏ logfile encapsulation
- ❏ managed nodes
- ❏ the message browser
- ❏ message groups
- ❏ message ownership
- ❏ MPE/iX console message interception
- ❏ monitored objects
- ❏ SNMP event interception
- ❏ template groups
- ❏ templates for external interfaces

Note also the configuration tips in this section.

## Managed Nodes

By default, the management server is also configured as a managed node with the default templates for SNMP event interception, ITO message interception, logfile encapsulation and monitoring as described in this section.

The management server belongs to the node group `hp_ux`. You can add, modify, and delete node groups using the `Node Group Bank` window of the ITO GUI, while working as the ITO administrator.

## Message Groups

The `Message Group Bank` window displays the default Message Groups provided with ITO. For more information on individual message groups, see Table 5-1 on page 186.

**Table 5-1 ITO Default Message Groups**

| Message Group... | Description |
|---|---|
| Backup | Messages relating to backup/restore/archiving functionality (for example, `fbackup(1)`, **HP OpenView Omniback II**, **HP OmniStorage, Turbo-Store**). |
| Database | Messages relating to database problems |
| Job | Messages relating to job streaming. |
| Hardware | Messages relating to hardware problems |
| Misc | Messages which cannot be assigned to any other message group. If a message does not have a message group assigned or the message group is not configured, the message will belong to the Misc message group. This message group cannot be deleted. |
| NetWare | Messages generated by Novell NetWare managed nodes |
| Network | Messages relating to network/connectivity problems. |
| OS | Messages relating to malfunctions of the operating system, I/O, and so forth. |
| OpC | Messages generated by ITO itself. This message group should not be used by `opcmsg(1\|3)`.The ITO message group cannot be deleted. |
| Output | Messages relating to print spooling/hard-copy functionality (for example, `lp(1)`, `lpr(1)`, **HP OpenView OpenSpool**). |

| Message Group... | Description |
|---|---|
| Performance | Messages related to hardware (CPU, disk, process) and software (for example, **HP OpenView PerfView**) malfunctions. |
| SNMP | Messages generated by SNMP traps. |
| Security | Messages related to security violations or attempts to break into a system. |

You can add, modify, or delete message groups with the `Message Group Bank` window on the ITO GUI, while working as ITO administrator.

## The Message Browser

The `Message Browser` window contains key information concerning incoming messages. Each line of the `Message Browser` window displays a single message and its attributes. ITO displays a value beneath each attribute for each message. A dash indicates that the message does not have a value matching the attribute: for example, a dash in the **A** column indicates that no **automatic action** has been configured for this message. See Figure 5-1 on page 189.

### Understanding the Message Browser Headline

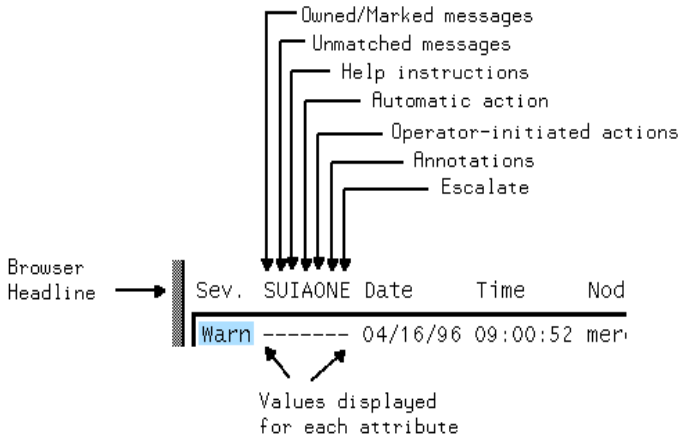
The first column in the `Message Browser` window headline is **Sev.**, which tells you at a glance the severity status of the message. The ITO administrator assigns a severity level to a message based on its importance in a given operator's environment. To comply with telecom standards, ITO recognizes six severity levels. Table 5-2 on page 188 describes ITO's severity levels:

**Table 5-2 Message Severity Levels**

| Severity Level... | is color coded... | and means that... |
|---|---|---|
| **Crit**ical | Red | a service-affecting condition has occurred and immediate corrective action is required |
| **Maj**or | Orange | the severity of the problem is relatively high and normal use of the object is likely to be impeded |
| **Min**or | Yellow | a problem of relatively low severity has occurred, which should not impede normal use of the object |
| **Warn**ing | Cyan | a potential or impending, service-affecting fault has occurred. Action should be taken to diagnose and correct the problem |
| **Norm**al | Green | message output is expected: for example, a process is starting or completing, or status information is displayed |
| **?** Unknown | Blue | the severity level cannot be determined |

**NOTE** The severity column of the `Message Browser` window provides a maximum of four characters to indicate a message's severity level. Table 5-2 on page 188 shows this abbreviated form in **bold, underlined** text.

**Figure 5-1 Message Attributes and Values**




The additional message attributes that appear in the `Message Browser` headline are shown in Figure 5-1 on page 189 and described in the following list:

**S** **Owned/Marked Message State**

A flag in this column indicates either that a user has taken note (Marked) or ownership (Owned) of a message or that the message is a **notification** message. The four types of flag that you may expect to find in this column indicate that a message is:

| | |
|---|---|
| **O** | owned by the user of the browser on view |
| **X** | owned (and therefore restricted in terms of access) by someone other than the user of the browser on view |
| **M** | marked by the user of the browser on view |
| **N** | a notification message |

Only ITO users can own or mark messages, and a message may only be disowned or unmarked by its owner or the administrator. For more information, see “Message Ownership” on page 191.

**U** **Unmatched Message**

An Unmatched Message does not match any of the filters defined for a message source. Filters are sets of conditions which configure ITO to accept or suppress messages. These messages require your special attention because they can represent problems for which no preconfigured action exists. In general, you should inform the ITO administrator of unmatched messages so that they can improve the corresponding message, or suppress conditions.

**I** **Help instructions**

Instructions help you resolve the problem. If available, these instructions are displayed in the `Message Details` window.

**A** **Automatic Action**

Indicates that an automatic action has been configured for the message, and gives the status of the action. The value of the attribute tells you if the action:

| | |
|---|---|
| **S** | was successful |
| **F** | has failed |
| **R** | is running |

**O** **Operator-initiated Action**

Indicates that an operator- initiated action has been configured for the message, and gives the status of the action. You start these actions after reviewing the message. The value of the attribute tells you if an action is:

| | |
|---|---|
| **X** | available |
| **S** | successful |
| **F** | failed |
| **R** | running |

**N** **Annotations**

Indicates if annotations exist for this message. You can review annotations for procedures used to resolve similar problems by using the `History Browser` window.

**E** **Escalations**

Indicates if the message has been escalated to (or from) another ITO server. The value of the attribute tells you the message has:

| | |
|---|---|
| **E** | been escalated *to* you *from* another server |
| **T** | been escalated *by* you *to* another server |

**Date** Specifies the date the message was received on the ITO management server.

**Time** Specifies the time the message was received on the ITO management server.

**Node** Specifies the node that issued the message.

**Application** Specifies the application that was affected by, or detected, the message.

**MsgGroup** Specifies the message group the message belongs to.

**Object** Specifies the object which was affected by, detected, or caused the message. This can be, for example, a printer which sent a message when it stopped accepting requests, or a backup device that sent a message when a backup stopped.

**Description** Displays the text of the message. You can review the message's original text in the `Original Message` window, accessible from the `Message Details` window.

## Message Ownership

The ITO message ownership feature allows the user to **mark** or **own** a message and, as a consequence, restrict access to it. Marking a message indicates that an operator or administrator has taken note of a message. Owning a message indicates that, depending on how the environment has been configured, an operator or administrator either wishes or has

been forced to take charge of a message in order to carry out actions associated with that message. In addition, ITO provides different ways to configure the way message ownership is displayed and enforced.

## Ownership Display Modes

There are two **ownership-display modes** in ITO:

- ❏ Status propagation
- ❏ No Status propagation (Default)

If the display mode is set to `No Status propagation`, a message's severity color changes when it is owned or marked. ITO uses the following default colors to indicate ownership:

**Pink** messages that are owned by you

**Beige** messages that are owned by someone else

In addition, a flag indicating ownership appears in the own-state column (S) in the `Message Browser` window, and the own-state color bar at the bottom of the `Message Browser` window reflects the new number of messages owned. In this display mode, the status of a message that is owned or marked is ignored for the purposes of status propagation in the `Managed Nodes`, operator `Message Group`, `Node Bank`, `Node Group Bank` and administrator's `Message Group Bank` windows, as well as the ITO Alarm symbol in the Node Submap.

If the ownership-display mode is set to `Status propagation`, then the status of all messages whether they are owned or not is used in reflecting status propagation in the related symbols of other submap windows. In this display mode, the only indication that the a message is owned is a flag in the own-state column in the `Message Browser` window.

For more information on which flags you might expect to find in the own-state column and what they mean, see "Understanding the Message Browser Headline" on page 187. For information on how to go about setting the ownership and ownership-display modes, see the *HP ITO Administrator's Guide to Online Information*.

## Message-ownership Modes

The administrator determines ownership policy by selecting one of the following default ownership modes allowed in ITO:

**Optional** The user has explicitly to take ownership of a message.

**Enforced** Ownership of messages is no longer optional: it is enforced.

**Informational** The concept of ownership is replaced with that of marking/unmarking. A “marked” message indicates that an operator has taken note of a message.

In **optional** mode, the owner of a message has exclusive read-write access to the message: all other users who have this message in their browser have only limited access to it. In optional mode, only the owner of a message may:

- ❏ perform operator-initiated actions related to a message
- ❏ escalate a message
- ❏ acknowledge a message; that is, move a message to the history database

In **enforced** ownership mode, an operator either chooses explicitly to take ownership of a message or, on attempting to perform operations on a message that is not owned by anybody, that message is assigned to him automatically. In **enforced** mode, ownership of a message will be assigned to the operator who attempts to:

- ❏ perform operator-initiated actions relating to a message
- ❏ escalate a message
- ❏ unacknowledge a message; that is, move a message from the history database to the active database

In **informational** mode, a **marked** message indicates that an operator has taken note of a message. Marking a message is purely for informational purposes: it does not restrict or alter operations on the message in the way that either optional or enforced mode does. An operator may only unmark messages he himself has marked.

## Template Groups

The template administrator uses the `Message Source Templates` window to add, modify, or delete templates and template groups. Table 5-3 on page 194 lists the default template groups provided with ITO and describes briefly what each does:

**Table 5-3 ITO Default Template Groups**

| Template Group | Description |
|---|---|
| **Default** | Default template groups delivered with ITO |
| **AIX** | Templates for AIX agent |
| **AIX with HACMP** | Templates for AIX agents running HACMP |
| **DYNIX/ptx** | Templates for DYNIX/ptx agent |
| **Digital UNIX** | Templates for Digital UNIX agent |
| **ECS Agent** | Event correlation templates for the ITO agent [a] |
| **ECS Management Server** | Event correlation templates for ITO management server [a] |
| **HP-UX 10.x** | Templates for HP-UX 10.x agent |
| **HP-UX 11.x** | Templates for HP-UX 11.x agent |
| **IBM OS/2** | Templates for IBM OS/2 agent |
| **IRIX** | Templates for SGI agent |
| **MC/ServiceGuard** | Templates for MC/ServiceGuard support |
| **MPE/iX** | Templates for MPE/iX agent |
| **Management Server** | Templates for the ITO Management Server |
| **NCR** | Templates for NCR agent |
| **Netware** | Templates for Netware agent |
| **Olivetti** | Templates for Olivetti agent |
| **PerfView** | Templates for Perfview integration |
| **Pyramid** | Templates for Pyramid agent |

| Template Group | Description |
|---|---|
| **SCO OpenServer** | Templates for SCO OpenServer agent |
| **SCO UnixWare** | Templates for SCO UnixWare agent |
| **SINIX 5.43** | Templates for SINIX 5.43 or earlier agent |
| **SINIX 5.44** | Templates for SINIX 5.44 or later agent |
| **SMS (Windows NT** | Templates for Windows NT Systems Management Server |
| **Solaris** | Templates for Solaris agent |
| **Windows NT** | Templates for Windows NT agent |

a. See Table 5-12 on page 236 for more information on supported platforms for ECS.

You can add, modify, or delete template groups with the `Message Source Templates` window in the ITO GUI.

## ITO Users

ITO provides a number of user configurations whose default settings may be used as a base that can be customized to match the requirements of individual organizations. The user configurations that come as standard are the:

- ITO administrator
- **opc_op** operator
- **netop** operator
- **itop** operator

To start the ITO GUI, enter the following command:

**opc**

Enter your user name and password in the `User Login` dialog box which subsequently appears. See Table 5-4, “ITO User Names and Passwords” for a list of default user names and passwords for all preconfigured users.

**Table 5-4 ITO User Names and Passwords**

| Default User | Default User Name | Default Password |
|---|---|---|
| ITO administrator | opc_adm | OpC_adm |
| Template Administrator | Configurable | Configurable |
| **opc_op** operator | opc_op | OpC_op |
| **netop** operator | netop | NeT_op |
| **itop** operator | itop | ItO_op |

In the interests of security, set up a new password using the `Change Password` window after logging in to ITO for the first time. The administrator can also use the `Modify User` window to change the password of each configured user.

On HP-UX systems running the HP VUE GUI, you can start the ITO GUI by opening the `System_Admin` folder in the `Application Manager` window and double-clicking the ITO GUI symbol. A short introduction to ITO is also available by clicking the ITO symbol in the `System_Info` folder of the general toolbox. On HP-UX systems running the HP CDE GUI, the ITO GUI icon is in the toplevel `Application Manager` window. For information describing how to bypass the login dialog box, see the `opc(1)` man page.

When a user starts an ITO operator GUI session, the working directory is defined by environment variable `$OPC_HOME` (if set) or `$HOME`. If neither `$OPC_HOME` nor `$HOME` is set, then `/tmp` is the default working directory. For more information on access to files and file permissions in ITO, see “File Access and Permissions” on page 451: for more information on common ITO variables, see “Variables” on page 291.

## The ITO Administrators

ITO supports only one ITO administrator, whose responsibility it is to set up and maintain the ITO software: multiple template administrators may be configured using the `Add User` window to manage message-source templates. The ITO administrator's login name, `opc_adm`, cannot be modified. Template administrators are set up by the ITO administrator in the GUI: their administrative responsibility is limited to template management.

## The ITO Operators

ITO provides three default operators which are preconfigured and have distinct areas of responsibility. The default operators are:

- opc_op
- netop
- itop

For more information on the scope of each default operator, see the *HP OpenView IT/Operations Concepts Guide*. The following tables show you at a glance which node groups, message groups, applications and application groups are assigned by default to each of the operators.

**Table 5-5 Default Node Groups for the ITO Operators**

| Node Group | opc_op | netop | itop |
|---|---|---|---|
| HP-UX | ✓ | | ✓ |
| Net Devices | | ✓ | ✓ |

**Table 5-6 Default Message Groups for the ITO Operators**

| Message Group | opc_op | netop | itop |
|---|---|---|---|
| Backup | ✓ | | ✓ |
| Databases | ✓ | | ✓ |
| Job | ✓ | | ✓ |
| Misc. | ✓ | | ✓ |
| Network | ✓ | ✓ | ✓ |

| Message Group | opc_op | netop | itop |
|---|---|---|---|
| OpC | ✓ | | ✓ |
| OS | ✓ | | ✓ |
| Output | ✓ | | ✓ |
| Performance | ✓ | | ✓ |
| SNMP | ✓ | ✓ | ✓ |
| Security | ✓ | | ✓ |

It is important to remember that although the various operators may have the same message group icon in their respective `Message Groups` window, the messages each operator receives and the nodes those messages come from are not necessarily the same: the responsibility matrix chosen by the administrator for a given operator determines which node group sends which messages to which operator.

For example, although, by default, all ITO operators have the `Network` message-group icon in their respective `Message Groups` window, the node groups that send messages associated with the `Network` message group vary according to the operator. The origin of the messages depends upon the selection the administrator makes in a given operator's responsibility matrix.

**Table 5-7 Default Application Groups for the ITO Operators**

| Application Groups | opc_op | netop | itop |
|---|---|---|---|
| Net. Activity | | ✓ | ✓ |
| Net. Config | | ✓ | ✓ |
| Net. Diag. | | | ✓ |
| NNM Tools | | | ✓ |
| NT Tools | | | ✓ |
| OV Services | | ✓ | ✓ |

| Application Groups | opc_op | netop | itop |
|---|---|---|---|
| SNMP Data | | ✓ | ✓ |
| Tools | | | ✓ |
| UN*X Tools | | | ✓ |

The applications and application groups assigned by default to the ITO users reflect the responsibility given to them by the administrator. Table 5-7 on page 198 and Table 5-8 on page 199 show you at a glance which applications and applications groups are assigned by default to each user. ITO allows you to add, delete, and move applications and application groups (as well as nodes, node groups, message groups and so on) by dragging and dropping or copying and pasting. In this way, the administrator can use the default settings as a base for configuring users and responsibilities that match the needs of individual environments.

**Table 5-8 Default Applications for the ITO Operators**

| Applications | opc_op | netop | itop |
|---|---|---|---|
| Broadcast | ✓ | | ✓ |
| Demand Poll | | ✓ | |
| Disk Space | ✓ | | |
| IP Map | | ✓ | ✓ |
| ITO Status | ✓ | | ✓ |
| Locate Route via SNMP | | ✓ | |
| MIB Browser | ✓ | ✓ | |
| Motif Sam | ✓ | | |
| Physical Terminal | ✓ | | ✓ |
| Ping | | ✓ | |
| Print Status | ✓ | | |
| Processes | ✓ | | |
| Remote Ping | | ✓ | |

| Applications | opc_op | netop | itop |
|---|---|---|---|
| Telnet (xterm) | | ✓ | |
| Test IP | | ✓ | |
| Virtual Terminal | ✓ | | ✓ |

## UNIX Access to the Managed Node for ITO Users

By default, the UNIX user cannot log into the managed node directly; this is the result of an asterisk (*) in the password field of `/etc/passwd`.

Access to ITO's Virtual Terminal application, and to other applications in the Application Desktop using the **Window (Input/Output)** option (see the `Add/Modify Application` window) only work if the user is allowed to log into the managed node on which the application is to be run. The following methods can be used to enable logins:

- Provide a *$HOME*`/.rhosts` entry on the managed node for every UNIX user from the management server. *$HOME* is the home directory of the executing user on the managed node.
- On the managed node, provide a `/etc/hosts.equiv` entry for the management server. This solution is preferable to the method above if you log in or run applications on the managed node as many different users.
- Set a password for the executing user on the managed node, if not yet done. Use this password in the corresponding ITO windows.

## Access to Windows NT Nodes for ITO Users

The UNIX user has only limited access to Windows NT managed nodes, most notably; via ITO's **virtual terminal** application. This application is a part of the Windows NT agent, and is not available unless the agent is running on the Windows NT node. The virtual terminal can be invoked from **ITO Application Group: NT Tools** by double clicking the appropriate icon. No password is required.

It is not possible to direct the Windows NT terminal's display to a UNIX terminal. Because of this, access via the virtual terminal is restricted to command-line actions. Any programs that invoke a graphical user interface cannot be used.

# Applications

ITO provides the following applications and application groups in the administrator's default `Application Bank` window:

**Table 5-9 Administrator's Applications and Application Groups**

| Name | Application | Application Group |
|---|---|---|
| Broadcast | ✓ | |
| ITO Status | ✓ | |
| Jovw | | ✓ |
| MPE Tools | | ✓ |
| Net Activity | | ✓ |
| Net Config | | ✓ |
| Net Diag | | ✓ |
| NetWare Config | | ✓ |
| NetWare Performance | | ✓ |
| NetWare Tools | | ✓ |
| NNM Tools | | ✓ |
| NT Tools | | ✓ |
| OS/2 Tools | | ✓ |
| OV Services | | ✓ |
| Performance | ✓ | |
| Physical Terminal | ✓ | |
| Reports | | ✓ |
| SNMP Data | ✓ | |

| Name | Application | Application Group |
|---|---|---|
| Tools | | ✓ |
| UN*X Tools | | ✓ |
| Virtual Terminal | ✓ | |

## Broadcast

Broadcast is an ITO application that allows you to issue the same command on multiple systems in parallel.

- **UNIX**:

  Default user: **opc_op**.

  Default password: none required, because application is started via the ITO action agent.

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

- **MPE/iX**:

  Default user: **MGR.OVOPR**.

  Default password: none required, because application is started via the ITO action agent.

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

- **Windows NT**:

  Default user: **opc_op**.

  Default password: none required, because application is started via the ITO action agent.

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

### Disk Space

ITO shows the current disk usage:

- **UNIX**:

  Command issued: **`opcdf`**

  (This is a script calling `bdf` on HP-UX, and `df` on Solaris, AIX, NCR UNIX SVR4, SGI IRIX, SCO OpenServer, SCO UnixWare, Digital UNIX (OSF/1), DYNIX/ptx, Olivetti UNIX, Pyramid DataCenter/OSx, and SINIX/Reliant.)

  Default user: **`opc_op`**.

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

- **MPE/iX**:

  Command issued: **`discfree d`**

  Default user: **MGR.OVOPR**.

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

- **Windows NT**

  Returns information about all drives on the system, including floppy drives, CD-ROM drives, and network drives

  Default user: **HP ITO account**.

### ITO Agent Status

ITO Agent Status shows the status of the ITO agent on a selected system. This command runs on the management server.

Run the command:

**`/opt/OV/bin/OpC/opcragt -status $OPC_NODES`**

Default user: **root** (user must be **root**)

Default password: none required, because application is started via the ITO action agent.

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

### Jovw Applications

This group contains the following applications:

- Highlight in IP Map

  Starts jovw with the submap of the selected node.

- Jovw

  Starts jovw to get network view.

- OVlaunch

  With the `ovlaunch` command you can start the JMib Browser and Jovw.

### MIB Browser

This is `xnmbrowser`, the standard HP OpenView MIB Browser.

### OV Services and OV Applications

Depending upon the integration mechanism of HP OpenView applications, ITO logically distinguishes between **OV Services** and **OV Applications**. OV Services are not accessed by double-clicking their symbols, they are accessed from the menu bar. Some OV Services only start daemons. The administrator can see OV Service symbols in his `Application Bank` window. These can be copied to the operators' `Application Desktop` window, as required. For complete coverage of this topic, see the HP ITO Administrator's Guide to Online Information.

Double-clicking the HP OpenView symbol "OV Services" in the `Application Bank` window displays the following underlying OV Service symbols:

- IP Map
- MIB Grapher
- MIB Loader
- Topology Status Polling
- Demand Poll

NOTE **OV Services** and **OV Applications** are always started as user **opc_op**.

### PerfView

Double-clicking the `Performance` symbol in the `Application Bank` window displays the following underlying symbols:

- Start Glance
- Start PerfView

### Physical Terminal

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

- **UNIX**:

  Default user: **root**.

  Default password: none configured.

- **MPE/iX**:

  Default user: MANAGER.SYS.

  Default password: none configured.

- **Windows NT**

  Default user: administrator

  Default Password: none configured

### Print Status

Print Status shows the current status of spooling systems:

- **UNIX**:

  Command issued: **`lpstat -t`**

  Default user: **opc_op**.

  Default password: none required, because application is started via the ITO action agent.

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

- **MPE/iX**:

  Command issued: **`listspf`**

  Default user: **MGR.OVOPR**.

  Default password: none required, because application is started via the ITO action agent.

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

- **Windows NT**

  Print status is unavailable for Windows NT managed nodes.

### Processes (UNIX and MPE/iX)

ITO displays the status of the running processes:

- **UNIX**:

  Command issued: **`opcps`**

  (This is a script calling **`ps -eaf`** on HP-UX, AIX, Solaris, NCR UNIX SVR4, SGI IRIX, SCO OpenServer, SCO UnixWare, Digital UNIX (OSF/1), DYNIX/ptx, Olivetti UNIX, Pyramid DataCenter/OSx, and SINIX/Reliant.)

  Default user: **`opc_op`**.

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

- **MPE/iX**:

  Command issued: **`showproc; pin=1;system;tree`**

  Default user: **MANAGER.SYS**, because **`showproc`** requires SM capability.

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

- **Windows NT**

Command issued: **`itodiag.exe /processes`**

Default user: **HP ITO account**.

## Reports for the ITO Operators

This group contains the following reports that can be started as an application by the ITO operators:

- ❏ Active Message
- ❏ All Active Details
- ❏ All Active Messages
- ❏ All History Messages
- ❏ All Pending Messages
- ❏ History Message
- ❏ OpC Error Report
- ❏ Pending Message

## System Administration Manager (SAM) — Motif and ASCII (HP-UX)

ITO can start the ASCII or Motif version of the SAM user interface on HP-UX systems. Note that the Motif interface is only available on HP-UX versions 9.0 and higher.

- ❏ **Motif SAM**

  Command issued: **`sam`**

  Default user: **root** (user must be **root**!)

  Default password: none required, because application is started via the ITO action agent.

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

- ❏ **ASCII SAM**

  Command issued: **`sam`**

  Default user: **root** (user must be **root**!)

  Default password: none configured.

Start in window (input/output)

### System Management Interface Tool (SMIT) (AIX)

ITO can start the SMIT (System Management Interface Tool) Xuser interface on AIX systems.

Command issued: **`smit`**

Default user: **`root`** (user must be **`root`**!)

Default password: none required, because application is started via the ITO action agent.

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

### Virtual Terminal and Applications Configured to Use Window (Input/Output)

For a virtual terminal connection to UNIX systems, ITO uses `rlogin` for remote login.

**NOTE** Make sure that the `rlogind` has *not* been configured with the `-B` (for banner file) option in the `inetd.conf` file; this causes problems with the remote login procedure for Window (Input/Output) applications.

If an `.rhosts` (or `/etc/hosts.equiv`) entry is available for the specified user, or if the default or configured password fits, a remote login is performed. For a more detailed explanation, see “UNIX Access to the Managed Node for ITO Users” on page 200.

Default user: **`opc_op`**

Default password: none configured

For a virtual terminal connection to MPE/iX systems, ITO 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 “ARPA-to-NS Node-Name Mapping for MPE/iX” on page 128.

Default user: **MGR.OVOPR**

**NOTE** IBM OS/2 telnet does not require a user name, only the password associated with a given user name. To use virtual terminal, click: `Customized startup`, and enter the password along with a dummy user name.

Refer to “Virtual Terminal PC” on page 225 for information about a Virtual Terminal on a Windows NT managed node.

# Windows NT Applications (Intel & DEC Alpha-based)

This section lists and defines the default applications in the `Windows NT 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 NT applications can be customized for your particular situation and requirements.

## Cancel Reboot

This application will cancel a system reboot command that was issued from the ITO reboot application for the selected Windows NT node.

Default: **`itosdown.exe /a`**

#### Description of Values Returned

See “Reboot” on page 216.

## Diagnostics

This application collects general diagnostic information for the selected Windows NT node.

Default: **`itodiag.exe`** (returns all information listed below)

#### User Configurable Parameters:

**`osversion`** Returns operating system information.

**`hardware`** Returns hardware information.:

- Processor type 386, 486, 586 (Pentium), x686 (Pentium Pro), DEC Alpha
- number of processes in the system

**memory** Returns the following memory information:

- Total paging-file size (NT swap file)
- Available paging-file
- physical location of the page file and its limits (minimum, maximum)

**network** Returns network information.

**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:<br>REMOVABLE (i.e., a floppy drive) REMOTE (i.e., a network connection) FIXED (i.e., a local hard drive) CD-ROM (i.e., a CD disk drive) |
| **FILE SYSTEM** | Returns one of these file system types:<br>NTFS NTFAT DOS HPFS OS/2 |
| **TOTAL** | Returns the total size of the drive in Megabytes. |
| **FREE** | N/A will be reported for the name, File system, and total and free space, if the drive is not fixed and the disk is currently inserted (floppy drive or CD- ROM) or if there is a network connection that requires a password (which is case for administrator connections C$, D$ etc.). |

**processes** Returns the following process information:

- ID
- Name

- Priority (higher number -> 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 which 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 NT service layer, the Executive routines, and the Windows NT 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 NT IP Configuration. This consists of the:

- Ethernet adapter card name
- IP Address
- Subnet Mask
- Default Gateway

**Description of Values Returned:**

Refer to the User Configurable Parameters for this application.

## ITO Install Log

This application returns the contents of the ITO installation log from the selected Windows NT node.

Default: `cmd.exe /c "type c:\temp\inst.log"`

**User Configurable Parameters:**

None.

## Installed Software

This application returns the names of the software that has been entered in the registry on the selected Windows NT node. Only software that has created a subtree in the registry will be listed. This will only include Windows NT software. Older software (e.g., Windows 3.1) will not be shown.

This function returns all the subtrees from the registry "local machine" under the key "Software". All software written for Windows NT will create a subkey under "Software" to store external parameters. The itoreg.cfg file is used to filter out unwanted information. See "Reg Viewer" on page 217, for a sample `itoreg.cfg` file.

Default: `itoreg.exe /enum 3 /key Software /initkey lm`

**User Configurable Parameters:**

| | |
|---|---|
| `/enum X` | Returns the subtrees from the specified key. Information will be printed out to the depth specified by X. |
| `/key <NAME>` | Defines the starting point of the subtree to be processed |
| `/initkey` | Defines which registry hive to search for <key>. |

**NOTE** For a full description of the NT registry refer to the Windows NT documentation.

#### Description of Values Returned:

Refer to the User Configurable Parameters for this application, and to the Windows NT documentation.

### 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`" will be 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, refer to the Windows NT documentation.

### LM Sessions

This application lists sessions between the selected Windows NT node and other computers on the network. If the selected system is acting as a logon server, it will show sessions of the users for which it has validated logons. 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`, refer to the Windows NT 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 NT 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. |

## Local Users

This application prints the name of the user who is locally logged onto the selected Windows NT node. If you need more information about the users and sessions, use the Show Users application.

Default: **itouser.exe /local**

#### User Configurable Parameters:

See “Show Users” on page 223.

#### Description of Values Returned:

See “Show Users” on page 223

## Memory Load

This application returns information about the current memory usage of the selected Windows NT node. If you need more information about the Windows NT node, use the Diagnostics application.

Default: **itodiag.exe /memory**

#### User Configurable Parameters:

See“Diagnostics” on page 209.

#### Description of Values Returned:

See “Diagnostics” on page 209.

## NetBios Sessions

This application displays protocol statistics and current TCP/IP connections using NBT (NetBIOS over TCP/IP) for the selected Windows NT node.

Default: **nbstat.exe -s $OPC_NODE**

#### User Configurable Parameters:

For a full description of `nbstat.exe`, refer to the Windows NT documentation.

## PerfMon Objs

This application returns all of the performance objects that are defined on the selected Windows NT node. A non-English NT installation will return 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 NT systems easier.

Default: **`opcprfls.exe`**

**User Configurable Parameters:**

| | |
|---|---|
| **`/a`** | Returns all the performance monitor objects found on the system (this setting is default). |
| **`/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`** | Returns a maximum of ten instances, if more are defined it will print out the message "`MULTIPLE INSTANCES, TOO MANY TO LIST`" (this setting is default). |
| **`/f`** | Returns full list, will print 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. On a German NT system for example, 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 ITO agent can monitor any of the performance objects in either US English or the local language, but US English will be valid on all NT machines, regardless of the local language.

**Description of Values Returned:**

Refer to the User Configurable Parameters for this application.

## Process Kill

This application kills all processes that are running under the configured name on the Selected Windows NT node. If the user does not have the rights to kill the process, an error will be 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. (As this function uses the registry to get all the process names, it does not show the .exe after executable files— this information is not stored in the registry.) |

**NOTE** Under NT, a user with administrator rights can kill any process, but normal users can only kill processes that are running under their account name. If you want the ITO operator to be able to kill any process, configure the application to run under HP ITO account.

**Description of Values Returned:**

Refer to the User Configurable Parameters for this application.

## Reboot

This application will shutdown and reboot the selected Windows NT nodes.

Default: **`itosdown.exe /t 120 /r /w`**

**User Configurable Parameters:**

| | |
|---|---|
| **`/m <msg>`** | Returns shutdown <msg> in a pop-up window on the node. |
| /**`t <sec>`** | Specifies the delay (in seconds) before the system shutdown occurs. |
| /**`a`** | Aborts an ITO initiated system shutdown. |

| | |
|---|---|
| **/r** | Automatic reboot after shutdown. If this option is not set, the system will only shutdown, but can only be restarted manually. |
| **/f** | Force system shutdown. Processes are not allowed to delay the shutdown for local user interaction (e.g., to ask if 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 this occurs, the management server will receive an error message. |

**Description of Values Returned:**

Refer to the User Configurable Parameters for this application.

## Reg Viewer

This application returns the values and subkeys for the define key of the Selected Windows NT node. Example:

To view the ITO Agent configuration, modify the application to use:

```
/enum 1 /initkey LM /key Software\Hewlett-Packard\OpenView\ITO
```

Default: None, this application requires an entry from the table below.

**User Configurable Parameters:**

**Table 5-10 Registry Viewer Application Options**

| |
|---|
| To view a key/value:<br>**/view /initkey lm\|cu\|cr\|us /key <path> [/valuename <name>]** |
| To set a key or value:<br>**/set /initkey lm\|cu\|cr\|us /key <path> [/valuename <name> /value <value>/type REG_SZ\|REG_DWORD]** |
| To delete a key or value:<br>**/delete /initkey lm\|cu\|cr\|us /key <path> [/valuename <name>] [/force] [/set]** |

| |
|---|
| To scan registry for pattern:<br>**`/scan <pattern> /initkey lm\|cu\|cr\|us /key <path> [/view]`** |
| To enumerate a registry tree (thereby printing out registry keys to the set depth: emum uses a config file that verifies keys that should not be processed):<br>**`/enum <depth> /initkey lm\|cu\|cr\|us /key <path> [/view]`** |
| To execute a registration script: **`/file <filename> /initkey lm\|cu\|cr\|us`** |

**`/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 a entry type (REG_DWORD | REG_SZ).

**`valuename <name>`** Define 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;

}
```

## Server Config

This application displays settings for the Server service for the selected Windows NT node.

Default: **`net.exe config server`**

#### User Configurable Parameters:

For a full description of `net.exe`, refer to the Windows NT documentation.

#### Description of Values Returned:

| | |
|---|---|
| **`Server Name`** | The name of the server |
| **`Comment`** | Comment for the server that is displayed in Windows NT Screens and with the NET VIEW command |
| **`Software version`** | Version number. |
| **`Server is active on`** | The network connections that the server is using. |
| **`Server hidden`** | Specifies whether the server's computer name appears on display listings of servers. Note that hiding a server does not alter the permissions on that server. |
| **`Maximum Logged On Users`** | Maximum open files per session. |

## Server Stats

This application displays in-depth statistics about the Server service for the selected Windows NT node.

Default: **`net.exe statistics server`**

#### User Configurable Parameters:

For a full description of `net.exe`, refer to the Windows NT documentation.

#### Description of Values Returned:

For a full description of `net.exe` refer to the Windows NT documentation.

## Shares

This application lists the external connections that are available on the selected Windows NT node. All shares ending with **$** are hidden shares that the NT system makes available for remote administration by default.

Default: **`net.exe share`**

#### User Configurable Parameters:

None.

#### Description of Values Returned:

**`Share name`** The full name of the available netbios share.

**`Resource`** The location of the share on the local machine.

**`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`** The share for default IPC's.
- **`Remote Admin`** The share to the local windows NT system location.

## Show Drivers

This application lists all drivers that are present on the selected Windows NT node.

Default: **`itomserv.exe /list d`**

**User Configurable Parameters: see**

"Show Services" on page 221

**Description of Values Returned:**

| | |
|---|---|
| **`NAME`** | True name of the service. If you wish to perform actions on the service, this is the name that should be used. |
| **`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, **`Started`** (i.e., Running), **`Paused`**, or **`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. |

## Show Services

This application returns a list of the services that are configured on the selected Windows NT system. If the ITO user does not have the rights to obtain information about a service, "NA" will be 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> |

| | | |
|---|---|---|
| **/list s \| d \| a** | | Print a list of installed services: |
| | **s** | List all NT system services. |
| | **d** | List all NT device drivers. |
| | **a** | List all installed services. |
| **/e** | | Set the exit status to a numerical value:<br><br>0 = RUNNING<br>1 = NOT RUNNING<br>2 = START_PENDING<br>3 = STOP_PENDING<br>4 = CONTINUE_PENDING<br>5 = PAUSE_PENDING<br>6 = PAUSED |

**NOTE** Although the **/e** parameter is not useful from the 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** | | The name that is normally displayed to the user. |
| **Status** | | The status of a service can be Started, Paused, or 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. |

## Show Users

This application displays information about local users and sessions on the selected Windows NT Node.

Default: `itouser.exe /u`

#### User Configurable Parameters:

| | |
|---|---|
| `/u` | Returns user information for the system. This includes the name of the current user, the domain this user is logged into, and the server that validated the log-on. |
| `/s` | Returns full session information for the system. This includes system name, net BIOS name, current local user name, type of the client, the number of open sessions and the 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:

Refer to the User Configurable Parameters for this application.

## Start Services

This application will start the requested service on the selected Windows NT 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 machine.

Default: `itomserv.exe /start <service name>`

#### User Configurable Parameters:

"Show Services" on page 221.

## Stop Services

This application stops the requested service. Since administrative rights are required to stop and start Windows NT services, the user must be defined as HP ITO Account, and not opc_op.

Default: `itomserv.exe / stop <service name>`

User Configurable Parameters: see “Show Services” on page 221

## TCP/IP Status

This application displays protocol statistics and current active TCP/IPnetwork connections for the selected Windows NT node

Default: **`netstat.exe`**

User Configurable Parameters: Refer to the Windows NT documentation.

#### Description of Values Returned:

| | |
|---|---|
| **`Proto`** | The protocol that is used for the connection. |
| **`Local Address`** | The local machine name and port number. |
| **`Foreign Address`** | The full name of machine that it is connected to plus the port number (the port number can also be **`nbsession`**, which is a netbois connection over TCP/IP). |
| **`State`** | The current state of the connection. |

## Used Shares

This application returns a list of connections that the selected Windows NT 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` refer to the Windows NT documentation.

#### Description of Values Returned:

| | |
|---|---|
| `Status` | The state of the connection (e.g., `OK, Disconnected` means that the drive connection is defined but not connected). |
| **`Local`** | The local drive letter that is used to access the connection. |
| **`Remoted`** | The name of the machine and the share that is used. |

**Network** The type of network that is providing the connection, (e.g., Microsoft Windows Network, or 3rd party NFS software).

### Virtual Terminal PC

This application opens a terminal with command-line capabilities to the target Windows NT system. All output is redirected to the Virtual Terminal on the management server.

Default: **opcvterm.exe**

#### User Configurable Parameters:

None

### Workst Stats

This application displays in-depth statistics about the workstation service for the selected Windows NT node.

Default: **net.exe statistics workstation**

#### User Configurable Parameters:

For a full description of `net.exe`, refer to the Windows NT documentation.

#### Description of Values Returned:

For a full description of `net.exe`, refer to the Windows NT documentation.

## Novell NetWare Applications

This section lists and defines the default applications in the `NetWare Tools`, `NetWare Config` and `NetWare Performance` application groups.

ITO for NetWare can manage any NetWare server that is running the NetWare Management Agent (NMA). You must install the NMA on each server you want to manage.

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 and network interfaces, disks and disk controllers, volumes, queues, users, connections, open files, and installed software.

For print servers, NMA 2.1 or later provides additional queue information that is not available for servers running the older version of NMA.

## NMA 2.1 Agent

The NMA provides real-time server performance data about the NetWare server alarms that can either be sent to the network and system management consoles or be locally processed by the ITO agent and then forwarded to the ITO 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 ITO console or Novell ManageWise console. The NetWare agent NLMs are:

- `NWTRAP.NLM` - 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 are supported by NMA including all 3.x and 4.x NetWare servers, SFT III servers, SMP servers, and Mirrored Servers. These agents are all provided and supported by Novell and can be purchased as a separate Part No. from the Novell ManageWise console.

## Performance Monitoring

Novell NMA 2.1 Agent NLMs enable you to monitor performance statistics such as CPU utilization, 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 ITO agent via SNMP traps.

NMA monitoring is enabled by configuring the NMA configuration files `NWTREND.INI` and `TRAPTARG.CFG` on the NetWare server. Configuration of these files is not part of the ITO configuration and distribution framework.

In addition to the monitors provided by NMA, ITO users can also create their own ITO templates to monitor any integer MIB variables supported by NMA. This allows ITO users to monitor NetWare server variables not monitored internally by the NMA.

### NetWare Config

The following application icons are available by default in the `NetWare Config` window:

- Down & Reboot
- Down & Restart

**NOTE** Down & Reboot and Down & Restart cannot be started on NetWare SFT III systems.

- Restart NMA

The user opc_op can execute these application on the NetWare server.

### NetWare Performance

The following application icons are available by default in the `NetWare Performance` window:

- 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.

### NetWare Tools

The following application icons are available by default in `NetWare Tools` window. The user opc_op can execute all of these applications on the NetWare server except the Xconsole application, which is only used to run a NetWare console in an X window on the ITO console.

**NOTE**

Note that on NetWare SFT III systems starting applications of the application group NetWare Tools 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.

**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 the Users action is the Connection action's emphasis on data relating specifically to connections. This 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 and allows you to determine whether or not 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 (TM) 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 (copies its content to standard output - similar to the UNIX `cat` command):

Default: **`showfile <file_name>`**

Please note that these applications must be started via the customized-startup application so that additional parameters such as the name of an NLM can be entered.

**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 an NLM:

Default: **`itoload <nlm_name>`**

Unloads an NLM:

Default: **`itounload <nlm_name>`**

Starting arbitrary NLMs is supported via the `itoload` and `itounload` commands. These applications must be started via a customized start-up so that additional parameters can be entered.

**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) - NetWare 4.0 or later
- ❏ Permanent Memory Pool (KB) - 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 ITO 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 which require an additional parameter <server_name>, enter the name of the NetWare server where the actions are being executed.

The NMA actions are described below. Note that 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 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, server up-time, OS description

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's server disk storage space is divided into volumes. "Volume" 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 the disks, and which users are 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 which 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 and is only present in the ITO database as a warning that the password for the remote console access may be different to the user opc_op's password.

## OS/2 Applications

Table 5-11, "OS/2 Applications," on page 233 lists and defines the default applications in the `OS/2 Applications` window in the `ITO Application Bank`.

**Table 5-11 OS/2 Applications**

| Application | Command | Description |
|---|---|---|
| Check Filesystem | `CHKDSK.EXE` | OS/2 native command |
| Repair Filesystem | `CHKDSK.EXE` | OS/2 native command |
| Reboot Node | `os2boot.exe` | Reboots the OS/2 system; requires OS/2 native utility setboot.exe. |

| Application | Command | Description |
|---|---|---|
| List running processes | `opcps.cmd` | Displays the status of processes and their threads running on OS/2 managed node. Uses OS/2 native utility PSTAT.EXE. |
| List mounted drives | `opcdrive.cmd` | Displays drives (and types) mounted on an OS/2 managed node. |
| Display Free Space | `opcfree.cmd` | Displays free space, as well as percentage of utilization, of both local and network drives mounted on an OS/2 managed node. |

## ITO Control Agent Application on OS/2 Managed Nodes

The ITO control agent on OS/2 managed nodes is a Presentation Manager application which displays a window that lets you start, stop, query the status of, and kill the ITO agents. There is no command line interface available for the ITO control agent.

**NOTE**

Only the kill operation stops *all* ITO agent processes. The stop operation stops all agent processes except for the ITO message agent and the ITO control agent.

## Actions and Programs on OS/2 Managed Nodes

The ITO action agent on OS/2 managed nodes can execute all those programs the shell (`CMD.EXE`) can execute, as well as actions encapsulated in DLLs (Dynamic-link Library). For example, frequently used monitoring actions for OS/2 managed nodes reside in the DLL `opcvend.dll`. This configuration improves performance because actions are executed very quickly once the DLL is loaded into active memory. The notation for calling DLL-encapsulated actions is:

<*name_of_DLL*>-><*name_of_entry_function*>

See the templates `os2_swap_util` or `os2_disk_util` for examples.

The default configuration for loading and unloading DLLs can be changed by adding the following parameters to the `\opt\OV\bin\OpC\install\opcinfo` file on the OS/2 managed node:

- `OPC_OS2_MAX_NBR_LOADED_DLLS`

  Specifies the maximum number of DLL that can be loaded simultaneously. The default value is 10 and should be sufficient for most installations.

- `OPC_OS2_EXTERN_DLL_TIMEOUT`

  Specifies the timeout in seconds after which an unused DLL is unloaded. The default is 180 seconds (3 minutes). If this parameter is set to 0, the DLL is never unloaded. This is not recommended because while a DLL is loaded in active memory, new versions cannot be distributed from the management server. If frequent distributions are required, it is recommended that the value of this parameter is set to a value lower than 10 seconds.

### User-supplied REXX Scripts on OS/2 Managed Nodes

REXX is the default scripting language in OS/2. REXX scripts can, for example, be used as external monitors or as actions. Note that REXX command must be delimited by a semicolon or by a CR/LF. If user-supplied scripts do not conform to these rules, the actions are not executed successfully.

The ITO action agent does not exit until all running actions have completed. Therefore, REXX scripts or executables must not run in an endless loop. Use the option `DETACH` if an endless script or executable is required. `DETACH` places a program in the background and returns the command to the script immediately.

## Event Correlation

ITO' event-correlation runtime engine is available for both the ITO management server and the ITO agent and currently runs on the platforms listed in Table 5-12. For more information on the concepts behind event correlation as well as the way it works in ITO, see the *HP OpenView IT/Operations Concepts Guide*. For help in setting up event correlation in ITO, see the section on tasks in the HP ITO Administrator's Guide to Online Information.

**Table 5-12 ITO Event-correlation Runtime: Supported Platforms**

| Platform | ITO Management Server | ITO Agent |
|---|---|---|
| HP-UX 10.x | ✓ | ✓ |
| HP-UX 11.x | ✓ | ✓ |
| Solaris: 2.51, 2.6, 7 | | ✓ |
| Windows NT: 3.51, 4.0 | | ✓ |

## Logfile Encapsulation

For detailed information about encapsulated logfiles, refer to the appropriate template in the ITO GUI. Note that the 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.

**Table 5-13 Encapsulated Logfiles on AIX Managed Nodes**

| Logfile | Description | Template Name |
|---|---|---|
| `/var/adm/aix_sulog` | Switch user logfile. | Su (AIX) |
| `/var/adm/audit log` | Auditing information logfile | Audit Log (AIX) |
| `/tmp/syslog` [a] | Syslog daemon logfile | Syslog (AIX) |
| `/etc/security/failed login` (binary format) | History of AIX failed logins | Bad logs (AIX) |
| `/var/adm/wtmp` (binary format) | History of logins, logouts and data changes | Logins (AIX) |
| `/var/adm/ras/errors` (binary format) | Messages generated by the AIX kernel | Kernel Logs (AIX) |

a. Refer to `/etc/syslog.conf` to determine or to set the actual syslog logfile name and the events to be logged.

**Table 5-14 Encapsulated Logfiles on AIX HACMP Managed Nodes**

| Logfile | Description | Template Name |
|---|---|---|
| /var/adm/cluster.log | HACMP cluster logs | HACMP logfile (AIX) |

**Table 5-15 Encapsulated Logfiles on Digital UNIX Managed Nodes**

| Logfile | Description | Template Name |
|---|---|---|
| /var/adm/cron/log | Cron logfile | Cron (Digital UNIX) |
| /var/adm/messages [a] | OS messages | OS Msgs (Digital UNIX) |
| /usr/adm/sialog [b] | SIA logfile | SIA (Digital UNIX) |
| /var/adm/wtmp | History of logins | Logs (Digital UNIX) |
| /usr/adm/lplog [c] | Line printer daemon logfile | Lplog (Digital UNIX) |

a. /var/adm/messages must be present in the /etc/syslog.conf file.
b. If /var/adm/sialog is not present, add it using: **touch /var/adm/sialog**
c. /var/adm/lplog must be present in /etc/syslog.conf file

Before editing syslog.conf on your Digital UNIX system, please read the man page syslog.conf(1M). If /var/adm/messages is *not* already included in syslog.conf, add the following line using tabs, *not* spaces:

```
kern.debug      /var/adm/messages
```

After editing the /etc/syslog.conf file, create the file /var/adm/messages (for example, using the touch command) with the following ownership and permission:

```
-rw-r-----   1 root     adm messages
```

Then restart the syslogd process.

**Table 5-16 Encapsulated Logfiles on HP-UX 10.x Managed Nodes**

| Logfile | Description | Template Name |
|---|---|---|
| `/var/adm/sulog` | `su(1)`; Switch user logfile | Su (10.x HP-UX) |
| `/var/adm/cron/log` | `cron(1M)`; Clock daemon logfile | Cron (10.x HP-UX) |
| `/var/adm/syslog /syslog.log` | `syslogd(1M)`; Syslog daemon logfile | Syslog (10.x HP-UX) |
| `/etc/rc.log` | Messages during system boot up | Boot (10.x HP-UX) |
| `/var/adm/btmp` (binary format) | History of bad login attempts | Bad Logs (10.x HP-UX) |
| `/var/adm/wtmp` (binary format) | History of logins, logouts, and data changes | Logins (10.x HP-UX) |
| `/var/opt/OV/log/OpC/ dmesg.out` | Messages generated by the HP- UX 10.x kernel | Kernel Logs (10.x HP-UX) [a] |
| `/var/adm/ syslog/mail.log` | `sendmail(1)` logfile | Mailqueue (10.x HP-UX) |

a. For this template to work, you must first start the ITO Kernel Message Logger (`opckmsg`). This is most easily done by adding the command **`/opt/OV/bin/OpC/opckmsg`** to the system boot file. A corresponding entry is provided (commented with "#") by installing ITO on HP-UX 10.x managed nodes. You therefore only need to delete the comment sign ("#") from the line "# `start_opckmsg`", for the template to work.

**Table 5-17 Encapsulated Logfiles on NCR UNIX SVR4 Managed Nodes**

| Logfile | Description | Template Name |
|---|---|---|
| /var/adm/loginlog | History of NCR UNIX SVR4 failed logins | Bad Logs (NCR UNIX SVR4) |
| /var/cron/log | Cron logfile | Cron (NCR UNIX SVR4) |
| /etc/.osm | NCR GIS (NCR) UNIX OS messages | OS Msgs (NCR UNIX SVR4) |
| /var/adm/sulog | Switch user logfile | Su (NCR UNIX SVR4) |
| /var/adm/wtmpx | History of logins | Logs (NCR UNIX SVR4) |

**Table 5-18 Encapsulated Logfiles on Olivetti UNIX Managed Nodes**

| Logfile | Description | Template Name |
|---|---|---|
| /var/cron/log | Cron logfile | Cron (Olivetti UNIX) |
| /var/adm/messages [a] | Olivetti OS messages | OS Msgs (Olivetti UNIX) |
| /var/adm/sulog | Switch user logfile | Su (Olivetti UNIX) |
| /var/adm/wtmpx | History of logins | Logs (Olivetti UNIX) |
| /var/lp/logs/lpsched | Printer services logfile | Lp Serv (Olivetti UNIX) |
| /var/lp/logs/requests | Printer Requests logfile | Lp Req (Olivetti UNIX) |

a. You must manually create the /var/adm/messages in the /etc/syslog.conf file.

**Table 5-19 Encapsulated Logfiles on Pyramid DataCenter/OSx Managed Nodes**

| Logfile | Description | Template Name |
|---|---|---|
| /var/cron/log | Cron logfile | Cron (PYRAMID) |
| /etc/.osm | Pyramid OS messages | OS Msgs (PYRAMID) |
| /var/adm/sulog | Switch user logfile | Su (PYRAMID) |
| /var/adm/wtmpx | History of logins | Logins (PYRAMID) |
| /var/adm/badlog | History of bad logins | Bad Logs (PYRAMID) |
| /usr/spool/lp/logs/lpsched | Line printer deamon logfile | Lp Serv (PYRAMID) |
| /usr/spool/lp/logs/requests | Printer requests logfile | Lp Req (PYRAMID) |

**Table 5-20 Encapsulated Logfiles on SCO OpenServer Managed Nodes**

| Logfile | Description | Template Name |
|---|---|---|
| /usr/lib/cron/log | Cron logfile | Cron (SCO OpenServer) |
| /usr/adm/messages | OS messages | OS Msgs (SCO OpenServer) |
| /usr/adm/sulog | Switch user logfile | Su (SCO OpenServer) |
| /etc/wtmp | History of logins | Logs (SCO OpenServer) |
| /usr/adm/syslog | Syslog daemon logfile | Syslog (SCO OpenServer) |
| /usr/spool/lp/logs/lpsched | Printer services logfile | Lp Serv (SCO OpenServer) |
| /usr/spool/lp/logs/requests | Printer requests logfile | Lp Req (SCO OpenServer) |

**Table 5-21 Encapsulated Logfiles on SCO UnixWare Managed Nodes**

| Logfile | Description | Template Name |
|---|---|---|
| /var/cron/log | Cron logfile | Cron (UnixWare) |
| /var/adm/messages[a] | OS messages | OS Msgs (UnixWare) |
| /var/adm/sulog | Switch user logfile | Su (UnixWare) |
| /var/adm/wtmpx | History of logins | Logs (UnixWare) |
| /var/lp/logs/lpsched | Printer services Logfile | Lp Serv (UnixWare) |
| /var/lp/logs/requests | Printer Requests Logfile | Lp Req (UnixWare) |

a. Requires the logfile /var/adm/messages in the file /etc/syslog.conf

**Table 5-22 Encapsulated Logfiles on SGI IRIX Managed Nodes**

| Logfile | Description | Template Name |
|---|---|---|
| /var/adm/loginlog | History of failed login attempts | Bad Logs (IRIX) |
| /var/cron/log | Cron logfile | Cron (IRIX) |
| /var/adm/sulog | Switch user logfile | Su (IRIX) |
| /var/adm/SYSLOG[a] | Syslog daemon logfile | Syslog (IRIX) |
| /var/adm/wtmpx | History of logins | Logins (IRIX) |

a. requires the logfile /var/adm/SYSLOG in the file /etc/syslog.conf

**Table 5-23 Encapsulated Logfiles on Sequent DYNIX/ptx Managed Nodes**

| Logfile | Description | Template Name |
|---|---|---|
| /usr/lib/cron | Cron logfile | Cron (DYNIX/ptx) |
| /usr/adm/messages | OS messages | OS Msgs (DYNIX/ptx) |
| /usr/adm/sulog | Switch user logfile | Su (DYNIX/ptx) |
| /var/adm/wtmp | History of logins | Logs (DYNIX/ptx) |

| Logfile | Description | Template Name |
|---|---|---|
| /usr/spool/adm/syslog | Syslog daemon logfile | Syslog (DYNIX/ptx) |
| /usr/spool/lp/logs/lpsched | Printer services logfile | Lp Serv (DYNIX/ptx) |
| /usr/spool/lp/remotelp | Remote printer services log | Rlp Serv (DYNIX/ptx) |
| /usr/spool/lp/logs/requests | Printer requests logfile | Lp Req (DYNIX/ptx) |

**Table 5-24 Encapsulated Logfiles on Siemens Nixdorf SINIX/Reliant Managed Nodes**

| Logfile | Description | Template Name |
|---|---|---|
| /var/cron/log [a] | Cron logfile | Cron (SINIX) |
| /etc/.osm | SINIX OS messages | OS Msgs (SINIX) |
| /var /adm/sulog [b] | Switch user logfile | Su (SINIX) |
| /var/adm/wtmpx | History of logins | Logins (SINIX) |
| /var/adm/loginlog [c] | Bad login attempts | Bad Logs (SINIX) |

a. Default setup is used in the /etc/default/cron file
b. Default setup is used in /etc/default/su file
c. You must manually create the /var/adm/loginlog file

**Table 5-25 Encapsulated Logfiles on Solaris Managed Nodes**

| Logfile | Description | Template Name |
|---|---|---|
| /var/adm/loginlog | History of Solaris failed logins | Bad Logs (Solaris) |
| /var/cron/log | Cron logfile | Cron (Solaris) |
| /var/adm/messages | System logfile | Syslog (Solaris) |

| Logfile | Description | Template Name |
|---|---|---|
| /var/adm/sol_sulog | Switch user logfile | Su (Solaris) |
| /var/adm/wtmpx | History of logins | Logins (Solaris) |
| /var/opt/OV/tmp/OpC/dmesg.out | Messages generated by the Solaris kernel | Kernel Logs (Solaris) |

**Table 5-26 Encapsulated Logfiles on Windows NT Managed Nodes**

| Logfile | Description | Template Name |
|---|---|---|
| System Eventlog | Logs system events | dflt_SysEvlog |
| Application Eventlog | Logs all events of integrated applications | dflt_ApplEvLog |
| Security Eventlog | Logs all audit information | dflt_SecEvlog |
| SMS | Logs all SMS specific NT events | NT_SMS |

There are no preconfigured logfile templates available for OS/2 managed nodes. However, it is possible to monitor any text file. For example, the output of remote access daemons such as `ftpd`, `rshd`, or `telnetd`, can be redirected to a file which can then be monitored by the ITO Logfile Encapsulator. Logfile templates are easily created in the `Message Source Templates` window of the ITO GUI if you know the name and the full path of the file to be monitored.

## SNMP Trap and Event Interception

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

The ITO event interceptor is supported on the following platforms:

- AIX 4.1, 4.2, and 4.3 (direct port access mode)

- ❏ HP-UX 10.x and 11.x
- ❏ Novell NetWare 4.1, 4.11 with NMA 2.1
- ❏ Solaris 2.5 and above
- ❏ Windows NT 3.51 and 4.0

The following kinds of traps can be intercepted:

- ❏ Well-defined traps, such as system coldstart, network interface up/down, and so forth.
- ❏ HP OpenView internal traps, for example, those originating from netmon.

## ITO Distributed Event Interception

ITO Distributed Event Interception allows you to intercept SNMP traps on systems other than the ITO management server. This provides performance benefits by allowing the local processing of messages. 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.

- ❏ Basic Configuration

  1. Make sure that SNMP devices have only one SNMP destination, or that there is only one system serving as the NNM collection station for the management server (preferably, the collection station connected via the fastest network). The destination system(s) for SNMP devices on HP-UX nodes is set in the `/etc/SnmpAgent.d/snmpd.conf` file with a **`trap_dest:<nodename>`** statement.
  2. 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.

- ❏ Configuration to Avoid Duplicate Messages

  Make certain that an ITO agent (and thus, an ITO 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.

### Event Interception on Novell NetWare Managed Nodes

There are two preconfigured templates for Novell NetWare:

- ❏ NetWare NMA 2.1 Threshold Traps
- ❏ NetWare NMA 2.1 Traps

NetWare NMA 2.1 threshold traps can be used to filter traps originating from the NetWare NMA when one of the 25 NMA thresholds is exceeded.

NetWare NMA 2.1 traps template filters the 379 traps that can be generated by the NMA module when an important event on the NetWare server occurs.

### Event Interception with ECS

`opctrapd` connects by default to the correlated event flow of `pmd`. You can change this behavior by adding an appropriate statement to the opcinfo file on the managed node. Syntax:

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

`opctrapd` connects to the default ECS stream of pmd. If required, you can configure `opctrapd` to connect to a specific ECS stream of pmd by specifying the ECS stream in the opcinfo file:

```
SNMP_STREAM_NAME <stream_name>
```

## ITO Message Interception

By default, any message submitted via the **opcmsg(1)** command or via the **opcmsg(3)** API is intercepted. For message attribute defaults, logging options and so forth, see the template, **opcmsg(1|3)**.

See also “EMS Integration” on page 332 for an example how opcmsg intercepts messages from other applications.

## MPE/iX-console Message Interception

ITO is able to intercept messages that are sent to the MPE/iX console. Some of these messages already have a predefined message classification, which ITO maps where possible to a message group and severity level. Table 5-27 on page 246 shows how MPE/iX classifications are mapped to ITO Message Groups.

For details about the MPE/iX console messages which are intercepted, inspect the MPE/iX console template `MPE Cons Msgs` in the `Message Source Templates` window.

**Table 5-27 Default Message Mapping on MPE/iX Managed Nodes**

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

For information on how MPE/iX messages are mapped to the ITO severity levels, see Table 5-28 on page 246.

**Table 5-28 MPE/iX and ITO Message Mapping Severity**

| MPE Severity Level | ITO Severity Level |
|---|---|
| 0 | Unknown |
| 1 | Normal |
| 2 | Warning |
| 3 | Critical |

## Mapping NMEV Markers

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

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

`p` — MPE/iX Message Severity mapped to ITO severity; if it is not in the range of 0 to 3, it is an invalid marker and the pattern is treated as normal text. (See Table 5-28 on page 246 for the possible values.)

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

`aaa` — MPE/iX Application ID identifying the source of the message, mapped to the ITO 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 5-29 shows how NMEV markers are mapped in ITO.

Some of the entries in the ITO Message Group column are not configured as default ITO message groups when ITO is installed. Messages sent to those message groups are routed to the message group `Misc` as described in Table 5-28 on page 246. Create these message groups if you want those messages to be routed to groups other than `Misc`.

**Table 5-29 NMEV Marker Mapping**

| MPE/iX Application ID | ITO Message Group | Application/OS Subsystem |
|---|---|---|
| 052 | Performance | Laser/RX |
| 053 | Database | Allbase/SQL |
| 194 | Network | Public Networking |

| MPE/iX Application ID | ITO Message Group | Application/OS Subsystem |
|---|---|---|
| 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 Mgr |
| 217 | Storage | Store/Restore |
| 218 | Job | Jobs/Sessions |
| 220 | OS | Process Manager |
| 221 | Logging | System Logging |
| 222 | OS | Transaction Mgmt |
| 224 | Logging | User Logging |
| 225 | Hardware | SPU Switchover |
| 226 | OS | Reply Info Table |
| 227 | OS | System Manager |
| 228 | Output | High End Printer |
| 229 | Hardware | Diagnostic-System |
| 230 | OS | Command Interpreter |

| MPE/iX Application ID | ITO Message Group | Application/OS Subsystem |
|---|---|---|
| 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 |

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 ITO-to-MPE/iX mapping is available for an MPE/iX console message intercepted by ITO, the original MPE/iX classification is used as a default value and the message appears in the message group `Misc` until you configure a message group that more accurately suits your requirements. If you require different mapping, you can apply the ITO concept of message regrouping.

The ITO attribute mapping is defined in the file `CONSDESC.COMMANDS.OVOPC`, delivered by default with the MPE agent installation. See “Generating a New NMEV Marker” on page 249 for more information about how to configure this file to map NMEVs other than the ones defined in Table 5-29.

## Generating a New NMEV Marker

The ITO Console Interceptor supports all methods of generating NMEV event messages. An NMEV event marker can be generated in the following ways:

- ❏ by inserting the marker into the text of a TELLOP command.
- ❏ by inserting the marker into a parameter for calling the PRINTOP command.
- ❏ by calling the NMEVENT intrinsic by way of a program.

The NMEV marker string can be placed in TELLOP messages. This can be useful for generating messages to ITO 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 but it is recommended that all applications that generate ITO events use the opcmsg(3) call instead of the NMEVENT API.

New NMEV markers may be added to the consdesc file so that ITO can map user-defined NMEV markers to user-defined ITO message groups, application and object fields. It is not recommended to create user-defined IDs because it is possible that the user-defined application IDs could conflict with HP-defined ID in the future, if HP added entries to the default consdesc file. 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 and must be uncompressed before you can start editing it. Place your customized version of this file into the following directory on the management server, and distribute it using the Install / Update ITO Software and Configuration window. You do not need to compress it; ITO does that for you.

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

After the distribution the file is located at CONSDESC.COMMANDS.OVOPC on the MPE/iX managed node.

**NOTE**

You must restart the MPE/iX console interceptor on your MPE/iX managed node to activate the changes in the file CONSDESC.COMMANDS.OVOPC:

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

## Monitored Objects

**Table 5-30 Object Thresholds on the Management Server**

| Object | Description | Threshold | Polling Interval |
|---|---|---|---|
| `disk_util` | Monitors disk space utilization on the root disk | 90% | 10m |
| `distrib_mon` | Monitors the software distribution process | 20% | 10m |
| `mondbfile` | Monitors free space on disk, and the remaining space available for Oracle autoextend datafiles | 0% | 10m |
| `proc_util` | Monitors process table utilization | 75% | 5m |
| `swap_util` | Monitors SWAP utilization; this value can only be monitored on HP-UX versions 8.07 or higher | 80% | 5m |

Table 5-31 illustrates what the threshold values are for the various monitors supplied with ITO for the managed nodes and how often it is compared to the actual value. Although in most cases threshold values and polling intervals are the same across platforms some of the utilities do not run on all the platforms. Such instances are indicated in Table 5-31 by footnotes. You may want to adjust the polling interval to a value more suitable to your environment.

**Table 5-31 Object Thresholds on the Managed Nodes**

| Object | Description | Threshold | Polling Interval (mins) |
|---|---|---|---|
| cpu_util | Monitors CPU utilization: requires the sar program | 95%[a] | 2[b] |
| disk_util | Monitors disk space utilization on the root disk | 90% | 10 |
| Inetd | Number of executing instances of inetd (Internet Daemon) | 0.5 | 5 |
| MailQueue Length | Length of the sendmail queue: number of unsent mail messages | 30 | 2[c] |
| proc_util | Monitors process table utilization | 75%[d] | 5[e] |
| sco_tmp | Size in disk blocks of the ITO /tmp directory on a SCO OpenServer managed node | 1000[f] | 60[g] |
| sendmail | Number of executing instances of sendmail | 0.5 | 5[h] |
| swap_util | Monitors SWAP utilization. In the case of HP-UX, versions 8.07 or higher only | 80% | 5 |

a. Digital UNIX = 90%: No AIX or HP-UX 10.x
b. Digital UNIX = 10 mins: No AIX or HP-UX 10.x,
c. No SCO OpenServer or SINIX
d. No Digital UNIX
e. No Digital UNIX
f. SCO OpenServer only
g. SCO OpenServer only
h. No SCO OpenServer or SINIX

**NOTE** No preconfigured monitors are available for Novell NetWare managed nodes.

**Table 5-32 Object Thresholds on Windows NT Managed Nodes**

| Object | Description | Threshold | Polling Interval (mins) |
|---|---|---|---|
| dflt_disk_util_NT | Monitors free disk space on C: drive | 10% | 10 |
| dflt_cpu_util_NT | Monitors processor use. A message is sent only if the threshold is exceeded for four consecutive minutes | 95% | 1 |
| dflt_rpcss_NT | Monitors the RPC services. | 90% | 30 |

**Table 5-33 Object Thresholds on OS/2 Managed Nodes**

| Object | Description | Threshold | Polling Interval (mins) |
|---|---|---|---|
| os2_disk_util | Monitors disk space utilization on C: disk | 90% | 10m |
| os2_cpu_util[a] | Monitors processor utilization | 95 | 1m |
| os2_swap_util | Monitors SWAP utilization | 16 MB | 5m |
| inetd_mon | Checks if Inetd (Inet Daemon) is running | 0.5 | 30m |
| snmpd_mon | Checks if snmpd is running | 0.5 | 10m |
| mib2_mon | Checks if mib_2 is running. | 0.5 | 10m |
| inetd_mon_ext[b] | External monitor for Inetd | 0.5 | scheduled action dependent |

| Object | Description | Threshold | Polling Interval (mins) |
|---|---|---|---|
| `snmpd_mon_ext` | External monitor for Snmpd | 0.5 | schedule action dependent |
| `mib2_mon_ext` | External monitor for Mib_2 | 0.5 | schedule action dependent |
| `Multiple external monitors`[c] | Scheduled action that checks which processes are running | N/A | 5m |

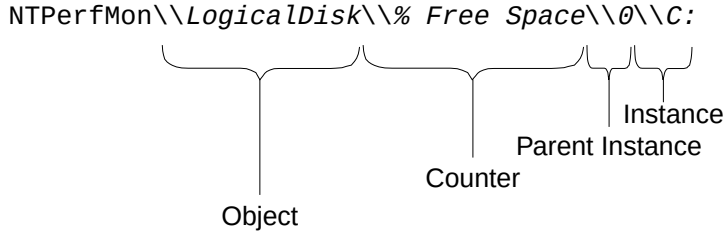
a. Requires TME NetFinity; see "Software Requirements for OS/2 Managed Nodes" on page 38.
b. Used with the scheduled action `Multiple external monitors`.
c. Requires external monitors to be configured for each process.

## Monitoring Objects in the Windows NT Performance Monitor

The ITO Threshold Monitor can be configured to monitor objects in the Windows NT Performance Monitor.

To monitor Windows NT objects, set the Monitor to `Program`, then in the `Monitor Program or MIB ID` field, enter **`NTPerfMon\\`**. This case-sensitive designator should preface all requests to the NT performance monitor. The syntax for requests is shown in Figure 5-2 on page 255, and explained below.

**Figure 5-2 NT Performance Monitor Syntax**




The language for the command may be either in English, or in the local language defined for the Windows NT system where the template will be used. English should be used if the template is intended for use in more than one system with different languages.

### Object and Counter

- These values are fixed labels that can be found for each object you want to monitor by using the NT Performance Monitor (found in the NT Tools group).
- These labels are not case-sensitive, but must include any spaces as shown in Figure 5-2 on page 255. In this example, **`LogicalDisk`**, **`logicaldisk`**, or **`LOGICALDISK`** will work correctly, but **`Logical Disk`** will not.
- If you omit the % sign from the counter label, the monitor returns the raw value instead of the percentage.

### Parent Instance and Instance

- These values vary according to what is being monitored. The example in Figure 5-2 on page 255 shows **`0`**, (in this case, the **`SCSI`** port) and **`C:`** (in this case, the drive letter). Valid values can be found using NT Performance Monitor (found in the NT Tools group). Parent instance and instance of the example will appear as `0==>C` in the Performance Monitor.
- These fields may also be filled with a question mark (**`?`**), which will allow the string to match any valid value. If the example in Figure 5-2 on page 255, were modified to look like this: **`NTPerfMon\\LogicalDisk\\% Free Space\\? \\C:`** the template will match the C: drive regardless of which SCSI port it is associated with.

- A parent instance may or may not exist. If there is no parent instance, simply omit it from the syntax. If there were no parent instance for the example in Figure 5-2 on page 255, the line would look like this:
  **`NTPerfMon\\LogicalDisk\\% Free Space\\C:`**

ITO will attempt to locate the objects when the agent is started, or when a new template is assigned to the node. If ITO cannot immediately locate the object, it will wait for two minutes and then search again. If ITO 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.

## Monitoring MIB Variables of TME NetFinity on OS/2 Managed Nodes

The ITO monitor agent can be configured to monitor MIB variables provided by the TME NetFinity product. The following prerequisites must be met on the OS/2 managed node:

- TME NetFinity must be installed (TME NetFinity is pre-installed with OS/2 Warp 4.0)
- the file `NETVIEW_PATH\BIN\AGENT\DMISA.MAP` must contain the following entry:

  “1.3.6.1.4.1.2.5.11.1.10” 1 1 1 1 “TME 10 NetFinity Services” 0 0

  where `NETVIEW_PATH` is the directory where the SystemView agent is installed (OS/2 Warp 4.0 SNMP daemons)

  If the MIB OID (Object Idenitifer) 1.3.6.1.4.1.2.5.11.1.10 is already used, use the next free one (only the last number will differ), but make sure that the template on the management server reflects that change.
- Start the DMI subagent (DMISA.EXE, part of SystemView agent); if it is already running, stop and restart it.

Table 5-34 on page 257 gives an overview of all MIB variable attributes of TME NetFinity. You can retrieve the same information by entering:

**`snmpwalk -c public <`*`myhost.domain.com`*`> \`**
**`1.3.6.1.4.1.2.5.11.1.10`**

where <*myhost.domain.com*> is the name of your system.

**Table 5-34 Attribute IDs of TME NetFinity MIB Variables**

| Attribute Name | Attribute ID | Value |
|---|---|---|
| CPU Utilization | 2872344980 | Percent |
| Drive C: Space Used | 1663545058 | Megabytes Used |
| Drive D: Space Used | 1663545059 | Megabytes Used |
| Drive C: Space Remaining | 1663545570 | Megabytes Free |
| Drive D: Space Remaining | 1663545571 | Megabytes Free |
| IP Packets Sent | 1314150980 | Packets/Sec |
| IP Packets Received with Errors | 1314150981 | Packets/Sec |
| Locked Memory | 1653400672 | Megabytes |
| Memory Usage | 1653400673 | Megabytes |
| Print Jobs Queued | 107264 | Jobs |
| Process Count | 2872344981 | Processes |
| Swap file size | 1921839360 | Megabytes |
| Swap space remaining | 1921839361 | Megabytes |
| TCP Connections | 1314150982 | TCP Connections |
| TCP/IP Sockets | 1314150983 | TCP/IP Sockets |
| TCP/IP Interface 0 - Unicast Packets Sent | 1314140225 | Packets/Sec |
| TCP/IP Interface 0 - Broadcast Packets Sent | 1314140226 | Packets/Sec |
| TCP/IP Interface 0 - Bytes Sent | 1314140227 | Bytes/Sec |
| TCP/IP Interface 0 - Unicast Packets Received | 1314140228 | Packets/Sec |
| TCP/IP Interface 0 - Broadcast Packets Received | 1314140229 | Packets/Sec |

| Attribute Name | Attribute ID | Value |
|---|---|---|
| TCP/IP Interface 0 - Bytes Received | 1314140230 | Bytes/Sec |
| Thread Count | 2872344982 | Threads |
| UDP Datagrams Sent | 1314150977 | Packets/Sec |
| UDP Datagrams Received | 1314150978 | Packets/Sec |

#### Calculating the Value of a MIB Variable

MIB variables have the following format and can be calculated by replacing the angle brackets with the desired value:

<*OID*>.2.5.11.1.10.1.3.1.<*X*>.6.<*ID*>

where:

- <*OID*> is the Object Identifier entered in the file `DMISA.MAP`
- <*X*> specifies the attribute to be monitored; see Table 5-35

**Table 5-35 Attribute Values of TME NetFinity MIB Variables**

| Value | Attribute |
|---|---|
| 1 | Attribute ID |
| 2 | Attribute Name |
| 3 | Current Value (integer) |
| 4 | Current Value (thousands) |
| 5 | Current Value (string) |
| 6 | Value Units |
| 7 | Recording enabled |

- <*ID*> is the attribute ID; see Table 5-34, “Attribute IDs of TME NetFinity MIB Variables,” on page 257

Once you have calculated the value of the MIB variable and written a program or script to monitor this value, you configure a threshold monitor template in the `Message Source Templates window`.

### Monitoring MIB Objects from other Communities

MIB objects can also be monitored from communities other than public. To do this, add the following line to the `opcinfo` file on the managed node (see Table 10-3 on page 399 for the location of the `opcinfo` file on all platforms):

**`SNMP_COMMUNITY <community>`**

where *<community>* is the community for which the `snmpd` is configured.

If `SNMP_COMMUNITY` is not set, the default community public is used. See the documentation supplied with the SNMP daemon for information about determining the configuration of `snmpd`.

## Templates for External Interfaces

ITO provides an example for calling an external trouble ticket system or external notification service in:

`/opt/OV/bin/OpC/extern_intf/ttns_mail.sh`

This script sends a corresponding mail to all operators responsible for that message.

Customer scripts and programs for calling external interfaces can also be placed in `extern_intf`, if it is intended they be erased when de-installing ITO.

**NOTE**

If your script is a shell script, the first line must contain a statement such as the following.

`#!/usr/bin/sh`

Otherwise the execution of your script or program may fail.

By default, no notification is configured. Notification maintenance is available under the `Actions:Utilities->Notification Service…` menu. Again, by default, no trouble ticket system interface is configured either. You can set up one using the `Actions:Utilities->Trouble Ticket…` menu.

## General Configuration Tips Regarding File Names

If you 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
```

make sure that the file names are not longer than 8 characters. The characters underscore ( `_` ) and dash ( `-` ) are not allowed.

MPE/iX does not distinguish between upper and lower case letters.

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

# Database Reports

ITO provides preconfigured reports for the administrator and for operators. In addition, customized reports can be created using the report writer supplied with the installed database or any other report-writing tool. The reports may be:

- displayed in a window
- saved to a file
- printed.

You may define the printer using the X resource, `OpC.printCommand` in the general application defaults file:
`/opt/OV/lib/X11/app-defaults/<`*language*`>/Opc`

or in your private file: `$HOME/.Xdefaults`

In addition, you can use ITO's enhanced reporting features in conjunction with the OpenView Service Reporter functionality to retrieve specific information directly from the database and publish and view the resulting reports in graphically rich formats on the web. For more information, see the documentation supplied with the OpenView Service Reporter product and the *HP OpenView IT/Operations Concepts Guide*.

## Reports for Administrators

You can access ITO administrator reports by selecting `Actions:Utilities->Reports...` in the ITO GUI. Note, however, that if you are in any of the administrator's browser windows, you can only access operator reports.

**Table 5-36 Preconfigured Reports for the ITO Administrator**

| Report Name | Description |
|---|---|
| Action Report | Action audit report for all operators showing ITO user, UNIX user, source (GUI, API, CLI, etc), date, time, report area and action (un/successfull). Only available for audit level, “Full”. |
| All Active Messages | Report on the number of active messages per message group |
| All History Messages | Report on all history messages for an operator (short description) |
| Audit Report | Report on all areas of all users showing; ITO users, source (GUI, API, CLI), date, time, report area and any associated actions. The “audit-level” setting determines which areas are included in the report. |
| ITO Error Report | Review of the ITO error logfile on the management server: `/var/opt/usr/OV/log/OpC/mgmt_sv/opcerror` [a] |
| Logon Report | Logon audit report for all operators ITO user, showing UNIX user, source (GUI, API, CLI, etc), date, time, report area (logon/off) and (un/successfull) actions. This report is only available for audit levels above “Login Times”. |
| Nodes Overview | Report on all configured nodes showing node name, machine type, node type (message-allowed, controlled etc), license, heartbeat polling settings. |
| Node Config Report | Report on all resulting template to node assignments |
| Node Report | Detailed report on a selected managed node |
| Node Groups Overview | Report on all configured Node Groups indicating which nodes and external nodes belong to which node groups |
| Node Group Report | Detailed report on a selected Node Group, similar to “Nodes Overview” plus user and message-group assignments for the given node group. |
| Oper. Active Message | Report on all active messages for an operator (short description) |
| Oper. Active Details | Report on all active messages for an operator (detailed description) |

| Report Name | Description |
|---|---|
| Operator Overview | Short description of all configured operators, including real and logon names, role, rights and responsibilities. |
| Operator Report | Detailed report on a selected operator: includes responsibility matrix (node and message groups), available applications, and assigned user profiles. |
| Operator Pending Messages | Short description of pending messages for a given operator |
| Operator History Messages | Short description of history (acknowledged) messages for a given operator |
| Templates Overview | Lists all templates and shows to which template groups the various templates belong. |
| Templates Summary | Report about *all* aspects of *all* templates: this might take a long time to generate. |
| Template Detail | Detailed report on one selected template |
| Unmonitored | Report on configured but currently unmonitored objects indicating, for example, unassigned node group or message group combinations |
| User Action Report | Same as “Action Report” but for one selected user |
| User Audit Report | Same as “Audit Report” but for one selected user. |
| User Logon Report | Same as “Logon Report” but for one selected user |
| User Profile Overview | Report on all configured user profiles. |
| User Profile Report | Detailed report on one selected user profile |
| Working ITO Users | Report on all ITO users who are currently logged on giving, for example, the IP address of their machine |

a. For more information about the logfiles containing the errors, see the section “On The ITO Management Server” on page 460.

Additional reports can be defined by customizing the file:

```
/etc/opt/OV/share/conf/OpC/mgmt_sv/reports/<lang>/\
admin.rpts
```

If no absolute path is specified, the output of all ITO administrator reports is saved by default in the directory of the Unix user that started the ITO administrator session. This directory is defined by $OPC_HOME, if set, $HOME, or `/tmp` in that order. All files that are created when the administrator saves report output are owned by the administrator's Unix user, which may but need not be root.

## Reports for Operators

ITO operator reports are accessed by selecting `Actions:Utilities->Reports...` from the menu bar of the `Message Browser` window.

**Table 5-37 Preconfigured Reports for ITO Operators**

| Report Name | Description |
|---|---|
| All Active Messages | Short report on *all* active messages seen by the user who runs the report |
| All Active Details | Detailed report on *all* active messages seen by the user who runs the report |
| All History Messages | Brief report on *all* history messages seen by the user who runs the report. |
| All Pending Messages | Brief report on *all* pending messages see by the user who runs the report |
| All Pending Details | Detailed report on *all* pending messages seen by the user who runs the report |
| ITO Error Report | Review of the ITO error logfile on the management server: `/var/opt/OV/log/OpC/mgmt_sv/opcerror` [a] |
| Sel. Active Message | Report on selected active messages |
| Sel. Active Details | Detailed report on selected active messages |
| Sel. History Message | Report on selected history (acknowledged) messages |

| Report Name | Description |
|---|---|
| Sel. History Details | Detailed report on selected history (acknowledged) Messages |
| Sel. Pending Messages | Brief report on selected pending messages |
| Sel. Pending Details | Detailed report on selected pending messages |

a. For more information about the logfiles, see the section "On The ITO Management Server" on page 460.

You can define additional reports by customizing the file:

```
/etc/opt/OV/share/conf/OpC/mgmt_sv/reports/<lang>/\
oper.rpts
```

Whenever an operator saves report output to a file without specifying an absolute path (starting with "/") the file is stored in the operator's Unix working directory, which is defined by $OPC_HOME (if set), $HOME, or `/tmp` in that order or priority. In addition, the file is owned by the operator's unix user, not by opc_op, unless the operator logged in as unix user opc_op. The permissions of the file will be according to the umask as set before the ITO Operator GUI was started.

## Long-term Reports

ITO allow's you to generate statistical and trend-analysis reports over a defined period of time. These reports can be configured to cover periods from as little as a few days to as much as weeks or even months.

Note that the tool `/opt/OV/bin/OpC/opcdbmsgmv` moves all messages that are marked as acknowledged to the history-message tables in the database, where they are retained with little or no negative impact on operational tasks. Although automatically started every two hours by the ITO control manager, `opcdbmsgmv` also may be called manually for trouble-shooting purposes.

## Report Security

For reasons of security, ITO restricts access to the database for report-writing tools to a database user, **opc_report**, who has read-only access. The opc_report user makes use of the Oracle report role

**opc_report_role**, which is a kind of database user profile that may also be used in cases where it is necessary to allow additional database users access to the database in order to create reports using information in the ITO database tables.

SQL*Net requires a listener process running on the database node in order to accept net connections. The listener process accepts connection requests from any legal database user. If you wish to tighten security still further, there are products available (for example, from Oracle) which help improve general communication security in this area. For more information, see the Oracle product documentation.

**NOTE** The web-reporting server must be on the same side of any firewall as the ITO database server. Any other configuration is not supported.

# Flexible-management Configuration

This section describes the conventions that need to be adhered to when setting up flexible management using the example templates provided in ITO. The section provides information on:

- flexible management templates, including:
  - follow-the-sun configuration
  - configuring responsible managers
  - switching management responsibility
  - service hours and scheduled outages
- template keywords
- time templates and time zone handling
- syntax conventions
- practical examples

For additional help concerning the tasks involved in setting up the flexible management features in ITO, see the sections on flexible-management tasks in the HP ITO Administrator's Guide to Online Information.

## Templates for Flexible Management

ITO provides a set of ASCII templates which you can copy and edit to define the ITO features required to set up and use flexible management features in a widely-distributed environment. Table 5-38 provides a brief description of each template, which are located in the following directory:

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

Several examples of the syntax to be used when configuring time templates are provided at the end of the section. For specific help with using the templates to set up flexible management features, see the section on flexible-management tasks in the HP ITO Administrator's Guide to Online Information.

**Table 5-38 Example Templates for ITO Flexible Management**

| Template Name | Description |
|---|---|
| backup-server | Defines the responsible managers for an ITO **backup server**. Management responsibility can be switched to a backup server if the ITO primary server fails. This template defines two management servers (M1) and (M2); management server M2 can act as a backup server for management server M1. |
| escmgr | Defines the responsible managers for **message escalation**. This template defines two management servers (M1) and (M2); management server M2 has permission to escalate messages, at any time, to management server M1. |
| example.m2 | Example template combining the follow-the-sun and service-oriented message distribution functions. |
| example.m3 | Additional example template for the follow-the-sun functions. |
| followthesun | Defines the time templates and responsible managers for ITO **follow-the-sun** responsibility switching. This template defines three management servers (M1), (M2), and (M3) which can switch responsibility at different times of the day and week. |
| hierarchy | Defines the target management server to which messages can be escalated in the hierarchical escalation of messages to a central management server MC. |
| hier.specmgr | Provides an example of hierarchical management responsibility in which SNMP traps are sent to the local management server; all other messages are sent to the primary management server. |
| hier.time.all | Provides an example of hierarchical management responsibility switching between two servers according to a follow-the-sun time template. |
| hier.time.spec | Provides an example of hierarchical management responsibility in which SNMP traps are sent to the local management server; all other messages are sent to the primary management server according to a follow-the-sun time template. |

| Template Name | Description |
|---|---|
| `hierarchy.agt` | Defines the responsible managers for hierarchical management responsibility switching for **all nodes**. This template defines two management servers `M1` and `MC` where `M1` is configured as the **primary manager** for all nodes, and `MC` is configured as an **action-allowed manager** for all nodes. |
| `hierarchy.sv` | Defines the responsible managers for hierarchical management responsibility switching for **regional management servers**. |
| `msgforw` | Defines the responsible managers for **manager-to-manager message forwarding**. This template defines the message-forwarding target rules. |
| `outage` | Defines the period of time in which a service is to be provided or a system (such as a database server) or service is scheduled to be unavailable. |
| `service` | Defines the responsible managers for **service-related message distribution**, for example, competence centers, etc. This template defines a local management server (`M1`), and two examples of service centers: a database service center (`DBSVC`) and an application service center (`ASVC`). |

## Keywords in Flexible-management Templates

The following is a list of the keywords (and their definition) that ITO uses to define the various elements required in a flexible management configuration:

- CONDSTATUSVARS

  See: “The Condition-status Variable” on page 278

- RESPMGRCONFIG

  Start of the responsible manager configuration.

- DESCRIPTION

  A string containing a short manager description.

- SECONDARYMANAGERS

A secondary ITO manager of an agent. This management server has permission to take over responsibility and become the primary ITO manager for an agent.

- SECONDARYMANAGER
- NODE <*node*>

  The node name of the SECONDARYMANAGER.

- DESCRIPTION

  A string containing the description of the SECONDARYMANAGER.

❑ ACTIONALLOWMANAGERS

An ITO manager that is allowed to execute actions on the managed node and to which the action response (for example, command broadcast) is sent. Only the primary ITO manager can configure action-allowed managers for an agent.

- ACTIONALLOWMANAGER
- NODE

  The node name of the ACTIONALLOWMANAGER. You can use the variable `$OPC_PRIMARY_MGR` to specify that this will always be the primary manager.

- DESCRIPTION

  A string containing a short description of the SECONDARYMANAGER.

❑ MSGTARGETRULES

- MSGTARGETRULE

  Rules to configure the MSGTARGETRULECONDS and the MSGTARGETMANAGERS.

- DESCRIPTION

  A string containing the description of the MSGTARGETRULE.

❑ MSGTARGETMANAGERS

An ITO manager to which the agents send ITO messages and the action responses that correspond to those ITO messages (result of automatic actions). An ITO message is sent to only one ITO manager.

This is also used to escalate messages from one manager to another.

- MSGTARGETMANAGER

  Management server to which you forward a message.

**NOTE**

Always specify the IP address of the target management server as **0.0.0.0**. The real IP address is then resolved by the domain name service (DNS).

- TIMETEMPLATE

  The name of the corresponding time template. You can use the variable $OPC_ALWAYS if the time condition is always true. When you use this keyword, message transfer to the target manager will *not* depend on the time.

- OPCMGR

  The node name of the ITO Manager. You can use the keyword, $OPC_PRIMARY_MGR to denote that this will always be the primary manager.

- MSGCONTROLLINGMGR

  Attribute of a message target manager enabling it to switch control of a message.

- NOTIFYMGR

  Attribute of a message target manager enabling it to notify itself. This is set by default if no attribute is defined for the message target manager.

- ACKNONLOCALMGR

  Attribute for a message rule to force a direct acknowledgment of a notification message on a source management server.

❑ MSGTARGETRULECONDS

- MSGTARGETRULECOND

  These conditions tell the agent to which management server to send specific messages, based on message attributes and/or time. The message agent evaluates the message target conditions by reading the file mgrconf. If the mgrconf file does not exist, the

messages are sent to the management server name stored in the `primmgr` file. If the `primmgr` file does not exist, messages are sent according to the `opcsvinfo` file.

- DESCRIPTION

  A string describing the message target rule condition.

- SEVERITY

  A severity level from: Unknown, Normal, Warning, Minor, Major, Critical.

- NODELIST

  A list of nodes.

  - NODE <*node*>

    A node can be specified in different ways, for example: `NODE IP 0.0.0.0 hpbbn` If the node is defined using the format IP <*ipaddress*> or IP <*ipaddress*> <*string*>, you should normally use the IP address “0.0.0.0”. The real IP address is then resolved by the domain name service (DNS).

- APPLICATION

  A string containing the application name.

- MSGGRP

  A string containing the name of the message group.

- OBJECT

  A string containing the name of the object.

- MSGTYPE

  A string containing the description of the message type.

- MSGCONDTYPE

  Two condition types are possible:

  - Match

    The condition is true if the specified attributes are matched.

  - Suppress

    The condition is true if the specified attributes are not matched.

- MSGOPERATION

  Three types are possible, see Table 5-39 on page 277:

  - Suppress
  - Log-only
  - Inservice

## Template Syntax

You can use the syntax described in the following sections as a basis for configuring flexible management features (for example, the switching of responsibility between managers) in the template files provided. For further information, see the man pages `opcmom(4)` and `opcmomchk(1m)`, and the `README` file in the template directory:

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

In the syntax examples that follow, the “e” character represents an empty string.

A pound or hash sign (#) must precede any comments in a template. ITO considers all characters up to the new line a comment. If you want to use quotation marks in a syntax string, escape the quotation marks with a backslash. For example, `\"quotation\"`.

## Syntax for Responsible Manager Configuration

```
respmgrconfigs ::= <respmgrconfigs> RESPMGRCONFIG DESCRIPTION
                   <string> <respmgrconds> | e
respmgrconds   ::= SECONDARYMANAGERS <secondmgrs>
                    ACTIONALLOWMANAGERS <actallowmgrs>
                   [MSGTARGETRULES <msgtargetrules>]
secondmgrs     ::= <secondmgrs> SECONDARYMANAGER NODE <node>
                   [DESCRIPTION <string>] | e
actallowmgrs   ::= <actallowmgrs> ACTIONALLOWMANGER NODE <node>
                   [DESCRIPTION <string>] | e
msgtargetrules ::= <msgtargetrules> MSGTARGETRULE DESCRIPTION
                   <string> <msgtargetrule> | e
msgtargetrule  ::= MSGTARGETRULECONDS <mtrconditions>
                   MSGTARGETMANAGERS <msgtargetmgrs>
                   | MSGTARGETRULECONDS <mtrconditions>
                   MSGTARGETMANAGERS <msgtargetmgrs>
                   ACKNONLOCALMGR
mtrconditions  ::= <mtrconditions> MSGTARGETRULECOND DESCRIPTION
                   <string> <mtrcond> | e
mtrcond        ::= <mtrcond> SEVERITY <severity> | <mtrcond>
                   NODE <nodelist> | <mtrcond> APPLICATION
                   <string> | <mtrcond> MSGGRP <string> |
```

```
                    <mtrcond> OBJECT <string> | <mtrcond> MSGTYPE
                    <string> | <mtrcond> MSGCONDTYPE
                    <msgcondtype> | e

severity       ::= Unknown | Normal | Warning | Critical | Minor
                   | Major
msgcondtype    ::= Match | Suppress
nodelist       ::= <node> | <nodelist> <node>
node           ::= IP <ipaddress> | IP <ipaddress> <string>
                  | OTHER <string>
string         ::= “any alphanumeric string”
ipaddress      ::= <digits>.<digits>.<digits>.<digits>
```

## Syntax for Time Templates

```
timetmpls      ::= <timetmpls> TIMETEMPLATE <string> DESCRIPTION
                   <string> <conditions> | e
conditions     ::= TIMETMPLCONDS <timetmplconds> | e
timetmplconds  ::= <timetmplconds> TIMETMPLCOND <timetmplcond>
timetmplcond   ::= [TIMECONDTYPE <timecondtype>] [TIME FROM
                   <time> TO <time>] [WEEKDAY <weekday>]
                   [DATE <exact_date>] | e
timecondtype   ::= Match | Suppress
time           ::= <hh>:<mm>
weekday        ::= ON <day> | FROM <day> TO <day>
exact_date     ::= ON <date> | FROM <date> TO <date>
day            ::= Monday | Tuesday | Wednesday | Thursday
                  | Friday | Saturday | Sunday
date           ::= <mm>/<dd>/<yyyy> |<mm>/<dd>/*
```

## Syntax for Management Responsibility Switching

```
configfile := [TIMETEMPLATES <timetmpls>] RESPMGRCONFIGS
              <respmgrconfigs>
```

## Syntax for Message Target Rules

```
msgtargetmgrs ::= <msgtargetmgrs> MSGTARGETMANAGER TIMETEMPLATE
                  <string> OPCMGR <node> | <msgtargetmgrs>
                  MSGTARGETMANAGER TIMETEMPLATE <string> OPCMGR
                  <node> MSGCONTROLLINGMGR | <msgtargetmgrs>
                  MSGTARGETMANAGER TIMETEMPLATE <string> OPCMGR
                  <node> NOTIFYMGR | e
```

You can replace the <*string*> variable with $OPC_ALWAYS to specify that the time condition is always true. To specify that the current primary manager is always used as the message target server, replace the <*node*> variable with $OPC_PRIMARY_MGR

## Syntax for Service Hours and Scheduled Outages

In the following description of the syntax rules for templates used to define service hours and scheduled outages, the “e” character represents an empty string:

```
configfile  :=  [TIMETEMPLATES  <timetmpls>]
                [CONDSTATUSVARS] <statusvarsdef>]
                RESPMGRCONFIGS <respmgrconfigs>
```

Syntax for the declaration of condition status variables:

```
statusvarsdef ::= <statusvarsdef> CONDSTATUSVAR <string> <bool> |e
```

Syntax for the Time Template:

```
timetmpls       ::=  <timetmpls> TIMETEMPLATE <string> DESCRIPTION
                     <string> <timetmpldefs> <conditions> |e
timetmpldefs    ::=  TIMEZONETYPE  <timezonetype> TIMEZONEVALUE
                     <string>|  e
timezonetype    ::=  Fix | Local
conditions      ::=  TIMETMPLCONDS  <timetmplconds>  |  e
timetmplconds[1]   ::=  <timetmplconds>  TIMETMPLCOND
                     <timetmplcond>
timetmplcond    ::=  [TIMECONDTYPE  <timecondtype>]  [TIME  FROM
                     <time>  TO  <time>]  [WEEKDAY  <weekday>]
                     [DATE  <exact_date>]  |  e
timecondtype    ::=  Match  |  Unmatch [1]
time            ::=  <hh>:<mm>
weekday         ::=  ON  <day>  |  FROM  <day>  TO  <day>
exact_date      ::=  ON  <date>  |  FROM  <date>  TO  <date>
day             ::=  Monday  |  Tuesday  |  Wednesday  |  Thursday
                     |  Friday  |  Saturday  |  Sunday
date            ::=  <mm>/<dd>/<yyyy>  |<mm>/<dd>/*
```

Syntax for service hours and scheduled outages

```
respmgrconfigs  ::=  <respmgrconfigs>  RESPMGRCONFIG DESCRIPTION
                     <string>  <respmgrconds>  |  e
respmgrconds    ::=  MSGTARGETRULES  <msgtargetrules>
msgtargetrules  ::=  <msgtargetrules> MSGTARGETRULE
                      DESCRIPTION  <string>  <msgtargetrule>  |  e
msgtargetrule    ::=  MSGTARGETRULECONDS  <mtrconditions>
                     MSGOPERATIONS  <msgoperations>
mtrconditions    ::=  <mtrconditions>  MSGTARGETRULECOND
                     DESCRIPTION   <string>  <mtrcond>  |  e
mtrcond          ::=  <mtrcond>  CONDSTATUSVAR  <string>  |
                      <mtrcond>  SEVERITY  <severity>  |
                      <mtrcond>  NODE  <nodelist>  |
                      <mtrcond>  APPLICATION  <string>  |
                      <mtrcond>  MSGGRP  <string>  |
                      <mtrcond>  OBJECT  <string>  |
                      <mtrcond>  MSGTYPE  <string> |
                      <mtrcond> TEXT <string>[2]   |
                      <mtrcond>  SERVICE <string> [2]  |
                      <mtrcond> MSGCONDTYPE <msgcondtype>  |  e
bool            ::=  True  | False
severity        ::=  Unknown  |  Normal  |  Warning  |  Critical
                     | Minor   |  Major
msgcondtype     ::=  Match  |  Unmatch
```

---

1. Service hours only
2. Pattern matching only available in <string>

```
nodelist        ::=  <node>  |  <nodelist>  <node>
node            ::=  IP  <ipaddress>  |  IP  <ipaddress>  <string>
                     |  OTHER  <string>
string          ::=  "any  alphanumeric  string"
ipaddress       ::=   <digits>.<digits>.<digits>.<digits>
```

**NOTE** You can replace the <string> variable with $OPC_ALWAYS to specify that the time condition is always true.

Syntax for Message Operations:

```
msgoperations  ::=  <msgoperations> MSGOPERATION  TIMETEMPLATE
                    <msgoperation> <msgoperations>  MSGOPERATION
                    TIMETEMPLATE <string>  <msgoperation>

msgoperation   ::=  INSERVICE|SUPPRESS|LOGONLY
```

**NOTE** The time template is compared with the creation time of the message on the managed node. Message creation time is always defined in GMT.

## Templates for Service Hours and Scheduled Outages

The ITO administrator configures service hours and scheduled outages on the management server with a template similar to the one used to configure flexible management. The syntax used to configure service hours and scheduled outages is the same as that used to configure flexible management and consequently may be checked with the opcmomchk tool. For more information on template syntax, see "Syntax for Time Templates" on page 274 and "Syntax for Service Hours and Scheduled Outages" on page 274. The template for service hours and scheduled outages allows you to **suppress**, **log only**, or buffer (**inservice**) messages that match certain conditions for defined time periods.

The template is located in the following directory: /etc/opt/OV/share/conf/OpC/mgmt_sv/tmpl_respmgrs/outage. Before making any changes, copy the file to the working directory; /etc/opt/OV/share/conf/OpC/mgmt_sv/work_respmgrs. Once the template file is ready for use, it should be moved to the directory; /etc/opt/OV/share/conf/OpC/mgmt_sv/respmgrs, and a new ITO session started in order for the new configuration to be read and implemented. Note that the templates must not be renamed: ITO looks for specific, template file name. For more information on how to set up both service hours and scheduled outages, see the section on Flexible Management Tasks in the HP ITO Administrator's Guide to Online

Information. Table 5-39 on page 277 shows the parameters in the template used to define service hours and scheduled outages and gives a brief explanation of their scope:

**Table 5-39 Parameters for the Service-Hours Template**

| Parameter | Description |
|---|---|
| SUPPRESS | In the context of service hours and scheduled outages: *delete* messages. Message-related actions triggered by the ITO management server are *not* started if the SUPPRESS option is defined. |
| LOGONLY | Send matching messages to the history browser. |
| INSERVICE | If the message condition matches and the time template condition does *not*, send messages to the Pending-Messages Browser, where they remain until the **unbuffer** time condition is matched or the message is manually unbuffered. |

**NOTE**

Scheduled outages and service hours may be configured by an external application. However, the designated external application must create the template for outages and service hours and use the `opccfgout(1M)` command to control outages.

Messages buffered in the `Pending Messages Browser` window are automatically moved to the `Message Browser` window as soon as the specified buffer time expires. You can change this behavior by setting the value of the OPC_AUTO_DEBUFFER parameter in the `opcsvinfo` file on the ITO management server to FALSE. IN this case, messages remain in the `Pending Messages Browser` window.

In addition, you can change the value of the message attributes:

- Forward to Trouble Ticket
- Forward to Notification Interface

and, in conjunction with the time template, forward messages to a trouble-ticket or notification interface according to time of day. For example, set the following values in the service-hours template to forward messages to the Trouble-Ticket interface:

```
MSGOPERATION TIMETEMPLATE “SLA_cust1” TROUBLETICKET True
MSGOPERATION TIMETEMPLATE “SLA_cust2” NOTIFICATION False
```

For more information on these and other variables, see “Syntax for Service Hours and Scheduled Outages” on page 274.

**The Condition-status Variable.** Status variables for conditions allow you to enable and disable conditions dynamically. The conditions are used in message-target-rules conditions and must be declared at be beginning of the template *after* the `TIMETEMPLATES` values. ITO allows the declaration of several variables for one conditions as well as one variable in several conditions. For example, an external interface can set the state of many conditions with one call. The following abbreviated (...) example of a template defining service hours sets the condition status variable for SAP to true:

```
TIMETEMPLATES
...
CONDSTATUSVARS
        CONDSTATUSVAR “sap” True
...
RESPMGRCONFIG
...
     MESSAGETARGETRULECONDS
        MESSAGETARGETRULECOND
           DESCRIPTION “Filter SAP messages”
           CONDSTATUSVAR “sap”
APPLICATION “Sap”
     MSGOPERATIONS
        MSGOPERATION
           INSERVICE
```

**NOTE**

Status variables are persistent: they are not affected by the message manager stopping and restarting.

**The Time zone String.** Since the creation time of an ITO message is always defined in UTC regardless of where in the world the managed node is located, ITO messages also contain an indication of the difference between UTC and the local time on the managed node. In this way, the

ITO management server is able to calculate the local time of the managed node which sent the message and decide whether or not it is appropriate to act.

Service Hours are usually defined in terms of the local time on the managed node. For example, a service provider uses the Service Hours template to tell the ITO management server that managed nodes in various time zones must be supported between 08:00 and 16:00 local time. Templates for Scheduled Outages define time in terms of the local time on the server providing the service that is scheduled to be unavailable. For example, the administrator of an ITO management server in the UK knows that a SAP server situated in Eastern United States will be unavailable for maintenance reasons between 22:00 and 02:00 US EST.

The templates for scheduled outages and service hours on the ITO management server can contain a string that defines a fixed local time zone (e.g. EST for US Eastern Standard Time). The ITO management server uses the value of the time zone string and the time (in UTC) to calculate the fixed local time on the given management server for which an outage has been scheduled. The following example illustrates the syntax for the time zone string:

```
TIMEZONETYPE FIX TIMEZONEVALUE EST
```

By default, ITO evaluates time conditions for both service hours *and* scheduled outages by comparing the time frame defined for each condition to the time the message is received on the ITO management server. However, this behavior can be modified by setting a parameter in the `opcsvinfo` file in the following manner:

- to force the ITO management server to use the message creation time on the local managed node to evaluate scheduled outage hours rather than the message arrival time on the ITO management server, enter the following string in the `opcsvinfo` file:

  ```
  OPC_OUTAGE_USE_CREATE_TIME TRUE
  ```

- to force the ITO management server to use the message creation time on the local managed node to evaluate defined service hours rather than the message arrival time on the ITO management server, enter the following string in the `opcsvinfo` file:

  ```
  OPC_SERVHRS_USE_AGENT_TZ TRUE
  ```

This string instructs the ITO management server to apply the time frame for service hours defined on the ITO management server (e.g. 08:00 -- 16:00) as a sliding time frame for managed nodes in their respective local time zone.

**NOTE**

It is important to ensure that the local time is correctly set on the managed node.

**The Command-line Interface.** The message manager does not automatically read the configuration template for outages and service hours each time the template file is modified, for example by the system administrator or an external application. The command-line tool `opccfgout(1M)` may be used to start the reconfigure request:

```
opccfgout -update
```

Additional options allow you to set status variables for the conditions:

```
opccfgout -set_cond <cond_stat_var>
[-true|-false|-default]
```

To list the current status of the status variables, enter:

```
opccfgout -list_cond <cond_stat_var>|-all
```

## The Message-forwarding Template

ITO allows you to control both the generation of notification messages to be sent to remote management servers and the switch of control for a message with one, single template which you configure and assign to the source management server and check using the tool `opcmomchk`. ITO stores the message-forwarding template in:

```
/etc/opt/OV/share/conf/OpC/mgmt_sv/respmgrs/msgforw
```

The configuration and syntax in the template is similar to that required for the message-escalation template except that:

- You can specify more than one target management server per message
- Target management servers to which you forward a message can also have the attribute MSGCONTROLLINGMGR set in order to be able to switch control of a message themselves
- Target management servers to which you forward a message can also notify themselves by setting the attribute NOTIFYMGR

- Setting the attribute ACKNONLOCALMGR per message rule forces a direct acknowledge of a notification message on the source management server

The template accepts any of the following message attributes in a message condition (for more information on message attributes see the man page `opcmom(4)`):

- OBJECT
- APPLICATION
- MSGGRP
- SEVERITY
- NODE
- MSGCONDTYPE

The administrator can set several parameters to configure message forwarding on the various target managers. These parameters are required for the management of system and network resources and can be added directly to the `opcsvinfo` file on each target management server. Table 5-40 provides more information about these parameters, their default values, and a short description of the function of each parameter. The value of the parameters must be set for each target manager. If no value is specified, the default value is set.

**Table 5-40 Message Forwarding Parameters**

| Parameter Name | Default Value | Description |
|---|---|---|
| OPC_ACCEPT_NOTIF_MSSGS | TRUE | accept notification messages from other management servers |
| OPC_ACCEPT_CTRL_SWTCH_MSGS | TRUE | accept control-switched messages from other management servers |
| OPC_ACCEPT_CTRL_SWTCH_ACKN | TRUE | accept acknowledgment for control-switched messages from other management servers |
| OPC_FORW_NOTIF_TO_TT | FALSE | forward notification messages to trouble ticket or notification service |

| Parameter Name | Default Value | Description |
|---|---|---|
| OPC_FORW_CTRL_SWTCH_TO_TT | TRUE | forward control-switch messages to trouble ticket or notification service |
| OPC_SEND_ACKN_TO_CTRL_SWTCH | TRUE | send acknowledge to control-switched messages |
| OPC_SEND_ANNO_TO_CTRL_SWTCH | TRUE | send annotation to control-switched messages |
| OPC_SEND_ANT_TO_CTRL_SWTCH | TRUE | send action-related data to control-switched messages |
| OPC_SEND_ANNO_TO_NOTIF | TRUE | send annotation to notification messages |
| OPC_SEND_ANT_TO_NOTIF | TRUE | send action-related data to notification messages |
| OPC_ONE_LINE_MSG_FORWARD | FALSE | controls forwarding in larger manager hierarchies |

## Time Templates

A time template consists of:

- The name used to refer to the time template.
- The time conditions.

  Each time condition defines a specific time period and contains the definition of the time, day of the week, and/or date. The local time zone is always used to evaluate the template.

**NOTE**

When specifying a time, use the 24-hour clock notation. For example, instead of 1:00 p.m., enter 13:00.

An example of a time template is shown in the section “Syntax for Time Templates” on page 274. You can also see the man page `opcmom(4)`, and the example templates in the following directory:

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

**NOTE**

To correct time differences between the different time resources used by the ITO C-routines and the MPE/iX intrinsics and commands, the **TIMEZONE** variable must be set on MPE/iX managed nodes. If not, messages can be sent to the wrong management server as they are processed using the incorrect time. For information about setting the **TIMEZONE** variable for MPE/iX nodes, see Chapter 2 of the *HP OpenView IT/Operations Administrator's Reference*.

The following examples show various ways to specify time formats in the time templates:

- No Time

  If you do not specify a particular time, day of the week, or year, ITO assumes that you want the condition to be true for 24 hours, from 00:00 to 24:00 every day of the year.

  ITO requires you set up a time template for the message target rules even if the scheduled action does not depend on time. You can use the variable OPC_ALWAYS to configure time templates when the condition is always true.

- Specific Dates or Times

  If you specify a condition, ITO assumes the conditions should continually exist for the time/day specified. For example:

  - If you specify only Tuesday, ITO will evaluate the condition as true every Tuesday from 00:01 to 23:59 throughout the year, every year. Use the syntax:

    ```
    WEEKDAY ON Tuesday
    ```

  - Specifying January 1 and nothing else will match a condition every January 1st of every year. Use the syntax:

    ```
    DATE ON 01/01/*
    ```

- Time Periods

  For example:

  - To set a time period from 7:00 to 17:00, use the syntax:

    ```
    TIME FROM 7:00 TO 17:00
    ```

  - To set a time period from Monday to Friday, use the syntax:

    ```
    WEEKDAY FROM Monday TO Friday
    ```

- To set a time period from the year 1995 to 2000, use the syntax:

  **`DATE FROM 01/01/1995 TO 12/31/1999`**

- To set a time on December 31 1998, from 23:00 to 23:59, use the syntax:

  **`TIME FROM 23:00 TO 23:59 DATE ON 12/31/1998`**

If you include the day of the week (for example, Monday April 1, 1997), ITO cross-checks the day and date you have entered to make sure that they match the calendar. If they do not match, however, the action will not be correctly completed. ITO does not issue an error message.

❑ Dates or Periods Using a Wildcard (*)

For example:

To set a condition for December 1st every year, use the syntax:

**`DATE ON 12/01/*`**

To set a condition from August 6th to September 10th every year, use the syntax:

**`DATE FROM 08/06/* TO 09/10/*`**

## Keywords for Time Templates

❑ TIMETEMPLATE <*string*>

<*string*> contains the template name.

❑ DESCRIPTION

A string containing a short description of the time template.

❑ TIMETMPLCONDS

- TIMETMPLCOND
- TIMECONDTYPE

  A time condition defines a single time interval. Several time conditions together comprise a time period. A time condition allows you to use combinations of time, day of the week, and date to define a time period.

**NOTE** At least one of the following parts must be used for the definition. ITO does not interpret any one of the following parts as “always”.

- Match

  If the current time is within the defined time period, the time condition is true.

- Suppress

  If the current time is within the defined time period, the time condition is false.

- TIME FROM <*time*> TO <*time*>

  Specify a time period. Set the <*time*> using the format:

  <*HH*>:<*MM*>

**NOTE** The FROM <*time*> must be before the TO <*time*>. For example: `FROM 18:00 TO 24:00` or `FROM 0:00 TO 6:00`

- WEEKDAY

  You can specify every day of the week: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday

  - ON <*day*>

    At one day of the week, for example Sunday.

  - FROM <*day*>TO <*day*>

    A time period, for example:

    FROM Monday TO Wednesday

- DATE

  The date must have one of the following formats:

  <*MM*>/<*DD*>/<*YYYY*> <*MM*>/<*DD*>/<*YY*> <*MM*>/<*DD*>/*

  Note: ITO will not check that the time period is correct. For example 10/35/* will not be recognized as an invalid date.

  ON <*date*> FROM <*date*> TO <*date*>

# Example Templates for Flexible Management

This section provides a number of example templates which illustrate a simple implementation of selected flexible management features:

- “Management Responsibility Switch”
- “Follow-the-Sun Responsibility Switch”
- “Message Forwarding between Management Servers”
- “Service Hours”
- “Scheduled Outage”

## Management Responsibility Switch

```
#
# Configuration file
# /etc/opt/OV/share/conf/OpC/mgmt_sv/respmgrs/f887818
# and managed node hptest with
# the IP address 15.136.120.24 (= f887818 in hex notation)
#
TIMETEMPLATES
    TIMETEMPLATE “shift1”
        DESCRIPTION “Time Template 1”
        TIMETMPLCONDS
            TIMETMPLCOND
                TIMECONDTYPE Match
                TIME FROM 10:00 TO 14:00
                WEEKDAY FROM Monday TO Friday
            TIMETMPLCOND
                TIMECONDTYPE Match
                TIME FROM 17:00 TO 24:00
                WEEKDAY FROM Monday TO Friday
    TIMETEMPLATE “shift2”
        DESCRIPTION “Time Template 2”
        TIMETMPLCONDS
            TIMETMPLCOND
                TIMECONDTYPE Match
                TIME FROM 6:00 TO 18:00
                WEEKDAY FROM Monday TO Friday
                DATE 1/1/95
RESPMGRCONFIGS
    RESPMGRCONFIG
        DESCRIPTION “responsible mgrs for agents in Europe”
        SECONDARYMANAGERS
            SECONDARYMANAGER
                NODE IP 0.0.0.0“hptest.bbn.hp.com”
                DESCRIPTION “Boeblingen”
            SECONDARYMANAGER
                NODE IP 0.0.0.0 “hpsystem.bbn.hp.com”
                DESCRIPTION “Boeblingen gateway”
        ACTIONALLOWMANAGERS
            ACTIONALLOWMANGER
                NODE IP 0.0.0.0 “hptest.bbn.hp.com”
                DESCRIPTION “Boeblingen”
```

```
            ACTIONALLOWMANGER
                NODE IP 0.0.0.0 “hpsystem.bbn.hp.com”
                DESCRIPTION “Boeblingen gateway”
            ACTIONALLOWMANGER
                NODE IP 0.0.0.0 “$OPC_PRIMARY_MGR”
                DESCRIPTION “ITO primary manager”
    MSGTARGETRULES
        MSGTARGETRULE
            DESCRIPTION “other messages”
            MSGTARGETRULECONDS
            MSGTARGETMANAGERS
                MSGTARGETMANAGER
                    TIMETEMPLATE “shift2”
                    OPCMGR NODE IP 0.0.0.0 “system.aaa.bb.com”
```

## Follow-the-Sun Responsibility Switch

```
#
# Time-template configurations for follow-the-sun functions
#
# Three responsible managers are used in this example
TIMETEMPLATES
        # time template 1
        TIMETEMPLATE ”shift1”
        DESCRIPTION ”Time Template 1 ”
        # Time template for shift1
        # this include the time from 17:00 to 24:00  and from
        # 0:00 to 6:00
        # on the weekday Monday to Friday
           TIMETMPLCONDS
               TIMETMPLCOND
                  TIME FROM 0:00 TO 6:00
                  WEEKDAY FROM Monday TO Friday
               TIMETMPLCOND
                  TIME FROM 17:00 TO 24:00
                  WEEKDAY FROM Monday TO Friday
        TIMETEMPLATE ”shift2”
        DESCRIPTION ”Time Template 2 ”
        # Time template for shift2
        # this includes the time from 6:00 to 17:00
        # on the weekday Monday to Friday
           TIMETMPLCONDS
               TIMETMPLCOND
                  TIME FROM 6:00 TO 17:00
                  WEEKDAY FROM Monday TO Friday
        # time template 3
        TIMETEMPLATE ”shift3”
        DESCRIPTION ”Time Template 3 ”
        # Time template for shift3
        # this include the time from 0:00 to 24:00 (the whole day)
        # on the weekday Saturday and Sunday
           TIMETMPLCONDS
               TIMETMPLCOND
                  TIME FROM 0:00 TO 24:00
                  WEEKDAY FROM Saturday TO Sunday
#
# Responsible Manager Configurations for follow the sun
# functionality
#
```

```
RESPMGRCONFIGS
   RESPMGRCONFIG
   DESCRIPTION ″responsible managers M1 ″
      SECONDARYMANAGERS
         SECONDARYMANAGER
            NODE IP 0.0.0.0 ″M1″
            DESCRIPTION ″secondary manager M1″
         SECONDARYMANAGER
            NODE IP 0.0.0.0 ″M2″
            DESCRIPTION ″secondary manager M2″
         SECONDARYMANAGER
            NODE IP 0.0.0.0 ″M3″
            DESCRIPTION ″secondary manager M3″
      ACTIONALLOWMANAGERS
         ACTIONALLOWMANAGER
            NODE IP 0.0.0.0 ″M1″
            DESCRIPTION ″action allowed manager M1″
         ACTIONALLOWMANAGER
            NODE IP 0.0.0.0 ″M2″
            DESCRIPTION ″action allowed manager M2″
         ACTIONALLOWMANAGER
            NODE IP 0.0.0.0 ″M3″
            DESCRIPTION ″action allowed manager M3″
      MSGTARGETRULES
         MSGTARGETRULE
         DESCRIPTION ″target rule description ″
            MSGTARGETRULECONDS
            # for all messages
            MSGTARGETMANAGERS
               MSGTARGETMANAGER
               # target manager from 17:00 to 24:00
               # and 00:00 to 6:00
               # from Monday to Friday
                  TIMETEMPLATE ″shift1″
                  OPCMGR IP 0.0.0.0 ″M1″
               # target manager from 6:00 to 17:00
               # from Monday to Friday
               MSGTARGETMANAGER
                  TIMETEMPLATE ″shift2″
                  OPCMGR IP 0.0.0.0 ″M2″
               # target manager on the whole weekend
               MSGTARGETMANAGER
                  TIMETEMPLATE ″shift3″
                  OPCMGR IP 0.0.0.0 ″M3″
```

## Message Forwarding between Management Servers

If you install the following simple example of a message-forwarding template on a server called **Source**, Source will:

- Forward messages with message group DATABASE to a database expert center (**dbexpert**) and pass control of the message to this center, inform a second server (**dbnotify**) and, finally, cause the message to be acknowledged directly on the local ITO server

- Inform another server (**Treasury**) about messages concerning financial and CAD applications
- Inform server (**master**) about critical messages coming from nodes x1 and x2

```
TIMETEMPLATES
# none

RESPMGRCONFIGS
        RESPMGRCONFIG
        DESCRIPTION “msg-forwarding target specification”
                MSGTARGETRULES
                     MSGTARGETRULE
                     DESCRIPTION “Database”
                          MSGTARGETRULECONDS
                             MSGTARGETRULECOND
                             DESCRIPTION “Database messages”
                                MSGGRP “DATABASE”
                          MSGTARGETMANAGERS
                             MSGTARGETMANAGER
                                TIMETEMPLATE “$OPC_ALWAYS”
                                OPCMGR IP 0.0.0.0 “dbexpert”
                                MSGCONTROLLINGMGR
                             MSGTARGETMANAGER
                                TIMETEMPLATE “$OPC_ALWAYS”
                                OPCMGR IP 0.0.0.0 “dbnotify”
                          ACKNONLOCALMGR
                     MSGTARGETRULE
                     DESCRIPTION “Financial Application”
                          MSGTARGETRULECONDS
                             MSGTARGETRULECOND
                             DESCRIPTION “Financial appl. msg”
                                APPLICATION “xyz”
                             MSGTARGETRULECOND
                             DESCRIPTION “CAD appl. messages”
                                APPLICATION “CAD”
                                OBJECT “objxy”
                          MSGTARGETMANAGERS
                             MSGTARGETMANAGER
                                TIMETEMPLATE “$OPC_ALWAYS”
                                OPCMGR IP 0.0.0.0 “Treasury”
                     MSGTARGETRULE
                     DESCRIPTION “Crit. events from imp. systems”
                          MSGTARGETRULECONDS
                             MSGTARGETRULECOND
                             DESCRIPTION “”
                                SEVERITY Critical
                                NODE IP 0.0.0.0 “x1”
                             MSGTARGETRULECOND
                             DESCRIPTION “”
                                SEVERITY Critical
                                NODE IP 0.0.0.0 “x2”
                          MSGTARGETMANAGERS
                             MSGTARGETMANAGER
                                TIMETEMPLATE “$OPC_ALWAYS”
                                OPCMGR IP 0.0.0.0 “master”
```

## Service Hours

The following example template defines service hours for a SAP server with the node name **saparv01**. This node has to be in service on weekdays from 08:00 hours to 16:00 hours.

```
TIMETEMPLATES
   # time template
   TIMETEMPLATE “service hours”
   DESCRIPTION “template match for service hours”
      TIMETMPLCONDS
          TIMETMPLCOND
             TIME FROM 08:00 TO 16:00
             WEEKDAY FROM Monday TO Friday

RESPMGRCONFIGS
   RESPMGRCONFIG
   DESCRIPTION “Define service hours for a SAP server”
      MSGTARGETRULES
          MSGTARGETRULE
          DESCRIPTION “Buffer msg outside service hrs for SAP”
             MSGTARGETRULECONDS
                MSGTARGETRULECOND
                DESCRIPTION “Node with SAP server”
                NODE IP 0.0.0.0 “sapsrv01”
             MSGOPERATIONS
                MSGOPERATION
                TIMETEMPLATE “outside service hours”
                INSERVICE
```

## Scheduled Outage

The following example template defines a scheduled outage that suppresses all messages relating to the application **oracle** from node **sapsrv01**.

```
CONDSTATUSVARS
   CONDSTATUSVAR “ora_on_sapsrv01” False
RESPMGRCONFIGS
   RESPMGRCONFIG
   DESCRIPTION “define outage for oracle on node orasv01”
      MSGTARGETRULES
         MSGTARGETRULE
         DESCRIPTION “outage for oracle on node orasv01”
            MSGTARGETRULECONDS
               MSGTARGETRULECOND
               DESCRIPTION “Node with oracle server”
               CONDSTATUSVAR “ora_on_sapsrv01”
               NODE IP 0.0.0.0 “sapsrv01”
               APPLICATION “oracle”
            MSGOPERATIONS
               MSGOPERATION
               SUPPRESS
```

# Variables

This section lists and defines the variables that can be used with ITO, and gives an output example, where appropriate. Each variable is shown with the required syntax.

**NOTE**

It is also often useful to surround the variable with quotes, especially if it may return a value that contains spaces.

## Environment Variables

The variables listed below can be used before starting up ITO.

`$OPC_BRC_HISTSIZE(env variable)`

Returns the value of the environment variable for the length of the user's Broadcast Command history. The maximum number of commands saved is 128 per user.

`$OPC_ENV(env variable)`

Returns the value of the environmental variable for the user who has started ITO, for example `PATH, NLS_LANG, EDITOR, SHELL, HOME, TERM`.

`$OPC_HOME`

Returns the working directory of the user who starts an ITO GUI session. If `$OPC_HOME` is not set, the working directory is `/tmp`. If the unix user that started the ITO GUI has no write permission in `/tmp`, an error message is displayed but the GUI still starts.

## SNMP Variables

The variables listed below can be used in most SNMP logfile text entry fields (exceptions are noted). The variables can be used within ITO, or passed to external programs.

`<$#>`

Returns the number of variables in an enterprise-specific SNMP trap (generic trap 6 Enterprise specific ID). Sample output: 2

| | |
|---|---|
| <$*> | Returns all variables assigned to the trap. Sample output: `[1] .1.1 (OctetString): arg1 [2] .1.2 (OctetString): kernighan.c.com` |
| <$@> | Returns the time the event was received as the number of seconds since the Epoch (Jan 1, 1970) using the *time_t* representation. Sample output: `859479898` |
| <$1> | Returns one or more of the possible trap parameters that are part of an SNMP trap. (<$1> returns the first variable, <$2> returns the second variable, etc.) |
| <$\>1> | Returns all attributes greater than *n* as *value* strings, useful for printing a variable number of arguments. `<$\>0>` is equivalent to `$*` without sequence numbers, names, or types. Sample output: `richie.c.com` |
| <$\>+1> | Returns all attributes greater than *n* as *name:value* string. Sample output: `.1.2: richie.c.com` |
| <$+2> | Returns the nth variable binding as *name:value*. (Note: not valid in the command field.) Sample output: `.1.2: ritchie.c.com` |
| <$\>-n > | Returns all attributes greater than *n* as *[seq] name (type): value* strings. Sample output: `[2] .1.2 (OctetString): kernighan.c.com` |
| <$-2> | Returns the nth variable binding as *[seq] name-type:value*. (Note: not valid in command field.) Sample output: `[2] .1.2 (OctetString): ritchie.c.com` |
| <$A> | Returns the node which produced the trap. Sample output: `ritchie.c.com` |
| <$C> | Returns the community of the trap. Sample output: `public` |
| <$c> | Returns the event's category. Sample output: `SNMP` |
| <$E> | Returns the enterprise ID of the trap. Sample output: `.1.3.6.1.4.1.11.2.17.1` |
| <$e> | Returns the enterprise object ID. Sample output: `.1.3.6.1.4.1.11.2.17.1` |

| | |
|---|---|
| <$F> | Returns the textual name of the remote pmd's machine if the event was forwarded. Sample output: `kernighan.c.com` |
| <$G> | Returns the generic trap ID. Sample output: `6` |
| <$MSG_OBJECT> | Returns the name of the object associated with the event. This is set in the `Message Defaults` section of the `Add/Modify SNMP Trap` window. Note: this returns the default object, not the object set in the conditions window. |
| <$N> | Returns the event name (textual alias) of the event format specification used to format the event, as defined in the Event Configurator. Sample output: `OV_Node_Down` |
| <$O> | Returns the name (object identifier) of the event. Sample output: `.1.3.6.1.4.1.11.2.17.1.0.58916865` |
| <$o> | Returns the numeric object identifier of the event. Sample output: `.1.3.6.1.4.1.11.2.17.1.0.58916865` |
| <$R> | Returns the true source of the event. This value is inferred via the transport mechanism which delivered the event. Sample output: `kernighan.c.com` |
| <$r> | Returns the implied source of the event. This may not be the true source of the event if the true source is proxying for another source, such as when a monitoring application running locally is reporting information about a remote node. Sample output: `richie.c.com` |
| <$S> | Returns the specific trap ID. Sample output: `5891686` |
| <$s> | Returns the event's severity. Sample output: `Normal` |
| <$T> | Returns the trap time stamp. Sample output: `0` |
| <$V> | Returns the event type, based on the transport from which the event was received. Currently supported types are SNMPv1, SNMPv2, CMIP, GENERIC, and SNMPv2INFORM. Sample output: `SNMPv1` |
| <$X> | Returns the time the event was received using the local time representation. Sample output: `17:24:58` |

<$x> Returns the date the event was received using the local date representation. Sample output: 03/27/97

## Logfile, Console, and ITO Interface Templates

The variables listed below can be used in most logfile, Console, and ITO Interface template text entry fields (exceptions are noted). The variables can be used within ITO, or passed to external programs.

<$OPTION(N)> Returns the value of an optional variable that is set by opcmsg or opcmon (for example, <$OPTION(A)> <$OPTION(B)>, etc.). Refer to the opcmsg or opcmon man page for information about how to set this variable.

<$MSG_APPL> Returns the name of the application associated with the message. This name is set in the Message Defaults section of the Add/Modify Logfile or Add/Modify Console Messages windows. However, if a console message already has a value for this field, <$MSG_APPL> is not overwritten by an entry in the Add/Modify Console Messages window. Sample output:
/usr/bin/su(1) Switch User

<$MSG_GRP> Returns the default message group of the message, as set in the Message Defaults section of the Add/Modify Logfile, Add/Modify Console Messages, Add/Modify Interface Messages window. Sample output: Security

<$MSG_SEV> Returns the default value for the severity of the message. This is set in the Message Defaults section of the Add/Modify Logfile, Add/Modify Console Messages, Add/Modify Interface Messages window.
Sample output: Normal

<$MSG_TEXT> Returns the full text of the message. Sample output:
SU 03/19 16:13 + ttyp7 bill-root

<$MSG_TYPE> Returns the default name set for Message Type. This is set in the Add/Modify Console Messages or Condition No. window.

<$OPC_MGMTSV> Returns the name of the current ITO management server. Sample output:
`richie.c.com`

The following variables are only available for the MPE/iX console message source template. See “Generating a New NMEV Marker” on page 249 for a description of the format of the NMEV marker and how it is generated.

<$NMEV_SEV> Returns the severity of the message as set within the NMEV marker, if the marker is present in the original messages.
Sample output: `2`

<$NMEV_APPL> Returns the MPE/iX Application ID that is set within the NMEV marker, if the marker was present in the original message.
Sample output: `05`

<$NMEV_CLASS>
Returns the class field that was set within the NMEV marker, if the marker was present in the original message.
Sample output: `194`

## Threshold Monitor Templates

The variables listed below can be used in most threshold monitor template text entry fields (exceptions are noted). The variables can be used within ITO, or passed to external programs.

<$MSG_ID>
Returns the unique identity number of the message, as generated by the message agent. (Note: suppressed messages do not have message IDs.) Sample output:
`6e998f80-a06b-71d0-012e-0f887a7c0000`

<$MSG_NODE>
Returns the IP address of the node on which the message originates. Sample output: `14.136.122.123`

<$MSG_NODE_NAME>
Returns the name of the node on which the message originates. Sample output: `richie.c.com`

<$NAME>

Returns the name of a threshold monitor. This is set in the `Monitor Name` field of the `Add/Modify Monitor` window. Sample output: `cpu_util`

`<$THRESHOLD>`

Returns the value set for a monitor threshold. This is set in the `Threshold:` field on the `Add/Modify Monitor` window. Sample output: `95.00`

`<$VALAVG>`

Returns the average value of all messages reported by the threshold monitor. Sample output: `100.00`

`<$VALCNT>`

Returns the number of times that the threshold monitor has delivered a message to the browser. Sample output: `1`

`<$VALUE>`

Returns the value measured by a threshold monitor. Sample output: `100.00`

## Broadcast Applications and User Interface

The variables listed below can be used in most broadcast application text entry fields (exceptions are noted). The variables can be used within ITO, or passed to external programs.

`$OPC_ENV(env variable)`

Returns the value of the environment variable for the user who has started ITO, for example `PATH, NLS_LANG, EDITOR, SHELL, HOME, TERM`.

`$OPC_EXT_NODES`

Returns the node pattern of all external nodes that are selected at the time the application is executed. The names are separated by spaces.

`$OPC_GUI_CLIENT`

Returns the hostname of the client where the Java-based GUI is currently running.

`$OPC_MSGIDS_ACT`

Returns the Message IDs (UUIDs) of the messages currently selected in the Active/All and any openView Message Browser(s). Note that if the same message is selected in more than one of these browsers, the

duplicate selections will be ignored. Sample output:
```
85432efa-ab4a-71d0-14d4-0f887a7c0000
a9c730b8-ab4b-71d0-1148-0f887a7c0000
```

`$OPC_MSGIDS_HIST`

Returns the Message IDs (UUID) of the messages currently selected in the History Message Browser. Sample output:
```
edd93828-a6aa-71d0-0360-0f887a7c0000
ee72729a-a6aa-71d0-0360-0f887a7c0000
```

`$OPC_MSGIDS_PEND`

Returns the Message IDs (UUID) of the messages currently selected in the Pending Messages Browser. Sample output:
```
edd95828-ac2a-71d0-0360-0f887a7c0000
ee96729a-ada9-71d0-0360-0f887a7c0000
```

`$OPC_NODES`

Returns the names of all regular nodes that are selected at the time the application is executed. The names are separated by spaces. The nodes need not be in the node bank. Nodes can be selected directly in a submap of the IP Map. Sample output:
```
kernighan.c.com richie.c.com
```

`$OPC_USER`

Returns the name of the ITO user who is currently logged in on the management server. Sample output:
```
opc_adm
```

## Time Templates

The variables listed below can be used in ITO time templates. See `/etc/opt/OV/share/conf/OpC/mgmt_sv/tmpl_respmgrs/example.m2`. For example.

| | |
|---|---|
| `$OPC_ALWAYS` | This variable allows you to specify that the time condition is always true. |
| `$OPC_PRIMARY_MGR` | This variable enables ITO to always send the messages to the current primary manager. |

# 6 Installing/Updating the ITO Configuration on the Managed Nodes

This chapter describes how to install/update the ITO configuration on the managed nodes. In addition to this chapter, you should also read the *HP OpenView IT/Operations Concepts Guide*, for a fuller understanding of the elements and the windows you can use to review or customize them.

# Configuration Installation/Update on Managed Nodes

This section contains information concerning the distribution of the ITO agent configuration within your environment.

## Script and Program Distribution to Managed Nodes

ITO enables you to distribute commonly-used scripts and programs to the managed nodes. ITO only distributes these scripts and programs if they are not installed on the managed node, or if a newer version is available on the management server. However, in order to reduce network traffic and speed up distribution, note the following points:

1. Put only commonly used binaries into the

   `/var/opt/OV/share/databases/OpC/mgd_node/customer/\<`*arch*`>/{monitor|actions|cmds}`

   subdirectories, because the entire directory contents are installed on each specified node, where <*arch*> is:

   - ❏ hp/s700/hp-ux
   - ❏ hp/s700/hp-ux10
   - ❏ hp/pa-risc/hp-ux11
   - ❏ hp/s800/hp-ux
   - ❏ hp/s800/hp-ux10
   - ❏ hp/s900/mpe-ix
   - ❏ dec/alpha/unix
   - ❏ ibm/intel/os2
   - ❏ ibm/rs6000/aix
   - ❏ ms/alpha/nt
   - ❏ ms/intel/nt
   - ❏ ncr/3000/unix

- ❏ novell/intel/nw
- ❏ olivetti/intel/unix
- ❏ pyramid/mips/unix
- ❏ sco/intel/unix
- ❏ sco/intel/uw
- ❏ sequent/intel/dynix
- ❏ sgi/mips/irix
- ❏ sni/mips/sinix
- ❏ sun/sparc/solaris

2. If you need a certain binary to be present only on specific systems, transfer the file manually. Furthermore, do not put the file in the default directory on the managed nodes. because the contents of this directory are erased each time the binaries are distributed. For example, do not put customized commands in the directory:

   `/opt/OV/bin/OpC/cmds`

3. Specify the full path name of the customized script in the appropriate ITO configuration. Alternatively, make sure the file is available via the *$PATH* settings of the executing user on the managed node.

   This is an example of a customized script to determine running processes, which can be called as an application on the Application Desktop or as a broadcast command:

   `/name/opc_op/scripts/my_ps`

   or

   `my_ps`

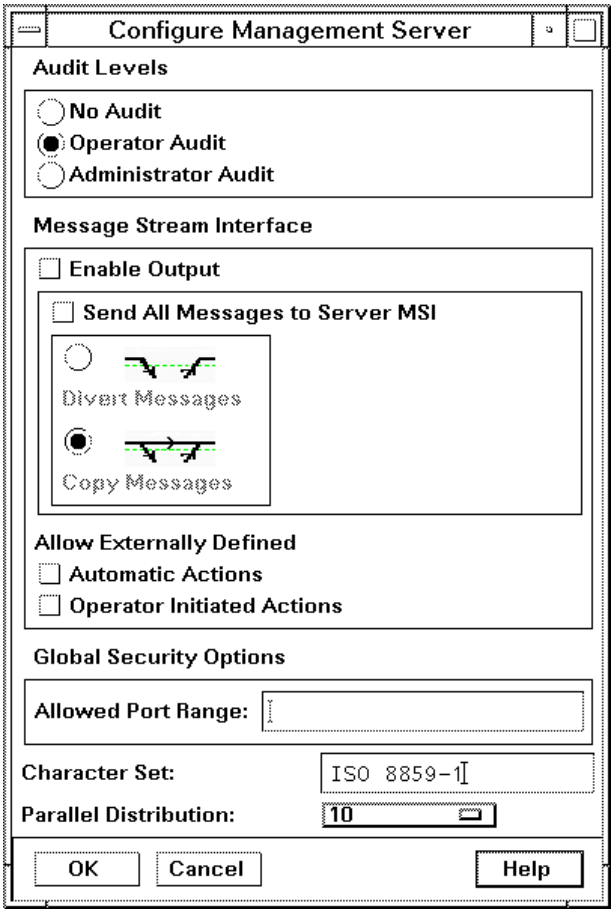
   and the *$PATH* variable of the executing user on the managed node must contain `/name/opc_op/scripts`.

4. If many distribution requests are handled by the distribution manager at the same time, the performance of other ITO services such as the message manager can slow down. If this happens, some managed nodes might not be able to receive data because the distribution manager is too busy, and a warning message is displayed. To avoid this:

   - Minimize the number of managed nodes getting new configuration data at the same time:

  - Select only a few nodes at a time in the `IP map`, `Node Bank`, or `Node Group Bank` window.
  - In the `Node Bank` or `Node Group Bank` window, open the `Configure Management Server` window by selecting `Actions: Server->Configure`... This is shown in Figure 6-1. Set a low number in the `Parallel Distribution` field. For more information, press **F1** to see help on this field.
- Reduce the process priority of `opcdistm` (distribution manager) on the management server using the `renice(1)` command.

**Figure 6-1 Configure Management Server Window**




5. If identical files for actions|cmds|monitor are found in the following directories:

   `/var/opt/OV/share/databases/OpC/mgd_node/customer/\<arch>`

   and:

   `/var/opt/OV/share/databases/OpC/mgd_node/vendor/\<arch>/<ito_version>/<package_type>`

   the customer's file is used in preference.

6. ITO compresses the `monitor|actions|cmds` binaries. Do not put a file into the following directory, if the same file name already exists with a .Z extension:

   `/var/opt/OV/share/databases/OpC/mgd_node/customer/\<arch>/{monitor|actions|cmds}`

### Tips for Script Program Distribution to UNIX Managed Nodes

- For mixed clusters, the `monitor|actions|cmds` scripts and programs need only be installed once for each architecture type, by selecting one appropriate cluster node.
- The file names of the `monitor|actions|cmds` binaries must not be longer than 14 characters (including the .Z extension if compressed). This limitation is set to ensure smooth processing on nodes running with short file names.

### Tips for Script Program Distribution to HP-UX Managed Nodes

Customer-written programs for HP 9000 series 700 computers (Technical Workstations) should be compiled using the -DA1.1 option (HP-PA compatibility mode). This is because these programs must also run on HP 9000 series 800 computers (Enterprise Servers). (ITO does not distinguish between these two architectures.) If this is not possible, the following symbolic link must be replaced by an ordinary s800/hp-ux directory tree for HP-UX 10.x managed nodes:

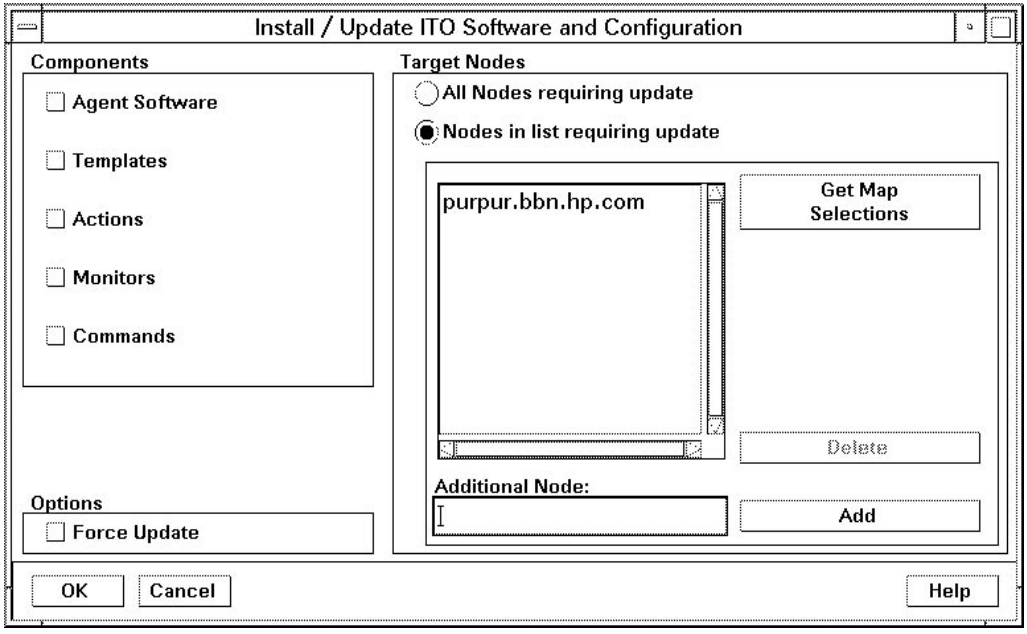
```
/var/opt/OV/share/databases/OpC/mgd_node/customer/hp\
/s800/hp-ux -> ../../s700/hp-ux
```

## Distributing the ITO Agent Configuration to the Managed Nodes

After customizing the configuration and assigning templates to managed nodes, distribute the managed node configuration by selecting both the appropriate managed nodes, and the **Templates** component in the `Install/Update ITO Software and Configuration` window. If no configuration change has been made since the last configuration distribution, no new distribution is triggered unless you select the **`Force Update`** option.

If you have configured actions or monitors in your templates, or commands in your Application Bank/Desktop, these binaries must be distributed as described in the following subsection.

**Figure 6-2 Install/Update ITO Software and Configuration Window**




## Installing/Updating Scripts and Programs on Managed Nodes

ITO provides the distribution of commonly-used scripts and programs. These can be called as automatic or as operator-initiated actions, or as scheduled actions. Furthermore, these scripts can be used for broadcasting commands or other procedures from the Application Desktop, or they can be used by the monitoring agent and logfile encapsulator.

To distribute the appropriate files, select the corresponding options in the `Install/Update ITO Software and Configuration` window. These scripts and programs are distributed only if they are not already installed on the managed node, or when a newer version is available on the management server.

**NOTE** To update only the changes in the configuration, do not select the **Force Update** option; the **Force Update** option (re-)distributes all files causing an increase in network load.

The scripts and programs must be located in the directories on the management server as listed in Table 6-1.

**Table 6-1 Location of Scripts and Programs Provided by Customers**

| Script/Program | Location [a] |
|---|---|
| Automatic, Operator -initiated, and Scheduled Actions | `/var/opt/OV/share/databases/OpC/mgd_node/customer\ /<arch>/actions/*` |
| Monitoring scripts/ programs used by monitoring agent and logfile encapsulator | `/var/opt/OV/share/databases/OpC/mgd_node/customer\ /<arch>/monitor/*` |
| Scripts/programs called via Command Broadcast or started from the Application Desktop | `/var/opt/OV/share/databases/OpC/mgd_node/customer\ /<arch>/cmds/*` |

a. Where <arch> is the platform-specific directory, for example: `hp/s700/hp-ux10`

On managed nodes, the scripts and programs are put into the directories listed in Table 6-2 and Table 6-3.

**Table 6-2 Temporary Directories for Distributed Scripts and Programs on Managed Nodes**

| Managed Node | Operating System | Temporary Directory |
|---|---|---|
| DEC Alpha | Windows NT | `/usr/OV/tmp/OpC/bin/alpha/actions`<br>`/usr/OV/tmp/OpC/bin/alpha/cmds`<br>`/usr/OV/tmp/OpC/bin/alpha/monitor` |
| DEC Alpha AXP | Digital UNIX | `/var/opt/OV/tmp/OpC/bin/actions`<br>`/var/opt/OV/tmp/OpC/bin/cmds`<br>`/var/opt/OV/tmp/OpC/bin/monitor` |
| HP 3000/900 | MPE/iX | `TMPACT.OVOPC`<br>`TMPCMDS.OVOPC`<br>`TMPMON.OVOPC`<br>`.ZOVOPC` (for compressed files) |
| HP 9000/[78]00 | HP-UX 10.x and 11.x | `/var/opt/OV/tmp/OpC/bin/actions`<br>`/var/opt/OV/tmp/OpC/bin/cmds`<br>`/var/opt/OV/tmp/OpC/bin/monitor` |
| IBM RS/6000, Bull DPX/20 | AIX | `/var/lpp/OV/tmp/OpC/bin/actions`<br>`/var/lpp/OV/tmp/OpC/bin/cmds`<br>`/var/lpp/OV/tmp/OpC/bin/monitor` |

| Managed Node | Operating System | Temporary Directory |
|---|---|---|
| Intel 486 or higher | DYNIX/ptx | `/var/opt/OV/tmp/OpC/bin/actions`<br>`/var/opt/OV/tmp/OpC/bin/cmds`<br>`/var/opt/OV/tmp/OpC/bin/monitor` |
| | Novell NetWare | `sys:/var/opt/OV/tmp/OpC/bin/actions`<br>`sys:/var/opt/OV/tmp/OpC/bin/cmds`<br>`sys:/var/opt/OV/tmp/OpC/bin/monitor` |
| | OS/2 | `\var\opt\OV\tmp\OpC\bin\actions`<br>`\var\opt\OV\tmp\OpC\bin\cmds`<br>`\var\opt\OV\tmp\OpC\bin\monitor` |
| | SCO OpenServer and UnixWare | `/var/opt/OV/tmp/OpC/bin/actions`<br>`/var/opt/OV/tmp/OpC/bin/cmds`<br>`/var/opt/OV/tmp/OpC/bin/monitor` |
| | Windows NT | `/usr/OV/tmp/OpC/bin/intel/actions`<br>`/usr/OV/tmp/OpC/bin/intel/cmds`<br>`/usr/OV/tmp/OpC/bin/intel/monitor` |
| NCR System 3xxx/4xxx/5xxx (Intel 486 or higher) | UNIX SVR4 | `/var/opt/OV/tmp/OpC/bin/actions`<br>`/var/opt/OV/tmp/OpC/bin/cmds`<br>`/var/opt/OV/tmp/OpC/bin/monitor` |
| Olivetti (Intel PCs) | Olivetti UNIX SVR4 | `/var/opt/OV/tmp/OpC/bin/actions`<br>`/var/opt/OV/tmp/OpC/bin/cmds`<br>`/var/opt/OV/tmp/OpC/bin/monitor` |
| Pyramid mips_r3000 | Pyramid DataCenter/OSx | `/var/opt/OV/tmp/OpC/bin/actions`<br>`/var/opt/OV/tmp/OpC/bin/cmds`<br>`/var/opt/OV/tmp/OpC/bin/monitor` |

| Managed Node | Operating System | Temporary Directory |
|---|---|---|
| Siemens Nixdorf | SINIX | `/var/opt/OV/tmp/OpC/bin/actions`<br>`/var/opt/OV/tmp/OpC/bin/cmds`<br>`/var/opt/OV/tmp/OpC/bin/monitor` |
| Silicon Graphics | IRIX | `/var/opt/OV/tmp/OpC/bin/actions`<br>`/var/opt/OV/tmp/OpC/bin/cmds`<br>`/var/opt/OV/tmp/OpC/bin/monitor` |
| Sun SPARCstation | Solaris | `/var/opt/OV/tmp/OpC/bin/actions`<br>`/var/opt/OV/tmp/OpC/bin/cmds`<br>`/var/opt/OV/tmp/OpC/bin/monitor` |

The binaries are located in the temporary directories only during the distribution phase. When distribution is completed, the local ITO action and monitor agents are stopped, the binaries moved/copied to their final destination, and the ITO action and monitor agents restarted.

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

| Managed Node | OS | Directory | Access Rights |
|---|---|---|---|
| DEC Alpha AXP | Digital UNIX | `/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) |
| DEC Alpha | WindowsNT | `/usr/OV/bin/OpC/alpha/actions` | Administrator (full access) |
| | | `/usr/OV/bin/OpC/alpha/cmds` | Administrator (full access) |
| | | `/usr/OV/bin/OpC/alpha/monitor` | Administrator (full access) |

| Managed Node | OS | Directory | Access Rights |
|---|---|---|---|
| HP 9000/700<br>HP 9000/800. | HP-UX 10.x and 11.x | `/var/opt/OV/bin/OpC/actions` | rwxr — r —<br>(owner: root) |
| | | `/var/opt/OV/bin/OpC/cmds` | rwxr-xr-x<br>(owner: root) |
| | | `/var/opt/OV/bin/OpC/monitor` | rwxr — r —<br>(owner: root) |
| HP 3000/900 | MPE/iX | `ACTIONS.OVOPC`<br>`cap=BA,IA,PM,MR,DS,PH` | R,X,L,A,W,S:AC |
| | | `COMMANDS.OVOPC`<br>`cap=BA,IA,PM,MR,DS,PH` | R,X:ANY;L,A,W,S:AC |
| | | `MONITOR.OVOPC`<br>`cap=BA,IA,PM,MR,DS,PH` | R,X,L,A,W,S:AC |
| IBM RS/6000,<br>Bull DPX/20 | AIX | `/var/lpp/OV/OpC/actions` | rwxr — r —<br>(owner: root) |
| | | `/var/lpp/OV/OpC/cmds` | rwxr-xr-x<br>(owner: root) |
| | | `/var/lpp/OV/OpC/monitor` | rwxr — r —<br>(owner: root) |

| Managed Node | OS | 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) |
| | OS/2 | `\var\opt\OV\bin\OpC\actions` | rwx[a] |
| | | `\var\opt\OV\bin\OpC\cmds` | rwx[a] |
| | | `\var\opt\OV\bin\OpC\monitor` | rwx[a] |
| | SCO OpenServer UnixWare DYNIX | `/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) |
| | WindowsNT | `/usr/OV/bin/OpC/intel/actions` | Administrator (full access)<br>Everyone (rx) |
| | | `/usr/OV/bin/OpC/intel/cmds` | Administrator (full access)<br>Everyone (rx) |
| | | `/usr/OV/bin/OpC/intel/monitor` | Administrator (full access)<br>Everyone (rx) |

| Managed Node | OS | Directory | Access Rights |
|---|---|---|---|
| NCR System 3xxx/4xxx/5xxx (Intel 486 or higher | UNIX SVR4 | /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) |
| Olivetti (INTEL PCs) | Olivetti UNIX | /var/opt/OV/bin/OpC/actions | rwxr-r- (owner: root) |
| | | /var/opt/OV/bin/OpC/cmds | rwxr-xr-r-x (owner: root) |
| | | /var/opt/OV/bin/OpC/monitor | rwxr-r- (owner: root) |
| Pyramid mips_r3000 | Data Center/ OSx | /var/opt/OV/bin/OpC/actions | rwxr-r-(owner: root) |
| | | /var/opt/OV/bin/OpC/cmds | rwxr-xr-r-x (owner: root) |
| | | /var/opt/OV/bin/OpC/monitor | rwxr-r- (owner: root) |
| Siemens Nixdorf | SINIX | /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) |

| Managed Node | OS | Directory | Access Rights |
|---|---|---|---|
| Silicon Graphics | IRIX | `/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) |
| Sun SPARCstation | Solaris | `/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) |

a. OS/2 has only write-access permission; files that can be read can also be executed if a read-only flag is set. OS/2 does not support a user concept.

The ITO action agent and monitor agent append the appropriate directories to the *$PATH* setting of the executing user.

# 7 Integrating Applications into ITO

This chapter describes how to integrate applications into ITO. The *HP OpenView IT/Operations Concepts Guide* provides more detailed information on the elements and the windows you can use to carry out the integration. See also the *HP OpenView IT/Operations Application Integration Guide* available with the HP OpenView IT/Operations Developer's Toolkit.

# Integrating Applications into ITO

ITO allows graphical invocation of applications ("point and click") by means of the operators' `Application Desktop`. A different set of applications can be assigned to each ITO operator to match specific requirements.

If you have purchased an application which is prepared for ITO integration (for example, HP OpenView OpenSpool, HP OpenView OmniBack II, or HP OpenView OmniStorage) you can integrate it quickly and easily using `opccfgupld(1M)`.

You can integrate applications into the following components of ITO:

- operators' `Application Desktop` or administrator's `ITO Application Bank`
- broadcast
- automatic/operator-initiated actions, and scheduled actions
- monitoring
- logfile encapsulation
- SNMP trap and message interception

This section also explains how ITO starts applications and broadcasts.

## Integrating Applications into the Application Desktop

You can add your own applications to the `ITO Application Bank` and assign them to an operator. The applications are then invoked when the operator double-clicks a symbol in the `Application Desktop`. You can add the following types of applications to the `ITO Application Bank`:

- ITO applications
- HP OpenView applications

### ITO Applications

Typically, ITO applications are utilities that provide services of a general nature. When integrated into the `Application Desktop`, they help build a set of management tools.

The application is invoked when the user double-clicks the icon that represents it. Information, such as selected nodes, can be passed as arguments to the applications, and the applications are invoked using the ITO access mechanisms. You add the application by filling in the appropriate fields in the `Add ITO Application` and `Add Internal Application` window. This is the easiest and quickest method to integrate an application into the `ITO Application Bank`. For further details, see the administrator's online help and the *HP OpenView IT/Operations Application Integration Guide*.

### HP OpenView Integrated Applications

Plug-in of HP OpenView integrated applications is provided by Application Registration Files (ARFs) which define how users access applications and how application processes are managed. HP OpenView applications also have access to HP OpenView windows through the HP OpenView Windows Applications Programming Interface (API). This is useful, for example, for generating application-specific submaps, as done by HP OpenView OpenSpool, HP OpenView OmniBack II, and HP OpenView OmniStorage. For more details about general HP OpenView application integration, see the *HP OpenView Windows Developers Guide*.

For more information concerning how to integrate HP OpenView applications into ITO, see the administrator's online help and *HP OpenView IT/Operations Application Integration Guide*.

## Examples of Application Integration Tasks

### Integrating the IP Map and Network Node Manager for IP

Applications which are a part of Network Node Manager are already integrated with the HP OpenView platform. Therefore, these applications can easily be integrated into ITO as OV Applications or OV Services.

However, note that:

- If you have defined them to do so in the application registration file (ARF), both OV Application and OV Service integrations can cause a daemon to start running when the ITO session is started.
- By integrating ITO as an OV Application you integrate a single action as a desktop icon (as defined in the ARF).
- By integrating ITO as an OV Service you integrate all actions as menu items (as defined in the ARF).

**NOTE**

New users who do not have the IP-Map application assigned can still log in to ITO and run the command; **`ovw -map <user_name>`**, which opens a "fake" IP Map for the specified user that is also present each time the same user subsequently starts ITO. However, the user cannot do anything with this faked IPMap as the full menus and services that are usually present in the `IP Map` window are not available in this instance. The ITO administrator should ensure that the directory tree `/var/opt/OV/share/databases/openview/mapdb` is owned by root.

### Allowing an Operator to View and Manage the opology of IP Networks in the IP Map.

1. Working as the administrator, from the menu bar of the root IP Map, select `Window:Application Bank`…. The `ITO Application Bank` window opens.
2. Double-click on the application group labeled `OV Services`.
3. Drag and drop the application labeled `IP Map` into an operator's `Assigned Applications` window to enable the operator to manage the IP topology.
4. (Re-)start the operator session.
5. Verify that the IP topology is being built under the IP Internet symbol in the root submap.

### Integrating "Ethernet Traffic HP" as an OV Application.

1. Working as the administrator, from the menu bar of the root IP Map, select `Window:Application Bank`…. The `ITO Application Bank` window opens.
2. As administrator, from the menu bar select `Actions:Applications->Add OV Application`…. The `Add OV Application` window opens.

3. In the Add OV Application window enter the following application attributes:

   Application Name: **Ethernet Traffic HP**

   OV Registration Application Name: **IP Graphs**

   OV Registration Action Identifier: **etherTrafficHP**

   And select [Use Objects selected by Operator].

4. Click on [OK].

5. Invoke this application as administrator and as operator:

   a. As administrator:

      Log out and log in again, to use this OV Application. Select a node and double-click on the Ethernet Traffic HP application in the ITO Application Bank.

      Drag and drop this OV application into an operator's Assigned Applications window to enable the operator to monitor the ethernet traffic. (Re-)start the operator's session.

   b. As operator:

      Select a node and double-click on the Ethernet Traffic application in the Application Desktop.

### Integrating "IP Activity Monitoring - Tables" as an OV Service.

1. Working as the administrator, from the menu bar of the root IP Map, select Window:Application Bank…. The ITO Application Bank window opens.

2. As administrator, from the menu bar select Actions:Applications->Add OV Service…. The Add OV Service window opens.

3. In the Add OV Service window enter the following application attributes:

   Application Name: **IP Monitoring - Tables**

   OV Registration Application Name: **IP Tables**

4. Click on [OK].

5. Invoke this application as administrator and as operator:

a. As administrator:

   Log out and log in again to use this OV Service, click on a node and select one of the menu items in the IP Map under `Performance:Network Activity` or `Configuration:Network Configuration`.

   Copy this OV Service into an operator's `Application Desktop` to enable the operator to monitor the IP tables.

b. As operator:

   (Re-)start your session, click on a node and select one of the menu items under `Performance:Network Activity` or `Configuration:Network Configuration`.

## Integrating the RPM Performance Tools

ITO provides preconfigured elements to integrate the HP RPM performance tools: MeasureWare Agent, PerfView, and GlancePlus. The following preconfigured elements are provided in the application group `Performance`:

- Start PerfView

  This application enables you to graph performance data on the selected managed node(s). This application runs on the management server and requires that HP PerfView is installed on the management server.

- Start Glance

  This application starts HP GlancePlus on the managed node. This requires that HP GlancePlus is first installed on the managed node.

In addition, ITO allows you to receive alarms from HP MeasureWare Agents. As performance data is collected by the MeasureWare agent, it is compared with the alarm conditions specified in the MeasureWare alarm definitions file to determine whether the conditions have been met.

When an alarm condition is met, an alarm is generated and a message is sent to the ITO agent. The ITO agent then forwards the alarm to the ITO user(s) responsible for performance messages. The user may select a performance alarm and then click on the `[Perform Action]` button in the Message Browser to cause PerfView to run locally and graph the MeasureWare metrics relating to the specific alarm to examine the relevant metrics.

ITO has predefined conditions in the `opcmsg(1|3)` template that allow it to integrate the MeasureWare alarming functionality into ITO. The opcmsg template defines the messages that can come from the MeasureWare agent, together with the operator-initiated action that starts PerfView.

To enable the PerfView/MeasureWare integration on an ITO agent, do the following:

1. Assign the `opcmsg(1|3)` template to all managed nodes.
2. Distribute the `[Commands]` and `[Templates]` components to the managed nodes.

To enable the GlancePlus integration, do the following:

❏ Distribute the `[Commands]` components to the managed nodes.

For more information, see the *HP OpenView MeasureWare Agent User's Manual* and the online help for HP PerfView and HP GlancePlus.

## Integrating PerfView 4.0 and MeasureWare Agents

PerfView 3.0 integration is based on the logfile encapsulation of PerfView's alarm log database (logfile `PerfView`, template group `Perfview`).With PerfView 4.0, the PerfView agent is replaced by MeasureWare software called PCS (Performance Collection Software). This software uses unique alarm definitions, which send alarms to the performance manager system. It is possible to configure the software to send:

❏ additional SNMP Traps in case of an alarm

❏ an ITO message via `opcmsg(1|3)`

ITO has predefined conditions in the `opcmsg(1|3)` template that allow it to use MeasureWare functionality on the ITO agent. To run the PerfView 4.0/MeasureWare integration on an ITO Agent, first install PerfView for all managed nodes monitored by PerfView/ITO, then perform the following steps:

1. Assign the `opcmsg(1|3)` template to all managed nodes.
2. Distribute the `[Commands]` and `[Templates]` components to the managed nodes.
3. Assign the PerfView 4.0/MeasureWare application to the appropriate operators.

## Running PerfView 3.0 and PerfView 4.0 in parallel

If you upgrade some managed nodes from PerfView 3.0 to the MeasureWare agent, remember to perform either one of the following two steps to avoid receiving redundant PerfView alarms:

- ❏ unregister MeasureWare agents from the PerfView 3.0 analysis station (PerfView's central alarm logfile)
- ❏ modify the `PerfView` logfile template in ITO to intercept only the events originating from those managed nodes where PerfView 3.0 is installed

## Allowing the Operator to Control ITO Agents

By default only an ITO administrator is allowed to start or stop ITO agents on the managed nodes via the ITO GUI. However, changes to this policy may be made by updating `ITO Status`, which ITO provides (in the `Application Bank`) as a preconfigured ITO Application.

If you wish to allow the operators to control ITO agents, make two copies of the "ITO Status" application, exchange the parameters, label and description texts and, finally, assign these applications to your operators. To do this, carry out the following steps:

1. From the menu bar, select `Window:Application Bank`…. The `Application Bank` window opens.
2. Select the application `ITO Status` from the `Application Bank`.
3. Copy this application using `Actions:Application->Copy` and modify it to become the `ITO Agents Start` application:
   a. Change the attributes as follows:

      `Application Name:` **`ITO Agents Start`**

      `Description:` **`Starting of ITO Agents`**

      `Application call:`

      **`/opt/OV/bin/OpC/opcragt -start $OPC_NODES`**

      `Start on Target Node List:` leave field empty

      `Executing user:` **`root`**

      `Password:` leave field empty

b. Select [No Window] (for example, X Application) from the option button.

c. Click on [OK].

4. Select again the application labeled ITO Status from the Application Bank.

5. Copy this application using Actions:Application->Copy and modify it to become the ITO Agents Stop application:

   a. Change the attributes as follows:

      Application Name: **ITO Agents Stop**

      Description: **Stopping of ITOAgents**

      Application call:

      **/opt/OV/bin/OpC/opcragt -stop $OPC_NODES**

      Start on Target Node List: leave field empty

      Executing user: **root**

      Password: leave field empty

   b. Select [No Window] (for example, X Application) from the option button.

   c. Click on [OK].

6. Assign the new applications to the appropriate users.

## Integrating Applications as Broadcast Commands

Applications can be launched on several systems at the same time using the ITO broadcast command facility in the Application Desktop/Application Bank.

The application must be accessible via the executing user's *$PATH* settings on UNIX systems, or the path must be fully qualified on the Broadcast Command window. Note that the application must be available on the managed node.

You can also distribute simple and widely used applications via ITO to managed nodes as explained in "Distributing the ITO Agent Configuration to the Managed Nodes" on page 305.

## Integrating Applications as Actions

An application or script may be configured to run as an automatic or operator-initiated action, or a scheduled action. An automatic action is triggered by a message received in ITO. An operator-initiated action is merely enabled by a message received in ITO; it is executed by the operator. Operator-initiated actions may also be triggered by the administrator, via the message browser. Scheduled actions are configured by the administrator and execute a routine task at a configured time. These actions are always performed by the ITO action agent, which operates as **root** on UNIX systems, as **AGENT.OVOPC** on MPE/iX systems, and as HP ITO Account on Windows NT systems. Note that the action must be available on the managed node.

**NOTE**

Note that HP ITO Account is part of the Administrator, Domain Administrator and User Administrator groups. If an action is prohibited for one of these groups, the HP ITO Account will not be able to perform that action.

The application must be accessible via the **root**'s *$PATH* settings on UNIX systems, or the path must be fully qualified on the corresponding message condition configuration window.

You can also distribute simple and widely used applications via ITO to the managed node as explained in "Distributing the ITO Agent Configuration to the Managed Nodes" on page 305.

## Integrating Monitoring Applications

Applications can be used for monitoring purposes if they deliver the monitored object status using the `opcmon(1)` command or `opcmon(3)` API.

The monitoring application must be accessible via the **root**'s *$PATH* settings on UNIX systems, or the path must be fully qualified on the corresponding monitor configuration window. Note that the application must be available on the managed node.

You can also distribute simple and widely used monitoring applications via ITO to the managed node as explained in "Distributing the ITO Agent Configuration to the Managed Nodes" on page 305.

## Application Logfile Encapsulation

Applications can be monitored by observing their logfiles. Logfile entries can be forwarded into ITO, or suppressed. The message can be restructured and ITO specific attributes can be set up. For more details refer to the `Message Source Templates` window of the ITO administrator's GUI.

**NOTE**

Most applications running on Windows NT systems use **Eventlogs**. The information in these databases can be extracted by the logfile encapsulator, but there are some differences in the set-up procedure. Refer to the ITO online help or the *HP OpenView IT/Operations Concepts Guide* for more information.

## Application Message Interception

The applications that ITO can make use of to integrate a message, include:

- Logfiles
- SNMP traps
- `opcmsg(1)` command
- opcmsg(3) API

These messages can then be either suppressed or forwarded according to the configuration of ITO. In addition, the message can be restructured, and ITO-specific attributes set up. For MPE/iX systems, ITO also supports console message interception.

For more details, see the `Message Source Template` window in the administrator's ITO GUI.

## Server Message Stream Interface API

Applications can also register to receive messages on the management server using the Message Stream Interface (MSI) API on the ITO management server. This interface lets you plug in event correlation engines, and statistical analysis tools to establish a link to other network and system management applications.

Messages are intercepted before they are added to the ITO database and before they are displayed in the ITO message browsers. For further information, see the documentation available with the HP OpenView IT/Operations Developer's Toolkit.

## How ITO Starts ITO Applications and Broadcasts on Managed Nodes

Before the application or the broadcast command is started on the managed node, the profile of the executing user is performed programmatically. Note the following restrictions concerning user profiles:

- Do not ask for specific user input in the profile. Instead, you can provide an appropriate default value, to be returned only when **Return** is pressed.

  For example, the following script for HP-UX 10.x produces an endless loop if no valid answer is specified.

```
#!/usr/bin/sh
TERM=""
while [ -z "${TERM}" ]
do
 echo "Type of terminal (hp|vt100): \c"
 read TERM
 if [ "${TERM}" != "hp" -a "${TERM}" != "vt100" ]
 then
   TERM=""
 fi
done
```

  The correct way to specify the default value is shown below. Note that if no valid answer is specified, a default value is used.

```
#!/usr/bin/sh
echo "Type of terminal (hp=default|vt100): \c"
read TERM
if [ "${TERM}" != "hp" -a "${TERM}" != "vt100" ]
then
  TERM=hp
fi
```

- Command broadcast and startup of the following applications (none of which require a separate terminal window) are done via the ITO action agent:

  - application configured as `Window (Output Only)`
  - application configured as `Window (Input/Output)`

- application configured as `No Window (eg X Application)`

During the profile execution `stdin`, `stdout` and `stderr` are not available, so you should avoid commands reading from standard input or writing to standard output/error. Especially avoid commands such as:

- `stty`
- `tset`
- startup of window (input/output) applications

❏ If a delay of more than 2 seconds occurs during output or input activity, ITO assumes that an error has occurred, and it stops execution. This could happen, for example, if a program runs for more than 2 seconds without generating output.

❏ Do not ask more than four questions in the user's profile, since ITO only answers up to four prompts with **Return**.

❏ Do not add a logout message to the user's profile because ITO adds the message at the end of the applications output. In addition, do not use sequences of escape characters in the profile because these are also added to the application output, causing it to be garbled.

## SMS Integration

The ITO/SMS integration is a collection of monitors and templates that provides the ITO NT agent with the ability to monitor an SMS installation in the PC subnet of an IT environment. This allows ITO users to monitor the environment of NT nodes, and to restart SMS services if they fail.

NT agents installed on every Site Server report SMS information about the entire SMS hierarchy *without* using any SMS mechanisms.

### Supported Versions of SMS

ITO supports both the English and the Japanese System Management Server (SMS) 1.2 on Microsoft Windows NT Server 3.51 and 4.0.

## How to integrate ITO with SMS

The ITO/SMS integration has two parts. The first consists of the standard NT application event log template, and the second consists of a specific SMS application event log template and fourteen threshold monitors. This sections explains how to set up and install these templates and monitors.

1. Assign the SMS monitors and templates to the appropriate NT servers.

   The SMS integration contains fourteen threshold monitors that monitor SMS services, an **UP** and **DWN** monitors for each service (see Table 7-1). One or both of these monitors should be assigned to the NT systems that run the services that the templates will monitor. The DWN monitor sends ITO 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 UP monitor sends ITO a message when the service is running again. (UP monitors never have an associated action.)

**Table 7-1 ITO SMS Monitors for SMS Services**

| ITO SMS Monitors | SMS Service | Restart* |
|---|---|---|
| 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 |

| ITO SMS Monitors | SMS Service | Restart* |
|---|---|---|
| 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 |

* OA = Operator Action; AA= Automatic Action

The Application Event Log template, `NT SMS`, must be assigned to any SMS Site Server of the SMS hierarchy, but cannot be assigned to the `logon`, `distribution`, or `helper` servers because duplicate reprocessing of problems will result. These servers are also logged into the NT 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.

   There are two templates that must be considered when customizing the template conditions for the SMS Site Server: the SMS-specific application event log template, and the default NT application event log template.

   A `suppress unmatched` condition is the first condition of the SMS application event log template. This condition suppresses all NT 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.

   The default NT Logfile encapsulator template, `dflt_ApplEvLog`, has a `forward unmatched` flag set by default. This means that 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 NT Logfile template. To avoid this problem, add one additional `suppress matched` condition at the beginning of the default NT 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 (and the agent as well, if it is not already installed).

## How SMS messages relate to ITO messages

When ITO reports SMS messages in the Message Browser, it assigns a Message Group and Message Object that is appropriate to the message. The tables below show how the SMS messages will be mapped in ITO.

**Table 7-2 SMS Message assignment to ITO Message Groups**

| SMS Message | ITO Message Group |
|---|---|
| All messages containing one of the words: inventory, job, package, instruction, or compress. | 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 |

**Table 7-3 SMS Event Assignment to ITO Message Objects**

| SMS Events | ITO Message Objects |
|---|---|
| All events that are related to setup, installation, 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 |

## EMS Integration

The Event Monitoring Service (EMS) provides a mechanism for monitoring system resources on HP-UX and sending notifications about these system resources when they change in an observable way. EMS has been integrated into ITO so that it is possible to forward EMS notifications to ITO via the opcmsg (3) API. EMS events complement the range of ITO message sources in that they provide data which is not immediately accessible to ITO; for example, monitors for the status of peripheral components.

Monitoring requests for EMS are configured using the EMS GUI client which is integrated into SAM, the HP-UX system administration tool. To start the EMS GUI, start SAM, for example from the `ITO Application Bank` window, and double-click on the `Resource Management` icon, then on the `Event Monitoring Service` icon. opcmsg(3) has been integrated into the EMS GUI and can be selected as a notification target for EMS events.

EMS also provides preconfigured conditions for the `ITO Interface Messages` template for use with ITO. The ITO-EMS template can be downloaded from `http://software.hp.com`; click on `High Availability`, then on `Event Monitoring Service Developer's Kit`. Download the tar file from the web page and follow the instructions given in the `readme.ito` file.

EMS is available from DART and must be installed before you can use the ITO-EMS templates. For more information about EMS, see the documentation supplied with the EMS product. EMS is only supported on HP Enterprise Servers running HP-UX 10.20 or 11.00.

# 8 ITO Language Support

This chapter describes the language dependencies of the ITO management server processes, managed node commands and processes, and the ITO GUI. It also describes the languages and LANG settings supported for the various ITO platforms. In addition, you will find information on the character sets supported by ITO.

# Language Support on the Management Server

On the management server, localization considerations impact:

- The language used for displaying the status messages of the ITO server and managed nodes in the ITO Motif GUI.
- The character set used for internal processing.

## Language of Messages on Management Server

When the ITO server processes are started, for example, with `ovstart ovacomm` and `ovstart opc`, the currently set locale is evaluated and the related message catalog is selected for use. This usually takes place during system boot, with `ovstart` being issued by:

```
/sbin/init.d/ov500
```

At this point, the *LANG* variable is set to C or not yet set.

If you require the ITO server processes to send their status messages in a different (supported) language, set *LANG* before **`ovstart ovacomm`** is called.

## Internal Processing Character Set on Management Server

ITO supports the Oracle database character sets:

- WE8ISO8859P1
- JA16SJIS

WE8ISO8859P1 is an 8-bit character set which corresponds to ISO8859-1 and supports most Western European languages. The **Shift -JIS** character set is used for the Japanese environment only.

The database character set is set during the ITO installation and determines the internal processing character set of the management server. The database and the ITO management server must have the same internal character set so that they are able to process data correctly and to minimize character set conversions during runtime. The

locale settings used to start the ITO processes must be compatible to the database character set. All input data on the management server must be given in this character set.

## ITO GUI Considerations

ITO uses the setting of the environment variable *LANG*, to determine the language of the message catalog and the GUI. When starting the ITO GUI, the following settings for this variable are supported:

- C, *.iso88591, *.roman8
- ja_JP.SJIS

In the Japanese version of ITO, most text entry fields in the GUI allow you to enter more characters than the database accepts. ITO returns a corresponding error message and asks you to reduce the number of entered characters.

Note that the `Message Browser` displays 8-bit characters (characters of the code value 128 or higher) as dots when *LANG* is set to C or C.iso88591. This only affects how messages are displayed in the GUI; the contents of the ITO database remain unchanged.

**TIP**

ITO also supports running an English ITO GUI in a Japanese environment. In this case, however, although you are running on a Japanese management server you will receive messages and some labels in Japanese, due to various HP OpenView platform restrictions.

If your management server is in a Japanese environment, but you want to receive English messages, set the following language variables as shown: `LANG=ja_JP.SJIS`, and `LC_MESSAGES=C`.

When working with international keyboards, make sure that you have set the *KBD_LANG* variable accordingly. For example, to enter German text containing an umlaut into the ITO GUI:

```
KBD_LANG=de_DE.iso88591; export KBD_LANG
```

### Important X-Resources used by ITO:

The fonts used through the resources described below must be compatible with the internal character set used by the management server. In other words, if you run an environment using the **ISO8859-1** character set, your fonts should be **iso8859-1** fonts. If not, some labels or messages may not display correctly.

ITO uses the system-wide X-resources for window titles and icon labels.

**Table 8-1 System-wide X Resources in a VUE and CDE Environment**

| Resource | Description |
|---|---|
| *FontList | Font used for window titles. |
| Vuewm*icon*fontList | Font used for icon titles. |

ITO-specific resources are set in one of the files listed below:

- English: `/opt/OV/lib/X11/app-defaults/C/Opc`
- Japanese: `/opt/OV/lib/X11/app-defaults/ja_JP.SJIS/Opc`

**Table 8-2 ITO-Specific X Resources Used for Fonts**

| Resource | Description |
|---|---|
| Opc.fixedTextFont | Font used in list boxes, for example, in the Message Browser. |
| Opc.variableTextFont | Font used for other labels in the GUI. |
| Opc.buttonFont | Font used for push buttons, for example, Close. |

# Language Support on Managed Nodes

## Language of Messages on Managed Nodes

ITO managed-node processes determine the language of their messages by the locale that is set. Therefore, if you want these processes to generate, for example, Japanese messages, you must make sure that the locale, and therefore *LANG*, is set appropriately before **`opcagt -start`** is called.

The locale for the ITO agents is set in the system startup script, for example `/etc/rc.config.d/opcagt` on HP-UX 10.x and 11.x. Set `START_LANG` to the locale you want the ITO agent to start in and restart your agents.

See Chapter 3, “File Tree Layouts on the Managed-Node Platforms,” for the location of the system resource files adapted by ITO on all supported agent platforms.

See Table 8-5 on page 341 for *LANG* settings supported on English managed nodes, and Table 8-6 on page 343 for *LANG* settings supported on Japanese managed nodes.

**NOTE** Windows NT, DEC Alpha NT, Novell NetWare, and OS/2 managed nodes use the NT System Language. A LANG environment variable is not available.

**NOTE** HP-UX, AIX, Solaris, Digital UNIX, and Windows NT (Intel-based) are supported in Japanese *and* English environments.

MPE/iX, SGI IRIX, SCO OpenServer, SCO UnixWare, NCR UNIX SVR4, Siemens Nixdorf SINIX, Sequent DYNIX/ptx, Olivetti UNIX, Pyramid DataCenter/OSx, OS/2, and Windows NT on DEC Alpha are only supported in the *English* environment.

### Fileset Requirements on Managed Nodes

Some operating systems must have a specific fileset installed for code-set conversion. See “Managed Node Requirements” on page 29 for software requirements on all managed node platforms.

## Character Sets for Internal Processing on Managed Nodes

The character sets available on platforms supported by ITO can differ from the character set used in the ITO database. Consequently, when a message is generated on a managed node, it must often be converted before it can be sent to the management server and stored in the database.

ITO takes care of this conversion. If necessary, automatic character-set conversions take place through ITO managed node processes before a message is sent to the server.

The character set supported for managed nodes depends on the environment. If you operate in an English environment, your database character set is `WE8ISO8859P1` (Oracle) and the following character sets are supported for ITO managed nodes:

**Table 8-3 Supported Character Sets on Managed Nodes in an English Environment**

| Platform | Character Set |
|---|---|
| HP-UX | ISO 8859-1, ROMAN8, ASCII |
| MPE/iX | ROMAN8 |
| Solaris, AIX, NCR UNIX SVR4, SCO OpenServer, SCO UnixWare, SGI IRIX, Digital UNIX (OSF/1), Sequent DYNIX/ptx, Siemens Nixdorf SINIX, Olivetti UNIX, Pyramid DataCenter/OSx | ISO 8859-1, ASCII |
| Windows NT (Intel and DEC Alpha), Novell NetWare, OS/2 | Multilingual ANSI Code Page 1252[a], ASCII |

a. Code Page 1252 is analogous to ISO 8859-1.

If you operate in a Japanese environment, your database character set is **Shift JIS**, and the following character sets are supported for ITO managed nodes:

**Table 8-4 Supported Character Sets on Managed Nodes in a Japanese Environment**

| Platform | Character Set |
|---|---|
| HP-UX, AIX, Solaris, Digital UNIX | Shift JIS[a], EUC [b], ASCII |
| Windows NT (intel-based) | Japanese ANSI Code Page 932 [c], ASCII |

a. For Solaris, Shift JIS is only supported with Solaris version 2.6 and higher.
b. 2-byte Extended UNIX Code.
c. Code Page 932 is analogous to Shift JIS.

The character set used for a node can be modified in the `Advanced Options` window of the `Add/Modify Node` window. All managed node processing is performed using this character set.

## The ASCII Character Set

ASCII is supported as internal character set on the managed node and as character set for the ITO Logfile Encapsulator. It is a 7-bit character set and therefore a subset of the 8-bit Shift JIS character set. This means that ASCII can be converted to Shift JIS without loss of data and enables you to manage English nodes (running with ASCII as internal character set) with a Japanese management server. Note however, that if you are using ASCII as the character set for internal processing ( in the `Node Advanced Options` window), you must also specify ASCII as the character set for the monitored logfile messages.

**NOTE**

To change the character set of the ITO Logfile Encapsulator on the managed node, you must first deassign and remove the logfile template from the managed nodes. Once the template has been successfully removed, stop and start the agent processes, change the character set from multibyte to ASCII, and assign and distribute the template.

To manage English nodes with a Japanese management server, you must assign templates to the managed node which only contain ASCII data. Japanese installations can upload English templates in addition to the multibyte Japanese templates from the ITO database but must change the template name to be able to do so. Make sure to set LANG=C before calling *opccfgupld(1M)*.

## External Character Set on Managed Nodes

All commands provided for ITO managed nodes, such as opcmsg(1M) or opcmon(1M), interpret (the character set of) their command line arguments by the locale setting. This character set may also be different from the database character set and the managed node processing character set. All command input is also converted before it is acted upon by any managed node processes.

The following table shows the values of *LANG* supported by ITO, and the related external character set, in an English environment.

**Table 8-5 External Character Sets in an English Environment**

| Platform | LANG | External Character Set |
|---|---|---|
| AIX | C<br><*lang*>.ISO8859-1<br><*lang*>.IBM-850 | ASCII<br>ISO 8859-1<br>OEM Code Page 850 |
| Digital UNIX | C<br><*lang*>.ISO8859-1 | ASCII<br>ISO 8859-1 |
| HP-UX 10.x/11.x | C<br><*lang*>.roman8<br><*lang*>.iso88591 | ASCII<br>ROMAN8<br>ISO 8859-1 |
| MPE/iX | NATIVE-3000 | ROMAN8 |
| Novell NetWare | LANG variable not available | ASCII<br>OEM Code Page 850<br>OEM Code Page 437<br>ANSI Code Page 1252 |

| Platform | LANG | External Character Set |
|---|---|---|
| OS/2 | LANG variable not available | ASCII<br>ISO 8859-1<br>OEM Code Page 437<br>OEM Code Page 850 |
| NCR UNIX SVR4, SCO UnixWare, SGI IRIX, Sequent DYNIX/ptx, Olivetti UNIX, Pyramid DataCenter/OSx | C<br><*lang*>.iso8859-1 | ASCII<br>ISO 8859-1 |
| SCO OpenServer | C<br><*lang*>.8859 | ASCII<br>ISO 8859-1 |
| Siemens Nixdorf SINIX | C<br><*lang*>.88591 | ASCII<br>ISO 8859-1 |
| Solaris | C<br><*lang*> | ASCII<br>ISO 8859-1 |
| Windows NT | LANG variable not available | OEM Code Page 850<br>OEM Code Page 437<br>ANSI Code page 1252<br>ASCII |

<*lang*> refers to any language that is supported by the operating system. Although it is possible to specify literally any language in this field, you can receive ITO messages only in a language supported by ITO. ITO only uses the value of *LANG* to determine the external character set. Messages are therefore in *LANG*=C in this case.

The following table shows the values of *LANG* supported by ITO, and the related external character set, in a Japanese environment.

**Table 8-6 External Character Sets in a Japanese Environment**

| Platform | LANG | External Character Set |
|---|---|---|
| AIX | C<br>ja_JP, <*lang*>.IBM-932,<br><*lang*>.IBM-eucJP | ASCII<br>Shift JIS<br>EUC |
| HP-UX 10.x and 11.x<br>Digital UNIX | C<br>ja_JP.SJIS<br>ja_JP.eucJP | ASCII<br>Shift JIS<br>2-byte EUC |
| Solaris | C<br>ja_JP.PCK[a]<br>ja | ASCII<br>Shift JIS[a]<br>EUC |
| Windows NT | LANG variable not available | ANSI Code page 932, ASCII |

a. Only with Solaris 2.6 and later.

## Character Sets supported by the Logfile Encapsulator

The ITO Logfile Encapsulator is capable of monitoring files with different character sets. You can specify a character set for each file monitored by ITO. The character set can be different from the character set defined for that managed node but must be compatible.

**NOTE** If you are using ASCII as the character set for internal processing (by setting the locale to C), you must also specify ASCII as the character set for the monitored logfile messages. ASCII is a subset of Shift JIS and can be converted without loss of data; Shift JIS logfiles cannot be converted to ASCII without risking loss of data.

Table 8-6 on page 343 shows all the supported character sets for various logfile messages.

**NOTE** Code Page 932 or Code Page 1252 are the only character sets valid for the NT EventLog.

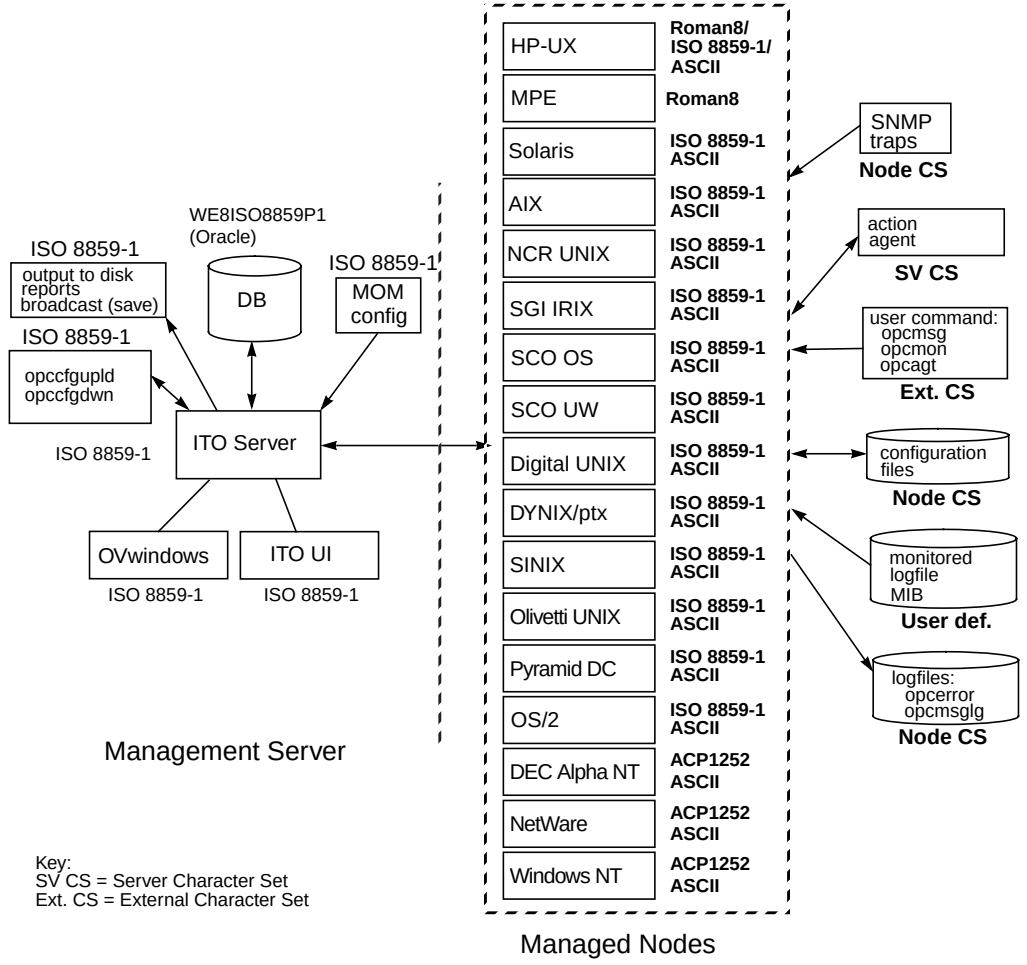
**Table 8-7 Character sets supported by the Logfile Encapsulator**

| Character Set | Windows NT Nodes | | HP-UX, Solaris, AIX, Digital UNIX Nodes | | NetWare, OS/2 Nodes | Other Nodes |
|---|---|---|---|---|---|---|
| | English | Japanese | English | Japanese | English | English |
| ASCII | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| ISO 8859-1 | | | ✔ | | ✔ | ✔ no MPE |
| ROMAN 8 | | | HP-UX | | | MPE |
| American EBCDIC | | | HP-UX | | | |
| Multilingual OEM code page 850 | ✔ | | AIX | | ✔ | |
| OEM US code page 437 | ✔ | | | | ✔ | |
| Multilingual ANSI code page 1252 | ✔ | | | | NetWare | |
| Japanese ANSI code page 932 | | ✔ | | | | |
| Shift JIS | | | | ✔ Solaris 2.6 | | |
| EUC (2-byte Extended UNIX code) | | | | ✔ | | |

# Character Conversion in ITO

## English Environment

**Figure 8-1** **ITO Configuration and Related Character Sets in an English Environment**



Management Server:

- Local Logfile entries (`opcerror`), history download, etc., are processed using the **ISO 8859-1** character set.
- Configuration upload and download is done using **ISO 8859-1**.

No runtime conversion is done on the management server. Conversion is only performed for managed node configuration files if the ITO agents on HP-UX or MPE/iX are running with the processing character set, **ROMAN8**.

Managed Nodes:

- Incoming SNMP events are always interpreted as being **ASCII**.
- Input through user commands is always converted from the external character set to the node character set.
- No input conversion is done for configuration files; configuration files are always in the node processing character set, as defined in the `Add/Modify Node` window.
- No output conversion is done for local ITO logfiles; the contents of logfiles are always in the node processing character set, as defined in the `Add/Modify Node` window.
- MIB processing is always performed in the node processing character set.
- Action agents receive their input in the management server character set, and convert it into the node processing character set, before actions are started.

## Example:

| | |
|---|---|
| Scenario | ITO agent-processing character set is **ROMAN8**.<br>*LANG*=de_DE.iso88591<br>opcmsg msg_text="This is a message with ä, ü, ö" |
| Conversion | Input conversion of the `opcmsg` is from **ISO8859-1** to **ROMAN8** before the ITO message interceptor evaluates the message attributes. |

Output conversion, before forwarding the message to the management server, is from **ROMAN8** to **ISO8859-1**/WE8ISO8859P1 (the database character set).

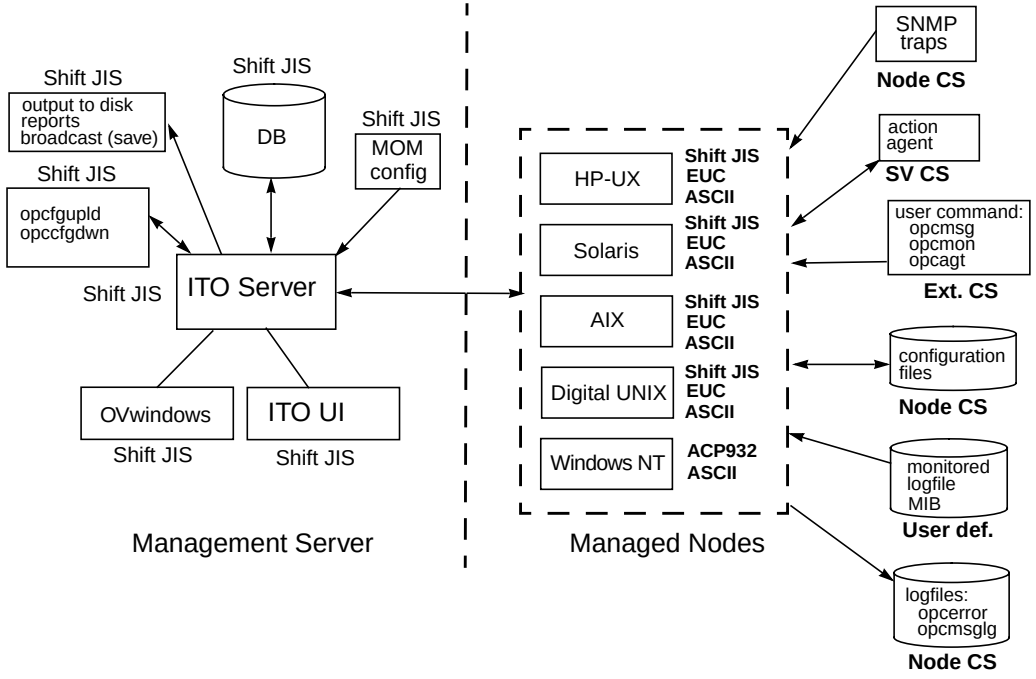
## Tips

On HP-UX, it is possible to define different character sets for different managed nodes. It is recommended that you set the character set most frequently used on each managed node. For example, if you mostly monitor logfiles with **ROMAN8** characters, you should use **ROMAN8** for your managed nodes. Similarly, if your environment mostly generates input data for ITO in the **ISO 8859-1** character set, you should set the managed node character set to **ISO 8859-1**. If in doubt, use **ISO 8859-1**.

Note that you can use a different character set for each managed node. You determine the managed node character set by the character sets used in your environment.

## Japanese Environment

**Figure 8-2** **ITO Configuration and Related Character Sets in a Japanese Environment**




Management Server:

- Local Logfile entries (`opcerror`), history download, and so on, are performed using the **Shift JIS** character set.
- Configuration upload and download is performed using **Shift JIS**.

No runtime conversion is done on the management server. Conversion is only performed for managed node configuration files if the ITO agents on HP-UX, Solaris, AIX, and Digital UNIX are running with the processing character set **EUC**.

Managed Nodes:

- Incoming SNMP events are always interpreted as **ASCII**.

- ❏ Input through user commands is always converted from the external character set to the node character set.
- ❏ No input conversion is performed for configuration files; configuration files are always in the node character set.
- ❏ No output conversion is done for local logfiles; the contents of logfiles is always in the node character set.
- ❏ MIB processing is always performed in the node character set.
- ❏ Action agents receive their input in the management server character set, and convert it into the node character set before actions are started.

## Example:

| | |
|---|---|
| Scenario | ITO agent-processing character set on an HP-UX 10.x managed node is **EUC**.<br>*LANG*=ja_JP.SJIS<br>opcmsg msg_text="This is a message with Shift JIS characters" |
| Conversion | Input conversion of the opcmsg is from **Shift JIS** to **EUC**.<br>Output conversion, before forwarding the message to the management server, is from **EUC** to **Shift JIS** (the database character set). |

## Tips

On HP-UX, it is possible to define different character sets for different managed nodes. It is recommended that you set the character set most frequently used on each managed node. For example, if you mostly monitor logfiles with **Shift JIS** characters, you should use **Shift JIS** for your managed nodes. Similarly, if your environment mostly generates input data for ITO in the **EUC** character set, you should set the managed node character set to **EUC**. If in doubt, use **Shift JIS**.

Note that you can use a different character set for each HP-UX managed node. You determine the managed node character set by the character sets used in your environment.

# Localized Object Names

Although most of the ITO-specific configuration can be localized, there are some restrictions.

### Restrictions

- Only ASCII characters are supported in node names.
- The name of ITO objects, for example, the template name, message group name, or node group name, is used as an internal identifier by ITO and therefore should not be localized. Names are only displayed in the ITO GUI if a label hasn't been specified. To display localized object names in the ITO GUI, assign a label to the object. You can then localize the label.

### Recommendations

Use only ASCII characters for:

- File names (for example, automatic actions, scheduled actions, monitor scripts and programs, full qualified Trouble Ticket interface, notification services, physical console).
- ITO operator names.
- Monitored object names.
- ITO operator passwords and the ITO administrator password.

ITO supports language dependencies for reports, Application Registration Files (ARFs), symbols, fields and ITO defaults.

# Flexible Management in a Japanese Environment

If your management server runs with the character set Shift JIS, but your managed nodes are running with the character set EUC, you must perform some extra configuration steps; namely you have to manually convert the MoM configuration file on the management server from Shift JIS to EUC, enter:

```
/usr/bin/iconv -f sjis -t euc <mom_orig> > <mom_new>
```

where <*mom_orig*> is the name of the original configuration file in Shift JIS, and <*mom_new*> is the IP address of the managed node in Hex, as returned by the command `opc_ip_addr`.

Alternatively, you can convert the `mgrconf` file on the EUC managed nodes.

**NOTE** The above conversion can also be applied to the `allnodes` file if all managed nodes are running EUC. In mixed environments, that is Shift JIS and EUC, you have to create node-specific configuration files.

# 9 An Overview of ITO Processes

This chapter provides a functional overview of ITO: it describes ITO manager and agent processes and subprocesses, and lists files used by ITO. The chapter is divided into sections that describe the following:

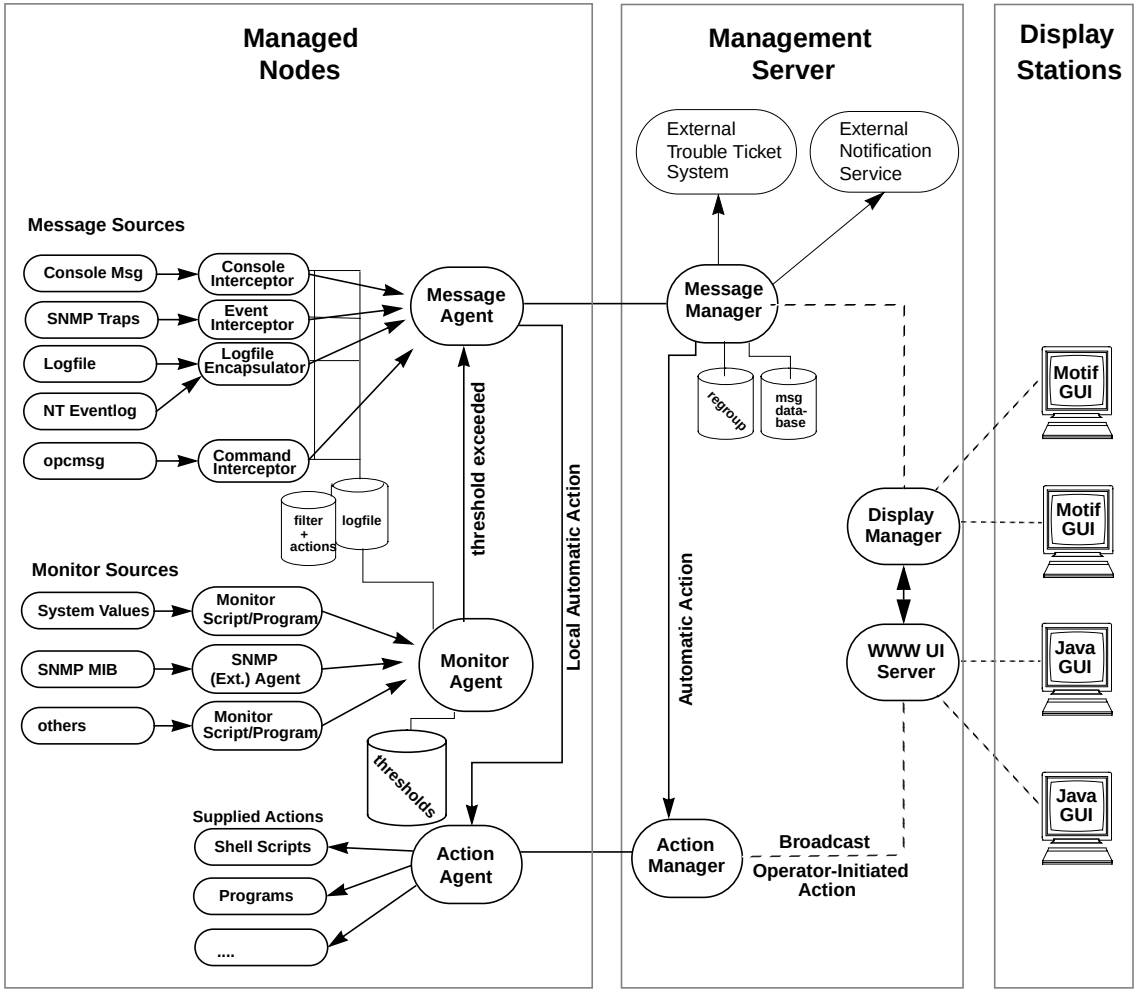
- Management Server Processes
- Managed Node Processes
- Secure Networking

Figure 9-1 on page 355 provides a functional overview of the major parts of ITO.

# Understanding ITO Processes

ITO's agents and managers communicate by means of Remote Procedure Calls (RPCs) based on DCE or NCS, files (=queues), pipes, or signals. These mechanisms apply to communication between the management server and the managed nodes as well as to communication between processes running locally on the management server.

**Figure 9-1 A Functional Overview of ITO**



For more information on how the processes communicate with one another and what each process does, see “Management Server Processes” on page 356 and “Managed Node Processes” on page 360.

## Management Server Processes

The following list gives details of which processes run on the ITO management server, what each process does, and, where necessary, how the processes interact:

`opc` The ITO GUI logon program is used by the ITO administrator and by ITO operators and calls either `opcuiadm` and `opcuiopadm` or `opcuiop` according to the User Name specified.

`opcactm` The **action manager** feeds the **action agents** with automatic and operator-initiated actions, scheduled actions, application-startup and broadcasting information via the **control agent**. In addition, external instruction texts are determined using this mechanism.

`ovoareqsdr` The **request sender** informs the **control agents** to start, stop, or update their local ITO agents. The **request sender** is also responsible for ITO's self-monitoring of ITO manager services, and for the heartbeat-polling of the managed nodes.

`opcctlm` The **control manager** starts and stops all other ITO manager processes, performs all licence checking, and controls the ITO database maintenance functionality.

`opcdispm` The **display manager** serves the ITO Motif-based GUI. The **display manager** also feeds the **action manager** with operator-initiated actions, application startup (not requiring a separate terminal) or broadcasting information issued by the ITO operator. Several ITO user GUIs may be active at the same time, but only one Motif-based GUI can be run for each ITO operator.

`opcdistm` The **distribution manager** distributes node-specific configurations to managed nodes in response to requests by the **distribution agent** (`opcdista`). Sub-processes (`opctts`) are forked for each parallel

distribution session. In addition, scripts and programs required for automatic and operator-initiated actions, scheduled actions, monitoring and broadcasting requests, can also be distributed via the **distribution manager**. The distribution manager also starts a child process, the **communication manager**, for inter-management-sever communication.

`opcecm` The **event-correlation manager** connects to the Server MSI to allow access to and modification of messages from the ITO message flow by the event-correlation (EC) engine. Depending on filters and conditions, the messages are then correlated and written back to ITO and appear in the `Message Details` window (available from the Message Browser) with the message source: MSI opcecm. Like all server processes, `opcecm` is controlled by the control manager, `opcctlm`.

`opcmsgm` The **message manager** receives messages from the managed nodes via the message receiver (`opcmsgr`). The messages can be re-grouped and logged by the message manager running on the management server. The message manager is also responsible for adding annotations, triggering notifications, and for forwarding the message to the **trouble-ticket and notification-service manager** for external notification and trouble- ticket generation.

`opcforwm` The **message forwarding manager** relieves the message manager `opcmsgm` of time-consuming tasks, such as sending messages to remote managers, in order to allow the message manager to manage messages more effectively. On the local, “source” management server, the message-forwarding manager receives data from the message manager (in the form of messages), the action manager (action responses) and the display manager (message operations such as acknowledge, add annotation, and so on).

The message-forwarding manager sends data to the message receiver on the “target” management server(s).

| | |
|---|---|
| `opcmsgr` | The **message receiver** collects all messages from managed nodes; it is an auxiliary process of the **message manager**, designed to guarantee quick message acceptance. `opcmsgr` accepts messages from NCS agents only. |
| `opcmsgrd` | Similar to `opcmsgr`, `opcmsgrd` accepts messages from NCS, DCE, and Sun-RPC agents. |
| `opctss` | The **distribution manager** subprocesses (`opctss`) transfer configuration data to the **distribution agent** using TCP/IP. |
| `opcttnsm` | The **trouble-ticket and notification-service manager** feeds the external notification interface and/or the external trouble-ticket interface with the appropriate message attributes. It is only an auxiliary process of the **message manager**, designed to guarantee high message throughput. If an external instruction text is specified for a message, `opcttnsm` evaluates this help text by way of the Action Manager. |
| `opcuiadm` | The ITO GUI for the ITO administrator, required for the administrator's configuration activities. Note that an additional `opcuiopadm` process is started. Runs as user root. |
| `opcuiop` | The ITO GUI for the ITO operator for message browsing and application startup. One instance of `opcuiop` runs for each operator. Runs as the operator's unix user. |
| `opcuiopadm` | The ITO GUI for the ITO administrator, required for the administrator's operator functionality (message browsing, application startup). Runs as the ITO administrator's unix user. |
| `opcuitadm` | The ITO GUI for the ITO template administrator, required for the template administrator's configuration activities. Runs as user root. |
| `opcuiwww` | The **opcuiwww** server process serves the ITO Java-based operator GUIs. It forwards all communication requests between the Java-based GUIs and the **display manager**. |

## ITO Files on the Management Server

The directory `/var/opt/OV/share/tmp/OpC/mgmt_sv` contains the files listed and explained in Table 9-1 on page 359.

**Table 9-1 Pipes and Queue Files on the Management Server**

| Server File Name | File Contents and Function |
|---|---|
| `actreqp/ actreqq` | Queue/pipe pipe used by the **display manager**, **message manager**, **TTNS manager**, (and **action manager**) to pass action requests to the **action manager** |
| `actrespp/ actrespq` | Queue/pipe used by the **message receiver**, **request sender**, and **action manager** to pass action responses to the **action manager** |
| `ctrlq/ctrlp` | Queue/pipe between the **display manager** and **control manager** |
| `cfgchanges` | File to inform the ITO management server processes about configuration changes; for example, regroup conditions, nodes, trouble-ticket, notification service. |
| `dispq<#> dispp<#>` | Queue/pipe between the **display manager** and GUI (`opcuiop`/`opcuiadm`). One instance for each ITO GUI that is running |
| `forwmgrp/ forwmgrq` | Queue/pipe between used by the **message manager**, **display manager**, **action manager**, and the **forward manager** to pass data to be forwarded to other management servers |
| `magmgrp/ magmgrq` | Queue/pipe between the **message dispatcher** and the **request handler** |
| `mpicdmp/ mpicdmq` | Queue/pipe used by the **display manager** and message-stream-interfaces to transfer control sequences for message-change event handling |
| `mpicmmp/ mpicmmq` | Queue/pipe used by the **message manager** and message-stream-interfaces to transfer control sequences for message handling via the MSI |

| Server File Name | File Contents and Function |
|---|---|
| `mpimmp/ mpimmq` | Queue/pipe used by the **message manager** and message-stream-interfaces to transfer messages from MSI-programs to the **message manager** |
| `msgmgrq/ msgmgrp` | Queue/pipe between the **message receiver** and **message manager**. |
| `oareqhdl` | File used by the Open Agent request handler to store connections to other processes. |
| `opcecap/ opcecaq` | Queue/pipe used to pass messages from the **message manager** to the **event correlation manager** |
| **pids** | ITO Manager's process IDs are controlled by the ITO **control manager**, which is also used for self-monitoring. |
| `rqsdbf` | Buffer file used by the **request sender** to store requests if the **control agent** on a given managed node can not be accessed |
| `rqsp/rqsq` | Queue/pipe between the **request handler** and the **request sender**. Also used by the **display manager** and the **action manager** |
| `trace` | Trace logfile: only available when tracing is activated; used for support purposes. For more information on how to active tracing refer to the section on troubleshooting. |
| `ttnsarp/ ttnsarq` | Queue/pipe used by the t**rouble-ticket manager** and **action manager** when message instructions have to be fetched by the **TTNS manager** |
| `ttnsq/ttnsp` | Queue/pipe between the **message manager** and **trouble-ticket manager** and **notification service manager**. |

## Managed Node Processes

The following list gives details of which processes run on the ITO managed node, what each process does, and, where necessary, how the processes interact:

`opcacta` The **action agent**, `opcacta`, is responsible for the starting and controlling of automatic and operator-initiated actions, and scheduled actions (scripts, programs). The **action agent** is also used for command broadcasting and for applications configured as **Window (Input/Output)** in the `Add/Modify` ITO `Application` window.

`opcdista` The **distribution agent** requests node-specific configurations from the **distribution manager** (`opcdistm`). Scripts and programs required for automatic and operator-initiated actions, scheduled actions, monitoring and broadcasting requests, can also be distributed via the **distribution manager**.

`opceca` The **event-correlation agent** connects to the agent MSI in the same way that the ECS runtime library is integrated into the ITO server. This connection allows access to and modification of messages from the ITO message flow on the agent; those messages modified by this process appear in the `Message Details` window (available from the Message Browser) with the message source "MSI: opceca". Like all agent processes, `opceca` is controlled by the **control agent**.

`opcle` The logfile encapsulator scans one or more application- and/or system-logfiles—including the Windows NT Eventlog—for messages or patterns specified by the ITO administrator. The logfile encapsulator forwards the scanned and filtered messages to the **message agent**.

`opcmona` The **monitor agent** monitors the following and checks the values it finds against predefined thresholds:

- ❏ system parameters (for example, CPU load, disk utilization, kernel parameters)
- ❏ SNMP MIBs
- ❏ other parameters if specified

If a threshold is exceeded, a message is generated and forwarded to the **message agent**. The polling interval of the monitored object can be configured by the ITO administrator. In addition, the `opcmon(1)` command

and `opcmon(3)` API can be used (asynchronously) to feed the **monitor agent** with the current threshold values.

Note that `opcmona` does not immediately begin monitoring when agents are started. Instead, it waits one polling interval, and only then executes the monitor script for the first time. Typically, polling intervals are of the order of 30 seconds to 5 minutes.

`opcmsga` — The **message agent** receives messages from the **logfile encapsulator**, the **monitor agent**, the **console interceptor**, the **event interceptor** and the **message interceptor** on the local system. The messages are forwarded to the **message receiver** running on the management server; if the connection to the management server has been lost, the messages are buffered locally. The **message agent** triggers local automatic actions by forwarding the task to the **action agent**.

`opcmsgi` — The message interceptor receives and processes incoming messages. The `opcmsg(1)` command and `opcmsg(3)` API can be used to forward messages into ITO. Conditions can be set up to integrate or suppress chosen message types.

`opcconsi` — The MPE/iX console message interceptor is the message interface for feeding MPE/iX console messages into ITO. Conditions can be set to integrate or suppress chosen message types.

`opcctla` — The **control agent** starts and stops all ITO agents, and performs ITO self-monitoring tasks. The **control agent** is informed of new configuration and distribution requests by the **request sender**.

`opctrapi` — The event interceptor is the message interface for feeding SNMP events into ITO. Conditions can be set to integrate or suppress selected message types.

## ITO Files on Managed Nodes

The location of the files that the various processes use on the managed node depends on the agent platform as described in Table 9-2 on page 363.

**Table 9-2 Locating Process-related Files on the Managed Nodes**

| Platform | File Location |
|---|---|
| AIX | `/var/lpp/OV/tmp/OpC` |
| DEC Alpha NT | `\usr\OV\tmp\OpC\<`*node*`>` |
| HP-UX 10.x and 11.x<br>Digital UNIX<br>NCR UNIX SVR4<br>Olivetti UNIX<br>OS/2<br>Pyramid DataCenter/OSx<br>SCO OpenServer<br>SCO UnixWare<br>Sequent DYNIX/ptx<br>SGI IRIX<br>Solaris | `/var/opt/OV/tmp/OpC` |
| MPE/iX | TMP.OVOPC |
| Novell NetWare | `SYS:/var/opt/OV/tmp/OpC` |
| Windows NT | `\usr\OV\tmp\OpC\<`*node*`>` |

The files that the ITO processes on the managed node use are described in Table 9-3 on page 364.

**Table 9-3 Pipes and Queue Files on the Managed node**

| Agent File Name | File Contents and Function |
|---|---|
| `actagtp/ actagtq` | Queue/pipe for pending action requests for the **action agent** filled by the **message agent** and the **control agent**. The **action agent** polls the queue every 5 seconds. |
| `monagtq/ monagtp` | Queue on UNIX systems between ITO monitor command `opcmon(1)` respectively ITO monitor API `opcmon(3)` and **monitor agent**. The **monitor agent** checks the queue after the termination of the triggered monitor scripts/programs or at least every 15 seconds, if externally monitored objects are configured. |
| `mpicmap/ mpicmaq` | Queue/pipe used by the **message agent** and message-stream-interfaces to transfer control sequences for message handling via the MSI. |
| `mpimap/ mpimaq` | Queue/pipe used by the **message agent** and message-stream-interfaces to transfer messages from MSI programs to the **message agent** |
| `msgagtdf` | File that holds any messages that cannot be passed to the management server (for example, if the network is down). The messages will be read from this file once the management server is available. |
| `msgagtp/ msgagtq` | Queue/pipe for local buffering of messages which have to be sent to the **message receiver** when the management server is not accessible. |
| `msgip/msgiq` | Queue (only on UNIX systems) between ITO message command `opcmsg(1)` or ITO message API `opcmsg(3)` and ITO message interceptor. |
| `opcecap/ opcecaq` | Queue/pipe to pass messages from the **message agent** to the **event correlation agent** |
| **pids** | Process IDs of ITO agents controlled by the **control agent**. |

| Agent File Name | File Contents and Function |
|---|---|
| `trace` (ASCII) | ITO trace logfile. For more information on activating tracing see the section on troubleshooting in the *HP OpenView IT/ Operations Administrator's Reference*. |
| **aa*** | Temporary files used by the **action agent**, for example, to store the action or application output written to `stderr` and `sdtout`. |
| **moa*** | Temporary files used by the **monitor agent** |

## ITO Agent Configuration Files

The ITO agent specific configuration files are described below. The file location is platform dependent as shown in Table 9-4 on page 365:

**Table 9-4 Locating Agent-configuration Files on the Managed Nodes**

| Platform | Agent File Location |
|---|---|
| AIX | `/var/lpp/OV/conf/OpC` |
| DEC Alpha NT | `\usr\OV\conf\OpC\<`*node*`>` |
| HP-UX 10.x and 11.x<br>Digital UNIX<br>NCR UNIX SVR4<br>Olivetti UNIX<br>OS/2<br>Pyramid DataCenter/OSx<br>SCO OpenServer<br>SCO UnixWare<br>Sequent DYNIX/ptx<br>SGI IRIX<br>Solaris | `/var/opt/OV/conf/OpC` |
| MPE/iX | `CONF.OVOPC` |
| Novell NetWare | `SYS:/var/opt/OV/conf/OpC` |
| Windows NT | `\usr\OV\conf\OpC\<node>` |

The directories in Table 9-4 on page 365 contain files which are listed in Table 9-5 on page 366. Table 9-5 also explains what the files do and whether or not the contents of the files are encrypted:

**Table 9-5 Agent-configuration Files and their Contents**

| File | Contents | Encrypted? |
|---|---|---|
| `le` | logfile encapsulation configuration | Yes |
| `msgi` | `opcmsg(1)` and `opcmsg(3)` message interceptor | Yes |
| `trapi` | SNMP event interceptor | Yes |
| `consi` | MPE/iX console interceptor | Yes |
| `monitor` | monitor agent template file | Yes |
| `mgrconf` | MOM configuration file | No |
| `primmgr` | MOM configuration file | No |
| `nodeinfo` | node specific ITO configuration information, for example, the logging directory, the type of managed node internal character set. All ITO agents read this file. | No |

## Process Security

Although IT/Operations carries out basic authorization checks independently of DCE when communication between the management server and the managed nodes is required, DCE allows the implementation of a much more stringent security policy at process level between, for example, an RPC client and an RPC server, specifically in the areas of authentication and data protection.

The level of data protection is chosen by the client, although the server has the option of deciding whether a chosen level is sufficient. ITO sees the concept of authentication in the context of either the RPC client or the RPC server. For example, just as a server needs to determine whether or not an incoming request is from a genuine ITO client, an RPC client also needs to be sure that the server it is calling is a real ITO server.

## Process Authentication

An important step in the authentication procedure that an ITO RPC process goes through involves the obtaining of a login context. Every secure RPC process has a login context, which it either inherits from its parent process or establishes itself. The login context requires a name (or **principal**) and a password (or **key)**. Since ITO processes usually run without any user interaction, reliance on an inherited login context is not sufficiently secure. So, each process creates its own login context with a name and password that must be registered at the DCE security service. However, like UNIX, multiple processes may run within the same login context. Management and maintenance of the login context is carried out internally by the control agent and control manager.

Once the authentication process has completed successfully, a connection is established, and the RPC request-reply sequence starts. Authentication can be limited to the connection, the first RPC Client-Server call or all RPCs between client and server. The following simple example of communication between an RPC client and an RPC server illustrates the procedure in the context of ITO. In this case, the RPC client is the message agent on the managed node, and the RPC server is the message receiver on the management server:

1. The message agent (RPC client) reads its password from the key file.
2. The message agent uses the password to log in to the security server, procure a login context, and obtain a server ticket.
3. The message agent sends an RPC request to the message receiver (RPC server).
4. The message receiver compares the ticket with the password contained in the key file.
5. If the password matches, the message receiver tells the message agent to proceed with its RPC request.

## Process Names and Passwords

In ITO, both the management server and the managed nodes run RPC clients and servers at the same time. This allows ITO to simplify a given process' requirements for configuration information prior to an RPC call, namely:

- ❏ name and own password
- ❏ security level

However, this configuration information must be present on both the management server and the managed node.

ITO associates two **names** with the two types of node in its environment, namely: one each for the management server and the managed node. All management server processes then run under the name associated with the management server, and all managed node processes under the identity of the name associated with the managed node.

In addition, ITO allows you to select and configure the security level your particular environment requires for an individual managed node: the value is stored in the given managed node's `opcinfo` file and in the relevant entry in the database on the management server. In this way, security on a given managed node may be changed to handle, for example, the addition of sensitive connections through a firewall.

ITO may be configured in such a way as to be able to overcome a situation where, owing to the temporary unavailability or mis-configuration of the security service, a process is required either to run in unauthenticated mode or to fail. For example, if a management server process such as the request sender receives an authentication failure when calling a control agent on a managed node, an error message is generated, which appears in the `Message Browser` window. The administrator is then able to take immediate corrective action, for example, by temporarily changing the security level on the managed node in question to allow the retransmitted request to succeed.

# Secure Networking

ITO's concept of securing a network is based on the idea of improving the security of the connection between processes either within a network or across multiple networks as well as through routers and other restrictive devices. For example, you could limit access to a network or a section of a network by restricting the set of nodes (with or without ITO agents running on them) that are allowed to communicate with the management server across restrictive routers or even a packet-filtering firewall. It is not important to ITO which element, the server or the network of managed nodes, is inside or outside the firewall. For example, a network of nodes inside a firewall could be managed by a management server outside the firewall. Conversely, a management server inside a firewall can manage nodes in or outside.

One way of limiting access to a network and consequently improving the network's inherent security would be to restrict to a specific range of ports all connections between ITO processes on the management server and a managed node. To simplify matters, ITO sets the default value on the managed node to "No security" and allows you to select the security configuration node by node. In this way, the administrator can change a given node's security level depending, for example, on whether or not there is a need for a given node to communicate across a firewall or through a restricted router.

## The RPC Client/Server Connection

A connection between an RPC-server and an RPC-client needs at least two ports: one on the server machine, one on the client. Each ITO process that is either an RPC client or RPC server has its own port for communication: the port remains blocked by the ITO process which owns it until the process exits, whereupon the port becomes free for dynamic assignment to the next RPC client-server request. For more information on dynamic port assignment in ITO, see "Processes and Ports" on page 370.

An RPC client using DCE or NCS does not automatically know the port number of the RPC server on the remote system and, consequently, has to obtain this information before initiating an RPC request. The first thing it does is to look up in the LLBD or RPCD on the remote system the specific port number of the RPC server it needs to talk to: the LLBD

or RPCD always runs on UDP 135, a reserved port which must be accessible even through a firewall. Once it has the port number of the RPC server, the RPC client can initiate the RPC call.

## Processes and Ports

In addition to the checks and controls that a DCE environment supplies for authentication and data integrity both prior to and during connections between processes, ITO allows you to combat security breaches more effectively by restricting to a specific range which you define in the GUI the port numbers that processes may use. ITO then assigns these port numbers dynamically to the processes that are granted an RPC connection. The port numbers are configurable and are checked against the defined range each time an RPC server registers itself or an RPC client requests a connection.

If a service request for a port number within the range specified in the GUI is refused because none is available, the process starts anyway and ITO assigns a port number outside the permitted range. However, a possible consequence of this is that the newly assigned port may not be available either. In this case, ITO generates an error message. For more information on how to set port ranges and the consequences of incorrect port assignment, see the HP ITO Administrator's Guide to Online Information.

### Dynamic Port Assignment through a Firewall: Example Scenario

If the security precautions of a given environment require that a restriction be applied to the nodes, ports or protocols that are allowed to pass a packet-filtering firewall, the administrator might configure the firewall to enable, for example, the port range 1050 to 1300 on the managed nodes and ports 1200 to 1500 on the server for ITO traffic. The administrator does this by "switching off" all port numbers not in the specified range to traffic in the direction specified. The only exception to this is port 135 which is used for access to the RPCD/LLBD and must not be blocked. All ITO-specific traffic then has to go through the designated ports. The scenario described below would be the consequence of such a configuration:

- The Control Agent on a managed node registers TCP/UDP port 1050 in its unique RPCD/LLBD and listens there for ITO traffic.

- ❏ The Message Receiver on the server registers TCP/UDP port 1200 in its unique RPCD/LLBD and listens there for ITO traffic.
- ❏ The Distribution Manager on the server registers TCP/UDP port 1051 in its unique RPCD/LLBD and listens there for ITO traffic.
- ❏ RPC clients doing lookups in the RPCD/LLBDs find this information and request connections to the Control Agent, Message Receiver and so on at the port numbers listed.

Note that, in addition to allowing you to restrict the allocation of port numbers, ITO also allows you to work through firewalls that implement NAT (Network Address Translation) by configuring the file `/opt/OV/share/conf/OpC/mgmt_sv/opc.hosts` on the ITO management server in the following manner:

```
<alternative_ip_address> <agent_node_name_known_to_the_server>
```

In the ITO GUI, you set up the ITO node with the IP-address that the ITO server knows through its DNS-server or hostname resolution. In the `opc.hosts` file, you tell the ITO management server that it should accept another IP-address for this node.

## Restrictions and Recommendations

If the systems participating in the ITO environment are connected via a fast network (LAN), it is generally recommended that you choose UDP rather than TCP as the DCE RPC protocol. UDP requires significantly less overhead and is therefore faster and less demanding of resources. If the managed nodes and management server are connected over a slow or busy network (WAN, X.25 etc.), or even if the volume of data to be transmitted is large, it is more reliable to use TCP. Note that TCP requires at least one socket to be permanently open for each managed node.

However, if you do choose the DCE RPC (UDP) option as the communication type between managed node and management server, you should bear in mind that ITO's configuration distribution and Common Agent bulk transfer both require a plain TCP socket connection to be open. So, if for example a packet-filtering firewall system is located between a management server and managed node communicating via DCE RPC (UDP) and the firewall has a specific range of ports opened (reflected in the ITO configuration), this range must always be open for TCP, too.

# 10 Tuning, Troubleshooting, Security, and Maintenance

This chapter contains information for administrators who perform system maintenance, performance tuning, and troubleshooting. It also describes some important security information, and how to change the hostname and IP address of your management server and manged nodes.

# Performance Tuning

In general, you can carry out the following to improve system performance:

- ❏ Increase the RAM, in order to reduce disk swapping
- ❏ Upgrade the CPU
- ❏ Do not use the LAN/9000 logging and tracing commands `nettl(1M)` and `netfmt(1M)` unless absolutely necessary
- ❏ Use different physical disks for the file systems and for swap space
- ❏ Use high-bandwidth network links between the management server, managed nodes and display stations

## Improving SNMP Management Platform Performance

To improve SNMP management platform performance, reduce or eliminate those HP OpenView Network Node Manager processes which are not used, or are used only infrequently:

- ❏ Stop `netmon(1M)`, increase its polling interval, or un-manage segments which are not of interest.
- ❏ Reduce the amount of memory used by `ovwdb(1M)` (the HP OpenView Windows object database daemon) for managing large numbers of nodes.
- ❏ Do not use the logging and tracing options provided for the HP OpenView Network Node Manager daemons (`trapd, netmon`, etc.) unless absolutely necessary.
- ❏ Configure the management server as a secondary Domain Name Server.
- ❏ Reduce the number of background graphics in the HP OpenView submaps to the minimum.

- ❏ Suppress the appearance of the ITO Alarm Severity symbol in the HP OpenView submaps by changing the ITO app-defaults file. Set the line `Opc.statusPropOnAllNodes` in the file `/opt/OV/lib/X11/app-defaults/<`*language*`>/Opc` to `False`. The default setting is `True`.

For details about HP OpenView Network Node Manager performance tuning, refer to the corresponding part of the "Configuration" chapter in the *HP OpenView Network Node Manager Administrator's Reference*. See also the *HP OpenView SNMP Management Platform Performance and Configuration Guide*.

## Improving Database Performance

Split the database over several disks as described in your Oracle database manuals.

Periodically reorganize the database, by running `opcdbreorg (1M)`. This frees unused pages as well as restructuring the index tables. For more details, see the `opcdbreorg (1M)` man page.

In addition, you should periodically tune the database by running `optimizedb` followed by `sysmod`. Note, however, that during this process, applications cannot work on the database.

For details about an Oracle database, see the documentation supplied with the database and the online documentation in `/opt/OV/ReleaseNotes/opc_db.tuning`.

## Improving ITO's Performance

To both increase the speed of the GUI and to reduce the memory needed to run it, reduce the number of active and acknowledged messages in the Message Browsers:

- ❏ Specify more precise filters (message conditions) for capturing messages.
- ❏ Specify more (local) automatic actions with automatic message acknowledgment after successful operation.
- ❏ Download the history database of acknowledged messages more often.
- ❏ Improve processing performance on the management server by:

1. Reducing the number of managed nodes for parallel configuration distribution (`Configure Management Server` window, [Actions: Server: Configure...]).
2. Making sure operators close any `View-` and `History-Browser` windows not currently required. This reduces:
   - the amount of RAM required for the GUI
   - the time required for updating Browser windows when new messages are intercepted or acknowledged.
3. Minimizing overlapping operator workspaces. In other words, an operator should only be allocated the same nodes and message groups as another operator, if it is absolutely necessary.

❏ Increase the heartbeat-polling interval for the managed node activity check.

Improve processing performance on the managed nodes by:

❏ Using message-text match conditions with the case-sensitive check as often as possible. This flag can be set in several places, including the `Advanced Options` window of the `Add/Modify/Copy Logfile` window.

❏ Changing the sequence of the message and suppress conditions so that those most frequently required are near the top of the list. This prevents much wasted processing of conditions which cannot find a match to a logfile. (`Message and Suppress Conditions` window.)

❏ Setting the polling interval for logfile (`Modify Logfile` window) and threshold monitoring (`Modify Monitor` window) as high as is possible, while at the same time receiving adequate data.

# Troubleshooting: Recommended Practices

Following these practices helps you isolate, recover from, and often prevent, problems:

- ❏ Make sure that both the management server and the managed node system meet the hardware, software, and configuration prerequisites. See the *HP OpenView IT/Operations Installation Guide for the Management Server* for a list of prerequisites.
- ❏ Make sure all the required patches are correctly installed
- ❏ Make sure that the following directories are included in your *PATH*:
  - `/opt/OV/bin/OpC`
  - `/opt/OV/bin/OpC/install`
- ❏ Do not modify HP OpenView product files, such as X resources, without retaining copies of the original files.
- ❏ Make sure that you are not using up too much of your management station's CPU and system resources by collecting too much data, or by setting polling intervals which are too frequent for object monitoring.
- ❏ Use **`ovstatus opc`**, **`ovstatus ovoacomm`** or **`opcsv -status`**, and **`opcagt -status`** (**`opcragt -status`**) to check whether all processes are up and running. If not, simply restart the missing processes.

# Troubleshooting: Tracing

ITO provides a tracing facility which helps you to investigate the cause of a problem. For example, if processes or programs abort, performance is greatly reduced, or unexpected results appear. Trace logfiles can provide pointers to where and when the problem occurred.

Tracing can be activated for specific management server and/or agent processes by adding a statement to the `opcsvinfo` and/or `opcinfo` file. To simplify the interpretation of the trace logfile, tracing can be activated for specific functional areas by specifying one or more functional areas in the trace statement. “Activating Tracing” on page 380 shows how to use the trace statement, and Table 10-1 gives a list of all available functional areas that may be used for tracing. Note that some areas are not available for some processes.

**Table 10-1 Functional Tracing Areas**

| *<area>* | Description |
|---|---|
| ACTN | Actions |
| ALIVE | Agent-alive check |
| ALL | All tracing areas (except DEBUG) |
| DB | Database |
| DEBUG | Debugging information (very detailed)[a] |
| DIST | Distribution |
| GUI | User interface |
| INIT | Initialization |
| INST | Installation |
| INT | Internal |
| LIC | Licensing |
| MISC | Miscellaneous |
| MSG | Message flow |

| *<area>* | Description |
|---|---|
| NAME | Name resolution |
| NLS | Native Language support |
| OCOMM | Open agent communication |
| PERF | Performance |
| SEC | Security |

a. Use this option carefully as it provides extensive and detailed information.

## Activating Tracing

You can activate the ITO trace facility for the management server and/or the agent processes by modifying the following files:

- Management server processes:

  `/opt/OV/bin/OpC/install/opcsvinfo`

- HP-UX 10.x and 11.x managed node processes (refer to Table 10-3, “Location of the opcinfo File on ITO Managed Nodes,” on page 399 for file locations on other supported platforms):

  `/opt/OV/bin/OpC/install/opcinfo`

  or:

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

**NOTE**

When changing the attributes of a managed node, the `nodeinfo` file is overwritten by the distribution process. It is therefore recommended that you include the trace statement in the `opcinfo` file.

1. Add **OPC_TRACE TRUE** in the `opcsvinfo` and/or `opcinfo` file.
2. Select the appropriate functional area or management server/agent process by including one of the following statements:

   `OPC_TRACE_AREA <area>[,<area>]`

   `OPC_TRC_PROCS <proc>[,<proc>] (selected server/agent process)`

   `OPC_DBG_PROCS <proc>[,<proc>] (erver/agent process with DEBUG)`

See Table 10-1 “Functional Tracing Areas” for a list of all available areas. **MSG** and **ACTN** are enabled by default.

**NOTE** Spaces are not allowed between entries in the lists for OPC_TRACE_AREA and OPC_TRC_PROCS.

3. To receive verbose trace information output, add:

   ```
   OPC_TRACE_TRUNC FALSE
   ```

   OPC_TRACE_TRUNC TRUE is enabled by default.

4. Inform the running ITO software of the configuration change as user **root**:

   - management server processes:

     **/opt/OV/bin/OpC/opcsv -trace**

     or restart the management server processes:

     **/opt/OV/bin/OpC/opcsv -start**

   - managed node processes:

     **/opt/OV/bin/OpC/opcagt -trace**

     or re-start the managed node processes:

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

The following example shows an opcsvinfo file with tracing activated:

```
######################################################################
# File:         opcsvinfo
# Description:  OpC Installation Information of Management Server
# Package:      HP OpenView IT/Operations
# Status:
#
# (c) Copyright Hewlett-Packard Co. 1998
#
######################################################################
OPC_INSTALLED_VERSION A.05.00
OPC_MGMT_SERVER arthur.ashe.hp.com
OPC_INSTALLATION_TIME 23/01/98 15:06:18
OPC_TRACE TRUE
OPC_TRACE_AREA INT,ACTN
OPC_TRACE_TRUNC FALSE
######################################################################
# end of opcsvinfo
######################################################################
```

## Interpreting the Trace File

The trace information is written to the following trace logfile:

- Management server trace file:

  `/var/opt/OV/share/tmp/OpC/mgmt_sv/trace`

- HP-UX 10.x and 11.x managed node trace file (refer to Chapter 3 of the *HP OpenView IT/Operations Administrator's Reference* for file locations on other supported platforms):

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

The general format of the trace information is the following:

<*mm/dd/yy*> <*hh:mm:ss*> <*process_name*>(*pid*)[<*area*>]: <*detailed information*>

| | |
|---|---|
| mm/dd/yy | date |
| hh:mm:ss | time |
| process_name | process name |
| pid | process ID |
| area | functional area as specified in the trace statement |
| detailed information | detailed information about the process |

**NOTE** New trace information is appended to existing trace logfiles. It is therefore recommended to delete the file to prevent it from becoming too large.

# Troubleshooting: Characterizing the Problem

When you encounter a symptom associated with a problem, make a note of all associated information:

- ❏ Scope: What is affected?
  - Distinguish between management server and managed node problems.
  - If you suspect that a problem lies on a managed node, try to duplicate it on a different node, to find out whether it is node-specific.
  - Distinguish between the administrator GUI and the operator GUI.
  - If you suspect that a problem lies with an operator, try to test it on another operator, to see whether the problem can be duplicated.
- ❏ Context: What has changed? Determine if anything has changed on your network or with the product configuration:
  - Hardware
  - Software
  - Patches
  - Files
  - Security
  - Configuration
  - Name services
  - Routing
  - Utilization
- ❏ Duration: How long, and how often? Is the problem consistent (fails every time) or intermittent (fails only sometimes)?

## Debug Information for OS/2 Managed Nodes

On OS/2 managed nodes, ITO provides an REXX (OS/2 scripting language) script, `\opt\OV\bin\OpC\utils\opcclct.cmd`. Run this script when you are in a situation that requires attention of a support engineer.

The script collects all necessary information and gathers important files on the OS/2 managed node, and gives instructions how to send this information to the support team. This may help to reduce response time from your support team.

# Troubleshooting: General Considerations

Consider the following when troubleshooting ITO:

- ITO is an application that is both memory- and swap-space intensive. Problems may occur simply due to the exhaustion of resources.
- Communication between the ITO management server processes is based on DCE remote procedure calls, which may cause occasional failures and time-outs of manager/agent communications.
- If you are using the Berkeley Internet Name Domain (BIND) or similar name services on your network, pay special attention to hosts with multi-hosted interfaces (more than one LAN card).

# Troubleshooting: How ITO Reports Errors

This section describes how ITO processes and reports errors during operation. The section is broken down into three areas:

- Errors reported via logfiles.
- Errors reported via the Message Browser.
- The Error Dialog Box in the GUI.
- `stdout` and `stderr` in the shell.

## Errors Reported in Logfiles

Error messages are written to two different locations:

1. All errors detected by the ITO server or by agent processes are written to the appropriate log file.
2. In addition (if possible) an ITO message is generated for display in the Message Browser.

In event of a problem, you should always check the ITO error log files. The following list indicates where you may find information relating to the operations described:

- Errors reported by ITO manager processes on the management server during operation, are written to

  `/var/opt/OV/log/OpC/mgmt_sv/opcerror`

- Errors reported during the installation of software on the managed nodes, are written to the following file on the management server.

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

- Errors reported by agent processes during the operation of ITO are written (on the appropriate managed node) to the locations specified in Table 10-2 on page 387:

**Table 10-2 Errors Reported by the Agent Processes**

| Platform | File Name and Location |
|---|---|
| HP-UX 10.x and 11.x Solaris, NCR UNIX, SCO OpenServer, SCO UnixWare, DYNIX/ptx, Digital UNIX, SINIX/Reliant, Olivetti UNIX, Pyramid DC/OSx, IRIX | `/var/opt/OV/log/OpC/opcerror` |
| AIX | `/var/lpp/OV/log/OpC/opcerror` |
| Windows NT (alpha, intel) | `\usr\OV\log\OpC\opcerror` |

- Oracle database-related errors or errors from Oracle, are reported in the following logfile:

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

## Errors Reported via the Message Browser

In most cases when an error is written to the `opcerror` log files on the management server or on a managed node, ITO tries to generate a message and display it on the Message Browser of any users responsible for monitoring the message group, **OpC**.

Under certain circumstances, it is not possible to display a message in the operator GUI. In general, this occurs when a required process is not running or functioning (for instance, the message agent, message receiver, message manager, display manager, display receiver).

If a message is not found in the Browser, make sure that the workspace is configured to receive messages from that managed node.

### Forwarding Unmatched Messages

Unmatched messages, that is, messages that match neither message nor suppress conditions assume the default severity value assigned by the message source template that processed them. The user can change the severity value to enable messages that match the assigned severity level condition to be forwarded. However, it is recommended that the assigned default severity value “Unknown” not be used as the consequence could

be that messages relating to serious or critical problems are marked as "X" in the "U" (Unmatched) column in the message browser and, as a consequence, possibly ignored.

In addition, such unmatched messages should be reported to the ITO administrator, in order to improve the existing templates by adding appropriate message or suppress conditions.

## Errors Reported via the GUI Error Dialog Box

Any errors which relate to the GUI processes are displayed in an error dialog box, which automatically pops up when required. Typical error situations are:

- ❏ User errors:
  - syntax errors when typing input
  - semantic errors (for example, unknown system)
  - required objects not selected while performing a task
- ❏ Communication problems between user interface processes and the display manager (for example, an action cannot be performed because the management server is down). This includes errors reported from X applications and applications configured as **No Window** started from the Application Desktop, and errors reported by starting operator-initiated actions.
- ❏ Errors originating from HP OpenView functionality used in the GUI (for example, a submap can not be created, because the HP OpenView Windows map does not have write permissions).
- ❏ Problems in retrieving or writing data to or from the database (for example, it may not be possible to get detailed message information from the database).

All these errors are reported in the error log files. If problems with the database occur, the user receives a general message that a problem exists, while more detailed information is written to the error log file.

## Errors Reported via stderr and stdout

When starting ITO commands or scripts (for example, `opcagt` and `opcsv`), errors which occur during the operation are reported to the `stderr/stdout` device assigned to the calling shell. Errors reported by terminal applications started from the application desktop, are also displayed on `stderr` and `stdout`.

# Troubleshooting: When you Need More Information

Further information to help you troubleshoot is available in:

- The *HP OpenView IT/Operations Software Release Notes*, or the files in the **ReleaseNotes** directory:

  `/opt/OV/ReleaseNotes`

- ITO online help.
- The documentation set provided with ITO.
- HP OpenView documentation for the given platform.
- Oracle Database manuals.

# Troubleshooting: Specific Problems

This section provides problem descriptions and troubleshooting steps in the following areas:

- ❏ Management Server
  - Database
  - ITO Server Processes
  - ITO GUI
  - HP-UX and Services
- ❏ Managed Nodes
  - Installation Problems:
    - UNIX
    - MPE/iX
  - Runtime Problems:
    - Platform Independent
    - UNIX
    - HP-UX
    - MPE/iX
    - `llbd` and `dced/rpcd`
    - MIB Access
- ❏ Network File System

Security issues and system maintenance are discussed at the end of the chapter.

## Troubleshooting on the Management Server

This section includes descriptions of specific problems that may occur on the ITO management server and provides a solution. For other problems that are not listed here, you can refer to the following manuals:

- ”Troubleshooting” chapter in the *HP OpenView Network Node Manager Reference*.
- ”Troubleshooting” chapter in *HP OpenView Data Management Administrator's Reference*.
- Manuals supplied with the database.

## Oracle-specific Database Problems and Solutions

| | |
|---|---|
| Problem | ITO process cannot be started. The following error message (or similar) is displayed on standard error:<br>`Database error: ORA-01034 : ORACLE not available`<br>`ORA-07318 smsget = open error when opening sgadef.dbf file`<br>`HP-UX Error: 2: No such file or directory (OpC50-15)`<br>`Could not connect to database P:openview`<br>`Please check that the database processes are running (OpC50-2)` |
| Description | The Oracle database services are not running. |
| Solution | Start the Oracle database:<br>**`su oracle -c “{ORACLE_HOME}/bin/dbstart”`** |

| | |
|---|---|
| Problem | Creation of the ITO database was successful but `opcdbinst` or `opcdbinit` fails. |
| Description A | The database creation is done as Oracle DBA with connect internal. `opcdbinst` and `opcdbinit`, however, connect to the specific **ORACLE_SID** over the Oracle pipe driver as user **`opc_op`** |

| | |
|---|---|
| Description B | ITO connects to Oracle as user **opc_op** using OS authentication. Oracle allows you to define a prefix for OS authentication users. ITO adds the user **opc_op** with the assumption that no prefix is used. If you have defined a prefix, ITO will be unable to connect. |
| Solution A | Check that the file `/etc/oratab` exists. Check that `/etc/oratab` is readable by user **opc_op**. Check that `/etc/oratab` contains a line with your **ORACLE_SID**. Check that user **opc_op** is properly setup. |
| Solution B | If no other users of the database use OS authentication, you can change the prefix:<br>• Add or change the line defining the prefix in the file:<br>`${ORACLE_HOME}/dbs/init${ORACLE_SID}.ora`<br>**`os_authent_prefix = ""`**<br>• Stop all processes accessing the database<br>• Restart the Oracle database. The new prefix is now active. If other users also use OS authentication, you can change the prefix used by ITO as follows:<br>  • Destroy the ITO specific parts in the database using:<br>  **`opcdbsetup -r`**<br>  • Change the following line in the ITO database setup script `/opt/OV/bin/OpC/opcdbsetup` to contain the actual value:<br>  `OS_AUTHENT_PREFIX=""`<br>  • Setup the ITO database again using `opcdbsetup` |

| | |
|---|---|
| Problem | Could not connect to Oracle when using SQL*Net, with following error message:<br>`Database error: ORA-12158: (Cnct err, can't get err txt`<br>`See Servr Msgs & Codes Manual) (OpC50-15)` |
| Description | ITO connects as user **`opc_op`** to the database. For this reason, the current directory (the directory where you started ITO) must be readable by user **`opc_op`** |
| Solution | Allow read and execute access to all users to the directory from which you normally start ITO or change the directory to a directory accessible by **`opc_op`** before starting ITO |

| | |
|---|---|
| Problem | Cannot start Oracle database |
| Description | The Oracle database cannot be started because the Oracle resources are already in use. |
| Solution | Check that Oracle is not already running. Check whether some inter-process communication facilities are not freed by the Oracle processes: **`ipcs \| grep oracle`**. If there are some IPC facilities left, clean them up using: `ipcrm`. Check whether the Oracle SGA definition file, `${ORACLE_HOME}/dbs/sgadef${ORACLE_SID}.dbf` still exists, and if so, remove it.<br>If other instances of Oracle are running on the same system, shut down these instances before clearing semaphores and shared-memory using `ipcrm(1M)`. |

| | |
|---|---|
| Problem | Cannot create Oracle database. opcdbsetup exits with following error: `insufficient privileges, not connected` |
| Description | `Connect internal` requires that the primary group of the DBA user is dbaA. The default DBA user is the UNIX user oracle. |
| Solution | Correct the Oracle DBA user using SAM and assign him the group dba |

## ITO Server Problems and Solutions

| | |
|---|---|
| Problem | The ITO management server status is completely corrupted, even after the **`ovstop opc`** and **`ovstart opc`** sequence. |
| Description | Lots of corrupted messages in the message browser; lots of critical ITO error messages, ITO agents on managed nodes cannot be stopped/started, configuration distribution does not work, and so forth. Despite these symptoms, **`opcsv -status`** may report that not all ITO manager processes are correctly operating. |
| Solution | Perform the following steps:<br>1. Stop all ITO GUIs that are running, by exiting the ITO user interface ([File: Exit]).<br>2. Stop the ITO management server processes:<br>**`/opt/OV/bin/ovstop opc ovoacomm`**<br>3. Erase all ITO temporary files:<br>**`rm -f /var/opt/OV/share/tmp/OpC/mgmt_sv/*`**<br>Note that all pending messages (not yet saved in the database) and all pending actions (automatic actions, operator-initiated actions, scheduled actions, command broadcast) will be lost.<br>4. Restart the ITO management server process:<br>**`/opt/OV/bin/OpC/opcsv -start`**<br>5. Restart the ITO GUIs:<br>**`opc`** |

| | |
|---|---|
| Problem | Old (no longer interesting/valid) messages are sent to the external trouble ticket system and/or external notification service when restarting the ITO management server after a long down-time. |
| Description | The messages to be forwarded to the trouble external ticket system and/or external notification service will be queued in `/var/opt/OV/share/tmp/OpC/mgmt_sv/ttnsq` queue file under heavy system load or if one instance of the trouble ticket interface or notification service interface is already running. If the ITO management processes are stopped for a long time, the pending requests will be sent to the appropriate external interface after ITO Manager is restarted even if they are no longer of interest. |
| Solution | Erase **ttnsq** before starting the ITO management services again. |

| | |
|---|---|
| Problem | When starting the ITO administrator GUI, the HP OpenView Windows (ovw) **Root** window is created, but the following error message is immediately displayed:<br>`ovw: Could not resolve hostname (`*mgmt_server_host_name*`) for licensing` |
| Description | HP OpenView Windows (ovw) did not have permission to look up the name of the management server in `/etc/hosts` (this is necessary for license checking). |
| Solution | Make sure that `/etc/hosts` is readable for user **opc_op**:<br>**`chmod 444 /etc/hosts`** |

## ITO GUI Problems and Solutions on the Management Server

| | |
|---|---|
| Problem | ITO GUI aborts when using the HP OpenView copy and paste function. |
| Description | When copying HP OpenView objects from one submap to another using the standard HP OpenView copy and paste functions, the ITO GUI sometimes makes a core dump. |
| Solution | Install HP OpenView SNMP patch **DFIX1271**. Patches are available from your Hewlett-Packard representative. |

| | |
|---|---|
| Problem | Ungraceful abort of the ITO GUI, leaving some `ovhelp` processes still running. |
| Description | After ungraceful shutdown of the ITO user interface, `ovhelp` processes remain running. |
| Solution | If HP OpenView platform processes and ITO-related services are stopped, you can kill the remaining processes manually:<br>**`ps -eaf \| grep ovhelp`**<br>**`kill <proc_id>`** |

| | |
|---|---|
| Problem | HP OpenView Windows (ovw) objects have been hidden and are no longer visible. |
| Description | Using the third mouse button action “Hide Symbol” means the symbol will no longer be displayed on the map. In the OV status line the number of hidden symbols is shown. |
| Solution | Show symbols by clicking on [Edit: Show Hidden Objects: For This Submap]. |

| | |
|---|---|
| Problem | Icon Labels changed using OVW functionality do not appear to be updated. |
| Description | Changing the labels for icons on the ITO Node Bank, Node Group Bank, etc. using OVW functionality does not update the labels as stored in the ITO database; this means the OVW variable IPMAP_NO_SYMBOL_CHANGES has no effect. |
| Solution | Use the appropriate ITO dialog boxes (i.e. `Modify Node` window, `Modify Message Group` window, etc.) |

| | |
|---|---|
| Problem | Ungraceful abort of the ITO GUI leaving some GUI processes still running |
| Description | You receive the error message `The user is already logged on. (50-17)`, when logging on to ITO after the ITO GUI has crashed while users were still logged on. |
| Solution | Some GUI processes may still be running; check for the following processes and kill them:<br>`opcuiadm`<br>`opcuiop`<br>`opcdispr`<br>`ovw`<br>If these processes are not running, but you still receive the error message, delete the entry for logged-on operators from the ITO database:<br>**`su - oracle`**<br>**`svrmgrl`**<br>**`connect internal;`**<br>**`select * from opc_op.opc_op_runtime;`**<br>To delete the entry for a specific user (currently logged on):<br>**`delete from opc_op.opc_op_runtime where name = '<username>';`**<br>To delete the entry for a all users (currently logged on):<br>**`delete from opc_op.opc_op_runtime;`**<br>**`commit;`**<br>**`exit`**<br>**`exit`** |

## Troubleshooting on Managed Nodes

This section includes descriptions of specific problems that may occur on the ITO managed nodes and provides a solution.

1. Identify the ITO version installed on the management server by looking at the `/opt/OV/bin/OpC/install/opcsvinfo` file on the management server.

2. Check the entry OPC_INSTALLED_VERSION in the `opcinfo` file on the managed node. See Table 10-3 on page 399 for the location of the `opcinfo` file on the various agent platforms.

**Table 10-3 Location of the opcinfo File on ITO Managed Nodes**

| | |
|---|---|
| AIX | `/usr/lpp/OV/OpC/install/opcinfo` |
| DEC Alpha NT | `\usr\OV\bin\OpC\alpha\install\opcinfo` |
| Digital UNIX | `/usr/opt/OV/bin/OpC/install/opcinfo` |
| HP-UX 10.x and 11.x | `/opt/OV/bin/OpC/install/opcinfo` |
| MPE/iX | `OPCINFO.BIN.OVOPC` |
| NCR UNIX SVR4 | `/opt/OV/bin/OpC/install/opcinfo` |
| Novell NetWare | `sys:/opt/OV/bin/OpC/install/opcinfo` |
| Olivetti UNIX | `/opt/OV/bin/OpC/install/opcinfo` |
| OS/2 | `\opt\OV\bin\OpC\install\opcinfo` |
| Pyramid DataCenter/OSx | `/opt/OV/bin/OpC/install/opcinfo` |
| SCO OpenServer | `/opt/OV/bin/OpC/install/opcinfo` |
| SCO UnixWare | `/opt/OV/bin/OpC/install/opcinfo` |
| Sequent DYNIX | `/opt/OV/bin/OpC/install/opcinfo` |
| SGI IRIX | `/opt/OV/bin/OpC/install/opcinfo` |
| Siemens Nixdorf SINIX | `/opt/OV/bin/OpC/install/opcinfo` |
| Solaris | `/opt/OV/bin/OpC/install/opcinfo` |
| Windows NT | `\usr\OV\bin\OpC\intel\install\opcinfo` |

3. To obtain more detailed information, use the `what(1)` command for UNIX systems:

   For example, for HP-UX 10.x and 11.x managed nodes:

   ```
   what /opt/OV/bin/OpC/opc*
   ```

## ITO Installation Problems and Solutions on UNIX Managed Nodes

| | |
|---|---|
| Problem | The installation script `inst.sh (1M)` prompts for a password in an endless loop, even if the correct password has been specified. |
| Description | If no `.rhosts` entry is available for **root** on the managed node, the ITO installation will prompt for the root password. If you have specified the correct password and the message<br>`rexec: Lost connection`<br>is displayed, then possibly the management server is not yet known on the managed node. |
| Solution | Add the management server entry to `/etc/hosts` and/or update your Name Server if one is used. |

## ITO Installation Problems with Multi-homed Hosts

Installation of the ITO agent software includes distributing a `nodeinfo` file to the managed nodes. This file contains information about the managed node, such as the parameter `OPC_IP_ADDRESS`, used by the management server to identify the managed node in communication. The `nodeinfo` file is automatically updated when the administrator modifies the IP-address using the `Modify Node` window.

You need to follow these instructions when you specify an IP-address using the `opcmsg(1)` command to send messages to the management server.

Use the `netstat(1)` command to check if a host is multi-homed. An example of the HP-UX output follows:

```
# netstat -r
Routing tables
Destination     Gateway         Flags   Refs     Use  Interface
193.1.4.1       193.1.3.1       UH         0   36598  ni0
127.0.0.1       157.0.0.1       UH        52    1919  lo0
15.136.120      15.136.120.91   U         30   86115  lan0
193.1.3         193.1.3.1       U          7 2904156  ni0
15.136.121      55.136.121.11   U          0   11121  lan1
```

Where **ni0** is a point-to-point connection (PPL, SLIP, or PPP), and **lan0** and **lan1** are ethernet interfaces (**lo0** is present on every system and represents the loopback interface). In these environments, the following problems can occur:

- ❏ The agent processes on the managed node are up and running, but no messages are shown in the browser
- ❏ The control agent does not start and, as a result, no further ITO agent processes run
- ❏ The templates are not distributed to the managed node
- ❏ Actions and application results are not received by the management server

These problems are a result of:

- ❏ an incomplete name service configuration, or
- ❏ problems with IP connectivity (for example, missing routes to the other LAN interfaces).

**Incomplete Name Service Configuration.** Commonly the result of the host name for a managed node (or management server) stored in the name service not containing all host name/IP-address associations, incomplete name-service configuration prevents ITO from applying its authorization algorithm.

ITO checks the IP-address of the managed node and then sends a message to the IP-addresses for this node which it received from the name service. If ITO does not find the IP-address of the sender, it simply discards this message.

You can check the name service by using the `nslookup(1)` command in the following way:

```
# nslookup jacko

Name Server:  nameserver.bbn.hp.com
Address:  15.136.129.111
Name:    jacko.bbn.hp.com
Address:  15.136.123.138, 15.136.25.14
```

or, when `/etc/hosts` is used as the name service:

```
# nslookup jacko
```

```
Using /etc/hosts on :   jacko
Name:    jacko.bbn.hp.com
Address: 15.136.123.138
Aliases: jacko
```

Note that this command only returns the first IP-address when using `/etc/hosts` as the name service.

The managed node uses the IP-address of the first network interface card it finds (by scanning the internal network interface list). The order of the network interfaces depends on the interface type installed on the managed node. For example, if an X.25 and an Ethernet interface are installed, the IP-address of the X.25 interface is used by the managed node, since this interface comes before the Ethernet interface in the internal network interface list.

If the management server has stored the IP-address bound to the Ethernet interface of this managed node in its database, but the name service the management server uses has no association to the X.25 IP-address of the managed node, a message sent by this managed node will be rejected.

For example, if the managed node **jacko.bbn.hp.com** has the IP-addresses 193.1.1.1 for the X.25 interface, and 15.136.120.169 for the Ethernet interface. The name service used by the managed node is displayed as follows:

```
/etc/hosts
----------
15.136.120.169 jacko.bbn.hp.com jacko_15        # Ethernet
193.1.1.1 jacko.bbn.hp.com jacko_x.25           # X.25
```

The name service used by the management server has the following entry for **jacko. bbn.hp.com**:

```
/etc/hosts
----------
15.136.120.169 jacko.bbn.hp.com jacko
```

In the above scenario, as the message contains the IP-address 193. 1. 1.1 which is not known on the management server, a message to the managed node **jacko** would be rejected. There are two ways to resolve this problem:

1. Add the second X.25 IP-address to the management server's name service:

```
/etc/hosts
----------
15.136.120.169 jacko.bbn.hp.com jacko
193.1.1.1 jacko.bbn.hp.com jacko_x.25
```

and restart ITO.

2. In cases where it is not possible to add host name/IP-address associations (for example, in fire-wall environments), a special ITO configuration file can contain the association (this configuration file must be created manually):

   `/etc/opt/OV/share/conf/OpC/mgmt_sv/opc.hosts`

   ```
   ------------------------------------
   193.1.1.1           jacko.bbn.hp.com
   ```

   Then restart ITO.

It is also required that all IP-addresses of the management server are known by ITO. You can do this by either specifying all host name/IP-address associations in the name service, or by specifying it in the `opc.hosts` file as shown in the following example:

```
Management server “arthur.bbn.hp.com”
/etc/hosts
----------
193.1.4.1         arthur.bbn.hp.com arthur 193
15.136.121.2      arthur.bbn.hp.com arthur
192.1.1.1         arthur.bbn.hp.com arthur-fddi
```

Note that ITO uses the fully qualified hostname for identifying a managed node or management server, and for resolving the IP-addresses. Therefore, the name service entries of the following example will not solve the above problem:

```
/etc/hosts
----------
193.1.4.1         arthur.bbn.hp.com arthur 193
15.136.121.2.     arthur.bbn.hp.com arthur
192.1.1.1         arthur.bbn.hp.com arthur-fddi
```

In this case, the resolution of **arthur. bbn.hp.com** would only return 193.1.4.1, and not all three addresses.

**IP Connectivity.** You can check IP-connectivity by using the `ping(1M)` command as follows:

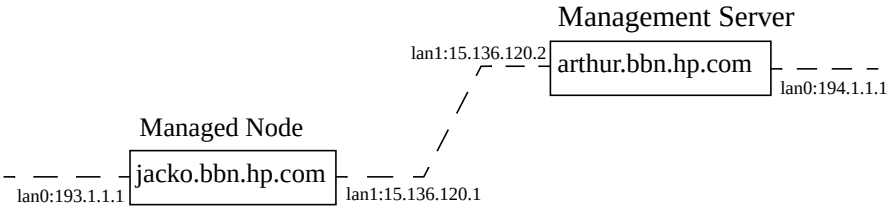
```
# ping 193.1.4.1
```

returns:

```
PING 193.1.4.1: 64 byte packets
----193.1.4.1 PING Statistics----
3 packets transmitted, 0 packets received, 100% packet loss
```

after pressing Ctrl-C. This indicates that no connection was possible using address 193.1.4.1.

If the following scenario were to exist:




The managed node and management server both have two LAN interfaces, but are only connected through the 15.136.120 subnet. There is no route from the management server to the managed node through the 193.1.1 subnet, or from the managed node to the management server through the 194.1.1 subnet respectively.

To use a specific subnet in this environment, you must select the IP-address of the managed node manually from the GUI. In the above scenario the communication should be bound to subnet 15.136.120. You can select the appropriate IP-address from either the `Add Node` or `Modify Node` window of the ITO administrator (the management server's name service must contain both IP-addresses for the node **jacko.bbn.hp.com**).

On the managed node, you must edit the `opcinfo` file in the platform-specific install directory (for more information, see Table 10-3 on page 399). To set the **path** which the managed node uses for communication with the management server, specify the following parameter in the `opcinfo` file: `OPC_RESOLVE_IP 15.136.120.2`. A corresponding `opcinfo` file could then look like the one shown in the following example:

```
######################################################################
# File:         opcinfo
# Description:  ITO Installation Information of Managed Node
# Package:      HP OpenView IT/Operations
######################################################################
OPC_INSTALLED_VERSION A.05.00
OPC_MGMT_SERVER arthur.ashe.tennis.com
OPC_INSTALLATION_TIME 10/13/98 13:37:44
OPC_RESOLVE_IP 15.111.222.333
######################################################################
# end of opcinfo
######################################################################
```

After these changes, the managed node's agents must be restarted using:

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

Note that the changes in `opcinfo` are lost when the ITO agent software is re-installed.

## Installation Problems and Solutions on MPE/iX Managed Nodes

| | |
|---|---|
| Problem | Installation aborts because MPE/iX system name is not known on the management server. |
| Description A | The LAN card is not configured with the **ieee** option required for **vt3k** operations. |
| Solution A | Get the current lanconfig statement from `/etc/netlinkrc` on the management server, and resubmit the command with the additional **ieee** parameter.<br>**grep lanconfig /etc/netlinkrc**<br>**lanconfig…ieee** |

| | |
|---|---|
| Description B | No ARPA-to-NS node-name mapping is defined in `/etc/opt/OV/share/conf/OpC/mgmt_sv/vt3k.conf` and the NS node for the management server is not set, or it belongs to a different domain. |
| Solution B1 | Specify a corresponding mapping in **vt3k.conf**. (See the section "ARPA-to-NS Node-Name Mapping for MPE/iX" on page 128). |
| Solution B2 | Check and set the NS node name of the management server:<br>**nodename**<br>**nodename <ns_name>** |

| | |
|---|---|
| Problem | Installation aborts due to interactive logon/logoff UDC. |
| Description | ITO uses **vt3k** during ITO agent software installation. During the installation period, the interactive logon/logoff UDCs for **MANAGER.SYS, MGR.OVOPC** and **AGENT.OVOPC** are NOT supported. |
| Solution | Deactivate interactive logon/logoff UDCs. |

**NOTE** No interactive logon/logoff UDCs are allowed.

| | |
|---|---|
| Problem | MPE/iX “request replies” from the ITO management server via X-redirection from MPE/iX managed nodes can fail. |
| Description | Starting an X-application from the application desktop (or as an operator-initiated action etc.) produces the action annotation:<br>“`unknown node: ERROR can’t open display`” (or similar) |
| Solution | Check that the environment variable DISPLAY on the management server is set to a long hostname; for example `xyz.bbn.hp.com:0.0`, not `xyz:0.0`. This display-string is passed to the agent when it tries to start the X-application by redirecting the display to the management server. The agent may not be able to resolve the short hostname nor, as a consequence, start the X-application. If an operator-initiated or auto-action started the application, an annotation will be added. If a desktop application or broadcast command failed, an error dialog box pops up. |

| | |
|---|---|
| Problem | The agent software installation on MPE/iX managed nodes fails with the following error message:<br>`vt3k_opcchk failed` |
| Description | This happens when the variable LANG is set to a language other than C on the MPE/iX managed node. |
| Solution | Always set LANG to C before installing the ITO agent software. |

## Platform-independent Runtime Managed Node Problems and Solutions

| | |
|---|---|
| Problem | ITO does not work as expected after an OS upgrade. |
| Description | Updating the operating system might mean that ITO no longer works as expected. For example, system boot/shutdown files have been modified; the file system layout or the command paths could have been changed; the shared libraries have been modified, etc. |
| Solution | Check that the installed OS version is still supported by ITO:<br>**`/opt/OV/bin/OpC/agtinstall/opcversion -a`**<br>If the installed OS version is not supported by the current version of the ITO agents, ask your HP representative for assistance and available patches. |

| | |
|---|---|
| Problem | ITO configuration is not installed on the managed node. For this reason, the ITO logfile encapsulator, message interceptor, console interceptor and event interceptor do not run. |
| Description A | The managed node contains several LAN cards, and therefore several IP addresses. Possibly there are several host names. The ITO agents use an IP address not known on the management server for the corresponding host name. |
| Solution A | Make sure that all the IP addresses of all the managed nodes are known to the management server. Update the **Name Services** and/or `/etc/hosts` accordingly:<br>**`nslookup <managed_node>`** |
| Description B | As Description A, but the managed node in question belongs to a different sub-net or domain and is configured to have a short hostname. |
| Solution B | As Solution A, but also configure the managed node hostname as a fully qualified hostname. |

| | |
|---|---|
| Problem | After an application upgrade, ITO no longer works as expected. |
| Description | After the upgrade of installed applications on the managed node, logfile encapsulation, MPE/iX console message interception, and so forth, appear not to work properly. This could be caused by different message patterns, localized logfiles, different path and/or file name of the logfiles, and so forth. |
| Solution | Check the related application manual and update the ITO message sources accordingly. |

| | |
|---|---|
| Problem | X application cannot be started on a managed node. |
| Description | If you start an X application on a managed node, that system must be allowed to redirect the display to your display station. |
| Solution | Specify on your display station, for each managed node where X applications operate:<br>**`xhost + <managed_node>`**<br>To grant access to everyone:<br>**`xhost +`** |

| | |
|---|---|
| Problem | Application can no longer be started from the Application Desktop. |
| Description A | An application is no longer installed on the managed node. |
| Solution A | Re-install or remove the application from the administrator's Application Bank and/or the operator's Application Desktop. |
| Description B | An application has been upgraded, and its command path, access security or something else has been changed. |
| Solution B | Adapt the ITO default application startup accordingly. |
| Description C | User's password for default application startup has been changed. |

| | |
|---|---|
| Solution C | If you change the password on the managed nodes for default users of an application startup from the ITO Application Desktop, you must adapt the password in the ITO configuration, too. This is only necessary if the application is configured as having a **Window (Input/Output)**, and if no appropriate `.rhosts` or `/etc/hosts.equiv` entry is available. |
| Description D | When any kind of application is started (**Window (Input/Output); Window (Output Only); No Window**) the calling user's profile is executed. If the overall execution takes more than 2 seconds or before anything is written to standard output, ITO assumes that an error has occurred and the application startup will be terminated. |
| Solution D | Simplify the user's profile so that it executes faster or writes more information to standard output. Also, check that the user's profile does not prompt for specific input. |
| Description E | The command path length (inclusive of parameters) is too long for an application configured as having a **Window (Input/Output)**. Only 70 characters are available for command path and resolved parameters (such as *$OPC_NODES*). |
| Solution E | Do not specify the full command path. Put this path in the executing user's PATH variable. Avoid hard-coded parameters and only pass dynamic parameters. Instead of calling the application with lots of hard-coded parameters, use a script which internally calls the application with the required parameters. Instead of configuring this application to run in a **Window (Input/Output)**, set this option to **No Window**, and start an hpterm/xterm on that managed node. |

| | |
|---|---|
| Problem | Command broadcast or application startup does not work on all selected systems. |
| Description A | Not all systems are controlled. Command broadcasting and application startup is only granted on **controlled nodes** and not on **monitored**, **messages-allowed**, **disabled** or **message-allowed nodes**. |
| Solution A | Change the node type of the managed nodes to **controlled** (unless the node is an **external node**, in which case this is not possible). |
| Description B | The command or application is not available on all selected systems. |
| Solution B | Install the command or application where it is missing. |

| | |
|---|---|
| Description C | The command or application path is different; for example, `/usr/bin/ps` (HP-UX 10.x, 11.x). |
| Solution C. | Use (hard or symbolic) links or copy the command or application to the appropriate destination. Write a script/program which calls the right command or application, depending on the platform. For example: my_ps.sh<br>`#!/bin/sh`<br>`ARCH=‘uname -s‘`<br>`if [ ${ARCH} = ”HPUX” -o ${ARCH} = ”AIX” ]`<br>`then`<br>`/bin/ps -eaf`<br>`elif [ ${ARCH} = ”AIX” ]`<br>`then`<br>`/usr/bin/ps -ax`<br>`else’’`<br>`echo ”Unsupported architecture ${ARCH}”`<br>`exit 1`<br>`fi` |
| Description D | The command or application parameters are different. |
| Solution D | Write a script or program using the appropriate parameters; see the example above. |
| Description E | Inconsistent passwords for the calling user on the selected managed nodes. ITO provides only one common password for the assigned default operator on UNIX managed node as well as one common password for the assigned default operator on MPE/IX managed nodes. Furthermore, only one password can be specified for default application startup. So both command broadcasting (using customized user/password) or application startup will fail. Note that a password is only required for Window (Input/Output) applications, or if the customer changes the default settings. |
| Solution E | 1. Split your broadcast for systems having the same user password.<br>2. Provide a common password for all selected managed nodes. Be aware of applied password-aging mechanisms. Alternatively, for applications configured as using a Window (Input/Output), an appropriate `.rhosts` or `/etc/hosts.equiv` entry is also sufficient.<br>3. Use the assigned default user for command broadcasting and the startup of applications configured as using a Window (Input/Output). In this case, the action will be performed by the ITO action agent and no password need be provided. |

| | |
|---|---|
| Problem | ITO Agents are corrupt, even after running the **`opcagt -stop; opcagt -start`** sequence. |
| Description | **`opcagt -status`** reports that not all ITO agents are up and running; automatic or operator-initiated actions and scheduled actions are not executed, and applications are not started as requested. Actions are not acknowledged, even after a successful run. |
| Solution | Check the status of an ITO managed node by running the following command on that system locally:<br>AIX **`/usr/lpp/OV/OpC/opcagt -status`**<br>DEC Alpha NT **`\usr\OV\bin\OpC\alpha\opcagt -status`**<br>HP-UX10.x/11.x, Solaris, NCR UNIX SVR4, SGI IRIX, SCO OpenServer, SCO UnixWare, DYNIX/ptx, Digital UNIX, Olivetti UNIX, and Pyramid DataCenter OS/x, OS/2 **`/opt/OV/bin/OpC/opcagt -status`**<br>MPE/iX **`opcagt.bin.ovopc -status`**<br>Windows NT **`\usr\OV\bin\OpC\intel\opcagt -status`**<br>Check the local `opcerror` file for indications of where the problem may be originating. For the location of this file, see “Errors Reported in Logfiles” on page 386. If the ITO agent status is corrupt, even after the **`opcagt -stop; opcagt -start`** sequence, perform the steps specified in the following tables, working locally on the managed node as user **`root`**. All pending messages not yet sent to the management server and all pending actions (for example, automatic and operator-initiated actions, scheduled actions and command broadcast) will be lost. |

**Table 10-4 Clean-up and Restart of ITO Agents on HP-UX 10.x/11.x Managed Nodes**

| Task | HP-UX 10.x and 11.x Managed Nodes |
|---|---|
| 1. Stop ITO agents, including the control agent: | **/opt/OV/bin/OpC/opcagt -kill** |
| 2. Check that all ITO agents are stopped. [a] | **/opt/OV/bin/OpC/opcagt -status** |
| 3. Check the list of agent PIDs given by the **opcagt -status** command. If any PIDs are not stopped, use the `kill (1M)` command. Do *not* kill the ITO Kernel Message Logger `opckmsg` if running on the managed node. | **ps -eaf \| grep opc kill <proc_id>** |
| 4. Check that no ITO processes are still registered with the `llbd` or `dced/rpcd` daemons. | **/usr/sbin/ncs/lb_admin /opt/dce/bin/rpccp or /opt/dce/bin/dcecp** |
| 5. Remove temporary ITO files. | **rm -f /var/opt/OV/tmp/OpC/*** |
| 6. Restart ITO agents. [b] | **/opt/OV/bin/OpC/opcagt -start** |

a. If the managed node is also the ITO management server, stop the ITO user interfaces and manager services. To do this: 1. Check that all ITO GUIs are terminated (**ps -eaf | grep opcui**). If they are not, terminate them using the [File: Exit] or (Ctrl+E) functions on any HP OpenView submap owned by ITO or use the `kill(1)` command. 2. Stop the server processes: **ovstop opc ovoacomm**

b. If the managed node is also the ITO management server, restart the ITO user interfaces and manager services, too: **ovstart opc ovoacomm**

**Table 10-5 Clean-up and Restart ITO Agents on Other SVR4 Managed Nodes**

| Task | Solaris, NCR UNIX SVR4, SCO OpenServer, SCO UnixWare, SGI IRIX, Olivetti UNIX, Pyramid DataCenter/OSx, Digital UNIX, andOS/2 |
|---|---|
| 1. Stop ITO agents, including the control agent. | **/opt/OV/bin/OpC/opcagt -kill**<br>OS/2: use the GUI<br>Digital UNIX: **/usr/opt/OV/bin/OpC/opcagt -kill** |
| 2. Check that all ITO agents are stopped. | **opcagt -status** |
| 3. Check again that all ITO agents are stopped using the list of agent PIDs given by the **opcagt - status** command. If any are not stopped, execute the `kill (1M)` command. | **ps -eaf\|grep opc kill <proc_id>** |
| 4. Check that no ITO processes are still registered with the `llbd` or `dced/rpcd` daemons. | **/usr/sbin/ncs/lb_admin**<br>**/opt/dce/bin/rpccp**<br>or**/opt/dce/bin/dcecp**<br>OS/2: **\opt\dcelocal\bin\rpccp**<br>or **\opt\dcelocal\bin\dcecp** |
| 5. Remove temporary ITO files. | **rm -f /var/opt/OV/tmp/OpC/*** |
| 6. Restart ITO agents. | **/opt/OV/bin/OpC/opcagt -start** |

**Table 10-6 Clean-up and Restart of ITO Agents on AIX and MPE/iX Managed Nodes**

| Task | AIX | MPE/iX |
|---|---|---|
| 1. Stop ITO agents, including the control agent. | **/usr/lpp/OV/OpC/opcagt -kill** | **opcagt.bin.ovopc -kill** |
| 2. Check that all ITO agents are stopped. | **/usr/lpp/OV/OpC/opcagt -status** | **opcagt.bin.ovopc -status** |
| 3. Check again that all ITO agents are stopped using the list of agent PIDs given by the **opcagt-status** command. If any are not stopped, execute the `kill (1M)` command. | **ps -eaf\|grep opc**<br>**kill <proc_id>** | **showproc ;system;tree;pin=1** (MPE/iX processes cannot be killed) |
| 4. Check that no ITO processes are still registered with the `llbd` or `dced/rpcd` daemons. | **/etc/ncs/lb_admin**<br>**/opt/dce/bin/rpccp** or **/opt/dce/bin/dcecp** | **lbadmin.pub.hpncs** |
| 5. Remove temporary ITO files. | **rm -f /var/lpp/OV/tmp/OpC/*** | **purge@.tmp.ovopc** |
| 6. Restart ITO agents. | **/usr/lpp/OV/OpC/opcagt -start** | **opcagt.bin.ovopc -start** |

## UNIX Managed Node Runtime Problems and Solutions

| | |
|---|---|
| Problem | Automatic or operator-initiated action, scheduled action, command broadcast, or application hangs and does not terminate. |
| Description | Due to programming errors or requests for user input, automatic and/or operator-initiated actions, or scheduled actions can hang and not finish. |
| Solution | Determine the process ID of the endlessly running action using the `ps` command. Issue a `kill` command for the specific process ID. |

| | |
|---|---|
| Problem | Distribution of scripts or programs belonging to actions, monitor, or commands components fails. |
| Description A | No disk space is available to store scripts/programs in a temporary or target directory. See Table 6-2 on page 308 and Table 6-3 on page 310. |
| Solution A | Provide enough disk space and redistribute the appropriate components. |
| Description B | An instance of the program is running and cannot be overridden on UNIX platforms. ITO moves the `actions\|cmds\|monitor` directory to a directory with the same name and the extension `.old` before installing the latest binaries. Afterwards, all files in `.old` are erased. If this is not possible because text files are “busy”, the file and the directory are left. During reinstallation of the `actions\|cmds\|monitor` binaries, ITO tries once again to delete the entries in `the .old` directories. If this is not possible, the ITO control agent generates an error message and stops. For the location of the `actions\|cmds\|monitor` directories and `.old` directories see Table 6-3 on page 310. |
| Solution B | Find the still running instance of the `actions\|cmds\|monitor` binary and kill it manually; afterwards re-distribute the actions,, comands, etc. |

| | |
|---|---|
| Problem | User's profile is not executed as expected when broadcasting a command or starting an application. |
| Description | The profile of the executing user is executed before starting the command/application on the managed node. The profile execution might not work as expected under the following conditions:<br>• profile prompts in a loop for specific user input and does not provide a default setting, if only **Return** has been pressed<br>• strange terminal settings are done<br>• the profile execution spends more than 2 seconds |
| Solution | See "How ITO Starts ITO Applications and Broadcasts on Managed Nodes" on page 327. |

| | |
|---|---|
| Problem | Scripts or other actions on the managed node do not execute, and the action agent log file reports `script not found`. |
| Description | The PATH variable prepared by the action agent was changed by a startup file.<br><br>When ITO agents are started on a system where the korn shell is used and root's profile points to a startup file where *PATH* is set explicitly, the *PATH* variable set by the action agent is lost after the script is executed by korn shell. |
| Solution | Change the setup for user root so that the *PATH* variable is set by extending it `PATH=$PATH:`*/new/path/* |

| | |
|---|---|
| Problem | The following error message is displayed:<br>`Cannot create semaphore, invalid argument` |
| Description | Semaphores are not set up properly in the kernel. |
| Solution | Use `ipcs` to report on the status of the inter-process communication facilities. Re- configure the kernel accordingly. |

## MPE/iX Managed Node Runtime Problems and Solutions

| | |
|---|---|
| Problem | Extremely long time for command broadcasting and application startup. |
| Description | The command broadcasting and application startup are done within jobs. When the job limit is reached, the jobs are queued. Non-ITO jobs also increase the number of running/pending jobs. By default, ITO runs one job to control its agents and up to four additional jobs for command broadcasting and/or application startup. |
| Solution | Increment the job limit (**HPJOBLIMIT**) if required. |

| | |
|---|---|
| Problem | When distributing `command`, `action`, or `monitor` scripts or programs, it may happen that current actions, commands, and monitors cannot be replaced. |
| Description | The `commands`, `actions`, or `monitors` are still in use (scripts or programs are running; text file is busy). The user receives a warning to this effect. In most cases, this causes no problems, since the existing actions, monitors, or commands are not often modified (in other words, the newly-distributed files are equivalent to those in use). |
| Solution | If the user wants explicitly to change a program or script on MPE/iX which is running, he or she must: Stop the MPE agents:<br>**`opcragt -stop <MPE-NODE>`**<br>Repeat the distribution (the distribution will restart the agents again). |

| | |
|---|---|
| Problem | ITO agents stop processing due to too many files being open. |
| Description | If the permanent file, LASTUUID.PUB.HPNCS has not been created, NCS creates a temporary one, which it does not close. Over a period of time, it tries to re-creates this file many times. The result is that the number of open file descriptors increases, and the system table used to administrate open files is overloaded. It is then not possible to open any new files. |
| Solution | Check that the file LASTUUID.PUB.HPNCS exists:<br>**listf LASTUUID.PUB.HPNCS**<br>If the file does not exist, stop all ITO agents, working as user **AGENT.OVOPC**:<br>**opcagt.bin -kill**<br>Create a new file as user **MGR.HPNCS**:<br>**hello agent.ovopc**<br>**opcagt.bin -kill**<br>**hello mgr.hpncs**<br>**build lastuuid.pub.hpncs**<br>**hello agent.ovopc**<br>**opcagt.bin -start** |

| | |
|---|---|
| Problem | Command broadcast and application does not terminate. |
| Description | The command broadcasting and application startup are done within jobs named OPCAAJOB. If such a job does not terminate, perform the following solution. |
| Solution | 1. Check that a job OPCAAJOB is available; if so, get the job number(s) <*num*>:<br>**showjob**<br>2. If more than one job **OPCAAJOB** is available, determine the job number you need: for each found job number determine the corresponding spool file id <*spf_id*>:<br>**listspf o@;seleq=[jobnum=#j<num>]**<br>Check the spool file contents to determine the job number of the hanging job:<br>**print o<spf_id>.out.hpspool**<br>3. Delete the appropriate OPCAAJOB:<br>**abortjob #j<num>** |

| | |
|---|---|
| Problem | Invalid status returned for automatic operator-initiated actions when running in parallel and an action fails. |
| Description | ITO uses the same environment for running automatic and operator-initiated actions in parallel, so only one set of job control words (CIERROR, etc.) are available. If one action fails, the execution of all other actions is also interpreted as failed even if they were successful. |
| Solution | Re-run operator-initiated actions. Verify automatic action results using the appropriate tools, for example, virtual terminal, application startup, and remote command execution. |

| | |
|---|---|
| Problem | Automatic or operator-initiated action, or scheduled action does not terminate. |
| Description | Due to an endless loop programming error the automatic or operator-initiated action, or scheduled action does not terminate. |
| Solution | Find the programming error in your scripts/programs and restart the ITO agents after you have fixed the problem.<br>**`opcagt.bin.ovopc -start`** |

| | |
|---|---|
| Problem | Critical error message 30-511 when executing scheduled actions. |
| Description | The output of the scheduled action cannot be read correctly. |
| Solution | The scheduled action executes correctly; you can safely ignore this error message. |

| | |
|---|---|
| Problem | Setting the port range for MPE/iX managed nodes has no effect. |
| Description | You can set the port range in the `Node Advanced Options` window, but this doesn't have any effect. MPE/iX managed nodes cannot communicate with the ITO management server through a firewall. |
| Solution | There is no workaround available. |

## OS/2 Managed Node Runtime Problems and Solutions

| | |
|---|---|
| Problem | Action agent cannot redirect stdout and stderr. |
| Description | Action agent cannot redirect stdout and stderr. |
| Solution | Add the parameter `OPC_OS2_MAX_NBR_OPEN_FILES` to the `\opt\OV\bin\OpC\install\opcinfo` file to set the maximum number of open files to 100 (OS/2 default is 20). |

| | |
|---|---|
| Problem | ITO agent processes cannot be stopped. |
| Description | If you receive a message that some ITO agent processes could not be stopped, or if you find that agent processes are still running although the control agent exited, stop all running ITO agent processes. |
| Solution | Stop the processes by executing `\opt\OV\bin\OpC\utils\opckill.exe`. |

## RPC Daemon or Local Location Broker Problems and Solutions

| | |
|---|---|
| Problem | Control agent does not come up on node, or ITO error log file contains errors indicating an NCS or DCE problem. |
| Description | If a registered ITO process stops responding, even though it is running, there may be a problem with the NCS local location broker daemon (`llbd`), or the DCE RPC daemon (`dced/rpcd`). |
| Solution | For UNIX systems: check that the `dced/rpcd` is running on the management server, and that either an `llbd` or `dced/rpcd` is running on all managed nodes.<br>**`ps -eaf \| grep dced (rpcd)`**<br>**`ps -eaf \| grep llbd`**<br>You can use the tools `rpccp/dcecp` to check that `rpcd/dced` is running. You can use the tool `lb_admin` to check whether all registered services can still be reached or not. **For MPE systems:** If the problem occurs on an MPE node, this tool is also available, but under the name `lbadmin.pub.hpncs`. In addition, a tool called `ncktest.pub.hpncs` is available to check whether NCS is configured properly. The most important sub-commands for `ncktest` are:<br>• broker local debug<br>• config<br>• files<br>• loopback |

## Accessing the MIB of the Managed Node

To grant ITO access to the MIB of the managed node, you must ensure that the get-community-name is set in one of the following ways:

- Edit the `opcinfo` file on the managed node (see Table 10-3 on page 399 for the location of the `opcinfo` file on all platforms), and add the following line:

  **`SNMP_COMMUNITY <community>`**

  where *<community>* is the community for which the `snmpd` is configured.

  If `SNMP_COMMUNITY` is not set, the default community `public` is used. If it is set, the specified community name is used for snmp-get operations and should match one of the get-community strings in the `snmpd` configuration file.

- Or edit the configuration file for the SNMP daemon:

  on HP-UX 10.x and 11.x managed nodes:
  `/etc/SnmpAgent.d/snmpd.conf`

  `get-community-name`: enter the community name for the SNMP agent. More than one community name can be specified by adding a line for each community name. This can be set to one of the following:

  - When left empty:

    The SNMP agent responds to get requests using any community name.

  - If a community name is entered, the SNMP agent only responds to get requests using this community name, for example:

    **`get-community-name: secret`**

    **`get-community-name: public`**

ITO requires this access for:

- monitoring MIB effectively
- the automatic resolution of node attributes when you configure a new node in ITO.

For more details, see the related `snmpd` man page. For HP-UX, see the *HP OpenView SNMP Agent Administrator's Guide*.

## NFS Problems and Solutions

| | |
|---|---|
| Problem | The logfile encapsulator reports the warning message:<br>`Unable to get status of file <filename>. Stale NFS handle.` |
| Description | The logfile encapsulator can sometimes perceive logfiles set up on NFS as being open, even after they have been removed. This causes an attempted access to fail. |
| Solution | Change the policy by closing the logfile between reads. Select `Window: Message Source Templates` to open the `Message Source Templates` window. Make sure that logfiles are listed, click on the desired logfile, then on `[Modify…]`. In the `Modify Logfile` window, click on `[Close after Read]`.) |

# Changing Hostnames/IP Addresses

Frequently, a node has several IP addresses and hostnames. You may need to change an IP addresses if a node becomes a member of another sub-net. In this case, the IP address or fully qualified domain name may change

In general, on HP-UX systems, the IP address and the related hostname are configured in:

- `/etc/hosts`
- the **Domain Name Service** (DNS), or
- the **Network Information Service** (NIS)

ITO also configures the hostname and IP address of the managed nodes' management server in the management server database.

If you are moving from a non-name-server environment to a name-server environment (DNS, BIND), make sure the name server has access to the new IP address.

Hostnames work within IP networks to identify a managed node. While a node may have many IP addresses, the hostname is used to pin-point a specific node. The system hostname is the string returned when you use the UNIX `hostname(1)` command.

## Changing the Hostname/IP Address of the Management Server

Change the hostname and/or IP address of the management server in two stages. Firstly, set up the change by stopping processes and changing the name. Then, restart and reconfigure ITO for your changes to take effect. See the following section for information on how to change the hostname/IP address of the managed nodes.

**NOTE**

You must de-install the ITO agent software from the management server *before* changing the hostname of the management server. Re-install the ITO agent software when you have finished this task. For more information on de-installing and re-installing the agent software, see the *HP OpenView IT/Operations Installation Guide for the Management Server*.

## Before You Change the Hostname/IP Address of the Management Server

1. Stop *all* ITO processes on your management server. This includes the manager, agent and user-interface processes running on this system.

   a. Stop *all* running ITO user interfaces by selecting `Map:Exit`.

   b. When changing the *IP address* of the management server, stop the ITO agents on your management server.

      **`/opt/OV/bin/OpC/opcagt -kill`**

   c. Stop the ITO manager processes:

      **`/opt/OV/bin/ovstop opc ovoacomm`**

   d. Check that no ITO processes are running:

      **`ps -eaf | grep opc`**

   e. If an ITO process is still running, kill it manually:

      **`kill <`*`proc_id`*`>`**

      All ITO intelligent agents on ITO managed nodes will start buffering their messages.

2. Make sure the database is running. If it is not running, start it with the following commands:

   ```
   su - oracle
   $ORACLE_HOME/bin/svrmgrl
   connect internal
   startup
   exit
   exit
   ```

   For more information about the Oracle database, see the *HP OpenView IT/Operations Installation Guide for the Management Server*.

3. Change the ITO management server's IP-address and/or node name in the ITO database according to the “old/new name” naming scheme below:

   **`/opt/OV/bin/OpC/utils/opcchgaddr -force -label \`**
   **`<`*`label`*`> IP <`*`old_addr`*`> <`*`old_name`*`> IP <`*`new_addr`*`> \`**
   **`<`*`new_name`*`>`**

Where:

| | |
|---|---|
| **-force** | The name service is not consulted. The database is not checked for duplicate node names. |
| **-label <*label*>** | Modifies the label of the node to <*label*>. The new label is displayed in the Node Bank. |
| **<*old_addr*>** | The IP address of old node. |
| **<*new_addr*>** | The IP address of new (renamed) node. |
| **<*old_name*>** | The node name of old node. |
| **<*new_name*>** | The node name of new (renamed) node. |

4. Shut down the database:

```
su - oracle
$ORACLE_HOME/bin/svrmgrl
connect internal
shutdown
exit
exit
```

5. Stop OpenView and all other integrated services (including ITO):

```
/opt/OV/bin/ovstop
```

6. Modify the following ITO management server configurations:

   a. To change the *hostname*, edit the following files. Always replace any occurrence of the old hostname with the new one:

   ```
   /opt/OV/bin/OpC/install/opcsvinfo
   /var/opt/OV/share/databases/openview/ovwdb/ovserver
   /etc/opt/OV/share/conf/ovspmd.auth
   /etc/opt/OV/share/conf/ovwdb.auth
   /etc/opt/OV/share/conf/ovw.auth
   ```

   b. To change the *IP address*, check whether the file `/opt/OV/bin/OpC/install/opcinfo` contains the parameter `OPC_IP_ADDRESS`. If it does, update the file with the new IP address.

7. Reconfigure the ITO management server system with the new hostname/IP address. For details, see the *HP-UX System Manager's Guide*.

   To change the host name permanently, run the special initialization script `/sbin/set_parms`.

   Switching to a name server environment: If moving from a "non-name server" environment to a "name server" environment, make sure the name server has the new hostname/IP address available.

8. Restart your ITO management server system.

## Restarting and Reconfiguring the System After Changing a Hostname/IP Address

1. Stop the management server if it is running:

   ```
   /opt/OV/bin/ovstop opc ovoacomm
   ```

2. Start the OpenView Topology Manager Daemon Service:

   ```
   /opt/OV/bin/ovstart ovtopmd
   ```

3. If you changed the hostname, you must also update the ITO subagent configuration:

   ```
   rm /etc/opt/OV/share/conf/OpC/mgmt_sv/svreg

   touch /etc/opt/OV/share/conf/OpC/mgmt_sv/svreg

   opt/OV/bin/OpC/install/opcsvreg -add \
   /etc/opt/OV/share/conf/OpC/mgmt_sv/itosvr.reg
   ```

   To reconfigure additionally installed subagent packages, please refer to the manuals supplied with these packages.

4. If the `netmon` process automatically starts up when the system starts up, stop the `netmon` process:

   ```
   /opt/OV/bin/ovstop netmon
   ```

5. Remove all entries from the SNMP configuration cache:

   ```
   /opt/OV/bin/xnmsnmpconf -clearCache
   ```

6. Update the creation time of objects contained in the `ovtopmd` database. This will cause the objects to reappear in all maps the next time they are synchronized:

   ```
   /opt/OV/bin/ovtopofix -U
   ```

7. Restart the `netmon` process:

   **`/opt/OV/bin/ovstart netmon`**

8. Use the `ping` command to update OpenView's "knowledge" of the changed hostname:

   **`ping <`*`new_hostname`*`>`**

9. Update the OpenView Topology Database with:

   **`/opt/OV/bin/nmdemandpoll <new_name>`**

10. Make sure the database is running. If it is not running, start it with the following commands:

    ```
    su - oracle
    $ORACLE_HOME/bin/svrmgrl
    connect internal
    startup
    exit
    exit
    ```

    For information on the Oracle database, see the *HP OpenView IT/Operations Installation Guide for the Management Server*.

11. Start OpenView and all other integrated services (including ITO):

    **`/opt/OV/bin/ovstart`**

**NOTE** At this point the agent will start forwarding its buffered messages.

12. Start the ITO GUI, and log in as administrator.
13. Check that the templates are assigned to the new node (they should still be).
14. If you changed the hostname, re-distribute all Event-Correlation templates assigned to the management server. Select `Actions:Server->Install / Update Server Templates` from the menu bar of the `Node Bank` window.
15. Make the following changes depending on whether your system is the only management server in your environment or one of many operating in a flexible-management environment.

If you are not operating in a multi-management server environment (see `opcmom(4)`), perform the following steps on all managed nodes that are configured in the `Node Bank` and which are running an ITO agent:

a. Shut down the ITO agents:

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

b. Update the agent's `opcinfo` file with the ITO management server's new hostname. See Table 10-3 on page 399 for the location of the `opcinfo` file on the managed nodes.

c. Restart the ITO agent processes:

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

If you are running your system in a multi-management-server environment (using flexible-management features), carry out the following steps:

a. Perform steps **a** through **c** above only on those nodes that contain the modified ITO management server in their `opcinfo` file.

b. If the modified ITO management server is configured as a primary manager for some managed nodes, update those managed nodes by running the following command from the modified ITO management server:

```
/opt/OV/bin/OpC/opcragt -primmgr [ -all | \
[ -nodegrp <group>…] <node>…]
```

c. Make sure that your hostname/IP-address changes are reflected in all appropriate configurations and templates across the entire flexible-management environment. Refer to `opcmom(4)` for how to setup, modify or distribute the templates in a flexible-management environment.

16. If you have setup manager-to-manager message forwarding, you will need to modify the hostname and IP-address manually on all management servers that have the changed system in their node bank. In addition, check message-forwarding or escalation templates on the management servers concerned for occurrences of the old hostname/IP address and modify accordingly. The following file needs to be checked:

    `/etc/opc/OV/share/conf/OpC/respmgrs/msgforw/escmgr`

# Changing the Hostname/IP Address of a Managed Node

**NOTE**

When changing the *hostname* of a managed node, you must de-install the ITO agent software from that node before proceeding with the following step. Re-install the ITO agent software when you have finished with this task. For more information on de-installing and re-installing the agent software, see the *HP OpenView IT/Operations Installation Guide for the Management Server*.

1. On all ITO managed nodes whose *IP address* you want to change, stop the ITO agent processes:

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

2. On the management server, ensure that the database is running. If it is not running, start it now with the following command:

   ```
   su - oracle
   $ORACLE_HOME/bin/svrmgrl
   connect internal
   startup
   exit
   exit
   ```

   For more information about the Oracle database, see the *HP OpenView IT/Operations Installation Guide for the Management Server*.

3. On the management server system, for all the managed nodes that will be modified, change the ITO managed node's IP-address/node name in the ITO database according to the “old/new name” naming scheme below:

   ```
   /opt/OV/bin/OpC/utils/opcchgaddr -sync -force \
   -label   <label> IP <old_addr> <old_name> IP \
   <new_addr> \    <new_name>
   ```

   Where:

   | | |
   |---|---|
   | `-sync` | synchronizes any changes to hostname/IP address with the ITO run-time components. |

| | |
|---|---|
| **-force** | The name service is not consulted. The database is not checked for duplicate node names. |
| **-label <*label*>** | Modifies the label of the node to <*label*>. The new label is displayed in the Node Bank. |
| **<*old_addr*>** | The IP address of old node. |
| **<*new_addr*>** | The IP address of new (renamed) node. |
| **<*old_name*>** | The node name of old node. |
| **<*new_name*>** | The node name of new (renamed) node. |

4. For all ITO managed nodes you want to modify:

   a. Reconfigure the ITO managed node system to the new hostname/IP-address. If you are moving from a “non-name server” environment to a “name server” environment, make sure the name server has access to the new hostname/IP-address.

   b. Reboot your ITO managed node system.

   c. If the ITO agent processes did not automatically restart when you rebooted the system, restart them now:

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

5. Perform the following procedures on your management server:

   a. Stop netmon:

      **/opt/OV/bin/ovstop netmon**

   b. Remove all entries from the SNMP configuration cache:

      **/opt/OV/bin/xnmsnmpconf -clearCache**

   c. Update the creation time of objects contained in the ovtopmd database. This will cause the objects to reappear in all maps the next time they are synchronized:

      **/opt/OV/bin/ovtopofix -U**

   d. Restart netmon:

      **/opt/OV/bin/ovstart netmon**

6. On your management server for all ITO managed nodes whose hostname/IP-address you want to change:

   a. Use the `ping` command to update OpenView's "knowledge" of the changed hostname and IP address:

      **`ping <new_name>`**

   b. Update the OpenView Topology Database with:

      **`/opt/OV/bin/nmdemandpoll <new_name>`**

7. Resynchronize the ITO server processes and GUIs:

   a. Restart the ITO Administrator's and Operator's GUI, using ths following menu option in any of the main ITO windows:

      `File: Restart Session`

8. If the old hostname is referred to in any ITO templates (such as in the `Node` field in the `Actions` section of the `Conditions No.` window for remote automatic actions), perform steps **a** and **b** below. You have to do these workaround steps since `opcchgaddr` changes only 'central' tables containing node information; the internal ID is not modified. This means the template itself is not changed in the database. Therefore, the special flag indicating the template has been modified will not be set. Merely using `Force Update` will not update the database since ITO caches the templates as flat files if they have been distributed once.

   a. Force ITO to re-create templates out of the database by removing cached templates from the last distribution:

      **`cd /etc/opt/OV/share/conf/OpC/mgmt_sv/templates`**

      **`rm -f 'find . -type f'`**

   b. Distribute the modified configuration to all managed nodes using any template that refers to the modified hostname:

      1. In one of the main windows, select `Actions:Agents->Distribute`.
      2. In the `Distribute ITO Software and Configuration` window, select the component `[Templates]`.
      3. Select `[Force Update]` and `[Nodes in list requiring update]`.

4. Select the managed nodes in the `Node Bank` window, and click `[Get Map Selections]` in the `Distribute ITO Software and Configuration` window.
5. Click `[OK]`.

**If you are operating ITO in a distributed management server environment (Manager-of-Manager environment)**

If you are running ITO in a multi-management server environment (refer to `opcmom(4)` for more details), perform the following steps:

1. Follow steps 2 through 7 above on all management server systems that control or monitor the modified node.
2. Carry out step 8 on all ITO management server systems that refer in any ITO template to the old hostname.

# ITO Security

The steps that an administrator needs to carry out to improve system security involve much more than configuring software: in general terms, the administrator needs to look at system security first and then investigate problems that relate to network security. Finally, the administrator needs to investigate the security implications and possibilities that are addressed during the configuration of ITO itself. This section covers the areas mentioned in this paragraph, namely:

- System Security
- Network Security
- Port Security
- ITO Security

System security covers the problems that need to be addressed to allow the ITO management server and managed node to run on a “trusted” system. Network security involves the protection of data that is exchanged between the management server and the managed node and is primarily DCE related. ITO security looks at the security- related aspects of application setup and execution, operator-initiated actions, and so on.

## System Security

The following sections describe the areas that the administrator needs to address in order to install and run ITO on an HP-UX system that is C2 compliant. For information on how to make a system C2 compliant, see the relevant, product-specific documentation. Note that it is essential that the underlying operating system be rendered secure first.

The section on system security covers the following areas:

- General Security Guidelines in ITO
- Restrictions

## General Security Guidelines in ITO

A C2-secure or "trusted" system uses a number of techniques to improve security at system level. These techniques would include, amongst other things, the following:

- ❏ Imposing strict password and user authentication methods for the UNIX login
- ❏ Auditing networking, shared memory, file systems and so on
- ❏ Controlling access to terminals
- ❏ Managing access to files

For information about the implications these security recommendations can have with regard to the configuration of ITO, see "Restrictions" on page 436.

## Restrictions

Running ITO in a C2-secure environment imposes a number of important restrictions on the ITO configuration. Table 10-7 on page 436 lists those areas and provides a brief explanation of the cause of the restriction. It is the administrator's decision as to where security priorities lie.

**Table 10-7 Restrictions in a C2-secure Environment**

| Restricted Area | Explanation |
|---|---|
| ACLs | Although C2 recommends the use of ACLs, the OpenView file tree does not support them. In addition, `opc_backup` and `opc_restore` are not aware of ACLs. |
| Agent Installation | If root-login over the network is not allowed, the ITO agent has to be installed manually. For more information about installing the agent manually, see the *HP OpenView IT/Operations Installation Guide for the Management Server* |
| Application Passwords | Password aging and changing can lead to problems with remote application startup. |

## Network Security

Network security involves the protection of data that is exchanged between the management server and the managed node and is primarily DCE related. ITO addresses the problem of network security by controlling the authenticity of the parties, in this case the RPC client and server, before granting a connection and ensuring the integrity of data passed over the network during the connection.

Although ITO carries out its own, basic authorization checks when communication between the management server and the managed nodes is required, DCE allows the implementation of more stringent security at process level between an RPC client and an RPC server, specifically in the areas of authentication and privacy, or data protection.

The level of data protection is chosen by the client, although the server has the option of deciding whether a chosen level is sufficient, and ITO sees the concept of authentication in the context of either the RPC client or the RPC server. For example, in the same way that an RPC server needs to determine whether or not an incoming request is from a genuine ITO client, an RPC client also needs to be sure that the server it is calling really is an ITO server.

The section on network security covers the following areas:

- ❏ DCE Configuration
- ❏ Authentication
- ❏ Process names and passwords
- ❏ Port security
- ❏ Processes and port numbers

### Basic DCE Configuration

If you want to protect communication between the ITO management server and managed nodes using DCE's security mechanisms, you need to carry out some extra configuration steps. First of all, a DCE server installation must be available in the local network. The DCE server installation provides:

- ❏ Cell Directory Service (CDS)
- ❏ DCE security service
- ❏ DCE Distributed Time Service (DTS)

In addition, all participating nodes must be member of DCE cells, which are configured to trust each other.

ITO does not require specific DCE configuration. An installed DCE runtime (client part) including shared libraries and the RPC daemon (`rpcd`/`dced`) are sufficient. However, these components are necessary on all ITO managed nodes running a DCE, ITO agent. The client components include the necessary client parts for authenticated RPC, too. Consequently, it is not necessary to install additional DCE components on all managed nodes.

For more detailed information on DCE, see the product-specific documentation and “Configuring DCE Nodes to use Authenticated RPCs” on page 439.

## DCE Servers

It is necessary to have at least one Cell Directory Service and a security server running in a DCE cell. These systems should be reliable, sufficiently powerful (CPU, RAM), and connected via a fast network link to all participating ITO nodes. Although a DCE server system can also be an ITO management server or a managed node, it is recommended that the DCE servers be separate from the ITO management server in order to distribute demand on resources. It is also highly recommended that you consider the option of configuring the DCE server system as an ITO managed node. In this way, ITO can monitor the health and status of the DCE server system.

**NOTE**

In addition to the DCE runtime package, a dedicated, DCE, server system requires the DCE server components, which have to be purchased separately.

## DCE Nodes

Each managed node running the DCE ITO agent and each management server must be member of a DCE cell. The initial cell member must be a DCE server system—this step configures the DCE-cell administrator **cell_admin**, who plays an important role in all further DCE configuration. To configure a node to run in a DCE cell, use the DCE utility `dce_config`, which provides a menu-driven configuration of the local node. The user must run this utility on each node which is intended to be used for DCE authenticated RPC. ITO nodes which are not also DCE server systems have to be set up as client nodes. For details refer to the DCE installation manuals.

## Configuring DCE Nodes to use Authenticated RPCs

The DCE names and accounts, required by ITO to use authenticated RPCs, are set up by using `opc_sec_register_svr.sh` and `opc_sec_register.sh`. You need to run `opc_sec_register_svr.sh` once on the ITO management server and `opc_sec_register.sh` for each managed node which requires the ITO accounts, and only after you have configured the node (using `dce_config`) as part of a wider DCE environment. The final step in the configuration process involves using the ITO GUI to set the security level for the management server and individual managed nodes.

**NOTE**

`opc_sec_register_svr.sh` and `opc_sec_register.sh` require a DCE login context to complete successfully. Before running `opc_sec_register_svr.sh` or `opc_sec_register.sh` you must log into DCE as cell_admin, using the command `dce_login`. It is also important to switch to UNIX user root before logging into DCE. This applies to both the management server and the managed node.

To configure the ITO management server and managed nodes to use authenticated RPCs, perform the following steps:

1. Ensure that each managed node and the management server are members of a DCE cell as well as a DCE server system itself. To add a node to a DCE cell, run the DCE utility `dce_config` locally on each of the nodes to be added.
2. As UNIX user root, log in as the DCE user cell_admin, and execute the following command:

   **`dce_login cell_admin <`*`cell_admin password`*`>`**

   This opens a new shell with a DCE login context:
3. Execute the following script as UNIX user root once on the management server:

   **`/opt/OV/bin/OpC/install/opc_sec_register_svr.sh -s`**
4. Subsequently, you have to run the script as user root and with a valid DCE login context on each of the managed nodes that requires the DCE authentication of RPCs. This may be done remotely from the management server only if automatic password generation has been disabled for the managed node:

   **`/opt/OV/bin/OpC/install/opc_sec_register.sh <`*`node1`*`>\`**
   **`<`*`node2`*`> ...`**

Or locally on each of the managed nodes:

**/opt/OV/bin/OpC/install/opc_sec_register.sh**

These steps can be repeated if necessary.

**NOTE**

To undo any of the steps you have carried out using the script `opc_sec_register_svr.sh` or `opc_sec_register.sh` , use the `-remove` option.

5. Use the ITO GUI to select the appropriate security level for the managed node or management server using DCE RPCs. By default, the security level is set to “No Security”. To set or change the security level:

   a. Open the `ITO Node Bank` window.

   b. Click the node whose security level you want to change.

   c. Open the following sequence of windows:

      `Actions:Node->Set Defaults->Advanced Options`

      if you want to change the default setting for all nodes, or:

      `Actions:Node->Modify->Advanced Options`

      if you want to change the default setting for an individual node

   d. Fill in the relevant fields in the `Communications Parameters` section. ITO’s online help provides guidance on the options provided.

   e. Close the `Advanced Options` window.

   f. Click `[OK]` in `the ITO Node Defaults` or `Node Modify` window.

**NOTE**

Note that the domestic version of DCE (dced.Dom U.S./Canada only) must be installed. If you select a DCE Security Level in the `Node Advanced Options` window, but have no domestic version installed, the communication between the ITO agent and the management server will fail. If this happens, set the DCE Security Level to `No Authentication of RPCs`, and remove the appropriate entry in the managed node’s `nodeinfo` file. Then manually restart the ITO agents.

## Authentication

DCE's security mechanism allows you to protect the communication between server and managed node using DCE RPC. An important step in the authentication procedure that an DCE RPC process goes through involves the obtaining of a login context. A secure RPC process has a login context, which it either inherits from its parent process or establishes itself. The login context requires a name (or **principal**) and a password (or **key)**, which are checked by the DCE security server prior to a connection. Since ITO processes usually run without any user interaction, reliance on an inherited login context is not suitable. Consequently, the ITO processes create their own login context with a name and password that must be registered at the DCE security service.

The RPC clients use the login context to get a server-specific 'ticket' which will then be passed with each RPC. The client obtains this ticket from the DCE security service only if it has already passed the authentication process. This ticket contains a key which is not visible to the client application and known only to the security service and the server. The RPC server verifies the ticket using the server's password in the key file and rejects non- matching RPCs, i.e. if a client receives a successful response from the server, it knows that an authentic server processed the request. The only information the server has at this point is whether or not the client is authentic. Subsequently, it extracts from the RPC handle the following information:

- the client's name
- the level of protection the client has chosen

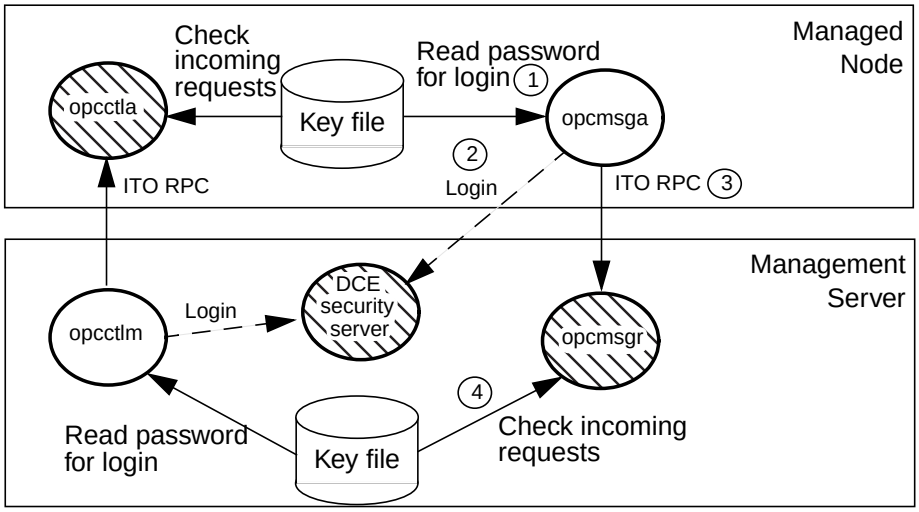
Once the authentication process has completed successfully, a connection is established, and the RPC call sequence initiates. You can configure ITO to carry out the authentication check at the RPC connection to a server, at the beginning of each RPC client-server call, or for each network packet.

In the context of ITO, Figure 10-1 on page 442 uses the example of message transmission to illustrate the authentication process the DCE client and server go through. The numerical call outs in Figure 10-1 on page 442 point to further information, which is provided in the following list:

1. The RPC client (`opcmsga`) reads its password from the key file
2. The RPC client logs in, gets a login context, and obtains a security-server ticket

3. The RPC client sends the RPC request
4. The RPC server (`opcmsgr`) checks the ticket with the password in the key file

**Figure 10-1 The DCE RPC Client-Server Authentication Process**




## Process Names and Passwords

In ITO, both the management server and the managed nodes run RPC clients and servers at the same time. Perhaps paradoxically, this allows ITO to simplify a given process' requirements for configuration information prior to an RPC call, namely:

- name and own password
- security level

However, this configuration information must be present on both the management server and the managed node.

In the context of DCE, ITO associates just two **names** (or principals) with the two types of node in its environment, namely: one each for the management server and the managed node. All management server process then run under the **name** associated with the management server, and all processes relating to the managed node in question run under the identity of the **name** associated with the managed node. For

example, if the ITO management server 'garlic.spices.com' and the managed node 'basil.herbs.com' are configured to run with authenticated RPCs the following principals will be created:

- opc/opc-mgr/garlic.spices.com
- opc/opc-agt/basil.herbs.com

In DCE, a name or principal (garlic.spices.com) belongs to a group (opc-mgr), which in turn belongs to an organization (opc). The only exception to this rule in ITO is the principal opc-agt-adm: opc-agt-adm is a member of the group and organization none, which is a special principal that is primarily used in the administration of accounts and passwords.

In addition, ITO allows you to select and configure the security level your particular environment requires for an individual managed node: the value is stored in the given managed node's nodeinfo file and on the management server in the relevant entry in the database. In this way, security on a given managed node may be changed to handle, for example, the addition of sensitive connections.

ITO may be configured in such a way as to be able to overcome a situation where, owing to the temporary unavailability or poor configuration of the security service, a process is required to run in unauthenticated mode or fail. For example, if a management server process such as the request sender receives an authentication failure when calling a control agent on a managed node, an error message is generated, which appears in the Message Browser window. The administrator is then able to take immediate corrective action, for example, by temporarily changing the security level on the managed node in question to allow the retransmitted request to succeed. However, care should be taken in situations such as this, since an error in the connection could in certain circumstances indicate that the system is under "attack".

## Port Security

One simple but effective way of limiting access to a network and consequently improving the network's inherent security is to restrict to a specific range of ports all connections between processes. This applies to all network traffic and not just RPCs. In the context of ITO, you can do this on two distinct levels:

- Packet-filtering firewalls may lock a range of ports to inbound or outbound traffic. If this is true, then:
- ITO's managed nodes and management server must be configured to restrict all RPC connections to the same range of port numbers as those specified at the firewall

A connection between an RPC server and an RPC client needs at least two ports; one on the server machine, one on the client. Each ITO process that is either an RPC client or RPC server has its own port for communication: the port remains blocked by the ITO process which owns it until the process exits, whereupon the port becomes free for dynamic assignment to the next RPC client-server request. For more general information on dynamic port assignment in ITO, see "Processes and Port Numbers" on page 444 and the *HP OpenView IT/Operations Concepts Guide*.

An RPC client using DCE or NCS does not automatically know the port number of the RPC server on the remote system and, consequently, has to obtain this information before initiating an RPC request. It does this by contacting the `llbd` or `rpcd` on the remote system and looking up the specific port number of the RPC server it needs to connect to. With this information, the RPC client sends the "real" request for "real" information to the RPC server at the port number it obtained.

**NOTE** The `llbd`/`rpcd` always runs on UDP 135, a reserved port which must always be accessible even through a firewall.

## Processes and Port Numbers

In addition to using the checks and controls that a DCE environment supplies for authentication and data integrity both prior to and during connections between processes, the administrator can combat security breaches within ITO by restricting to a specific range, defined in the GUI, the port numbers that ITO-specific processes use. Conversely, the ability to define this range of ports means that the administrator can also configure ITO to run in an environment where, for security reasons, routers or packet-filtering firewalls restrict the use of ports to a specific and, often, quite limited range.

ITO assigns port numbers dynamically to those processes that are granted an RPC connection. The port numbers are configurable and are checked against the range defined in the GUI each time an RPC server registers itself. Information relating to the assignment of ITO-specific port numbers may be found in:

- the `llbd` (for NCS)
- the `rpcd`/`dced` (for DCE)

**NOTE** NCS agents will not run on managed nodes where a DCE agent is installed and running unless NCS support is built into the `rpcd`/`dced`.

Table 10-8 on page 445 lists the ports that ITO requires. For more information on port restrictions in a firewall environment, see Figure 10-2 on page 449.

**Table 10-8 Port Allocation in ITO**

| Service | Protocol | Inbound Ports | Outbound Ports |
|---|---|---|---|
| NCS `llbd` | UDP | 135 | above 1023 |
| NCS `glbd` (licensing) | UDP | (broadcast) | above 1023 |
| DCE `rpcd` | UDP/TCP | 135 | above 1023 |
| `ftpd` | TCP | 20 (data transfer)<br>21 (control) | above 1023 |
| `rexecd` | TCP | 512 | below 1023 |
| `rlogind` | TCP | 513 | below 1023 |
| `telnetd` | TCP | 23 | above 1023 |
| `remshd` | TCP | 514 | below 1023 |
| DCE/NCS RPC server processes | UDP/TCP | configurable;<br>recommended: >1023 | above 1023 |
| ITO heartbeat polling | ICMP | - | - |

If a service request for a port number within the range specified is refused because none is available, the process will not start. If such an occurrence arises, you can stop the ITO server processes and use the utility `/opt/OV/bin/OpC/utils/opc_reset_ports` to delete the

defined port range on the management server. Subsequently, you will need to restart the server processes and increase the port range. On the managed node, you need to delete the variable *OPC_COMM_PORT_RANGE* in the `nodeinfo` file and restart the agents. You can then configure a bigger range for this managed mode and, after a successful distribution, restart the agent.

**Table 10-9 Ports Required by the ITO Agent**

| ITO Component | Agent Process | Ports Required [a] | Port Type/No [b] |
|---|---|---|---|
| rpc-server | `rpcd` | 1 | 135 |
| | control agent (`opcctla`) | 1 | - |
| rpc-client | message agent (`opcmsga`) | 2 | - |
| | distribution agent (`opcdista`) | 2 | - |
| | distribution agent (`opcdista`) to socket server | 1 | - |

a. m=number of ITO Server in parallel use
n = number of agents in parallel use
b. Local = connects to the display server on the local machine

**Table 10-10 Ports Required by the ITO Management Server**

| ITO Component | Server Process | Ports Required [a] | Port Type/No [b] |
|---|---|---|---|
| rpc-server | rpcd | 1 | 135 |
| | message receiver (`opcmsgrd`) | 1 | - |
| | distribution manager (`opcdistm`) | 1 | - |
| | display manager (`opcdispm`) | 1 | - |
| | socket server (`opctss`) | 1-10 | - |
| rpc-client | request sender (`ovoareqsdr`) | 2 * n | - |
| | action manager (`opcactm`) | 2 | local |
| | forward manager (`opcforwm`) | 2 * m + 2 | local |
| JAVA UI server | `opcuiwww` | 1 | 2531 |
| `opcragt` | | 2 * n | - |
| JAVA GUI (socket based) | | 1 | 2531 |
| ITO SE JAVA GUI | | 1 | 4348 |
| TT & notification service mgr | `opcttnsm` | 2 | local |

a. m=number of ITO Server in parallel use
n = number of agents in parallel use
b. Local = connects to the display server on the local machine

**NOTE** You need to stop and restart both the management server and the agent processes in order to enable any changes to (or initial configuration of) the port ranges on the ITO management server and the managed node.

It is important to remember that the port range applies to both the TCP and UDP protocols. However, although the RPC server attempts to register with both protocols in the same port range, the RPC clients only use the communication type selected for a given node in the `Node Defaults Advanced Options` window to contact a server. So, if the allocation of a UDP port in the desired range fails but the TCP port allocation succeeds, the connection will succeed if the communication type is set to TCP.

**NOTE** NCS always uses UDP.

**NOTE** MPE/iX managed nodes cannot communicate with the ITO management server through a firewall. Setting the port range has no effect.

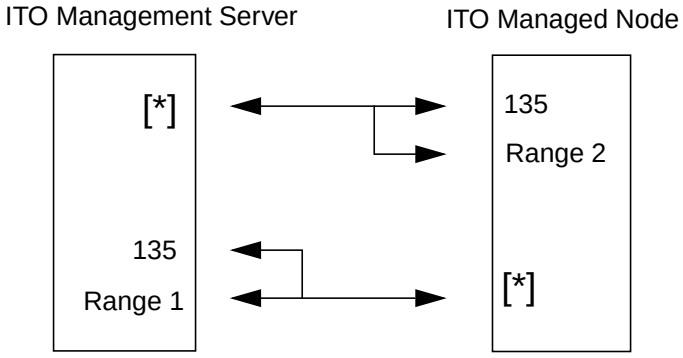
## Port Restrictions

Any router acting as a packet-filtering firewall in an ITO environment must be configured to keep the ports specified in Figure 10-2 open for communication between the ITO management server and the managed nodes. It is recommended that the minimum number of ports for the management server (specified in range 1 in Figure 10-2) be in the order of 50, although this depends on the number of calling managed nodes. The minimum port range on the managed node (range 2) should be 10. You set ranges 1 and 2 in the ITO GUI using the `Allowed Port Range` field in the `Configure Management Server` window and the advanced options part of the `Node Defaults` window and the `Node Modify` windows, respectively.

Setting the port range for ITO does not reserve the ports in the defined range exclusively for ITO processes. Other applications can register (accidentally or otherwise) on ports in the range you specify, and this can lead to a situation where, if the defined port range is small, no more ports are available for allocation to ITO at a given time. In addition, when you define the port range, you should take into account that extra ports are required for such processes as `opctss` (socket server), `opccmm, and opccma` which are spawned by the distribution manager `opcdistm`, and that an extra port is also required for each bulk transfer and distribution.

**NOTE** Although the allowed port range of given managed nodes may differ if the managed nodes are connected to the ITO management server through a different router, *all* managed nodes that use the *same* router must use the same port range.

**Figure 10-2 Compulsory Firewall Port Ranges in ITO**




The DCE environment variable *RPC_RESTRICTED_PORTS* controls the DCE RPC server runtime's tendency occasionally to open additional ports outside the range specified in ITO, when called by clients using UDP. Since the managed nodes may make DCE RPC calls (using UDP) to the rpcd on the management server, it is important that the `rpcd/dced` runs in an environment (on the management server) where the value of *RPC_RESTRICTED_PORTS* is set to match the port range defined both on the ITO management server and at the firewall. The value of *RPC_RESTRICTED_PORTS* needs to be set in the following way in the DCE system startup files. For example:

```
RPC_RESTRICTED_PORTS=tcp[range]1:udp[range1]
```

**NOTE** Whatever protocol you choose in the ITO GUI for RPC connections, the allowed port range you define must always be open for TCP in both directions at the firewall to allow for bulk data transmission.

# ITO Security

The administrator needs to investigate the security implications and possibilities that are addressed during the configuration of ITO itself. For example, managed nodes will only allow those management servers that it recognizes as action-allowed managers to execute operator-initiated actions. ITO security looks at the security-related aspects of application set up and execution, operator-initiated actions, and so on. The section on ITO security covers the following areas:

- ❏ Accessing ITO
- ❏ Program security
- ❏ Database security
- ❏ Application setup and execution
- ❏ Executing and forwarding actions
- ❏ The location of queue files

## Accessing ITO

Only ITO registered users can access the ITO GUI. By default, the users **opc_adm** and **opc_op** are available. The ITO user names and passwords have no direct relation to UNIX user names and passwords. However, it is possible to use UNIX user names, and if the user name is defined in the ITO database, the user is not prompted for a password. This is the fastest way to open an ITO GUI. Furthermore, it is recommended that system administrators map unix user names (1:1) to ITO operator names. In addition, The ITO administrator can change operators' passwords, but cannot see any new password an operator sets—the characters are masked by asterisks. By default, operators can, of course, change their own passwords.

To remove the change password functionality from all operators, comment the following lines:

```
Action "Change Password"
{
}
```

in `/etc/opt/OV/share/conf/OpC/mgmt_sv/appl/registration/\C/opc_op/opcop`

## File Access and Permissions

When a user starts an ITO operator GUI session, the working directory is defined by environment variable `$OPC_HOME` (if set) or `$HOME`. If neither `$OPC_HOME` nor `$HOME` is set, then `/tmp` is the default working directory. For more information on common ITO variables, see "Variables" on page 291.

If the unix user that started the ITO operator GUI has no write permission in the default working directory, an error message is displayed but the ITO GUI starts nonetheless. However, any subsequent attempt by the operator to write files to the default directory will fail unless the directory permissions are changed. This includes the automatic save of the broadcast-command history file. In addition, whenever an operator saves application, instruction, or report output to a file without specifying an absolute path, the file is stored in the user's working directory and owned by the operator's unix user ID, not by `opc_op` (unless the operator logged in as unix user opc_op). The permissions of the file will reflect the value of umask as set before the ITO operator GUI was started. Operators who want to share files with other operators need to set (or ask the system administrator to set) the appropriate file and group and permissions for the desired degree of sharing. ITO will no longer change any of these settings automatically. However, ITO operators are not able to make unauthorized changes, and all ITO configuration files remain secure. Any files that are created when the administrator saves report and application output are owned by the administrator's unix user and saved in the `$OPC_HOME` directory if no absolute path is specified.

**NOTE**

"Write" permission for the group can be overridden by "no write" permission for the owner. In addition, ITO operator ARFs (and related symbolic links and directories) that are changed by the administrator remain readable and traversable by *all* and not just `opc_op`.

## The Administrator GUI

In the Motif administrator GUI (the GUI that is started when the ITO user `opc_adm` logs on), the unix process that is used for making configuration changes, `opcuiadm`, runs with root permissions. However, `opcuiopadm`, the unix process that is used for the administrator's browser, runs under the unix user ID of the user who started the Motif administrator GUI rather than unix user `opc_op`.

It is neither necessary nor specifically recommended to start the Motif administrator GUI as a unix user with root privileges (user ID 0). In addition, when saving the output of database reports on the ITO configuration, the owner of the files that are written is the unix user who started ITO. Otherwise, the behavior of the administrator GUI is the same as the operator GUI.

## The Operator GUI

During installation the ownership and permissions of the `opcrlogin` utility will be set as follows:

```
-r-xr-x--- root opcgrp /opt/OV/bin/OpC/opcrlogin
```

In addition, when opening an ITO Virtual Terminal or starting an ITO Input/Output Application on a node, the `.rhosts` entry for the operator's unix user (if present) is used in preference to the entry for user `opc_op` in order to enable the operator to log on without entering a password.

Integrated applications (menu items introduced using an ITO "OV Service" application or registered actions represented by an ITO "OV Application") that are started from ITO start under the same unix user as the operator, which is not usually `opc_op`.

## Program Security

The HP-UX 10.x and 11.x programs `/opt/OV/bin/OpC/opc` and `/opt/OV/bin/OpC/opcuiadm`) have the s-bit (set user-ID on execution).

For MPE/iX, note that the job **OPCSTRTJ.BIN.OVOPC** contains the readable password of **AGENT.OVOPC** if the standard **STREAM** facility is used. If you have specified a customized *stream* command in the `Advanced Options` sub-window of the `Add/Modify Node` window, no password is inserted in **OPCSTRTJ.BIN.OVOPC**. Note that this entry is only established during first-time installation, or if the ITO entry is found in **SYSSTART.PUB.SYS**.

Change the job according to your security policies. The job is streamed during system boot by **SYSSTART.PUB.SYS** and is responsible for starting the Local Location Broker (if not yet running) and the ITO agents.

## Database Security

Security of the database is controlled by the operating system and by the database itself. Users must have an OS logon for either remote or local access to the data. Once a user is logged on, security mechanisms of the database control access to the database and tables.

For all other database security aspects see *Using Relational Databases with HP OpenView Network Node Manager* and the vendor's manuals supplied with the database.

## ITO Application Setup and Execution

Applications run under the account (user and password) specified by the administrator during application configuration. The action agent uses the information in this account before executing an application, that is, it switches to the user specified and then uses the name and password stored in the application request to start the application.

Application execution can be compromised by the use of password aging. Password aging is a feature of C2 that expires passwords after:

- a specific period of time has passed
- a specific date has been reached
- a certain number of unsuccessful login attempts have been made

Administrators need to bear in mind that if this feature is enabled, it could lead to application startup failures where the account that a given application uses is temporarily inaccessible. In this case, the user or system administrator has to change the password.

## Remote Login and Command Execution

Security issues concerning remote login and command execution are described here for ITO and for UNIX and MPE/iX platforms:

- If he does not apply the default user (setup by the ITO administrator) for command broadcast or application startup, the ITO operator must know the corresponding password. Otherwise, the command/application will fail.
- When starting applications configured as **Window (Input/Output)**:
  - the password must be specified with the application attributes

    -Or-

- an appropriate `.rhosts` entry or `/etc/hosts.equiv` functionality must be available

  -Or-

- the password must be specified interactively.

For more information on user accounts, access to files, and general file permissions, see “File Access and Permissions” on page 451.

## Passwords on DCE Managed Nodes

When executed on the management server with the **`-server`** option, the ITO utility `opc_sec_register_svr.sh` creates a special principal `opc-agt-adm` which has the permissions needed to modify accounts on the managed node. Normally, the ITO agents log into DCE at startup using the primary principal `opc/opc-agt/<hostname>`. However, if this login fails for any reason, the ITO control agent then attempts to login as `opc-agt-adm` and to generate a new random password for it's primary account. The new password will be updated in both the DCE registry and the local keytab file. Generally, the initial DCE login will fail in only the following situations, any of which may be rectified by logging in on the managed node and running `opc_sec_register.sh` manually:

- ❏ After installation (or after running for the first time in authenticated mode) and if the `opc_sec_register.sh` utility was executed on the management server to create the managed node account. In this case, the local keytab file doesn't exist. If `opc_sec_register.sh` has been executed locally on the managed node, it does create the requisite, local keytab file.
- ❏ The managed node's keytab file was removed or corrupted for any other reason.
- ❏ The managed node's password expired while the control agent was not running and, as a consequence, is the control agent is unable to login and generate a new one.

It is possible to simply disable or even remove the `opc-agt-adm` account using standard DCE utilities. However, if you do disable or remove the `opc-agt-adm` account, the automatic password recovery process will be compromised. This does not affect automatic password generation while the agent is running and password expiration is enabled.

## Passwords on UNIX Managed Nodes

The ITO default operator opc_op cannot login into the system via login, telnet, etc. due to a * entry in the `/etc/passwd` file. Furthermore, `.rhosts` entries are not provided. If you want to provide a virtual terminal or application startup (requiring a **Window (Input/Output)** for the ITO default operator, set the password or provide `.rhosts` or `/etc/hosts.equiv` functionality. Note that the **opc_op**'s password should be consistent for all managed nodes.

For example, the *$HOME*/.rhosts entry, where *$HOME* is the home directory on the managed node, of the executing user:

<*management_server*> opc_op

## Passwords on MPE/iX Managed Nodes

The ITO default operator **MGR.OVOPR** does not have a password assigned by default. You can set an appropriate password for user MGR, for his home group **PUB** or for the account **OVOPR**.

Also, note the following:

Account Passwords
: By default no passwords are set for account **OVOPC** and **OVOPR**.

Group Passwords
: By default no passwords are set for any group in account **OVOPC** and **OVOPR**.

User Passwords

**MGR.OVOPC**

By default no password is specified.

**AGENT.OVOPC**

By default no password is specified.

**MGR.OVOPR**

By default no password is specified.

## Passwords on Windows NT Managed Nodes

The password for the **HP ITO account** can be assigned during the installation of the agent software. If a password is not assigned, a default password will be created; a password is not assigned by default.

## Passwords on Novell NetWare Managed Nodes

The password for the default operator opc_op is not assigned during the installation of the agent software. For security reasons, it is strongly recommended to assign a password to opc_op, using NetWare tools, after the agent software is installed.

## Automatic and Operator-initiated Actions

Action requests and action responses can contain sensitive information (application password, application responses and so on), which might be of interest to intruders. In a secure system this might not be a problem. However, if these requests and responses have to pass through a firewall system or even over the Internet where packets may be routed through many unknown gateways and networks, then administrators need to think in terms of the measures required to improve security.

In addition, automatic and operator-initiated actions are currently executed as root. Consequently, in order to prevent security holes, it is essential that the administrator:

- protect any shell scripts (for example, those used to switch user) by assigning minimal rights
- choose carefully the commands which an application uses

## Queue Files

The queue files for the message interceptor (`msgiq`) and the monitor agent (`monagtq`) and used by `opcmsg` and `opcmon` for communicating with their corresponding processes have read/write permission for everyone. Sensitive messages can be read by displaying these queue files as a regular user.

In addition, the administrator also needs to take into account the fact that the `opcmsg` and `opcmon` commands allow anybody to send a message which triggers automatic action attached to a message even on another node.

# Auditing

ITO distinguishes between different **modes** and **levels** of audit control. The mode determines who is permitted to change the level of auditing; the level determines what kind of auditing information is being collected.

Your company policy determines which auditing mode, normal or enhanced, is used. Normal audit control is the default mode after installation. In normal mode the ITO administrator can change the level of auditing using the `Configure Management Server` window. Enhanced audit control can only be set by the user root, and cannot be reset without re-initializing the database.

You can select from the following audit levels:

- `[No Audit]`

  ITO does not maintain any auditing information.

- `[Operator Audit]`

  ITO maintains audit information about:

  - operator logins and logouts, including attempted logins
  - changes to the ITO user passwords
  - all actions started from the browsers and from the Application Desktop:

  Operator Audit is the default level after installation.

- `[Administrator Audit]`

  ITO maintains audit information about user logins and logouts, including attempted logins and changes to the ITO user passwords. In addition, ITO creates **audit entries** when actions are started from the message browsers and in the `Application Bank`, and when the configuration of ITO users, managed nodes, node groups, or templates changes. See Table 10-11 on page 458 for a complete overview of the audit areas that are included in this level.

**Table 10-11 Audit Areas of the Administrator Audit Level**

| Audit Area | Administrator Level | | |
|---|---|---|---|
| | GUI[a] | API[b] | CLI[c] |
| ITO User | | | |
| • logon | ✔ | ✔ | |
| • logoff | ✔ | ✔ | |
| • change password | ✔ | ✔ | |
| Actions, Applications, Broadcasts | | | |
| • start | ✔ | ✔ | |
| • add/modify/ delete | ✔ | ✔ | |
| Message Source Templates | | | |
| • add/modify/delete | ✔ | ✔ | ✔ |
| • add/modify/delete automatic and operator-initiated action | ✔ | ✔ | ✔ |
| • add/modify/delete condition | ✔ | ✔ | ✔ |
| Managed Nodes | | | |
| • configuration | ✔ | ✔ | |
| • distribution of actions, monitor, and commands | ✔ | ✔ | |
| • changes to node defaults | ✔ | | |
| • template assignment | ✔ | ✔ | |
| Node Groups | | | |
| • add/modify/delete | ✔ | ✔ | |
| • managed node assignment | ✔ | ✔ | |
| ITO User Configuration | | | |
| • add/modify/delete | ✔ | ✔ | |

| Audit Area | Administrator Level | | |
|---|---|---|---|
| | GUI[a] | API[b] | CLI[c] |
| Database Maintenance | ✔ | | |
| Trouble Ticket | ✔ | | |
| Notification | ✔ | | |

a. ITO creates an audit entry when the action is carried out using the GUI.
b. ITO creates an audit entry when the action is carried out using an API. Note that no entry in this column only indicates that no audit information is being collected; it does not indicate that no APIs are available.
c. ITO creates an audit entry when the action is carried out using a command line interface (CLI). Note that no entry in this column only indicates that no audit information is being collected; it does not indicate that no command line interfaces are available.

Note that if you change an existing audit level, the new level is applied only after the operator has begun a new ITO session.

Audit information can be written to a report for future review, and can be displayed in the `ITO Reports` window. You can view these reports on your screen, write them to a file, or print them.

**NOTE**

We strongly recommend that you download audit information regularly from the database if you have set the audit level to `Administrator Audit` and you are running ITO in a large environment with a high number of managed nodes and users. Otherwise your database may quickly run out of space.

See the HP ITO Administrator's Guide to Online Information for information about how to configure auditing.

# System Maintenance

You perform system maintenance on both the management server and on managed nodes. Management server maintenance is split into the following areas:

- ❏ System backups
- ❏ Database
- ❏ HP OpenView platform
- ❏ ITO directories and files

You can configure scheduled actions to help you with routine system-maintenance tasks. For more information on how to schedule actions, see the HP ITO Administrator's Guide to Online Information.

## On The ITO Management Server

ITO provides the following methods for backing up data on the ITO management server:

- `opc_backup` - off-line backup
- `ovbackup.ovpl` - automated backup

The ITO configuration is not only on the management server but also on the managed nodes. Consequently, if the restored configuration on the management server does not match the current configuration on a managed node, errors relating to missing instruction text or incorrectly assigned templates may occur. For this reason, it is recommended that after a backup has been restored, the templates, action, command and monitor scripts are redistributed to all managed nodes using the **`force update`** option.

Data backed-up with one tool must be recovered with the backup tool's corresponding restore tool. For example, use `opc_recover` to restore data backed up with `opc_backup`: similarly, `ovrestore.ovpl` must be used to recover data saved using `ovbackup.ovpl`.

**NOTE**

**Archive-log** mode is a term used in Oracle to denote a state in which periodic automatic saves of data are performed and any changes to data files stored in **redo log files**. These redo log files are subsequently

archived. For more information, see the appropriate Oracle documentation. For information on how to set up **Archive-log** mode in ITO, see “Maintaining the Database” on page 468 and the section on database tasks in the HP ITO Administrator's Guide to Online Information.

## Off-line Backup

The `opc_backup` tool offers two backup possibilities, which allow you to backup ITO configuration data only, include the current and history messages, too, or do a full backup that includes the ITO binaries and installation defaults. However, all ITO GUIs have to be shut down and all OpenView services stopped, including the ITO server processes. Then, the Oracle database is shut down, and a complete off-line backup is performed. If you are considering using this method to backup your data, the following advantages and disadvantages should be noted:

- archive-log mode is not needed, which means
  - better overall performance
  - less disk space required
  - you can only recover to the state of the most recent full backup
- binaries are backed up, too (if full mode is used)
- all OV services and GUIs have to be stopped

For an overview of the backup functions, see the following man pages: `opc_backup(1M)` and `opc_recover(1M)`.

## Automated Backup

ITO integrates its own backup and restore scripts with those provided by Network Node Manager (NNM), `ovbackup.ovpl`, and `ovrestore.ovpl` in order to carry out a complete automated backup of the database while the ITO GUI and server processes are running. This automated backup is designed to be run with a `cron` job or an ITO scheduled action. For more information on the NNM automated-backup scripts as well as the automated-backup scripts provided by ITO, see the sections; “The ovbackup.ovpl Command” and “The ovrestore.ovpl Command” on page 465.

If you are considering using the automated method to backup your data, you should take into consideration the following advantages and disadvantages:

- there is no need to exit the ITO GUI, although OVW actions are not possible for a short time, for example; starting applications in the `Application Desktop` window.
- ITO server processes, ITO Operator Web GUI, trouble ticket and notification services remain fully operational.
- a partial recovery of the Oracle database is possible, for example:
  - up to a given time
  - individual damaged tablespaces
- Oracle's archive-log mode must be enabled, which means:
  - reduced overall performance
  - more disk space required
- no binaries are backed up

Temporary files such as queue files are excluded from the backup. When the backup starts, the ITO GUI pops up a notification window and some OVW maps remain blocked for the duration of the backup. Any task that cannot be completed before the backup starts remains idle until the backup is finished and then resumes and completes.

Note that the backup does not include Oracle's online, redo, log files, which cannot be backed up while the database is running. However, Oracle does allow you to mirror these files on different disks so that they can be recreated in the event of problems. Refer to the Oracle documentation for more details.

The scripts provided by ITO for automated backups use Oracle's online backup method, which requires the database run in **archive-log** mode. Oracle's archive-log mode is not the default setting for the Oracle database: it has to be configured manually. Briefly, in archive-log mode, Oracle stores any changes to data files between full backups in numbered **redo log files**. The redo log files are used in the event of a crash to restore a configuration from the most recent, full backup. For more information see Oracle's product documentation. To enable archive-log mode in Oracle:

1. Close all ITO open sessions, and stop `ovw`. Enter: **`ovstop`**

2. Shutdown the database
3. Set the archive log parameters in the `init.ora` file:

   `$ORACLE_HOME/dbs/init${ORACLE_SID}.ora`

   a. Uncomment the following line to start the archive process:

      ```
      log_archive_start = true
      ```

   b. Uncomment the following line to specify the archive directory, and fill in the corresponding values for <*ORACLE_BASE*> and <*ORACLE_SID*>:

      ```
      log_archive_dest = <ORACLE_BASE>/<ORACLE_SID>/arch
      ```

**NOTE** For Oracle 8, remember to append a slash (/) to the directory path, for example: `<ORACLE_BASE>/<ORACLE_SID>/arch/`. If not, Oracle will use the wrong archive-log directory name.

   c. Uncomment the following line to define the names of the archived log files:

      ```
      log_archive_format = "T%TS%S.ARC"
      ```

4. Start-up the database and enable archive-log mode. Enter the following commands as user `oracle`:

   ```
   svrmgrl
   SVRMGR>connect internal
   SVRMGR>startup mount
   SVRMGR>alter database archivelog;
   SVRMGR>alter database open;
   SVRMGR>exit
   ```

5. After enabling archive-log mode, it is recommended you shutdown the database again and take a *full* off-line backup of the database as a foundation for later online backups.

**The opcwall Command.** The new command line utility `opcwall(1)` allows the administrator to notify any running ITO Motif GUIs of an imminent automated backup. For example, `opcwall` can be configured to inform users ten minutes before the backup is scheduled to start that, if they want to continue to work, they can use the Web GUI for the duration of the backup.

```
opcwall {-user <user_name>} <Message Text>
```

where <user_name> is the name of the operator you want to receive the message, and <message text> is the text of the message you want the operator to see. If the -user option is not specified, all operators receive the message.

**The ovbackup.ovpl Command.** The automated backup command ovbackup.ovpl pauses running processes and flushes their data to disk before backing up the NNM databases and the data of integrated applications. After the backup has completed, the NNM processes are resumed. The command accepts the following options:

```
ovbackup.ovpl [-operational] [-analytical] [-d \
<destination>]
```

If the **-d** option is *not* specified, the following default location is used; /var/opt/OV/tmp/ovbackup. If the **-d** option is specified, the following location is used; <destination>/ovbackup. The destination defined with the **-d** option must be a file system (which may be mounted) and should contain sufficient space to complete the backup. Approximately 300MB of free disk space is required to backup a fresh ITO installation: bigger environments wil require more space. The backup may then be completed by using a command such as fbackup to save the backup to an archive medium such as a tape device. For more information on the command-line options, see the man page ovbackup.ovpl(1M). Briefly, ovbackup.ovpl carries out the following high-level steps:

- Backup operational data (if the **-operational** option or no option at all is specified):

  1. Run all of the backup scripts found in the directory; $OV_CONF/ovbackup/pre_pause/ including the ITO script: ito_oracle.sh, which performs the on-line backup of the Oracle database outside the ovpause time-frame and moves the (old) archive log files to the staging area. These archive logs are *not* subsequently restored: they are only required if the backup is corrupt for some reason and an earlier backup has to be used.
  2. Call ovpause to pause all NNM processes (and block OVW API calls).
  3. Run all the backup scripts found in the directory; $OV_CONF/ovbackup/checkpoint/operational/ including the ITO script: ito_checkpoint.sh, which reads the current time stamp of Oracle, copies to the staging area those offline redo

logs not moved by `ito_oracle.sh` and copies the ITO configuration in the file system that is not backed up by `nnm_checkpoint.ovpl`.

The NNM script `nnm_checkpoint.ovpl` backs up all operational NNM databases and also backs up the directory `$OV_CONF`, which includes some ITO configuration files, the NNM database (flat) files, and the NNM configuration files.

4. Call `ovresume` to resume operation of NNM processes.
5. Run all of the backup scripts found in the directory; `$OV_CONF/ovbackup/post_resume`

- Backup analytical data (if the **`-analytical`** option or no option at all is specified):

  Run all of the backup scripts found in the directory; `$OV_CONF/ovbackup/checkpoint/analytical` including `nnm_checkpoint.ovpl` and backs up the NNM analytical repository if the embedded database is used.

**NOTE** `ovbackup.ovpl` stores progress information in the file: `/var/opt/OV/tmp/ovbackup.log`.

**The ovrestore.ovpl Command.** The `ovrestore.ovpl` command restores a backup or parts of a backup created with `ovbackup.ovpl` and accepts the following command-line options:

```
ovrestore.ovpl [-operational] [-analytical] [-d \
<destination>]
```

If you still have the backup on disk, you can use the **`-d`** option to specify the directory where the backup image resides. Otherwise, you will need to restore the image to disk from the archive medium first before running the `ovrestore.ovpl` command with the **`-d`** option. For more information on the command-line options, see the man page `ovrestore.ovpl(1M)`. Briefly, `ovrestore.ovpl` carries out the following high-level steps:

1. Check that no OpenView or integrated processes are running
2. Restore operational data (if the **`-operational`** option or no option at all is specified):

Run all of the restore scripts found in the directory; `$OV_CONF/ovbackup/restore/operational/` including `ito_restore.sh` and `nnm_restore.ovpl`. The `ito_restore.sh` script restores the Oracle database asking you to choose between the following restore options:

a. to the state of the last backup?

b. to the most recent state? - a rollforward is done based on the off-line redo logs from the backup and the off-line redo logs on the system.

3. Restore analytical data (if the **`-analytical`** option or no option at all is specified):

   Run all of the restore scripts found in the directory; `$OV_CONF/ovbackup/restore/analytical/` including `nnm_restore.ovpl`.

**NOTE** `ovrestore.ovpl` stores progress information in the same file as `ovbackup.ovpl`, namely: `/var/opt/OV/tmp/ovbackup.log`

The `ito_restore.sh` script which is integrated in the `ovrestore.ovpl` script allows you to restore the complete Oracle database either to the state of the backup or to the most recent state (a rollforward is done based on the off-line, redo logs). However, using Oracle's archive-log mode offers more possibilities. For example:

- you can retrieve single, corrupt data files from the backup and recover them with off-line redo logs.
- with a backup and off-line redo logs, you can recover data up to a specified point in time.

## Recovery Scenarios after an Automated Backup

The automated backup scripts backup only configuration data and dynamic data. Consequently, if binaries or static configuration files are lost, they have to be recovered (before the restore) in one of the following ways:

- Re-install ITO. If SD (Software Distributor) thinks ITO is already installed, you may need to use the option **`Reinstall Fileset`** even if the same revision already exists.

- Use a full offline backup that was taken with `opc_backup` with the **`full`** option
- Restore a full offline backup of the complete system

To restore the database to its state at the time of the last backup requires only data contained in the backup. This means, that the restore will work even if you have to re-install ITO. However, the restore is incomplete from an Oracle point of view, since it is not done to the *latest* state. In addition, Oracle log numbers are reset in the control files and in the online redo logs. The control files are restored from a backup control file, and missing online redo log files are re-created by the Oracle recover process.

Recovering the database to the latest state is a little more complicated. This scenario uses not only the data contained in the backup but also data on the system itself (online redo logs and archive logs since the last backup). In addition, this method may introduce inconsistencies between the configuration files (restored to the state of the backup) and the data in the database (restored to the latest possible state). Consequently, the recovery scenario will work only if the following restrictions apply:

- All control files must exist. Normally, control files are mirrored. If one of the control file still exists, it can be copied from one location to the other. However, this should be done by an Oracle DBA. The scripts will only restore to the latest state if all control files exist.
- All online redo log files must exist. Online redo log files can be mirrored. If one of the online redo log files in a log group still exists, it can be copied to the other locations. This should be done by an Oracle DBA. The scripts will only restore to the latest state if all redo log files exist.
- The Oracle log number has not been reset since the backup
- All archived redo logs made since the backup still exist
- No ITO users have been modified since the backup (this modifies files in the file system)
- No ECS templates have been added since the backup

**NOTE**

The ITO queue files are neither backed up with the automated backup scripts nor deleted during the restore. In addition, the messages in the queue files at the time of the backup are *not* in the database and are

processed only when the ITO processes are next restarted. If corrupt queue files prevent the server processes from being started, remove the queue files.

1. Stop all ITO server processes:

   ```
   /opt/OV/bin/ovstop
   ```

2. Remove a selected or all temporary files:

   ```
   rm -f /var/opt/OV/share/tmp/OpC/mgmt_sv/*
   ```

3. Restart the ITO server processes:

   ```
   /opt/OV/bin/ovstart
   ```

## Maintaining the Database

To ensure that the ITO database runs efficiently, you should perform the following tasks periodically:

- Download history messages and audit information using the `Database Maintenance` window.

  To restore previously backed-up history messages or audit information, see the `opchistupl(1m)` or `opcaudupl(1m)` man pages in the *HP OpenView IT/Operations Man Pages*.

- Backup the ITO configuration regularly. See the previous sections for more informations on what backup possibilities are available in ITO.

- Re-organize the database using `opcdbreorg`. This tool frees empty pages and re-organizes the B-trees. For more details, see the `opcdbreorg(1m)` man page.

- If a very large number of messages have been produced—perhaps by an inappropriately configured template—operators may find that their `Message Browser` takes a long time to open. In this case, as user root use the command-line utilities `opcack` or `opcackmsg` to acknowledge these messages and move them to the history database. For more details, see the `opcack(1m)` and `opcackmsg(1m)` man pages.

- The ITO database files automatically consume the extra disk space required to cope with any growth. If a disk runs out of space, you can use other disks to add additional files for a tablespace. See the Oracle information for more information.
- Every time a user runs the command; **`connect internal`**, Oracle adds an audit file to the directory; *$ORACLE_HOME*`/rdbms/audit`. Since the monitor template, `mondbfile`, runs the **`connect internal`** command every ten minutes or so, it is advisable to review the files in this directory regularly and remove them if necessary.

## Upgrading the Oracle Database Version

ITO A.04.00 supported Oracle 7.2.3, 7.3.3, and 7.3.4 (after recertification) on HP-UX 10.x, and Oracle 7.3.4 on HP-UX 11.0. ITO A.05.00 supports Oracle 7.3.4 and 8.0.5 on HP-UX 10.20 and Oracle 8.0.5 on HP-UX 11.0. Binaries for a given version of Oracle on HP-UX 10.20 are *not* the same as the binaries for the same Oracle version on HP-UX 11.0 - they are different releases. Consequently, if you upgrade the operating system from HP-UX 10.20 to HP-UX 11.0, you will have to upgrade the database, too.

**NOTE**

If you are using the HP-UX 10.20 operating system, we recommend you upgrade to Oracle 7.3.4. Since this version of the Oracle database is supported by both ITO 4.x and ITO A.05.00, you can verify that the database upgrade worked using the current ITO installation. This makes the subsequent ITO easier.

If you are using the *same* version of Oracle (7.3.4) for ITO 04.0x and A.05.00, you can maintain the old database. If you are going to upgrade the database version, you should download the configuration data with `opccfdwn(1m)`. You can choose to download messages, too. This configuration data can be uploaded to the new database using `opccfgupld(1m)` *after* you have installed the new ITO software.

Upgrade the Oracle database as described in the documentation supplied with the database. If you changed the setting of the *ORACLE_HOME* variable when upgrading the database, you will have to manually change the setting of *ORACLE_HOME* in the following files, which are created, modified, or used by ITO:

- `/etc/oratab`
- `/etc/profile`

- /etc/csh.login
- /etc/rc.config.d/ovoracle
- /etc/opt/OV/share/conf/ovdbconf

  You will need to change the database release entry and check the .profile and .cshrc files of the users that require access to the database, for example; oracle, root, and opc_op.

- /etc/tnsnames.ora (if SQL*Net is used)
- /etc/listener.ora (if SQL*Net is used)
- /etc/sqlnet.ora (if SQL*Net is used)

**NOTE**

Upgrading the Oracle database version (7.3.4 to 8.0.5) within ITO A.05.00:

- *ORACLE_HOME* may be set in the files listed above: but it is not a requirement.
- ITO creates a symbolic link libopcora.sl which points to the current Oracle installation. Change this link to point to the new (upgrade) installation. Enter:

  ```
  rm -f /opt/OV/libcl/libopcora.sl
  ln -s $ORACLE_HOME/lib/libclntsh.sl \
  /opt/OV/lib/libopcora.sl
  ```

## Database Configuration Tips

Although using Oracle's archivelog mode helps to reduce the loss of data after a backup and restore, Oracle offers additional ways to avoid data loss in the unlikely event that a disk fails. If you have access to more than one disk, it is recommended that you take a look at the following configuration tips and use the information to help you implement such a scenario in your own ITO environment:

- Move one or more Oracle control files to the second disk:

  1. Create the directories on the second disk:

     ```
     mkdir -p /u02/oradata/openview
     chown oracle:dba /u02/oradata/openview
     ```

2. Shutdown the database
3. Move selected control file(s) to a directory on the other disk, for example from disk /u01 to disk /u02:

   ```
   mv /u01/oradata/openview/control03.ctl \
   /u02/oradata/openview/control03.ctl
   ```

4. Modify the control file name(s) in: `$ORACLE_HOME/dbs/init${ORACLE_SID}.ora`, for example, from:

   ```
   control_files = (/u01/oradata/openview/control01.ctl,
                    /u01/oradata/openview/control02.ctl,
                    /u01/oradata/openview/control03.ctl)
   ```

   to the following:

   ```
   control_files = (/u01/oradata/openview/control01.ctl,
                    /u01/oradata/openview/control02.ctl,
                    /u02/oradata/openview/control03.ctl)
   ```

5. Restart the database

- Create a second (or even third) set of mirrored, online redo logs on the second (or third) disk. ITO installs Oracle in such a way that, by default, it has three redo log groups, each containing one member. The following example creates a second set of redo log files in the directory; `/u02/oradata/openview`. Modify the directory names (and repeat the steps) as required:

  1. Create the directories on the second disk, for example;

     ```
     mkdir -p /u02/oradata/openview
     ```

     ```
     chown oracle:dba /u02/oradata/openview
     ```

  2. Do the following as user `oracle` in `svrmgrl`:

     ```
     connect internal;
     ```

     ```
     alter database add logfile member
     '/u02/oradata/openview/redo01.log' to group 1;
     ```

     ```
     alter database add logfile member
     '/u02/oradata/openview/redo02.log' to group 2;
     ```

     ```
     alter database add logfile member
     '/u02/oradata/openview/redo03.log' to group 3;
     ```

```
exit
```

## Maintaining the HP OpenView Platform

- Erase the trap daemon logfile `/var/opt/OV/log/trapd.log` if you no longer need the entries. A large `trapd.log` can reduce the performance of ITO. A backup file `/var/opt/OV/log/trapd.log.old` is provided.

  For detailed information about system maintenance in HP OpenView, see the *HP OpenView Network Node Manager Administrator's Reference*.

## Maintaining ITO Directories and Files

- Do not clean up the mgmt_sv directory `/var/opt/OV/share/tmp/OpC/mgmt_sv` because it contains important runtime data. You can cleanup this directory if you are unable to use another solution or there are too many unprocessed and old messages.
- If you no longer need the logfiles, you should backup and then erase the continuously growing ITO software installation/update/de-installation logfile `/var/opt/OV/log/OpC/mgmt_sv/install.log`. The logfile `inst_err.log` and `inst_sum.log` do not continuously grow because they are generated for each ITO software (de-)installation and/or update.
- You should backup and then erase the ITO error/warning logfile `/var/opt/OV/log/OpC/mgmt_sv/opcerror` and its backups. ITO uses an automatic backup logfile mechanism having up to four files. If the `opcerror` logfile size is greater than 1 MB, ITO automatically performs the following:
  - if existent: move `opcerro2` to `opcerro3`
  - if existent: move `opcerro1` to `opcerro2`
  - move opcerror to `opcerro1`

## On ITO Managed Nodes

You should periodically backup, and then erase, local ITO logfiles (and their backups). ITO uses 90% of the specified log directory size for local message logging and 10% for error/warning logging. ITO also uses an automatic backup mechanism for the logfiles (four on UNIX systems, nine on MPE/iX). For example, the configured size of a UNIX log directory is 10 MB and is allocated in the following way:

- ❏ 9 MB for local message logging.

  Since there are four logfiles, if the `opcmsglg` file size is greater than 9/4 MB, ITO performs the following tasks:

  - if it exists, move `opcmsgl2` to `opcmsgl3`
  - if it exists, move `opcmsgl1` to `opcmsgl2`
  - move `opcmsglg` to `opcmsgl1`

- ❏ 1 MB for local error/warning message logging.

  Since there are four logfiles, if the `opcerror` file size is greater than 1/4 MB, ITO performs the following tasks:

  - if it exists, move `opcerro2` to `opcerro3`
  - if it exists, move `opcerro1` to `opcerro2`
  - move `opcerror` to `opcerro1`

Unless there is *no* alternative, or if there are too many unprocessed and old messages, *do not* clean up the directories listed in Table 10-12 on page 474: these directories contain important runtime data:

**Table 10-12 Managed Node Directories Containing Runtime Data**

| Operating System on the Managed Node | Directories Containing Runtime Data |
|---|---|
| AIX | /var/lpp/OV/tmp/OpC<br>/var/lpp/OV/tmp/OpC/bin<br>/var/lpp/OV/tmp/OpC/conf |
| DEC Alpha NT | \usr\OV\tmp\OpC\<node><br>\usr\OV\tmp\OpC\bin\alpha<br>\usr\OV\tmp\OpC\conf\<node> |
| HP-UX 10.x / 11.x, Digital UNIX, DYNIX/ptx, IRIX, NCR UNIX SVR4, Olivetti UNIX, Pyramid DataCenter/OSx, OS/2, SCO OpenServer, SCO UnixWare, SINIX/Reliant, Solaris, | /var/opt/OV/tmp/OpC<br>/var/opt/OV/tmp/OpC/bin<br>/var/opt/OV/tmp/OpC/conf |
| MPE/iX | TMP.OVOPC TMPACT.OVOPC TMPCMDS.OVOPC<br>TMPCONF.OVOPC TMPMON.OVOPC Z.OVOPC |
| Novell NetWare | SYS:/var/opt/OV/tmp/OpC<br>SYS:/var/opt/OV/tmp/OpC/bin<br>SYS:/var/opt/OV/tmp/OpC/conf |
| Windows NT | \usr\OV\tmp\OpC\<node><br>\usr\OV\tmp\OpC\bin\intel<br>\usr\OV\tmp\OpC\conf\<node> |

## HP-UX 10.x, and 11.x, and Window NT Managed Nodes

The following table describes where local logfiles reside on managed nodes running; HP-UX 10.x, and 11.x and Windows NT.

**Table 10-13 Local Logfiles on HP-UX 10.x, 11.x, and Windows NT Managed Nodes**

| Logfile | Windows NT | HP-UX 10.x and 11.x |
|---|---|---|
| Default Logfile path | `/usr/OV/log/OpC/<node>` | `/var/opt/OV/log/OpC` |
| ITO errors/warnings | `opcerror opcerro(1-3)` | `opcerror opcerro(1-3)` |
| ITO messages | `opcmsglg opcmsgl(1-3)` | `opcmsglg opcmsgl(1-3)` |

## AIX and MPE/iX Managed Nodes

The following table describes where local logfiles reside on managed nodes running AIX and MPE/iX.

**Table 10-14 Local Logfiles on AIX and MPE/iX Managed Nodes**

| Logfile | AIX | MPE/iX |
|---|---|---|
| Default Logfile path | `/var/lpp/OV/log/OpC` | `LOG.OVOPC` |
| ITO errors/warnings | `opcerror, opcerro(1-3)` | `OPCERROR OPCERRO(1-8)` |
| ITO messages | `opcmsglg, opcmsgl(1-3)` | `OPCMSGLG OPCMSGL(1-8)` |

Avoid local logging on MPE/iX managed nodes as far as possible, as this can slow down your system. This is because of the way in which seeks are implemented in large MPE/iX files.

Also, check the size of the file OPCMSGLG.LOG.OVOPC regularly and, after you have done a backup, purge the file. To limit the size of this file you can also change the value for Max. Size in the `Node Advanced Options` window.

## Other Managed Nodes

The following table describes where local logfiles reside for managed nodes running: Digital UNIX, DYNIX/ptx, NCR UNIX SVR4, Olivetti UNIX, Pyramid DataCenter/OSx, OS/2, SCO OpenServer, SCO UnixWare, SGI IRIX, SINIX.

**Table 10-15 Local Logfiles on Other Managed Nodes**

| Logfile | Digital UNIX, DYNIX/ptx, NCR UNIX SVR4, Olivetti UNIX, Pyramid DataCenter/OSx, OS/2, SCO OpenServer, SCO UnixWare, SGI IRIX, SINIX/Reliant, and Solaris |
|---|---|
| Default Logfile path | `/var/opt/OV/log/OpC` |
| ITO errors/warnings | `opcerror`, `opcerro(1-3)` |
| ITO messages | `opcmsglg`, `opcmsg (1-3)` |

# License Maintenance

ITO uses the OVKey license mechanism for the installation and maintenance of the product licenses. The OVKey license technology is based on node-locked licenses with license passwords in a license file - not on a central license server. One clear and significant advantage of this approach is that it is *not* necessary to set up a license server which handles the licenses. In addition, the product may be used even behind firewalls and in Service Guard environments. ITO provides a command -line tool, `opclic`, to maintain the licenses. For more information on the command-line interface, `opclic`,, see “ITO License Maintenance Tools” on page 478.

After installation, the ITO administrator replaces the **Instant-On** licence with the correct license. The licence maintenance tool `opclic` ensures that the license file does not contain more than one server license.

## License Types

License types relate very strictly to the ITO product structure. Each sub-product or licensable feature has its own license type and product number. However, not all licenses will be required for ITO to run. In some cases a message in the `Message Browser` window informs the customer when no license is available, or a license has expired. For more detailed information on the types of licenses available in ITO, see Table 10-16 on page 478.

**Table 10-16 License Types for ITO A.05.00**

| License Type | | Description |
|---|---|---|
| Management Stations | ITO Management Server | ITO license with 2 users |
| | Development Kit | Limited management server license with 5 Nodes and 1 User. NNM can manage a maximum of 25 objects with this license. |
| | Instant-On [a] | Same as the ITO management server license. Runtime = 120 days |
| | Emergency [a] | Same as the ITO management server license. Runtime = 14 days |
| | Evaluation | Evaluation license with full functionality. Runtime = 120 days |
| Management Server Upgrades | ITO Management Server upgrade for NNM | Full ITO management server license. |
| Extensions | ITO Managed Nodes | Managed node licenses |
| | ECS Designer | Not handled by ITO |
| | ANSE Security Extension | Enables secure communication |

a. Not installed with `opclic`: generated at runtime by the management server

## ITO License Maintenance Tools

ITO provides a command-line interface for the maintenance of licenses. The principal tool, `opclic` provides functions to:

- list the installed licenses
- add and delete licenses
- check for inconsistencies

- check whether the user has enough licenses for his environment

The `opclic` command accepts the following parameters and usage:

```
opclic          { -add <license_pwd> [-force] } |
                { -list } |
                { -delete } |
                { -report } |
                { -help }
```

For more information on what the various `opclic` parameters do, see Table 10-17 on page 479.

**Table 10-17 Command-line Options for `opclic`**

| Command -line Option | Description | Notes |
|---|---|---|
| add | adds new license passwords | • `opclic` does not allow more than one server license password in the license file.<br>• Passwords added using unsupported methods are invalid: ITO will not start, and the invalid password(s) must be removed with `opclic` (see also **`list`**).<br>• Use the optional **`force`** parameter to replace licenses. Note that the server-license password is *not* overwritten if the **`force`** parameter is not set: a warning message is written to `stdout` instead. |
| list | lists the installed ITO licenses | `opclic` supports <*license_types*>. For more information on what types of licence are available in ITO, see Table 10-16 on page 478. |

| Command -line Option | Description | Notes |
|---|---|---|
| delete | delete a specified license password <*license_pwd*> | • An ITO management server license may *not* be removed with the **`delete`** option: it can only be removed or replaced with:<br>**`-add <license_pwd> -force`** |
| report | list details of the installed licenses | • ITO management server license type: start/end time<br>• ITO managed node licenses [#total #used #free <Tier>]<br>• ITO user licenses [#total]<br>• warnings for duplicate or invalid license passwords |
| help | lists `opclic` usage information, including: | • all command-line parameters |

# A ITO Managed Node APIs and Libraries

This chapter provides information about:

- ITO APIs on Managed Nodes
- ITO APIs for Novell NetWare Managed Nodes
- ITO Managed Node Libraries
- Include Files on all Managed Nodes
- Managed Node Makefiles

# ITO APIs on Managed Nodes

**Table A-1 ITO APIs on Managed Nodes**

| API | Command | Description |
|---|---|---|
| n/a | `opcmack(1)` | Acknowledges an ITO message received from the message agent on the managed node and sent to the appropriate management server. |
| `opcmon(3)` | `opcmon(1)` | Feed the current value of a monitored object into the ITO monitoring agent on the local managed node. |
| `opcmsg(3)` | `opcmsg(1)` | Submit a message to the ITO message interceptor on the local managed node. |

See the appropriate man pages for detailed information about these commands.

**NOTE** The ITO commands `opcmon(1)`, `opcmack(1)`, and `opcmsg(1)` are not supported for Novell NetWare managed nodes.

An example of how the API functions are used is available in the file `opcapitest.c` on the management server in the directory `/opt/OV/OpC/examples/progs/`. See “Managed Node Makefiles” on page 497 for a list of the corresponding makefiles.

# ITO APIs for Novell NetWare Managed Nodes

A set of ITO agent APIs is provided for Novell NetWare agents. These APIs provide inter-process communication between ITO agents and the custom NLMs; in particular, the parent/child relationship. See Table A-2 on page 484 for more information about these APIs.

**Table A-2 ITO APIs on Novell NetWare Managed Nodes**

| Command | Description |
|---|---|
| `OVnlm_init()` | Must be the first function called in the main() function of an ITO-enabled NetWare Loadable Module (NLM). This function initializes the ITO related variables and returns a handle which must be used in all subsequent calls in this NLM. |
| `OVnlm_exit()` | Must be used to terminate the execution of ITO-enabled NLM instead of the usual exit() function. `OVnlm_exit()` is required to inform the parent ITO Agent NLM that the custom NLM has finished and to provide exit code to the parent. |

## Writing ITO-enabled NetWare Loadable Modules

An example of an action, HELLO.NLM, is given below. This action is executed by the ITO action agent and the output is captured as an ITO 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 );
}
```

An additional example is provided in the following file on the management server:

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

# ITO Managed Node Libraries

**NOTE**

Customer applications must be linked to ITO using the libraries and link and compile options given in Table A-3 on page 486. Integration is only supported if this is the case.

ITO C functions are available in a shared library. The related definitions and return values are defined in the ITO include file, `opcapi.h`. See Chapter 3, “File Tree Layouts on the Managed-Node Platforms,” on page 115 for the location of this include file on all supported platforms.

**Table A-3 Libraries for the ITO Managed Nodes**

| | | ITO Version | ITO A.03.xx | ITO A.04.xx | ITO A.05.00 |
|---|---|---|---|---|---|
| HP-UX 11.0 | DCE | **Library** | n/a | **`libopc_r.sl`** | **`libopc_r.sl`** |
| | | **Libraries linked to the ITO library.** | n/a | `/usr/lib/libdce.1`<br>`/usr/lib/libc.1` | `/usr/lib/libdcekt.1`<br>`/usr/lib/libpthread.1`<br>`/usr/lib/libnsl.1`<br>`/usr/lib/libc.1` |
| | | **Link and compile options** | n/a | `-lopc_r -ldce -lc_r` | `-lopc_r` |
| | | Description | n/a | The ITO A.04.xx HP-UX 11.x agent is a re-certified HP-UX 10.x agent and does not make use of any HP-UX 11.x specific features, for example Kernel Threads. | The HP-UX 11.x agent is a native 11.x agent and uses Kernel Threads which cannot be intermixed with Posix/DCE Threads.<br>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 ITO version A.04.02 software *must* be re-compiled on HP-UX 11.0 before the can be integrated with ITO version A.05.00. |

| | | ITO Version | ITO A.03.xx | ITO A.04.xx | ITO A.05.00 |
|---|---|---|---|---|---|
| HP-UX 10.01, 10.10, 10.20 | DCE | **Library** | **libopc_r.sl** | **libopc_r.sl** (libopc.sl –> libopc_r.sl) | **libopc_r.sl** (libopc.sl –> libopc_r.sl) |
| | | **Libraries linked to the ITO library.** | /usr/lib/libdce.1<br>/usr/lib/libc.1 | /usr/lib/libdce.1<br>/usr/lib/libc.1 | /usr/lib/libdce.1<br>/usr/lib/libc.1 |
| | | **Link and compile options** | -lopc_r -ldce -lc_r | -lopc_r (-ldce -lc_r) | -lopc_r |
| | | **Description** | libopc_r.sl is the reentrant version of the agent library for the use of DCE. It is not exchangeable with the NCS version. | The compatibility link from libopc.sl to libopc_r.sl was introduced with patch PHSS_15265 to match the documentation.<br>Linking libdce.sl and libc_r.sl was recommended but not necessary. | Last version with the compatibility link.<br>Linking of libdce.sl and libc_r.sl is not recommended. |
| HP-UX 10.01, 10.10, 10.20 | NCS | **Library** | **libopc78.sl** | n/a | n/a |
| | | **Libraries linked to the ITO library.** | /usr/lib/libnck.1 | n/a | n/a |
| | | **Link and compile options** | -lopc78 (-lnck) | n/a | n/a |
| | | **Description** | libopc78.sl is the reentrant version of the agent library for the use of NCS. It is not exchangeable with the DCE version. | n/a | n/a |

| | | ITO Version | ITO A.03.xx | ITO A.04.xx | ITO A.05.00 |
|---|---|---|---|---|---|
| HP-UX 9.00, 9.01, 9.03, 9.04, 9.05, 9.07 | DCE | **Library** | **libopc78_r.sl** | **libopc_r.sl**<br>(libopc78_r.sl –> libopc_r.sl) | n/a |
| | | **Libraries linked to the ITO library.** | /usr/lib/libdce.1<br>/usr/lib/libc_r.1 | /usr/lib/libdce.1<br>/usr/lib/libc_r.1 | n/a |
| | | **Link and compile options** | -D_REENTRANT<br>-lopc78_r -ldce -lc_r | -D_REENTRANT<br>-lopc_r -ldce -lc_r | n/a |
| | | **Description** | This library is not exchangeable with the NCS version. | Between ITO A.03.xx and ITO A.04.xx the name of this library was changed. On some systems a compatibility link is necessary.<br>This library is not exchangeable with the NCS version. | n/a |
| HP-UX 9.00, 9.01, 9.03, 9.04, 9.05, 9.07 | NCS | **Library** | **libopc78.sl** | **libopc78.sl** | n/a |
| | | **Libraries linked to the ITO library.** | /usr/lib/libnck.a<br>/lib/lib/lib.l | /usr/lib/libnck.a<br>/lib/lib/lib.l | n/a |
| | | **Link and compile options** | -lopc78 | -lopc78 | n/a |
| | | **Description** | This library is not exchangeable with the DCE version. | This library is not exchangeable with the DCE version. | n/a |
| MPE 5.0, 5.5, 6.0 | NCS | **Library** | **libapixl.lib.ovopc** | **libapixl.lib.ovopc** | **libapixl.lib.ovopc** |
| | | **Libraries linked to the ITO library.** | n/a | n/a | n/a |
| | | **Link and compile options** | info="Ih"<br>link cap=pm,ia,ba,mr,ds;&<br>rl=libcinit.lib.sys;&<br>xl=opcapixl.lib | info="Ih"<br>link cap=pm,ia,ba,mr,ds;&<br>rl=libcinit.lib.sys;&<br>xl=opcapixl.lib | info="Ih"<br>link cap=pm,ia,ba,mr,ds;&<br>rl=libcinit.lib.sys;&<br>xl=opcapixl.lib |
| | | **Description** | n/a | n/a | n/a |

| | | ITO Version | ITO A.03.xx | ITO A.04.xx | ITO A.05.00 |
|---|---|---|---|---|---|
| Sun Solaris 2.5, 2.5.1, 2.6, 7 | NCS | **Library** | **libopc.so** | **libopc.so** | **libopc.so** |
| | | **Libraries linked to the ITO library.** | | libov.a and libovutil.a are statically linked into libopc.so<br>/usr/lib/libw.so<br>/usr/lib/libnck.a<br>/usr/lib/libsocket.so<br>/usr/lib/libnsl.so<br>/usr/lib/libgcc.a | libov.a and libovutil.a are statically linked into libopc.so<br>/usr/lib/libw.so<br>/usr/lib/libnck.a<br>/usr/lib/libgcc.a<br>/usr/lib/libsocket.so<br>/usr/lib/libnsl.so |
| | | **Link and compile options** | -lopc | -lopc -lnsp -lov -lovutil (-lsocket -lnsl) | -lopc -nsp (-lsocket -lnsl) |
| | | **Description** | n/a | n/a | n/a |
| SunOS 4.1.3, 4.1.4 | NCS | **Library** | **libopcapi.a** | **libopcapi.a** | n/a |
| | | **Libraries linked to the ITO library.** | | | n/a |
| | | **Link and compile options** | -lopcapi (-lxpg -lc) | -lopcapi -lxpg -lc | n/a |
| | | **Description** | The example Makefile is incomplete. | n/a | n/a |

| | | ITO Version | ITO A.03.xx | ITO A.04.xx | ITO A.05.00 |
|---|---|---|---|---|---|
| AIX 3.2, 4.1, 4.2, 4.3 | DCE | **Library** | **libopc_r.o** | **libopc_r.a** (AIX 4.x)<br>**libopc_r.o** (AIX 3.2) | **libopc_r.a** |
| | | **Libraries linked to the ITO library.** | | AIX 3.2:<br>/usr/lib/libdce.a<br>/usr/lib/libpthreads.a<br>/usr/lib/libc_r.a<br>/usr/lib/libiconv.a<br>AIX 4.x:<br>/usr/lpp/OV/lib/libnsp.a<br>/usr/lib/libdce.a<br>/usr/lib/libiconv.a | /usr/lpp/OV/lib/libnsp.a<br>/usr/lib/libdce.a<br>/usr/lib/libiconv.a |
| | | **Link and compile options** | -D_THREAD_SAVE<br>-D_CMA_NOWRAPPERS_<br>-lopc_r -lpthreads -lc_r | -D_THREAD_SAVE (3.2)<br>-D_CMA_NOWRAPPERS_<br>-lopc_r -lpthreads -lc_r | -D_CMA_NOWRAPPERS_<br>-lopc_r -lpthreads -lc_r |
| | | **Description** | | | Version 3.2 is obsolete with ITO A.05.00.<br>**Note:**<br>Only ITO A.04.xx integrations built on AIX 4.x with above options can be run on ITO A.05.00 |
| AIX 3.2, 4.1, 4.2, 4.3 | NCS | **Library** | **libopc.o** | **libopc.o** | n/a |
| | | **Libraries linked to the ITO library.** | | /usr/lib/libnck.a<br>/usr/lib/libiconv.a | n/a |
| | | **Link and compile options** | -lopc | -D_THREAD_SAVE (AIX 3.2)<br>-D_CMA_NOWRAPPERS_<br>-lopc -lpthreads -lc_r | n/a |
| | | **Description** | AIX 3.2 only | | n/a |

| | | ITO Version | ITO A.03.xx | ITO A.04.xx | ITO A.05.00 |
|---|---|---|---|---|---|
| NCR UNIX SVR4 R.03.00, R.03.01, R.03.02 | NCS | **Library** | **libopc.so** | **libopc.so** | **libopc.so** |
| | | **Libraries linked to the ITO library.** | /usr/lib/libnck.a<br>/usr/lib/libsocket.so<br>/usr/lib/libnsl.a | /usr/lib/libnck.a<br>/usr/lib/libsocket.so<br>/usr/lib/libnsl.a | /usr/lib/libnck.a<br>/usr/lib/libsocket.so<br>/usr/lib/libnsl.a |
| | | **Link and compile options** | -lopc -lsocket -lnsl<br>-lc -lucb | -lopc -lsocket -lnsl<br>-lc -lucb -lnsp | -lopc -lsocket -lnsl<br>-lc -lucb -lnsp |
| | | **Description** | n/a | n/a | n/a |
| SGI IRIX 5.3, 6.2, 6.4, 6.5 | NCS | **Library** | **libopc.so** | **libopc.so** | **libopc.so** |
| | | **Libraries linked to the ITO library.** | /usr/lib/libnck.a<br>/usr/lib/libc.so | /opt/OV/lib/libnsp.so<br>/usr/lib/libnck.a<br>/usr/lib/libnsl.so<br>/usr/lib/libc.so | /opt/OV/lib/libnsp.so<br>/usr/lib/libnck.a<br>/usr/lib/libnsl.so<br>/usr/lib/libc.so |
| | | **Link and compile options** | -lopc -lsocket -lnsl | -lopc -lsocket -lnsl | -lopc -lsocket -lnsl |
| | | **Description** | n/a | n/a | n/a |
| Sequent DYNIX/ptx 4.0, 4.1.2, 4.1.3, 4.2.0, 4.4.0, 4.4.1, 4.4.2 | NCS | **Library** | **libopc.so** | **libopc.so** | **libopc.so** |
| | | **Libraries linked to the ITO library.** | /usr/lib/libncka.<br>/usr/lib/libintl.a<br>/usr/lib/libsocket.so<br>/usr/lib/librpc.so<br>/usr/lib/libnsl.so<br>/usr/lib/libinet.so<br>/usr/lib/libsec.a<br>/usr/lib/libseq.c | /usr/lib/libnck.a<br>/usr/lib/libinet.so<br>/usr/lib/libnsl.so<br>/usr/lib/librpc.so<br>/usr/lib/libsec.a<br>/usr/lib/libseq.a<br>/usr/lib/libsocket.so<br>/usr/coff/lib/libintl.a | /usr/lib/libnck.a<br>/usr/lib/libinet.so<br>/usr/lib/libnsl.so<br>/usr/lib/librpc.so<br>/usr/lib/libsec.a<br>/usr/lib/libseq.a<br>/usr/lib/libsocket.so<br>/usr/coff/lib/libintl.a |
| | | **Link and compile options** | -lopc -lnsp -lsocket | -lopc -lnsp -lsocket | -lopc -lnsp -lsocket |
| | | **Description** | No example makefile available. | n/a | n/a |

| | | ITO Version | ITO A.03.xx | ITO A.04.xx | ITO A.05.00 |
|---|---|---|---|---|---|
| Siemens Nixdorf SINIX/Reliant 5.41, 5.42, 5.43, 5.44 | DCE | **Library** | n/a | **libopc_r.so** | **libopc_r.so** |
| | | **Libraries linked to the ITO library.** | n/a | thr_cc is used which comes with its own libraries | thr_cc is used which comes with its own libraries |
| | | **Link and compile options** | n/a | -lopc_r -lnsp -ldce -lsocket_r<br>-lresolv_r -lm_r -lc | -lopc_r -lnsp -ldce -lsocket_r<br>-lresolv_r -lm_r -lc -lnsl_r_i |
| | | **Description** | n/a | Available as patch PHSS_13598. | n/a |
| Siemens Nixdorf SINIX/Reliant 5.41, 5.42, 5.43, 5.44 | NCS | **Library** | **libopc.so** | **libopc.so** | **libopc.so** |
| | | **Libraries linked to the ITO library.** | /usr/lib/libnck.a<br>/usr/lib/libsocket.so<br>/usr/lib/libnsl.so | 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 |
| | | **Description** | n/a | Available as patch PHSS_15160. | n/a |
| Pyramid DataCenter OS/x 1.1 | NCS | **Library** | n/a | **libopc.so** | **libopc.so** |
| | | **Libraries linked to the ITO library.** | n/a | | |
| | | **Link and compile options** | n/a | -lopc -lnsp -lnck -lsocket -lnsl<br>-lc -lucb | -lopc -lnsp -lnck -lsocket -lnsl<br>-lc -lucb |
| | | **Description** | n/a | n/a | n/a |

| | | ITO Version | ITO A.03.xx | ITO A.04.xx | ITO A.05.00 |
|---|---|---|---|---|---|
| SCO UnixWare 2.1 | DCE | **Library** | n/a | **libopc_r.so** | **libopc_r.so** |
| | | **Libraries linked to the ITO library.** | n/a | /usr/lib/libdce.so<br>/usr/lib/libsocket.so<br>/usr/lib/libnsl.so<br>/usr/css/lib/libgen.a | /usr/lib/libdce.so<br>/usr/lib/libsocket.so<br>/usr/lib/libnsl.so<br>/usr/css/lib/libgen.a |
| | | **Link and compile options** | n/a | -lopc_r -lnsp -lsocket -lnsl | -lopc_r -lnsp -lsocket -lnsl |
| | | **Description** | n/a | n/a | n/a |
| SCO OpenServer 3.0, 3.2vx | NCS | **Library** | **libopc.a** | **libopc.a** | **libopc.a** |
| | | **Libraries linked to the ITO library.** | no libraries linked with libopc | no libraries linked with libopc | no libraries linked with libopc |
| | | **Link and compile options** | -lopc -lsocket -lnsl_s -lx | -lopc -lsocket -lnsl_s -lx | -lopc -lsocket -lnsl_s -lx |
| | | **Description** | n/a | n/a | n/a |
| DEC Alpha Digital UNIX OSF/1 3.2, 4.0, 4.2, 5.0 | DCE | **Library** | libopc.so | **libopc_r.so** | **libopc_r.so** |
| | | **Libraries linked to the ITO library.** | /usr/lib/libnck.a<br>/usr/lib/libc.a<br>/usr/lib/libcxx.so<br>/usr/lib/libiconv.so | /usr/shlib/libiconv.so<br>/usr/shlib/libdce.so<br>/usr/shlib/libdce_r.so (optional)<br>/usr/shlib/libphtreads.so<br>/usr/shlib/libpthread.so<br>/usr/shlib/libmach.so<br>/usr/shlib/libexc.so<br>/usr/shlib/libc.so<br>/usr/shlib/libcxx.so | /usr/shlib/libiconv.so<br>/usr/shlib/libdce.so<br>/usr/shlib/libdce_r.so (optional)<br>/usr/shlib/libphtreads.so<br>/usr/shlib/libpthread.so<br>/usr/shlib/libmach.so<br>/usr/shlib/libexc.so<br>/usr/shlib/libc.so<br>/usr/shlib/libcxx.so |
| | | **Link and compile options** | n/a | -lopc_r | -lopc_r |
| | | **Description** | n/a | Available as patch PHSS_15055. | n/a |

| | | ITO Version | ITO A.03.xx | ITO A.04.xx | ITO A.05.00 |
|---|---|---|---|---|---|
| DEC Alpha Digital UNIX OSF/1 3.2, 4.0, 4.2, 5.0 | NCS | **Library** | n/a | **libopc.so** | n/a |
| | | **Libraries linked to the ITO library.** | n/a | /usr/lib/libnck.a<br>/usr/lib/libc.a<br>/usr/shlib/libiconv.so<br>/usr/shlib/libcxx.so | n/a |
| | | **Link and compile options** | n/a | -lopc | n/a |
| | | **Description** | n/a | n/a | n/a |
| DEC Alpha on Windows NT 3..51, 4.0 | DCE | **Library** | n/a | n/a | |
| | | **Libraries linked to the ITO library.** | n/a | n/a | Same as Windows. NT on Intel |
| | | **Link and compile options** | n/a | n/a | |
| | | **Description** | n/a | n/a | Use *.mak files to build. |
| Intel on Windows NT 3..51, 4.0 | DCE | **Library** | **opc.dll**<br>**opcappi.dll** | **opc.dll**<br>**opcapi.dll** | **opc.dll**<br>**opcapi.dll** |
| | | **Libraries linked to the ITO library.** | | | |
| | | **Link and compile options** | | | |
| | | **Description** | Use *.mak files to build. | Use *.mak files to build. | Use *.mak files to build. |

| | | ITO Version | ITO A.03.xx | ITO A.04.xx | ITO A.05.00 |
|---|---|---|---|---|---|
| Intel on OS/2 Warp 3.0, 4.0 | DCE | **Library** | n/a | **opcpblib.lib** | **opcpblib.lib** |
| | | **Libraries linked to the ITO library.** | n/a | DCEOS2.LIB<br>SO32DLL.LIB<br>TCP32DLL.LIB<br>DDE4MBS.LIB<br>OS2386.LIB<br>OPCNSP.LIB<br>OPCMEM.LIB | DCEOS2.LIB<br>SO32DLL.LIB<br>TCP32DLL.LIB<br>DDE4MBS.LIB<br>OS2386.LIB<br>OPCNSP.LIB<br>OPCMEM.LIB |
| | | **Link and compile options** | n/a | | |
| | | **Description** | n/a | *.LIB files reference some DLLs.<br>Available as patch PHSS_15162. | *.LIB files reference some DLLs. |
| Novell NetWare 4.1, 4.1 SFT III, 4.11, 4.11 SFT III | EZ-RPC | **Library** | n/a | **libopc.lib** | **libopc.lib** |
| | | **Libraries linked to the ITO library.** | n/a | No libraries linked. | No libraries linked. |
| | | **Link and compile options** | n/a | -DOPC_NW -DNW<br>-DCSM_ONC -bt=NETWARE | -DOPC_NW -DNW<br>-DCSM_ONC -bt=NETWARE |
| | | **Description** | n/a | libopc.lib is only used as archive library for API developers - it is not used at runtime. | libopc.lib is only used as archive library for API developers - it is not used at runtime. |
| Intel on Olivetti SVR4.2 2.4.1 | NCS | **Library** | n/a | **libopc.so** | **libopc.so** |
| | | **Libraries linked to the ITO library.** | n/a | /usr/lib/libnck.a<br>/usr/lib/socket.so<br>/usr/lib/libnsl.so | /usr/lib/libnck.a<br>/usr/lib/socket.so<br>/usr/lib/libnsl.so |
| | | **Link and compile options** | n/a | -lnsp -lsocket -lnsl -lc -lucb | -lnsp -lsocket -lnsl -lc -lucb |
| | | **Description** | n/a | | |

## Include Files on all Managed Nodes

**NOTE**

See “Libraries for ITO Integrations” on page 31 for important information about platforms that support both the NCS and the DCE ITO agent.

Table A-4 on page 496 gives the location of the ITO include files on all managed node platforms.

**Table A-4 ITO Include Files**

| Platform | OS | Include File |
|---|---|---|
| HP 9000/700<br>HP 9000/800 | HP-UX 10.x and 11.x | /opt/OV/include/opcapi.h |
| Sun SPARCstation | Solaris | /opt/OV/include/opcapi.h |
| IBM RS/6000 Bull DPX/20 | AIX | /usr/lpp/OV/include/opcapi.h |
| NCR 3xxx/4xxx (Intel 486 or higher) | UNIX SVR4 | /opt/OV/include/opcapi.h |
| Intel 486 or higher | SCO OpenServer | /opt/OV/include/opcapi.h |
| Intel 486 or higher | SCO UnixWare | /opt/OV/include/opcapi.h |
| Silicon Graphics Indigo | IRIX | /opt/OV/include/opcapi.h |
| DEC Alpha AXP | Digital UNIX | /usr/opt/OV/include/opcapi.h |
| Intel 486 or higher | DYNIX/ptx | /opt/OV/include/opcapi.h |
| Olivetti (INTEL PCs) | Olivetti UNIX SVR4 | /opt/OV/include/opcapi.h |
| Pyramid mips_r3000 | DataCenter/OSx SVR4 | /opt/OV/include/opcapi.h |
| HP 3000/900 | MPE/iX | OPCAPI.H.OVOPC |
| Intel 486 or higher | NT | \usr\OV\include\opcapi.h |

| Platform | OS | Include File |
|---|---|---|
| Intel 486 or higher | Novell NetWare | SYS:.opt/OV/include/opcapi.h,opcnwapi.h |
| DEC Alpha | NT | \usr\OV\include\opcapi.h |
| Intel 486 or higher | OS/2 | \opt\OV\include\opcapi.h |

An example of how the API functions are used is available in the file `opcapitest.c` on the management server in the directory `/opt/OV/OpC/examples/progs/`

## Managed Node Makefiles

The directory `/opt/OV/OpC/examples/progs` on the management server also contains the makefiles for building the examples. They use the correct compile and link options needed to get a correctly built executable.

- Makef.aix
- Makef.dec
- Makef.hpux10
- Makef.hpux11
- Makef.irix
- Makef.mpe-ix
- Makef.ncr
- Makef.nw
- Makef.oli
- Makef.os2
- Makef.ptx
- Makef.pyr
- Makef.sco
- Makef.sinix
- Makef.sinix-dce

- Makef.solaris
- Makef.uxw

For Windows NT use the Microsoft Developer Studio 4.2 or higher. See also `/opt/OV/OpC/examples/progs/README`

#### Management Server Makefile

The following makefile is available in the directory `/opt/OV/OpC/examples/progs` on the management server.

- Makef.hpsv (makefile for the management server on HP-UX)

# B Administration of MC/ServiceGuard

# Overview of HP MC/ServiceGuard

This appendix provides background information for system administrators working with ITO in HP MC/ServiceGuard clusters. It assumes that you are familiar both with MC/ServiceGuard and the general concepts of ITO. For more detailed information about MC/ServiceGuard, see the *Managing MC/ServiceGuard* manual. To install and configure ITO in an MC/ServiceGuard cluster, see Appendix B in the *HP OpenView IT/Operations Installation Guide for the Management Server*.

# Introducing MC/ServiceGuard

**Multi-Computer/ServiceGuard** is a powerful hardware and software solution that can switch control from one ITO management server to another if a management server fails. Critical information is stored on shared disks that are also mirrored. Uninterruptible power supplies (UPS) are also included to guarantee continuous operation if a power failure occurs.

A highly-available computer system is one that provides access to your data and applications if a system component fails, for example, a CPU or network-interface card.

When your system includes MC/ServiceGuard, your applications can be transferred automatically and quickly from a failed CPU to a functioning CPU. To provide this extra level of confidence, you must have the necessary system components. For example, two or more CPUs and two or more independent disks allow a configuration that eliminates single points of failure. In addition, MC/ServiceGuard also provides the software support to control the transfer of your applications to another CPU or network after a system failure. MC/ServiceGuard can also be used to transfer the control of the running applications to another CPU during maintenance of either management server.

The systems belonging to the MC/ServiceGuard installation make up a **ServiceGuard cluster**.

## Glossary of MC/ServiceGuard Terms

The following terms are used in this section:

| | |
|---|---|
| Package | An application together with associated programs, resources, and files. Control of the package may be transferred to another CPU in the event of failure of the original CPU or network. Note that a package can run only once in an SG cluster. |
| Service | A process that is monitored by MC/ServiceGuard. A service can be an application program, or the resources needed by an application program. Services are started by starting a package, and stopped by halting a |

| | |
|---|---|
| | package. If a service fails while a package is running, the package may be halted and restarted on an Adoptive Node. |
| MC/Service Guard Daemon | A daemon that monitors the state of the SG cluster, all nodes in the cluster, all network resources, and all services. The daemon reacts to failures and transfers control of packages. It also runs the package control script. |
| Original Node | The node on which the package is running before SG initiates a transfer of control. |
| Adoptive Node | A node to which SG can transfer control of a package. A package may have several adoptive nodes. Note that you can define packages that only run on a subset of all SG cluster nodes. |
| Adoptable Package | A package for which the control can be transferred to an adoptive node by SG. You can specify if and to where you want control of a package to be transferred in the event of failure or if you want the package to fail. |
| Package Custody | This is the node on which the package is currently running. |

# How MC/ServiceGuard Works

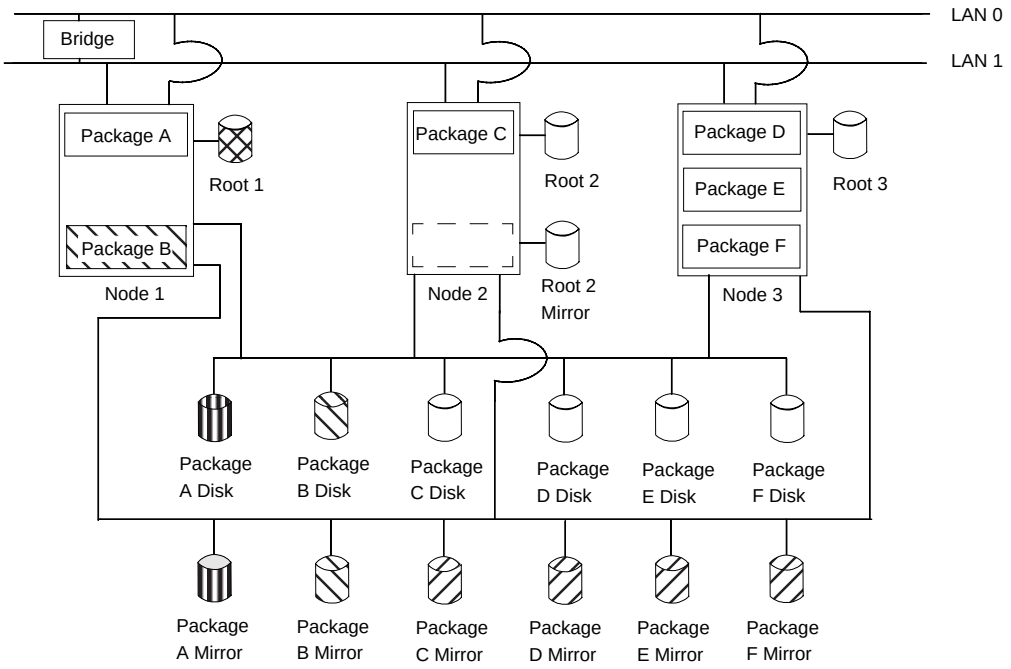
The following examples illustrate scenarios in which MC/ServiceGuard is used to switch control of a package between different cluster servers:

## Example 1: MC/ServiceGuard Package Switchover

The SG cluster shown in Figure B-1 represents a typical scenario:

- Node 1 runs the application packages A and B
- Node 2 is runs the application package C
- Node 3 is runs the application packages D, E, and F
- The nodes are connected by two redundant LANs connected by way of a bridge
- Each node has its own root disk and shares volume groups

**Figure B-1 MC/ServiceGuard Package Switchover: Before the Switch**

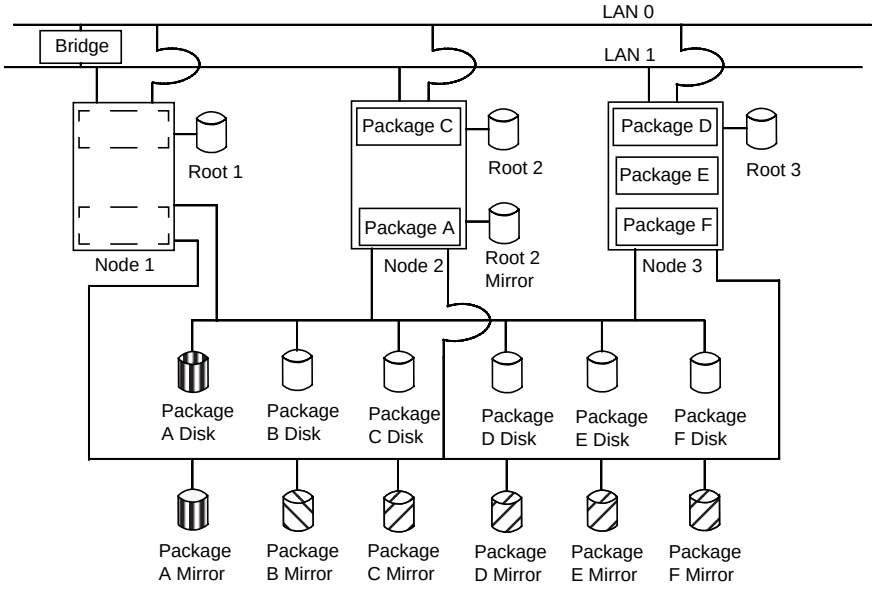



Assume that node 1 fails. Node 2 is an adoptive node for Package A, but for Package B no adoptive node is specified; therefore the applications specified in Package B will *not* be transferred in the event of node failure. However, Package B will be protected from a possible network failure by local network switching.

**NOTE** Transfering control of a package to another node does not transfer the program counter. Processes in a transferred package will restart from the beginning. If necessary, all processes in a package must be written so that they can detect such a restart.

When a node fails, the CPU is halted immediately using a Transfer Of Control (TOC) which is an immediate halt without a graceful shutdown.

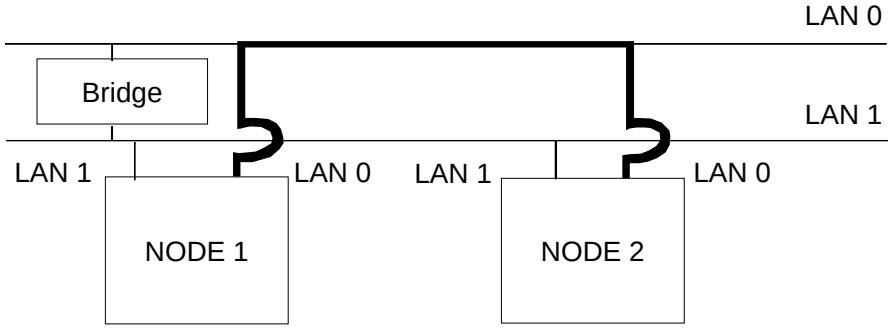
**Figure B-2 MC/ServiceGuard Package Switchover: After the Switch**




## Example 2: MC/ServiceGuard Local Network Switching

The example below shows two SG nodes connected by one virtual LAN. LANs 0 and 1 are connected by a bridge and act as one subnet. Node 1 and node 2 communicate by way of LAN 0. LAN 1 is in standby mode.

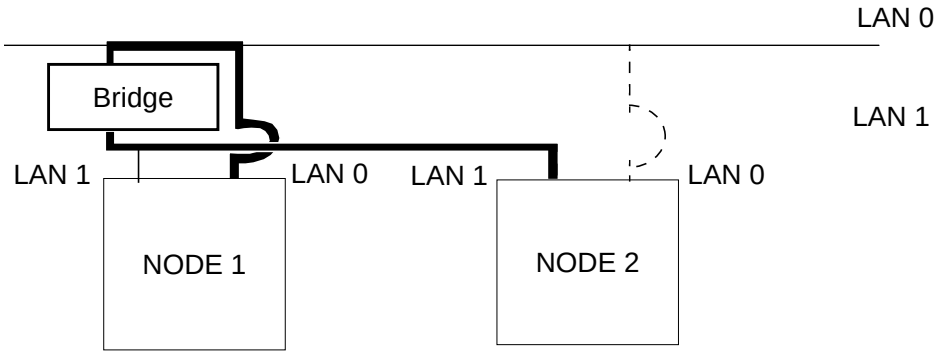
**Figure B-3 MC/ServiceGuard LAN Switchover: Before the Switch**



Assume that the LAN 0 network interface card on node 2 fails:

- The standby LAN interface, LAN 1, takes on the identity of LAN 0 on node 2. The subnet and IP addresses are switched to the hardware path associated with LAN 1. The switch is transparent at the TCP/IP level.
- MC/ServiceGuard re-routes communications without having to transfer the control of packages between nodes.

**Figure B-4 MC/ServiceGuard LAN Switchover: After the Switch**



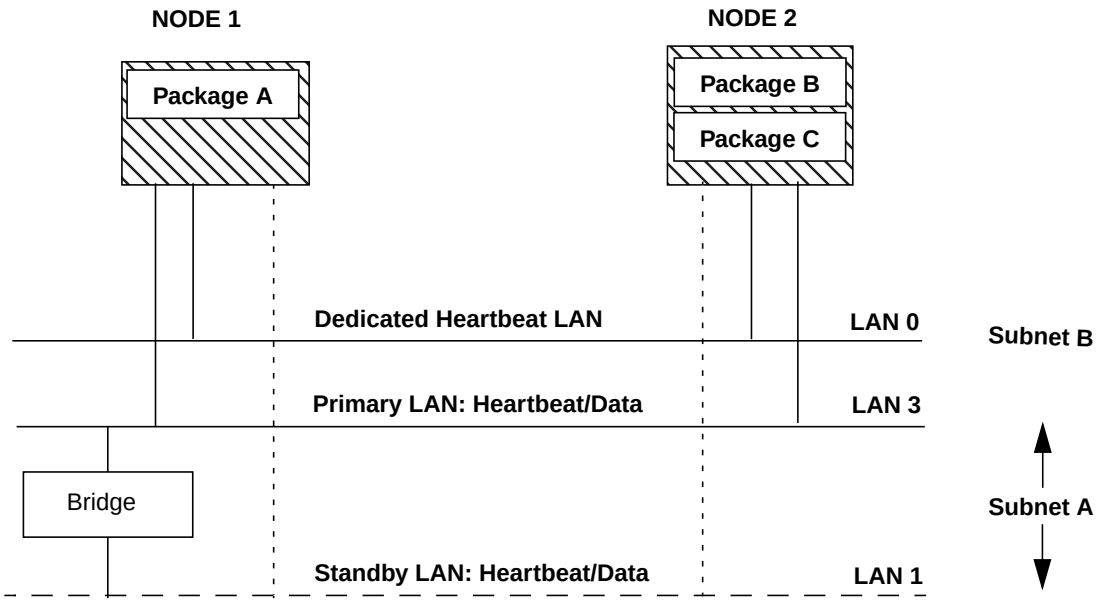

## MC/ServiceGuard Redundant Data and Control Subnets

In general, you have two redundant subnets for ServiceGuard clusters:

- A subnet used by the package applications for the data transfer, and
- A subnet used by SG to transfer the heartbeat signal to and from each SG node.

If your network traffic is very heavy, your SG clusters should have two or more subnets. It is common to find three LAN interfaces all bridged, with heartbeat over LAN0, LAN1 as standby for both, and LAN3 as the data LAN. LAN1 can backup either subnet.

**Figure B-5 MC/ServiceGuard Redundant Data and Heartbeat Subnets**




The heartbeat interval is set in the SG cluster configuration file. Heartbeat time-out is the length of time that the SG cluster will wait for a node's heartbeat before performing a transfer of package.

# MC/ServiceGuard and IP addresses

One of the many useful features of MC/ServiceGuard is the ability to assign multiple IP addresses to a single LAN interface card.

Each primary network interface card has a unique IP address. This address is fixed to the node and is not transferable to another node. Each *package* may also have a unique IP address that is associated with the package, and is taken over by the adoptive node if control of the package is transferred. The node that currently holds the IP address of a package controls that package.

## Portable IP Addresses

Each package may have its own hostname. The IP address of the package points to this hostname. You must assign a unique IP address and an optional hostname to each package. A program can then use its own hostname as the input to **gethostbyname()** which will return its IP address.

# MC/ServiceGuard and ITO

MC/ServiceGuard (SG) provides a mechanism to start and stop applications. This means that products running in an SG environment must provide a package containing information about how to start and/or stop the application. These packages are transfered between the SG cluster nodes if a switch-over occurs. The package is referred to as the **ITO SG** package in this section.

All SG cluster nodes have a hostname and a fixed IP address. In addition, an SG package has a hostname and an IP address that can be switched from one SG cluster node to another, together with the SG package.

## MC/ServiceGuard Support on the Management Server

NNM 5.0 does not support MC/ServiceGuard directly. In other words, it is not possible to create an NNM 5.0 ServiceGuard package. However, it is possible to run NNM 5.0 independently on each SG cluster node.

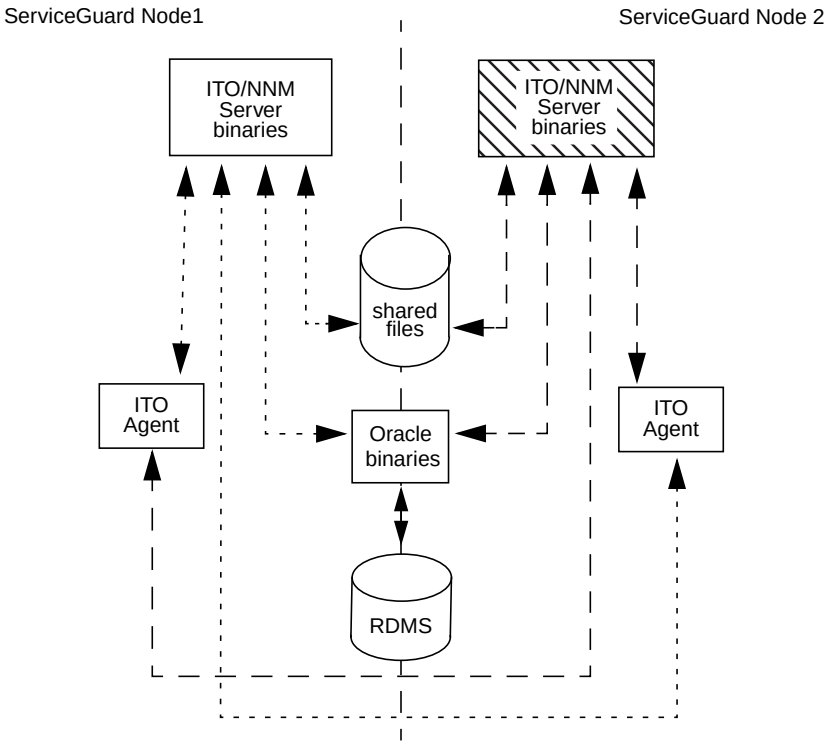
NMM 6.0 can run as a ServiceGuard package if tightly integrated in the ITO package. Since ITO 5.0, it is not supported to run NNM independently on each SG cluster node when ITO is running as MC/SG package.

**NOTE**

It would help to let the **netmon** run for one day on each cluster node before taking the ITO SG environment online. This enables the net to be discovered.

The following figure illustrates the concepts behind running ITO in an SG environment:

**Figure B-6 ITO Management Server on MC/ServiceGuard Systems: Conceptual View**




To reduce the amount of data on the shared disk, only `/var/opt/OV/share` and `/etc/opt/OV/share` are installed on the shared disk.

**NOTE** ITO can only be installed on a SG cluster node after the SG software is installed.

# Troubleshooting ITO in a ServiceGuard Environment

This chapter describes some of the problems you might encounter when working with ITO SG packages, and provides some specific troubleshooting hints. For more general troubleshooting information, see the troubleshooting section in the *Managing MC/ServiceGuard* manual.

## ITO SG Logfiles

MC/ServiceGuard and the ITO SG package use the following two logfiles:

- `/var/adm/syslog/syslog.log`

  This logfile contains general error messages from MC/ServiceGuard.

- `/etc/cmcluster/OpC/OpC.cntl.log`

  This contains the output of the ITO SG package during startup and shutdown.

If you do encounter problems with the ITO SG package, make sure that you check the contents of *both* files.

## Maintenance Notes for ITO/NNM and MC/ServiceGuard

The ITO MC/SG package can be set to maintenance mode to avoid a switch-over of the package when ITO is stopped. This is neoclassical when you run a backup or if a patch has to be installed. The shared disk and may the database must be available in this case. You can enable maintenance mode by touching the file `/tmp/mainNNM`. The monitor scripts `nnm.mon` and `ito.mon` does not trigger a package switch-over if the file `/tmp/mainNNM` exists

# C ITO Tables and Tablespaces in the Database

# ITO Tables in the Database

See the *HP OpenView IT/Operations Reporting and Database Schema* for detailed information about the ITO tables in the RDBMS.

# ITO Tables and Tablespace

An Oracle database uses tablespaces to manage the available disk space. You can assign datafiles of a fixed size to tablespaces. The size of the various datafiles assigned to a tablespace determines the size of the tablespace.

To increase the size of a tablespace, you must add a datafile of a particular size to the tablespace. You can do this interactively using the Oracle tool, Server Manager, or using the `sql` command: `alter tablespace add datafile`. Table C-1 on page 516 shows the default tablespace design and the assigned database tables.

For more information about improving the performance of your database see the online documentation in:

`/opt/OV/ReleaseNotes/opc_db.tuning`

**Table C-1 ITO Tables and Tablespaces in an Oracle Database**

| Tables/ Description | Table-space | Size | Remarks |
|---|---|---|---|
| opc_act_messages | OPC_1 | SIZE 4M<br>AUTOEXTEND ON NEXT 6M<br>MAXSIZE 500M<br><br>DEFAULT STORAGE (<br>INITIAL 2M<br>NEXT 2M<br>PCTINCREASE 0 ) | Tables with heavy load. Indexes not on the same disk as table, thus providing extra tablespace. |
| opc_anno_text<br>opc_annotation<br>opc_msg_text<br>opc_orig_ msg_text | OPC_2 | SIZE 5M<br>AUTOEXTEND ON NEXT 6M<br>MAXSIZE 500M<br><br>DEFAULT STORAGE (<br>INITIAL 1M<br>NEXT 1M<br>PCTINCREASE 0 ) | Tables with heavy load. Indexes not on the same disk as table, thus providing extra tablespace. |
| opc_node_names | OPC_3 | SIZE 1M<br>AUTOEXTEND ON NEXT 1M<br>MAXSIZE 500M<br><br>DEFAULT STORAGE (<br>INITIAL 256K<br>NEXT 256K<br>PCTINCREASE 0 ) | Table with very frequent access. |
| All other tables | OPC_4 | SIZE 20M<br>AUTOEXTEND ON NEXT 1M<br>MAXSIZE 500M<br><br>DEFAULT STORAGE (<br>INITIAL 32K<br>NEXT 256K<br>PCTINCREASE 0 ) | none |

| Tables/ Description | Table-space | Size | Remarks |
|---|---|---|---|
| Default tablespace of user opc_op | OPC_5 | SIZE 1M<br>AUTOEXTEND ON NEXT 1M<br>MAXSIZE 500M<br><br>DEFAULT STORAGE (<br>INITIAL 32K<br>NEXT 32K<br>PCTINCREASE 0 ) | none |
| opc_hist_messages | OPC_6 | SIZE 4M<br>AUTOEXTEND ON NEXT 1M<br>MAXSIZE 500M<br><br>DEFAULT STORAGE (<br>INITIAL 2M<br>NEXT 2M<br>PCTINCREASE 0 ) | Tables with heavy load. Indexes not on the same disk as table, thus providing extra tablespace. |
| opc_hist_msg_text | OPC_7 | SIZE 4M<br>AUTOEXTEND ON NEXT 1M<br>MAXSIZE 500M<br><br>DEFAULT STORAGE (<br>INITIAL 2M<br>NEXT 2M<br>PCTINCREASE 0 ) | Tables with heavy load. Indexes not on the same disk as table, thus providing extra tablespace. |
| opc_hist_orig_text | OPC_8 | SIZE 4M<br>AUTOEXTEND ON NEXT 1M<br>MAXSIZE 500M<br><br>DEFAULT STORAGE (<br>INITIAL 2M<br>NEXT 2M<br>PCTINCREASE 0 ) | Tables with heavy load. Indexes not on the same disk as table, thus providing extra tablespace. |

| Tables/ Description | Table-space | Size | Remarks |
|---|---|---|---|
| opc_hist_ annotation<br>opc_hist_anno_ text | OPC_9 | SIZE 4M<br>AUTOEXTEND ON NEXT 1M<br>MAXSIZE 500M<br>DEFAULT STORAGE (<br>INITIAL 2M<br>NEXT 2M<br>PCTINCREASE 0 ) | Tables with heavy load. Indexes not on the same disk as table, thus providing extra tablespace. |
| Temporary data (used for sorting) | OPC_TEMP | SIZE 1M<br>AUTOEXTEND ON NEXT 1M<br>MAXSIZE 500M<br>DEFAULT STORAGE (<br>INITIAL 512K<br>NEXT 512K<br>PCTINCREASE 0 ) | none |
| Index tablespace for active messages | OPC_INDEX1 | SIZE 10M<br>AUTOEXTEND ON NEXT 1M<br>MAXSIZE 500M<br>DEFAULT STORAGE (<br>INITIAL 1M<br>NEXT 1M<br>PCTINCREASE 0 ) | Other disk than for opc_act_ messages tablespaces. |
| Index tablespace for history messages | OPC_INDEX2 | SIZE 10M<br>AUTOEXTEND ON NEXT 1M<br>MAXSIZE 500M<br>DEFAULT STORAGE (<br>INITIAL 1M<br>NEXT 1M<br>PCTINCREASE 0 ) | Other disk than for opc_hist_ messages tablespaces. |

**Table C-2 Non-ITO Specific Tablespace**

| Tables/ Description | Tablespace | Size | Remarks |
|---|---|---|---|
| Tablespace containing the system tables. | SYSTEM | SIZE 50M<br>DEFAULT STORAGE (<br>INITIAL 16K<br>NEXT 16K<br>PCTINCREASE 50 ) | none |
| Temporary data. | TEMP | SIZE 2M<br>AUTOEXTEND ON NEXT 1M<br>MAXSIZE 500M<br>DEFAULT STORAGE (<br>INITIAL 100K<br>NEXT 100K<br>PCTINCREASE 0 ) | none |
| Rollback segments (this tablespace is not ITO specific) | RBS1 | SIZE 1M<br>AUTOEXTEND ON NEXT 1M<br>MAXSIZE 500M<br>DEFAULT STORAGE (<br>INITIAL 500K<br>NEXT 500K<br>MINEXTENTS 10<br>PCTINCREASE 0 ) | Tablespace with heavy load. |
| Tablespace for Oracle Tool Tables (e.g., report writer) | TOOLS | SIZE 1M<br>AUTOEXTEND ON NEXT 1M<br>MAXSIZE 100M<br>DEFAULT STORAGE (<br>INITIAL 100K<br>NEXT 100K<br>PCTINCREASE 0 ) | none |

# D ITO Man Pages Listing

This appendix provides a list of each man page for the HP OpenView IT/Operations Developer's Toolkit. To refer to the man pages, call them from the command line by using: **man <manpagename>**. If you wish to print the man pages, you can use the command:

```
man <manpagename> | col -lb | lp -d printer_name
```

# Overview of ITO Man Pages

You can access the following ITO man pages, either directly at the command line, or by way of the online help:

## Man Pages in ITO

| Man Page | Summary |
|---|---|
| call_sqlplus.sh(1) | Calls SQL*Plus. |
| inst.sh(1M) | Install ITO software on managed nodes. |
| inst_debug(5) | Debug an installation of the ITO agent software. |
| opc(1\|5) | Start the ITO GUI. |
| opc_audit_secure(1M) | Locks the audit level in the ITO database and allows directories for the history and audit download to be set. |
| opc_backup(5) | Back up the ITO configuration. |
| opc_backup(1M) | Interactively save ITO environment for Oracle. |
| opc_recover(5) | Recover the ITO configuration. |
| opc_recover(1M) | Interactively recover the ITO environment for Oracle. |
| opcack(1M) | Externally acknowledge active messages. |
| opcackmsg(1M) | Externally acknowledge active messages using message IDs. |
| opcackmsgs(1M) | Externally acknowledge active messages using specific message attributes. |
| opcactivate(1M) | Activate an ITO pre-installed agent. |

| | |
|---|---|
| opcadddbf(1M) | Add a new datafile to an Oracle tablespace. |
| opcagt(1M) | Administer agent processes on a managed node. |
| opcagtreg(1M) | Registration tool for subagents. |
| opcagtutil(1M) | Parse the agent platform file and perform operation with extracted data. |
| opcaudupl(1M) | Upload audit data into the ITO database. |
| opcaudwn(1M) | Download audit data into the ITO database. |
| opccfgdwn(1M) | Download configuration data from the database to flat files. |
| opccfgout(1M) | Configure condition status variables for scheduled outages in ITO. |
| opccfgupld(1M) | Upload configuration data from flat files into the database. |
| opcchgaddr(1M) | Change the node address of nodes in the ITO database. |
| opccltconfig(1M) | Configure ITO client filesets. |
| opcconfig(1M) | Configure an ITO management server. |
| opcdbidx(1M) | Upgrade the structure of the ITO database. |
| opcdbinit(1M) | Initialize the database with default configuration. |
| opcdbinst(1M) | Create or destroy the ITO database scheme. |
| opcdbpwd(1M) | Change the password of the ITO database user opc_op. |
| opcdbreorg(1M) | Re-organize the tables in the ITO database. |

| | |
|---|---|
| opcdbsetup(1M) | Create the tables in the ITO database. |
| opcdbupgr(1M) | Upgrade the ITO database from a previous version to the current version of ITO. |
| opcdcode(1M) | View ITO encrypted template files. |
| opcgetmsgids(1m) | Get message IDs to an original message ID. |
| opchbp(1M) | Switch heartbeat polling of managed nodes on/off. |
| opchistdwn(1M) | Download ITO history messages to a file. |
| opchistupl(1M) | Upload history messages into ITO database. |
| opcmack(1) | Acknowledge an ITO message by specifying the message ID. |
| opcmgrdist(1M) | Distribute ITO configuration between management servers. |
| opcmom(4) | Overview of ITO MoM functionality. |
| opcmomchk(1) | Syntax checking tool for MoM templates. |
| opcmon(1) | Forward value of monitored object to the ITO monitoring agent on the local managed node. |
| opcmsg(1) | Submit a message to ITO. |
| opcpat(1) | Test program for ITO pattern matching. |
| opcragt(1M) | Remotely administer agent services for ITO on managed node. |
| opcskm(3) | Secret-key management tool. |
| opcsqlnetconf(1M) | Configure the ITO database to use an SQL*Net connection. |
| opcsv(1M) | Administer ITO manager services. |

| | |
|---|---|
| opcsvreg(1M) | Registration tool for server configuration files. |
| opcsvskm(1M) | Secret-key management tool on the management server. |
| opcsw(1M) | Set the software status flag in the ITO database. |
| opctmpldwn(1M) | Download and encrypt ITO message source templates. |
| opcupgrade(1M) | Upgrade an earlier version of ITO to the current version (A.05.00). |
| opcwall(1) | Send a message to the currently logged in ITO users. |
| ovtrap2opc(1M) | Convert trapd.conf file and the ITO template file. |

## Man Pages for ITO APIs

| Man Page | Summary |
|---|---|
| opcmon(3) | Forward value of monitored object to the ITO monitoring agent on the local managed node. |
| opcmsg(3) | Submit a message to ITO. |

## Man Pages for the HP OpenView ServiceNavigator

| Man Page | Summary |
|---|---|
| opcservice(1M) | Configure the HP OpenView ServiceNavigator. |

## Man Pages for the ITO Developer's Kit APIs

| Man Page | Summary |
|---|---|
| msiconf(4) | Configuration file for the ITO message manager. |

| | |
|---|---|
| opc_comif_close(3) | Close an instance of the communication queue interface. |
| opc_comif_freedata(3) | Free data that was allocated by `opc_comif_read()`. |
| opc_comif_open(3) | Open an instance of the communication queue interface. |
| opc_comif_read(3) | Read information from a queue. |
| opc_comif_read_request(3) | Read information from a queue. |
| opc_comif_write(3) | Write information into a queue. |
| opc_comif_write_request(3) | Write information into a queue. |
| opc_connect_api(3) | ITO Connection API. |
| opc_distrib(3) | Distribute the ITO agent configuration. |
| opcagtmon_send(3) | Forward monitored object value to ITO. |
| opcagtmsg_api(3) | API to handle messages on ITO agents. |
| opcanno_api(3) | API to managed ITO message annotations. |
| opcapp_start(3) | API to start an ITO application. |
| opcappl_api(3) | API to configure and start ITO applications. |
| opcapplgrp_api(3) | API to configure ITO application groups. |
| opcconf_api(3) | API to get ITO configuration. |
| opcdata(3) | APIs for accessing the attributes of the ITO data structure. |
| opcdata_api(3) | Describes how to access the ITO data structure using the ITO Data API. |
| opcif_api(3) | API to work with the ITO Message Stream Interface. |
| opciter(3) | ITO iterator to step through opcdata container. |

| | |
|---|---|
| opcmsg_api(3) | Functions to manage ITO messages. |
| opcmsggrp_api(3) | Functions to manage ITO message groups. |
| opcmsgregrpcond_api(3) | Functions to create and modify ITO message regroup conditions. |
| opcnode_api(3) | Functions to configure ITO managed nodes. |
| opcnodegrp_api(3) | Functions to configure ITO node groups. |
| opcnodehier_api(3) | Functions to configure ITO node hierarchies. |
| opcprofile_api(3) | Functions to configure ITO user profiles. |
| opcregcond(3) | Set of APIs to access fields of the ITO registration condition structure. |
| opctempl_api(3) | Functions to configure ITO message source templates. |
| opctempfile_api(3) | Functions to configure ITO templates using template files. |
| opctemplgrp_api(3) | Functions to configure ITO template groups. |
| opctransaction_api(3) | Functions to start, commit, and rollback transactions. |
| opcuser_api(3) | Functions to configure ITO users. |

# Master Index

This index contains references to three ITO manuals. All page numbers are prefaced with a two letter abbreviation indicating the manual that contains the reference. For example, the index entry *security, CG:67, AR:349, AR:365,* shows that information about security can be found in the Concepts Guide on page 67, and also on pages 349 and 365 in the Administrator's Reference.

# Master Index

This index contains references to three ITO manuals. All page numbers are prefaced with a two letter abbreviation indicating the manual that contains the reference. For example, the index entry *security, CG:94, AR:397, AR:416,* shows that information about security can be found on page 94 in the Concepts Guide, and also on pages 397 and 416 in the Administrator's Reference.



**B**



AR = Administrator's Reference Guide; CG = Concepts Guide

# Master Index

This index contains references to three ITO manuals. All page numbers are prefaced with a two letter abbreviation indicating the manual that contains the reference. For example, the index entry *security, CG:94, AR:397, AR:416,* shows that information about security can be found on page 94 in the Concepts Guide, and also on pages 397 and 416 in the Administrator's Reference.



AR = Administrator's Reference Guide; CG = Concepts Guide

# Master Index

This index contains references to three ITO manuals. All page numbers are prefaced with a two letter abbreviation indicating the manual that contains the reference. For example, the index entry *security, CG:94, AR:397, AR:416,* shows that information about security can be found on page 94 in the Concepts Guide, and also on pages 397 and 416 in the Administrator's Reference.



AR = Administrator's Reference Guide; CG = Concepts Guide

# Master Index

This index contains references to three ITO manuals. All page numbers are prefaced with a two letter abbreviation indicating the manual that contains the reference. For example, the index entry *security, CG:94, AR:397, AR:416,* shows that information about security can be found on page 94 in the Concepts Guide, and also on pages 397 and 416 in the Administrator's Reference.



AR = Administrator's Reference Guide; CG = Concepts Guide

# Master Index

This index contains references to three ITO manuals. All page numbers are prefaced with a two letter abbreviation indicating the manual that contains the reference. For example, the index entry *security, CG:94, AR:397, AR:416,* shows that information about security can be found on page 94 in the Concepts Guide, and also on pages 397 and 416 in the Administrator's Reference.



AR = Administrator's Reference Guide; CG = Concepts Guide

# Master Index

This index contains references to three ITO manuals. All page numbers are prefaced with a two letter abbreviation indicating the manual that contains the reference. For example, the index entry *security, CG:94, AR:397, AR:416,* shows that information about security can be found on page 94 in the Concepts Guide, and also on pages 397 and 416 in the Administrator's Reference.



AR = Administrator's Reference Guide; CG = Concepts Guide

# Master Index

This index contains references to three ITO manuals. All page numbers are prefaced with a two letter abbreviation indicating the manual that contains the reference. For example, the index entry *security, CG:94, AR:397, AR:416,* shows that information about security can be found on page 94 in the Concepts Guide, and also on pages 397 and 416 in the Administrator's Reference.



AR = Administrator's Reference Guide; CG = Concepts Guide

# Master Index

This index contains references to three ITO manuals. All page numbers are prefaced with a two letter abbreviation indicating the manual that contains the reference. For example, the index entry *security, CG:94, AR:397, AR:416,* shows that information about security can be found on page 94 in the Concepts Guide, and also on pages 397 and 416 in the Administrator's Reference.



AR = Administrator's Reference Guide; CG = Concepts Guide

# Master Index

This index contains references to three ITO manuals. All page numbers are prefaced with a two letter abbreviation indicating the manual that contains the reference. For example, the index entry *security, CG:94, AR:397, AR:416,* shows that information about security can be found on page 94 in the Concepts Guide, and also on pages 397 and 416 in the Administrator's Reference.



AR = Administrator's Reference Guide; CG = Concepts Guide

# Master Index

This index contains references to three ITO manuals. All page numbers are prefaced with a two letter abbreviation indicating the manual that contains the reference. For example, the index entry *security, CG:94, AR:397, AR:416,* shows that information about security can be found on page 94 in the Concepts Guide, and also on pages 397 and 416 in the Administrator's Reference.



AR = Administrator's Reference Guide; CG = Concepts Guide

# Master Index

This index contains references to three ITO manuals. All page numbers are prefaced with a two letter abbreviation indicating the manual that contains the reference. For example, the index entry *security, CG:94, AR:397, AR:416,* shows that information about security can be found on page 94 in the Concepts Guide, and also on pages 397 and 416 in the Administrator's Reference.



AR = Administrator's Reference Guide; CG = Concepts Guide

# Master Index

This index contains references to three ITO manuals. All page numbers are prefaced with a two letter abbreviation indicating the manual that contains the reference. For example, the index entry *security, CG:94, AR:397, AR:416,* shows that information about security can be found on page 94 in the Concepts Guide, and also on pages 397 and 416 in the Administrator's Reference.



AR = Administrator's Reference Guide; CG = Concepts Guide

# Master Index

This index contains references to three ITO manuals. All page numbers are prefaced with a two letter abbreviation indicating the manual that contains the reference. For example, the index entry *security, CG:94, AR:397, AR:416,* shows that information about security can be found on page 94 in the Concepts Guide, and also on pages 397 and 416 in the Administrator's Reference.



AR = Administrator's Reference Guide; CG = Concepts Guide

# Master Index

This index contains references to three ITO manuals. All page numbers are prefaced with a two letter abbreviation indicating the manual that contains the reference. For example, the index entry *security, CG:94, AR:397, AR:416,* shows that information about security can be found on page 94 in the Concepts Guide, and also on pages 397 and 416 in the Administrator's Reference.



AR = Administrator's Reference Guide; CG = Concepts Guide

# Master Index

This index contains references to three ITO manuals. All page numbers are prefaced with a two letter abbreviation indicating the manual that contains the reference. For example, the index entry *security, CG:94, AR:397, AR:416,* shows that information about security can be found on page 94 in the Concepts Guide, and also on pages 397 and 416 in the Administrator's Reference.



AR = Administrator's Reference Guide; CG = Concepts Guide

# Master Index

This index contains references to three ITO manuals. All page numbers are prefaced with a two letter abbreviation indicating the manual that contains the reference. For example, the index entry *security, CG:94, AR:397, AR:416,* shows that information about security can be found on page 94 in the Concepts Guide, and also on pages 397 and 416 in the Administrator's Reference.



AR = Administrator's Reference Guide; CG = Concepts Guide

# Master Index

This index contains references to three ITO manuals. All page numbers are prefaced with a two letter abbreviation indicating the manual that contains the reference. For example, the index entry *security, CG:94, AR:397, AR:416,* shows that information about security can be found on page 94 in the Concepts Guide, and also on pages 397 and 416 in the Administrator's Reference.



AR = Administrator's Reference Guide; CG = Concepts Guide

# Master Index

This index contains references to three ITO manuals. All page numbers are prefaced with a two letter abbreviation indicating the manual that contains the reference. For example, the index entry *security, CG:94, AR:397, AR:416,* shows that information about security can be found on page 94 in the Concepts Guide, and also on pages 397 and 416 in the Administrator's Reference.



AR = Administrator's Reference Guide; CG = Concepts Guide

# Master Index

This index contains references to three ITO manuals. All page numbers are prefaced with a two letter abbreviation indicating the manual that contains the reference. For example, the index entry *security*, *CG:94*, *AR:397*, *AR:416*, shows that information about security can be found on page 94 in the Concepts Guide, and also on pages 397 and 416 in the Administrator's Reference.

AR = Administrator's Reference Guide; CG = Concepts Guide