

HP OpenView Operations for UNIX

Release Notes For HP 9000 PA-RISC 2.0 Servers

**Version 8.24
Edition 14**

Management Server on HP-UX PA-RISC



**Manufacturing Part Number: None
February 2007**

U.S.

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

Legal Notices

Warranty.

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

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

Restricted Rights Legend.

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

Hewlett-Packard Company
United States of America

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

Copyright Notices.

©Copyright 2004-2007 Hewlett-Packard Development Company, L.P.

No part of this document may be copied, reproduced, or translated to another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

This product includes software written by Info-ZIP (<http://www.info-zip.org/license.html>)

This product includes software written by Tim Hudson (tjh@cryptsoft.com)

This product includes lsof ©Copyright 2002 Purdue Research Foundation, West Lafayette, Indiana 47907.

Trademark Notices.

Adobe® is a trademark of Adobe Systems Incorporated.

Java™ and all Java based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

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

Netscape™ and Netscape Navigator™ are U.S. trademarks of Netscape Communications Corporation.

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California

OSF, OSF/1, OSF/Motif, Motif, and Open Software Foundation are trademarks of the Open Software Foundation in the U.S. and other countries.

SQL*Plus® is a registered U.S. trademark of Oracle Corporation, Redwood City, California

UNIX® is a registered trademark of the Open Group.

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

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

Zip® and UnZip® are U.S. registered trademarks of Info-ZIP.

Export and Cryptography Notice.

This software may not be exported, re-exported, transferred or downloaded to or within (or to a national resident of) countries under U.S. economic embargo including the following countries:

Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria

This list is subject to change.

This software may not be exported, re-exported, transferred or downloaded to persons or entities listed on the U.S. Department of Commerce Denied Persons List, Entity List of proliferation concern or on any U.S. Treasury Department Designated Nationals exclusion list, or to parties directly or indirectly involved in the development or production of nuclear, chemical, biological weapons or in missile technology programs as specified in the U.S. Export Administration Regulations (15 CFR 744).

In addition, please be advised that this software contains cryptography and is subject to U.S. cryptography export regulations.

1. What's in This Version

New Announcements with Release Notes Edition 14	10
OVO/UNIX 8 Media Kit Update	10
HP OpenView Operations for UNIX Configuration Value Pack Software	10
Key benefits	11
Powerful features	11
HP OpenView Smart Plug-ins (SPIs) for OVO for UNIX Update	14
HP OpenView Performance Agent (OVPA) 4.6 Deployables	14
Daylight Saving Time Operations Support	15
New and/or Updated Documentation	15
Dedicated Installation Guides for OVO/UNIX with HP Serviceguard	15
HTTPS Agent Concepts and Configuration Guide	15
Deploying OVO HTTPS Agents Using Radia Whitepaper	15
Using ECS Designer Remotely Whitepaper	15
New Announcements with Release Notes Edition 13	16
OVO/UNIX 8.24 Management Server Patch	16
High Availability through OVO/UNIX Server Pooling Whitepaper	16
Configuring Outbound-Only Communication Whitepaper	16
OVO/UNIX Management Server Enhancements	16
New Support Announcements	17
OVO/UNIX 8.16 HTTPS Agents	17
Management Server Support for Sun UltraSPARC T1 Processor	17
Java UI Enhancements	17
New Features with OVO/UNIX 8	18
Management Server	18
Supported Platforms	18
Administration Enhancements	18
Message Counter Feature: Severity and Message Text Updates	18
High Availability Environments	18
Pluggable Authentication Module (PAM)	19
Deployable OV Performance Agent	19
ECS 3.31 - 3.33 Runtime Support	20
OV Composer 3.31/3.33 Support	20
ECS 3.2 Designer Support	20
Localized Support for Japanese, Korean, Simplified Chinese and Spanish	20
Miscellaneous	23

Contents

HP OpenView Network Node Manager 7.51 Support	24
Supported Migration Paths	24
Java UI Enhancements	24
Operational Service Views in the Java GUI	26
Oracle Database	28
Oracle Database 10g Release 1 Support on HP-UX 11.11 and 11.23 PA-RISC	29
Oracle Database 10g Release 2 Support on HP-UX 11.11 and 11.23 PA-RISC	29
Oracle Standard Edition Support	29
Independent Database Support	29
OVO/UNIX 8 and Independent Database Server on Different Operating Systems	30
Oracle Real Application Clusters (RAC) Support	31
Service Navigator	31
Service Navigator Enhancements	31
Allowing Dynamic Configuration Changes in Service Navigator	33
Service Navigator Value Pack Support	33
SNVP 8.0 and 9.0 with Oracle 10g Release 2	33
HTTPS-Agents	33
Single-Port Communication	33
Windows Installation Server	33
Cluster Awareness for HTTPS Agents	34
DHCP Support for HTTPS Agents	34
SNMP Trap Interception for OVO/UNIX Agents	34
OVO/UNIX Agents Running as "Non-Root"	34
Multiple OVO/UNIX Configuration Servers	34
SNMP Trap Interception on Linux DCE Nodes	35
Common Criteria EAL-2 Certification	35
opcdelmsg Troubleshooting Utility	35
Handling IP node and non-IP node with the same node name	35
Changed Features	36
Installation of OVO Management Server	36
Configuration Settings on the OVO Management Server	36
Configuration Settings on HTTPS Managed Nodes	36
OVO Message Variables Passed into Instruction Text Parameter	37
Remote Actions Authorization	37
HTTPS Managed Nodes Policies	38
No Remote Access to the Service Engine	38

Locally Managed Tablespaces	38
Error Logging	38
Tracing.	39
OVO-SunMC Integration Kit	39
Default Templates for AIX, HP-UX, Linux, Sun Solaris, Tru64, and Microsoft Windows 39	
Changed Features with HP OpenView Operations for UNIX Developer's Toolkit.	51
Server API opcapp_start() Function Behavior Changed with OVO 8	51
Obsolete Features.	52
What's Not Yet Supported	54
What's Not Supported	55
Obsolescence Announcements for the Next Major OVO Release	56

2. Management Server and Java UI Installation Requirements

Management Server Hardware and Software Requirements	59
High Availability Environments	61
Cluster Awareness Support.	62
Certified Encoding and Character Sets on OVO/UNIX Management Servers.	63
Java UI Supported Platforms	64

3. HTTPS Agent Installation Requirements

HTTPS Agent Supported Platforms	70
HTTPS Agent Hardware Requirements	72
HTTPS Agent Software Requirements	72
HP-UX HTTPS Agent Software Requirements	73
Solaris HTTPS Agent Software Requirements	74
Linux HTTPS Agent Software Requirements	75
Microsoft Windows HTTPS Agent Software Requirements	76
AIX HTTPS Agent Software Requirements	77

4. DCE Agent Installation Requirements

DCE Agent Versions.	80
DCE Agent Hardware Requirements	83
HP-UX PA-RISC DCE Agent Software Requirements.	85
HP-UX Itanium DCE Agent Software Requirements	87
Sun Solaris (SPARC) DCE Agent Software Requirements	88

Contents

Linux DCE Agent Software Requirements	90
Microsoft Windows DCE Agent Software Requirements	92
AIX DCE Agent Software Requirements	96
Tru64 UNIX DCE Agent Software Requirements	98
Novell NetWare DCE Agent Software Requirements	99
SGI IRIX DCE Agent Platforms	100
IBM/Sequent ptx DCE Agent Software Requirements	101
SINIX RM/Reliant DCE Agent Platforms	102
OpenVMS DCE Agent and Smart Plug-In Software Requirements	103

5. HTTPS Agent Resource Requirements and Performance

Comparison Between HTTPS and DCE Agents	106
Comparison Between OVO 7.x and OVO 8 Agent-Related Management Server Components	107

6. Last-Minute Changes to Documentation

New Java GUI Enhancements	109
Introduction of R Flag for Read-Only Messages in Java UI Message Browser	109
Full Support for INFORM Own Mode in Java UI	109
Support for Daylight Saving Time Change in Year 2007	109
Java GUI Timezone Adjustments	110
Customized Message Group Icons	110
Application HTML Output as an Internal Webpage	111
Java GUI Connection Port Setting	111
Improved Cluster Error Handling and Logging	111
opccmachg CLI Tool	112
NNM 7.51 CD-ROM Installation Important Update	112
HP-UX 11.11 Prerequisites	112
Installation	112
Upgrading to Oracle 10g Release 2	113
Check the System Requirements	113
Prepare the Database for the Upgrade	113
Installation of Oracle 10.2.0.1 (Oracle 10g Release 2)	114
Configuring OpenView Products to Use the New Oracle Version	114
Mixed Flexible Management with OVO 7 and OVO 8	116
Assessing Your System Vulnerability with ovprotect	116

Message Counter Feature: Severity and Message Text Updates	117
ovoinstall Hangs if NNM 7.51 is Installed	118
Installing OVO/UNIX on VERITAS Cluster Server 4.1 on HP-UX 11.23 Itanium ..	118
Command Line Utilities opcinstrumdwn and opcpkgdwn	118
opcdelmsg Troubleshooting Utility	119
dtterm Default for Agent Installation.....	119
Security Advisory Guide	119
Message Attribute Synchronization between OVO Management Servers in MoM Environments.....	119
Separating Message Fields with Tabs	119
Command Line Utility opccfguser	120
Changed Behavior of the Java GUI 'Lock' Feature	120
Auditing for Service Navigator	120
Interoperability with OVO for Windows	121
Obtaining Automatically Updated opcuhttps After Patch Installation.....	121
Problems with Database Startup After Oracle 10.2.0.2 Patch Installation	121
Enhanced Auditing for the Java GUI	122
Disabling Data Collection for the Embedded Performance Component	122
SQL *Plus Missing for Independent Database Server Installation	122

7. Known Problems and Workarounds

Oracle Database Installation and Configuration.....	124
Management Server Upgrade/Migration	126
Uploading Upgrade Data	126
The Required Approach	127
Workarounds.....	128
New Installation of the OVO/UNIX Management Server	131
Installation Workarounds.....	131
New HA Installation of the OVO/UNIX Management Server.....	135
Upgrade of the OVO/UNIX Management Server Running in an HA Environment .	137
Management Server Runtime	139
Management Server Deinstallation	143
HTTPS Managed Nodes Installation	144
HTTPS Managed Nodes Runtime.....	150
HTTPS Managed Nodes and Proxies	153
HTTPS Managed Nodes and NAT Environments	154

Contents

DCE Managed Nodes	155
Embedded Performance Component (EPC, also known as CODA)	158
Deployable Performance Agent (OVPA)	159
Motif UI	160
Java UI	162
ECS/OV Composer	165
Reporting	166
Service Navigator Value Pack	167
Network Node Manager	168
Network Diagnosis Add-On Module	174
NDAOM	174
Problem Diagnosis Probe	174
Internet Services (OVIS)	175
Tracing and Troubleshooting	176
Localization	177
Japanese Version Issues	180
Korean Version Issues	182
Traditional Chinese Version Issues	184
Spanish Version Issues	186

Contents

1 What's in This Version

Your company's business success relies on high-quality IT services and IT infrastructure agility. To keep your IT services available and well performing, you need a proven operations management solution that gives you control over your ever-changing IT infrastructure. That solution is HP OpenView Operations for UNIX.

Operations for UNIX discovers, monitors, controls and reports on the availability and performance of your heterogeneous, large-scale IT environment. It consolidates information for all IT components that control your business: network, systems, storage, databases, and applications. With its service-driven approach, it shows what IT problems affect your business processes, helping you to focus on what's most important for your company's business success.

For a general overview about OVO/UNIX's feature set, refer to the *HP OpenView Operations Concepts Guide (UNIX)*, which is available in PDF format on the HP product manual website.

The following readme file describes the OVO/UNIX media CD contents and layout and help you to locate products and documentation:

```
/READMEHPUX_PA-RISC.txt
```

For more information about the new features included with OVO, download the OVO/UNIX presentation *What's New in HP OpenView Operations for UNIX 8* from the documentation web site listed below:

```
http://ovweb.external.hp.com/lpe/doc\_serv/
```

NOTE Check the following web site periodically for the latest versions of these release notes and other OVO/UNIX manuals:

```
http://ovweb.external.hp.com/lpe/doc\_serv/
```

Select "Operations for UNIX" and version 8.x.

The Release Notes document is a summary of the latest status of OVO. As new functionality is added, it will be reported here under the latest release number. Workarounds that are required can also be found in a section dedicated to each edition of these release notes. Cross references are also hyperlinks in pdf format and help you to find related sections more easily.

This section provides information about the following topics:

- New Announcements with Release Notes Edition 14
- New Announcements with Release Notes Edition 13
- New Features with OVO/UNIX 8
- Changed Features
- Changed Features with HP OpenView Operations for UNIX Developer's Toolkit
- Obsolete Features
- What's Not Yet Supported
- What's Not Supported
- Obsolescence Announcements for the Next Major OVO Release

New Announcements with Release Notes Edition 14

This section describes the new announcements and features that are introduced in this edition of the OVO/UNIX 8 Release Notes.

OVO/UNIX 8 Media Kit Update

An updated OVO/UNIX media kit is available, featuring a number of latest improvements and enhancements for OVO/UNIX 8. The media kit also includes the following:

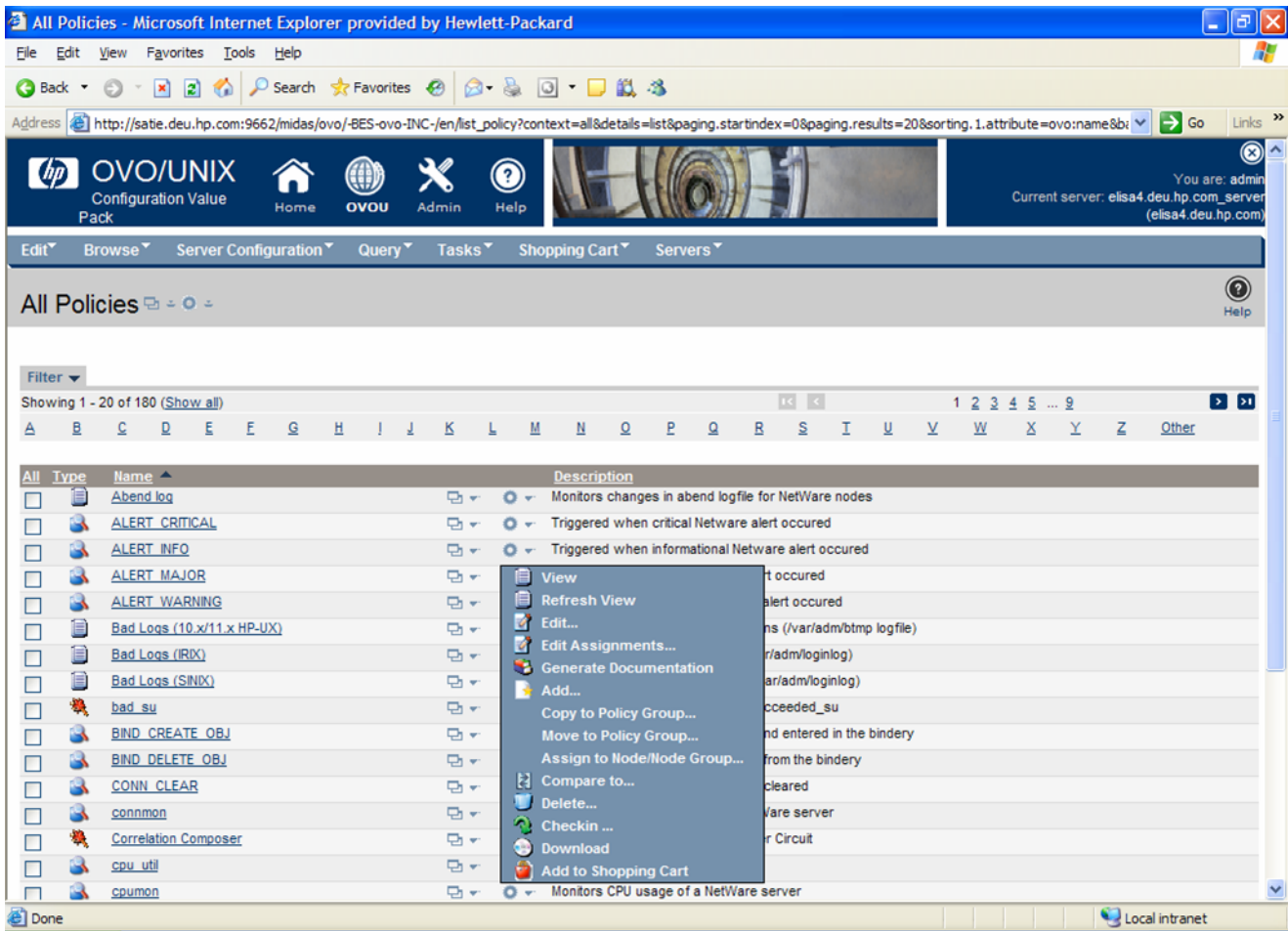
- “HP OpenView Operations for UNIX Configuration Value Pack Software”
- “HP OpenView Smart Plug-ins (SPIs) for OVO for UNIX Update”
- “HP OpenView Performance Agent (OVPA) 4.6 Deployables”

HP OpenView Operations for UNIX Configuration Value Pack Software

Many IT organizations face continuous cost pressure. If this is the case at your organization, you are probably challenged to manage more nodes and applications without additional staffing, while simultaneously improving the quality and transparency of the monitoring configuration. Now HP OpenView Operations for UNIX Configuration Value Pack software provides help for these challenges.

Concurrent, web-based access and a granular authorization model enable the delegation of configuration tasks to domain experts, thus reducing communication overhead and shortening time to delivery. Configuration reporting allows for better transparency, and configuration versioning and auditing helps you implement proper change and compliance management processes.

HP OpenView Operations for UNIX Configuration Value Pack is designed to increase productivity. This innovative software makes many Operations for UNIX administrative processes simpler and faster to execute, so you can get more value out of your HP OpenView investment.



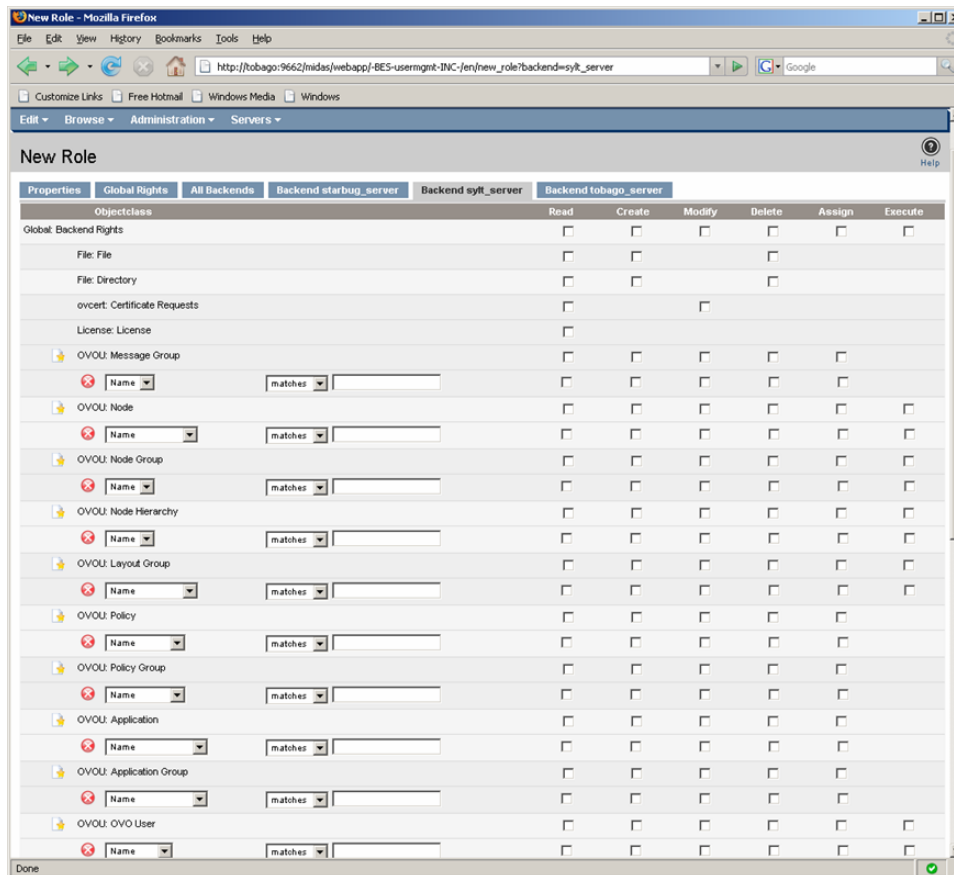
Key benefits

- Provide a web-based application for simplified, efficient configuration of HP OpenView Operations for UNIX.
- Support concurrent use by multiple administrators with different access rights.
- Improve navigation and editing of Operations for UNIX configuration items for better productivity.
- Enable comprehensive Operations for UNIX configuration reporting for increased transparency.
- Leverage easy-to-use configuration synchronization across multiple Operations for UNIX management servers.
- Use policy versioning and comparison capabilities to quickly identify configuration changes and differences.

Powerful features

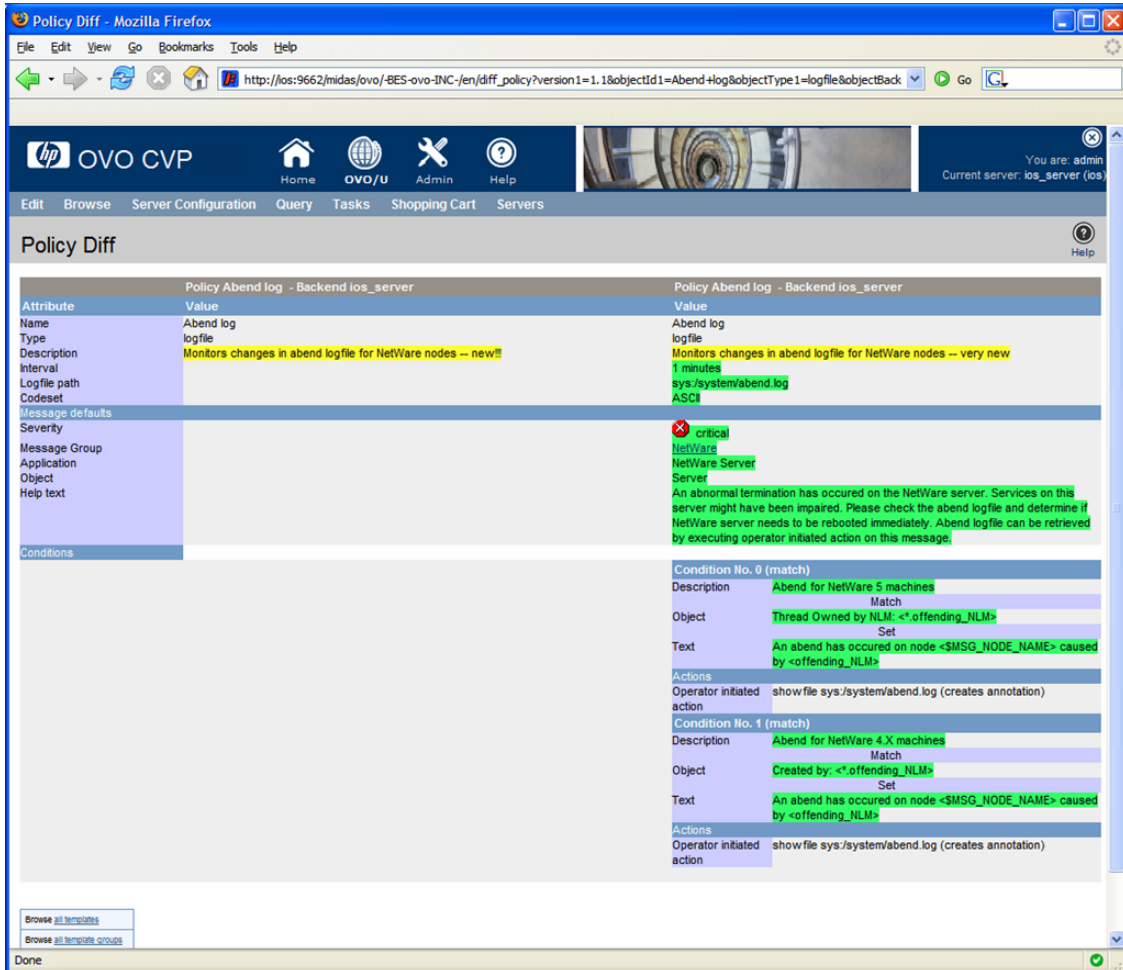
- **Expanded access capabilities**
Operations for UNIX Configuration Value Pack lets you have as many administrators as you need, and each can perform any task at any time according to their access rights. Now your application owners can

enter new nodes into a node group and assign and distribute policies themselves. This not only can cut the total time spent on such tasks, but can also greatly reduce time to market. And all changes can be audited, so you can adhere to compliance guidelines.



- Complete transparency**
 Operations for UNIX Configuration Value Pack gives you total transparency into the Operations for UNIX configuration. Here are just a few examples: See exactly what templates are assigned to a node, whether directly or via a node group; See every template group in which a template is used; See which messages have notification turned on; See which nodes or message groups are not in a responsibility matrix.
- Fast navigation**
 The ability to find the right policy quickly helps busy administrators stay productive. Operations for UNIX Configuration Value Pack gives you multiple methods to do this.
- Simple editing**
 The Operations for UNIX Configuration Value Pack policy editor greatly reduces the number of windows you need to navigate and also lets you open and edit multiple conditions at the same time. The cut, copy and paste functions make it easy to copy policies, conditions or text strings.
- Policy comparison**
 If you have ever had to analyze the difference between two policy versions, you will quickly appreciate the value of the policy comparison function. Select two policies or policy groups either from any active

Operations for UNIX server or from the version control system, and then Operations for UNIX Configuration Value Pack highlights changes, insertions and deletions. It can even show you if a condition has been moved to a new position.



- **Version control**

Developing a monitoring configuration for an application is just the same as developing a software application. There are many policies, scripts and configuration files that need to be there in the right version to enable the right result. Now the version control support in Operations for UNIX Configuration Value Pack makes this simple, providing a seamless integration with your installation of CVS (Concurrent Versions System).

Try it out - request the new Operations for UNIX Configuration Value Pack software media kit, and experience for yourself within a free 60-day evaluation period, how quickly and how much it improves the configuration processes for your Operations for UNIX installation.

OVO/UNIX Configuration Value Pack user documentation is available for download in the Operations for UNIX directory at the following location:

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

For more information about Operations for UNIX Configuration Value Pack features and/or availability, please contact your local HP representative or consult the HP OpenView Operations for UNIX Configuration Value Pack website available at:

www.hp.com/managementsoftware

(Products A-Z > Operations for UNIX > Operations for UNIX Configuration Value Pack)

HP OpenView Smart Plug-ins (SPIs) for OVO for UNIX Update

The November 2006 collection of HP OpenView Smart Plug-ins (SPIs) contain new and enhanced SPIs for versions 7 and 8 of HP OpenView Operations for UNIX. Please note that the media format has changed to DVD - what has previously been available on three separate SPI CDs is now included in one DVD.

New Smart Plug-Ins:

- Storage Essentials SPI
- HP Systems Insight Manager Integration

Updated Smart Plug-Ins:

- Oracle Application Server SPI
- BEA Tuxedo SPI
- BEA WebLogic Server SPI
- Informix
- Oracle
- Microsoft SQL Server
- Sybase
- IBM DB2
- IBM WebSphere Application Server SPI
- Microsoft Exchange Server SPI
- PeopleSoft SPI
- Remedy SPI
- SAP SPI

You can find a short description of each Smart Plug-in and a full product description in the HP OpenView SPI DVD Installation Guide, available by selecting Smart Plug-in DVD for OVO for UNIX at the following website:

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

HP OpenView Performance Agent (OVPA) 4.6 Deployables

HP OpenView Performance Agent Deployables for HP OpenView Operations for UNIX enable the central deployment & control of HP OpenView Performance Agent software on multiple managed systems via HP OpenView Operations for UNIX.

HP OpenView Performance Agent now offers support for heterogeneous virtualized environments: VMware ESX Server, HP-UX HPVM and IBM AIX LPAR. Another key new feature is the support for configurable logging intervals and new threshold-based logging and flush intervals. The new version also offers an enriched set of performance metrics.

Performance Agent 4.6 continues to support datacomm (same as OVPA4.5), ARM, Tools (extract, utility etc.) and the DSI interface. Please refer to Release Notes and other OVPA documentation for a detailed list of the additional features and requirements of version 4.6, available in the Performance Agent directory at the following location:

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

Daylight Saving Time Operations Support

HP is in the process of testing and certifying that current versions of HP Software products will support the DST change. Note that even though HP Software products may support the DST change, you still need to check that supporting software, such as Java, WebSphere, WebLogic and JBoss middleware and your systems' operating systems, supports the DST change as well.

OVO/UNIX Java UI already provides support for the daylight saving time. For the Windows platform, a JRE is bundled that supports the Daylight Savings Time change, for other OVO/UNIX Java UI platforms, refer to "Support for Daylight Saving Time Change in Year 2007" on page 109.

For more information on other products' support for daylight saving time operations, refer to the following website:

http://support.openview.hp.com/daylight_operations.jsp

New and/or Updated Documentation

The following new and/or updated user documentation is available:

Dedicated Installation Guides for OVO/UNIX with HP Serviceguard

Two new dedicated installation guides are available for users installing OVO/UNIX in an HP Serviceguard cluster using the basic OVO/UNIX installation scenario with a local database. Installation guides for HP-UX PA-RISC and HP-UX Itanium are available for download from the following location:

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

HTTPS Agent Concepts and Configuration Guide

An updated OVO HTTPS Agents Concepts and Configuration guide with comprehensive information on the possibility to restrict access rights and roles is available for download from the Operations for UNIX directory at the following location:

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

Deploying OVO HTTPS Agents Using Radia Whitepaper

A new whitepaper detailing instructions for installing and deploying OVO HTTPS agent for Windows using Radia is available for download from the Operations for UNIX directory at the following location:

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

Using ECS Designer Remotely Whitepaper

A new whitepaper detailing instructions on developing ECS Designer circuits on supported platforms and using them on other platforms is available for download from the Operations for UNIX directory at the following location:

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

New Announcements with Release Notes Edition 13

OVO/UNIX 8.24 Management Server Patch

OVO Management server patch is available for all supported OS platforms.

Table 1-1 Management Server patch 8.24

Patch Name	Management Server Platform		
	HP-UX PA-RISC	HP-UX Itanium	Solaris
OVO8 consolidated server 8.24	PHSS_35526	PHSS_35525	ITOSOL_00538

High Availability through OVO/UNIX Server Pooling Whitepaper

A new whitepaper is available for download to help you set up HP OpenView Operations for Unix Management Server pooling from the following website:

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

Configuring Outbound-Only Communication Whitepaper

OVO/UNIX has been enhanced to provide uni-directional secure communication between OVO management servers and OVO HTTPS agents through multiple firewalls and trust zones. A whitepaper is available for download from the following location:

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

NOTE `ovbbcrp` (Reverse Channel Proxy, RCP) is not supported on Windows HTTPS nodes. To use outbound-only communications with Windows HTTPS managed nodes, please configure those nodes to use an RCP (PROXY) running on a different platform. For further details please refer to the Configuring Outbound-Only Communication Whitepaper.

OVO/UNIX Management Server Enhancements

The following enhancement are available for the OVO/U Management Server:

- Improved Cluster Error Handling and Logging, see page 111
- New command-line tool for handling Custom Message Attributes `opccmachg`, see page 112
- Improved heartbeat monitoring for HTTPS agents

New Support Announcements

OVO/UNIX 8.16 HTTPS Agents

An updated version of the OVO/UNIX HTTPS Agent is available for download for most of the OVO/UNIX Agent supported platforms. Corresponding versions for Tru64 and Solaris for x86 will be provided in the near future. For detailed information refer to See “HTTPS Agent Supported Platforms” on page 70.

An update for the ovprotect security tool is also available for download from the following location:

`ftp://ovweb.external.hp.com/pub/ovprotect`

OVO Agent now also provides container support of Global and Local Zones for the HTTPS agents for Solaris 10.

Management Server Support for Sun UltraSPARC T1 Processor

With the latest OVO/UNIX Management Server patch, the Sun UltraSPARC T1 processor is now also supported with the following OVO/UNIX configuration:

- Oracle 10gR2 (patch level 10.2.0.2)
- NNM 7.51
- OVO/UNIX patch level 8.24

Java UI Enhancements

The following JavaGUI Client patch is available:

Table 1-2 JavaGUI Client Patch 8.24

	Management Server Platform		
Patch Name	HP-UX PA-RISC	HP-UX Itanium	Solaris
JavaGUI client 8.24	PHSS_35791	PHSS_35790	ITOSOL_00541

The following enhancements are available with this patch:

- Customized Message Group Icons, see page 110
- Support for Daylight Saving Time Change in Year 2007, see page 109
- Application HTML Output as an Internal Webpage, see page 111
- Java GUI Connection Port Setting, see page 111
- Introduction of R Flag for Read-Only Messages in Java UI Message Browser, see page 109
- Full Support for INFORM Own Mode in Java UI, see page 109

New Features with OVO/UNIX 8

This section describes the new announcements and features that are available with OVO/UNIX 8 compared with OVO/UNIX 7.

Management Server

This section describes the new announcements and features available on the management server.

Supported Platforms

The following platforms and operating system versions are supported with OVO/UNIX 8, and not with OVO/UNIX 7:

- ❑ HP-UX PA-RISC 11.23
- ❑ HP-UX Itanium 11.23
- ❑ Solaris 10
- ❑ HP Integrity Virtual Machines for the OVO Management Server running in a standalone and clustered configurations

Administration Enhancements

OVO/UNIX administration enhancements include:

- Motif Administrator GUI: Invisible Node Groups to keep user responsibility matrix configuration small, but use additional node group for other OVO Administrator tasks.
- OS-SPI for HP-UX, Solaris, Windows, Linux, AIX and Tru64 OVO DCE agents and OVO HTTPS agent platforms.
- Java API wrappers for *opcmon(3)* and *opcmsg(3)* for HTTPS and DCE agents.
- New APIs for adding, modifying, and deleting custom message attributes for OVO messages that are already stored in the OVO Oracle database.

These APIs are defined in `/opt/OV/include/opcsvapi.h`, their use is illustrated in example `/opt/OV/OpC/examples/progs/itomessage.c`.

The usage of these APIs requires an HP OpenView Operations for UNIX Developer's Toolkit License-to-Use for development support assistance from HP.

Message Counter Feature: Severity and Message Text Updates

OVO/UNIX has expanded the message counter feature for duplicate messages in the Java and Motif UIs. For more information, see page 117.

High Availability Environments

OVO/UNIX 8 supports High Availability environments as listed in "High Availability Environments" on page 61.

OVO/UNIX 8 HTTPS and 7 DCE agents can be used to run on and to manage High Availability environments.

Pluggable Authentication Module (PAM)

Pluggable Authentication Module (PAM) integration to externally authenticate the OVO/UNIX user during login into the Motif UI and the Java UI. This is the alternative to OVO/UNIX's internal authentication based on a username and corresponding password stored in the OVO database.

PAM provides a configuration file where the system administrator of the OVO/UNIX management server can specify the type of authentication mechanism to be used. It is possible to apply various authentication modules, such as UNIX */etc/passwd*, Kerberos, and LDAP.

NOTE Due to missing HP-UX Operating System patches, the PAM/Kerberos module is not yet officially certified with OVO/UNIX 8.

Deployable OV Performance Agent

With OVO/UNIX 8, Deployable OVPA versions 3.x and 4.5 are supported. Deployable OVPA 4.5 packages are available for OVO/UNIX 8 as part of the OVO/UNIX 8 media kit update as of January 2006 and also support HTTPS communication.

- Support for the following agent platforms is available.:
HP-UX, Solaris, Windows, Linux, AIX, and Tru64.

This release of the OVPA deployables for OVO/UNIX 8 Management Servers integrates the ability to deploy OVPA to the following platforms:

Table 1-3 Deployable Performance Agent Support

Managed node platform	Management server platform	
	HP-UX	Solaris
HP-UX OVO/UNIX 7 (DCE) and OVO/UNIX 8 (HTTPS)	OVPA C.04.50.00	OVPA C.04.50.00
Solaris OVO/UNIX 7 (DCE) and OVO/UNIX 8 (HTTPS)	OVPA C.04.50.00	OVPA C.04.50.00
Linux OVO/UNIX 7 (DCE) and OVO/UNIX 8 (HTTPS)	OVPA C.04.50.00	OVPA C.04.50.00
AIX OVO/UNIX 7 (DCE) and OVO/UNIX 8 (HTTPS)	OVPA C.04.50.00	OVPA C.04.50.00
Tru64 OVO/UNIX 7 (DCE) and OVO/UNIX 8 (HTTPS)	OVPA C.03.60.00 or OVPA C.03.61.00 OVPA C.04.50.00	OVPA C.03.60.00 or OVPA C.03.61.00 OVPA C.04.50.00

Table 1-3 Deployable Performance Agent Support (Continued)

Managed node platform	Management server platform	
	HP-UX	Solaris
Windows OVO/UNIX 7 (DCE) and OVO/UNIX 8 (HTTPS)	OVPA C.04.50.00	OVPA C.04.50.00

NOTE What OVPA version is installed depends on the DCE version installed on the Tru64 managed node. For more information, refer the release notes of OVPA/Tru64 C.03.60.00 or C.03.61.00.

This release of OVPA deployables also provides templates, commands, and actions for Openview performance agent group for the following managed nodes:

- HP-UX (HTTPS & DCE)
- Solaris (HTTPS & DCE)
- Linux (HTTPS & DCE)
- AIX (HTTPS & DCE)
- Tru64 (DCE)

Refer to OVPA documentation for more information.

ECS 3.31 - 3.33 Runtime Support

ECS 3.31 - 3.33 run-time files are supported on OVO/UNIX management servers and Solaris, HP-UX, and Microsoft Windows managed nodes.

OV Composer 3.31/3.33 Support

OVO 8 comes with a completely new integration module for OV Composer 3.31, HP's easy and free-of-charge component for event correlation. OV Composer 3.33 is offered with NNM 7.5. For more information, refer to the *OVO Administrator's Reference*.

ECS 3.2 Designer Support

ECS 3.2 Designer is supported for HP-UX 11.11, and for Solaris 8 and 9. See "What's Not Supported" on page 55 for more information about platforms which are *not* supported by ECS Designer.

Localized Support for Japanese, Korean, Simplified Chinese and Spanish

With OVO 8 the localized support in the following languages is supported:

- Japanese
- Korean
- Simplified Chinese
- Traditional Chinese
- Spanish

The extent of this support is detailed in the following tables as it is not the same for all languages.

Table 1-4 Localized Software and Online Help

Locale		English	Japanese	Korean	Simplified Chinese	Spanish
Java UI and OLH		✓	✓	✓	✓	✓
Motif UI and OLH		✓	✓			
Man Pages		✓				
Installation		✓	✓	✓	✓	✓
HTTPS Agent Message Catalogs	Event Action	✓	✓	✓	✓	✓
	Embedded Performance Agent	✓				
DCE Agent Message Catalogs	Event Action	✓	✓			
	Embedded Performance Agent	✓	✓			
Encoding/Database Character Set		ISO-885915 WE8ISO8859P15	Shift-Jis JA16SJIS	eucKR KO16KSC5601	hp15CN ZHS16CGB231280	ISO-885915@euro WE8ISO8859P15

NOTE Updated localized Java UI online help is not available on the OVO/UNIX 8.20 CDs, but is provided with a dedicated patch for the Java UI online help (see Table 1-5), for all supported languages stated in the Table 1-4.

Table 1-5 JavaGUI OLH Patch

Patch Name	Management Server Platform		
	HP-UX PA-RISC	HP-UX Itanium	Solaris
JavaGUI Online Help Patch 8.21	PHSS_34598	PHSS_34597	ITOSOL_00506

Table 1-6 OVO/UNIX Related Manuals and Whitepapers

Locale	English	Japanese	Korean	Simplified Chinese	Spanish
<i>Installation Guide for the Management Server</i>	Aug 06	Feb 06			
<i>Basic Installation Scenario with Local Database for HP Serviceguard Cluster Installation Guide</i>	Feb 07				
<i>OVO Concepts Guide</i>	Dec 05	Feb 06	Nov 05	Nov 05	
<i>OVO Administrator's Reference</i>	Oct 06	Feb 06	Nov 05	Nov 05	
<i>HP OpenView Operations Java GUI Operator's Guide</i>	Aug 06	Feb 06	Nov 05	Nov 05	Feb 06
<i>HTTPS Agent Concepts and Configuration Guide</i>	Feb 07	Feb 06	Nov 05	Nov 05	
<i>DCE Agent Concepts and Configuration Guide</i>	Aug 06	Feb 06			
<i>Service Navigator Concepts and Configuration Guide</i>	Aug 06	Feb 06	Nov 05	Nov 05	

Table 1-6 OVO/UNIX Related Manuals and Whitepapers (Continued)

Locale	English	Japanese	Korean	Simplified Chinese	Spanish
<i>Firewall Concepts and Configuration Guide</i>	Aug 06				
<i>Metrics for HP OpenView Performance Agent and HP OpenView Operations Agent ()</i>	Jan 05				
<i>HP OpenView Performance Agents Metrics Help Text</i>	Jan 05	Oct 04			
<i>OVO Reporting and Database Schema</i>	Dec 05				
<i>OVO Entity Relationship Diagrams</i>	Oct 04				
<i>OVO/UNIX Release Notes</i>	Sept 06 Edition 12	Sept 06 ^a Edition 11			
<i>Master Index</i>	Dec 05	Feb 06	Nov 05	Nov 05	
<i>OVO Application Integration Guide</i>	Sept 04				
<i>OVO Developer's Reference</i>	Aug 06	Feb 06	Nov 05	Nov 05	
<i>Security Advisory Guide^b</i>	✓				
<i>HTTPS Agent Clone Imaging whitepaper</i>	Nov 05				
<i>Dynamic Service Engine Extensions using Perl</i>	Sept 05				
<i>OVO/UNIX Performance Guide^c</i>	Mar 05				
<i>OVO/UNIX Product Support Matrix^d</i>	✓				
<i>Independent Database Server Whitepaper</i>	Sept 06				
<i>HTTPS-based Java GUI Support Whitepaper</i>	Oct 05				
<i>Service Navigator Automatic Actions Whitepaper</i>	Sept 06				
<i>Oracle Real Application Clusters (RAC) Support Whitepaper</i>	Sept 06				
<i>High Availability through OVO/UNIX Server Pooling Whitepaper</i>	Dec 06				
<i>Configuring Outbound-Only Communication Whitepaper</i>	Dec 06				
<i>Using ECS Designer Remotely Whitepaper</i>	Feb 07				
<i>Deploying OVO HTTPS Agents Using Radia Whitepaper</i>	Jan 07				

a. The latest available version of the OVO/UNIX Software Release notes may not be available in languages other than English, yet. Please consult also the English version of the Release Notes until the version in your preferred language is made available.

b. *Security Advisory Guide* is available through <http://support.openview.hp.com/news.jsp>.

c. *OVO/UNIX Performance Guide* is available through <http://support.openview.hp.com/news.jsp>.

d. *OVO/UNIX Product Support Matrix* is available through

http://support.openview.hp.com/sc/support_matrices.jsp

or by following the HP OpenView Support Matrix > HP OpenView Support Matrix - Part 1 - Operations and Service Navigator Value Pack links at

http://partners.openview.hp.com/ovcw/pricing/config_matrix.jsp

NOTE

Check the following web site periodically for the latest versions of localized manuals:

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

Miscellaneous

❑ **\$AGENT_USER**

Instead of hard coding a user name in a preconfigured application, you can set the `$AGENT_USER` variable. This allows you to always execute the application under the same user as the OVO agent.

❑ **Other New Variables**

The following variables allow you to use the template name, condition name and condition number in a message. These variables can be used for logfile monitoring, SNMP trap interception and the OVO message interceptor.

- `$CONDITION_NAME`
- `$CONDITION_NUMBER`
- `$TEMPLATE_NAME`

Using these variables, for example, filled into Custom Message Attributes, will enable you to quickly identify the matched template and condition numbers for situations where you want to refine your current configuration in a subsequent step.

NOTE These variables cannot be applied to Advanced Monitoring and the monitor agent.

❑ **New opctemplate Output for HTTPS Nodes**

The `opctemplate` listing format is changed for HTTPS nodes.

For example, for an HTTPS node, the output of the command:

```
opctemplate -l
```

takes the following format:

```
'configsettings' 'OVO settings' enabled  
'le' 'Cron (10.x/11.x HP-UX)' enabled  
'le' 'OSSPI-HPUX-BadLogs_1' enabled  
'le' 'OSSPI-HPUX-Boot_1' enabled
```

On a DCE node, the format remains as follows:

```
LOGFILE "perftest" enabled  
LOGFILE "tobi-test" enabled  
LOGFILE "dynamic-log" enabled  
LOGFILE "readbegin" enabled  
LOGFILE "close-test" enabled
```

NOTE `opctemplate` on HTTPS agents is only a wrapper for `ovpolicy`, but `opctemplate` does NOT list the `mgrconf` file as a policy when you are running OVO in a Flexible Management Server (MoM) environment.

❑ **File Permissions Remain Unchanged for HTTPS Agents**

Files deployed to HTTPS managed nodes retain their original permission after deployment using `opcdeploy` or `ovdeploy`.

Deployment to a DCE agent using `opcdeploy` or `opctranm` also changes the permissions to 600. These files cannot be executed on the managed node system before the appropriate permissions are set. To change the permissions, call `opcdeploy` or `opctranm` again (or define it in the `opctranm` truck file) with the corresponding `chmod` call.

HP OpenView Network Node Manager 7.51 Support

HP OpenView Network Node Manager 7.51 is certified for OVO 8. For more information about NNM 7.51, refer to the documents linked below:

NOTE It is very important that you consult the Migration Guide For Network Node Manager (NNM) 7.51 before migrating. There are some additional steps necessary if you are using Extended Topology or the dupip functionality in NNM.

IMPORTANT OVO/U management server URLs are inaccessible when NNM 7.51 patch is installed. See “Installation and Upgrade” on page 80 for instructions on resolving the problem.

❑ *What's New in Network Node Manager 7.51 and HP OpenView Network Node Manager 7.5 Runtime Release Notes* are available from:

http://ovweb.external.hp.com/ovnsmdp/pdf/nnm751_rlsnt/

❑ *Migration Guide For Network Node Manager (NNM) 7.51* available from:

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

Supported Migration Paths

- ❑ Install OVO for UNIX 8.10 on top of a stand-alone NNM 7.51 installation.
- ❑ Migrate OVO for UNIX 8.10 with NNM 7.01 installation to NNM 7.51.
- ❑ Migrate OVO for UNIX 7.1x with NNM 7.01 installation to OVO 8.10 with NNM 7.51.

Java UI Enhancements

Below you will find a list of Java UI enhancements in OVO/UNIX. For a complete description of Java UI functionality please read the HP OpenView Operations Java GUI Operator's Guide available from the OVO/UNIX CD or http://ovweb.external.hp.com/lpe/doc_serv/.

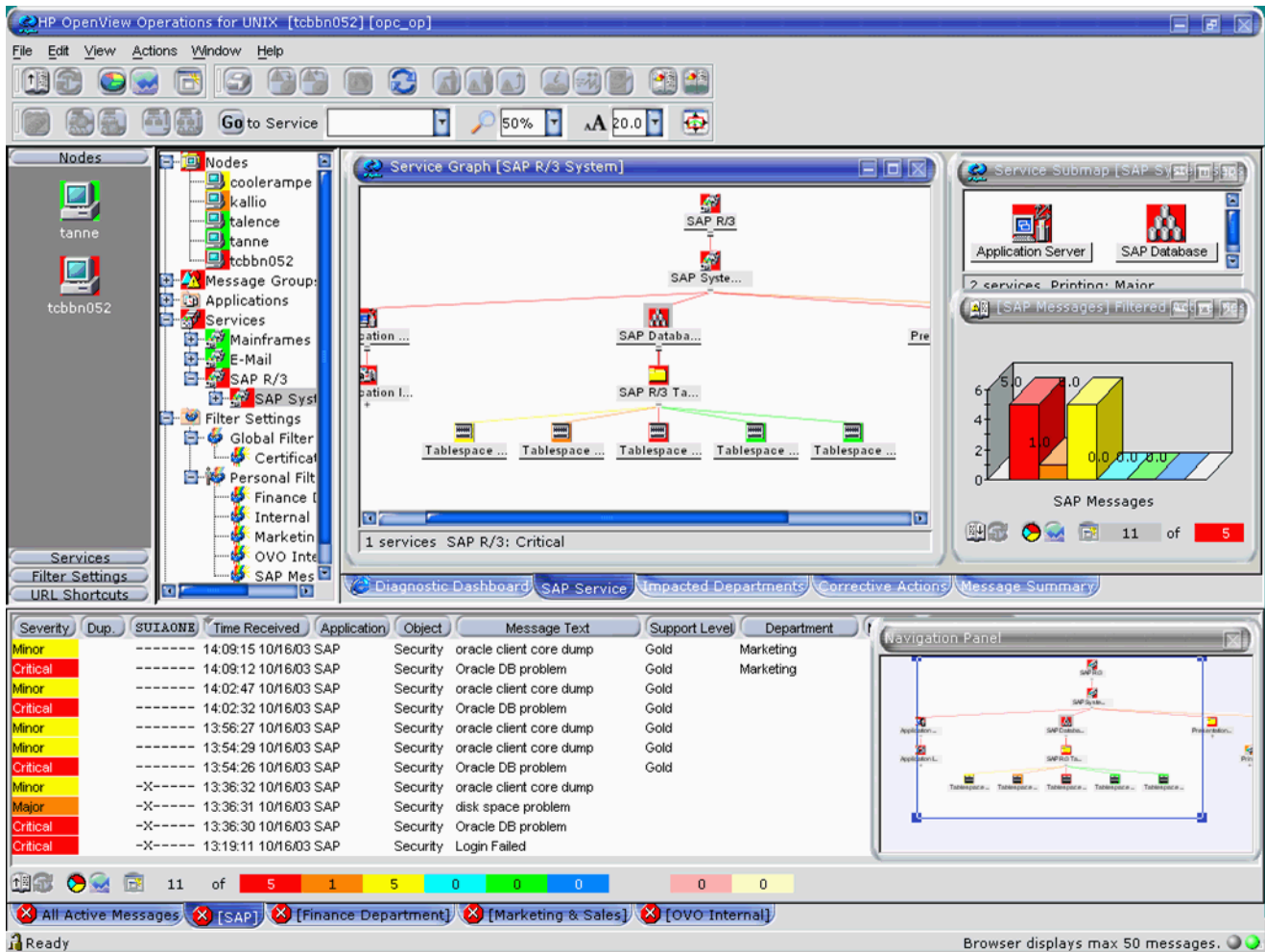
- Changed Behavior of the Java GUI ‘Lock’ Feature, see page 120
- The HTTPS-based Java GUI can be configured without the need for having the core agent installed on the Java GUI client. For more information about how to configure the port for the HTTPS-based Java GUI, refer to the following OVO/UNIX manuals: *Java GUI Operator's Guide* and *Administrator's Reference*, as well as to the *ito_op.Im* man page
- OVO Java GUI is able to reconnect to one or more backup management servers in case of server failure. For information about configuring backup management servers by setting one or more variables, refer to the OVO/UNIX *Administrator's Reference* guide

- Local Java GUI Configuration Files Loaded Before Global QXCR1000310425, see page HIDDEN
- Setting up HP OpenView Operations Service Navigator automatic actions, which are triggered upon a service status change, see *OVO/UNIX Service Navigator Automatic Actions Whitepaper*
- Auditing for Service Navigator, see page 120
- opcwall utility for Java GUI
- Acknowledging messages with bulk operations
- Separating message fields with tabs. See “Separating Message Fields with Tabs” on page 119
- HTTPS-based Java GUI support. For more information, refer to the *OVO Administrator’s Reference manual*.
- Graphical objects can be displayed as part of the OVO message in the Event Browser.
- Customizeable tool bar, for example, different areas for messages, message browser, services; additional tool bar options & buttons; customizeable layout.
- Remote APIs¹, for example for context-sensitive launch of applications such as the OVO Message Browser, and service tree.
- Drag and drop operations inside the Java GUI and on other applications on the system.
- Custom Message Attributes customization of OVO messages: add, modify and delete.
- Support of Cocoa style for Mac OS platform.
- Alignment of column content in Java UI Message Browser
- Customize Browser Layout via pop-up menu in Message Browser
- Proxy authentication in Java UI
- Message field sorting enhanced to support numerical data
- New Java UI Key Accelerators
- Customizing animated GIF images
- Different number of messages for active and history message browser
- Ability to use global Java GUI property files
- Ability to cancel loading of history messages
- Saving the Java UI settings while using the global Java UI settings
- Displaying URLs as hyperlinks in message browser columns and the Message Properties dialog box
- Forwarding Manager field in Java GUI
- Popup and menu item for creating a new history filter on the selected message
- Allowed users local configuration files loaded before the global configuration

1. The usage of these APIs requires an HP OpenView Operations for UNIX Developer’s Toolkit License-to-Use for development support assistance from HP.

- Setting up HP OpenView Operations Service Navigator automatic actions

Figure 1-1 JavaGUI Screenshot



Operational Service Views in the Java GUI

Service Navigator allows you to define dependencies among services. From the underlying messages in OVO/UNIX, it establishes a service hierarchy and assigns responsibilities to operators. You can then see the current service status in the Java GUI.

Until OVO/UNIX 8, each service in Service Navigator (SN) reflected only one status at a time. All messages in the active message browser were considered for the status calculation of services.

You can visualize more than one state per service and provide information to suit different users. For example:

- IT Managers may want to see service states which reflect the actual health of the managed environment including business services.
- Operators using Service Navigator Java GUIs may only want to see issues which are not already owned and being addressed by other operators.

With OVO/UNIX 8, there is an additional status, *Operational*, for services calculated from a set of messages, based on a different set of rules. The calculation only considers active messages that are NOT currently owned by operators. This means that services can be simultaneously made to display two statuses, based on a different set of messages, and possibly reflecting two different severities.

You can monitor and work with services displayed in the following two status calculation views:

❑ **Overall**

The service status view based on all messages present in the active message browser.

The Overall status calculation view displays these services in the same way, irrespective of the targeting message ownership status. In this example, these services are colored red. You can observe this in the object pane, service graph or map, and in the shortcut bar. When you take the ownership of the message, the severity of the service does not change until the message is acknowledged.

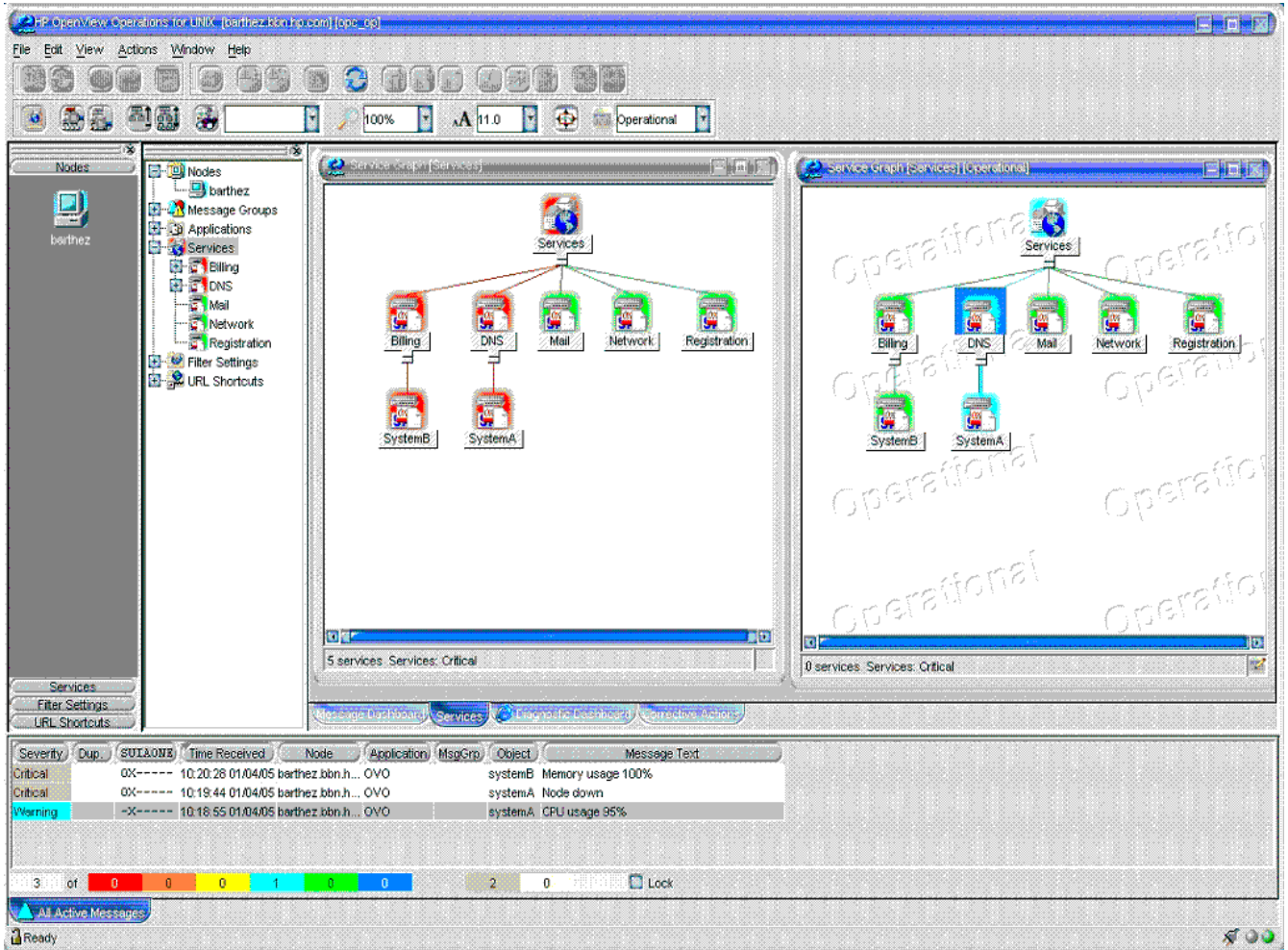
❑ **Operational**

The service status calculation view based on only non-owned messages present in the active message browser.

If your status calculation view is set to *Operational* and you take ownership of the message, the severities of the targeted service and all dependent services change back to the severity visible prior to the message arrival.

The benefit of the service operational view is that you can get an insight of how the service hierarchy would look if the message targeting a service is acknowledged, in other words, if the problem is solved. This is very useful, especially, if you monitor your services in both calculation views simultaneously as shown in Figure 1-2 on page 28.

Figure 1-2 Using Operational Service Views



For further information, refer to the HP OpenView Operations Java GUI Operator’s Guide available from the following location:

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

Oracle Database

This section describes the features related to the OVO database.

Table 1-7 presents the supported Oracle database versions for HP-UX PA-RISC.

Table 1-7 Supported Oracle Database Versions on HP-UX PA-RISC

Operating System	Oracle Database 9i Release (or Oracle for OpenView 9.2.0) with 9.2.0.2 Patch Set	Oracle Database 10g Release 1 with 10.1.0.4 Patch Set	Oracle Database 10g Release 2 with 10.2.0.2 Patch Set
HP-UX 11.11	✓	✓	✓

Table 1-7 Supported Oracle Database Versions on HP-UX PA-RISC (Continued)

Operating System	Oracle Database 9i Release (or Oracle for OpenView 9.2.0) with 9.2.0.2 Patch Set	Oracle Database 10g Release 1 with 10.1.0.4 Patch Set	Oracle Database 10g Release 2 with 10.2.0.2 Patch Set
HP-UX 11.23 PA-RISC		✓	✓

NOTE The Oracle compatible parameter specifies the release with which Oracle must maintain compatibility to. By default, ad OVO for UNIX installation wil set the Oracle compatible parameter to 9.2.0.0.0. However, OVO for UNIX can be used with Oracle database 10g in either Oracle 9 compatible mode or native Oracle 10g mode.

Oracle Database 10g Release 1 Support on HP-UX 11.11 and 11.23 PA-RISC

OVO/UNIX supports Oracle Database 10g Release 1 (10.1.0.4 patch level) Standard and Enterprise Edition. See the Installation Guide for the Management Server for more information on installing and using OVO/UNIX with Oracle Database 10g.

Oracle Database 10g Release 2 Support on HP-UX 11.11 and 11.23 PA-RISC

OVO/UNIX supports Oracle Database 10g Release 2 (10.2.0.2 patch level) with OVO/UNIX Management Server 8.22 or higher. See the Installation Guide for the Management Server for more information on installing and using OVO/UNIX with Oracle Database 10g.

Oracle Standard Edition Support

Oracle 9 Standard Edition, licensed for use with up to four-processors, including full clustering support, is supported by OVO/UNIX. All Oracle 9 versions from 9.2.0.2 are supported.

Independent Database Support

It is possible to install and configure the Oracle database used by the OVO/UNIX management server in a cluster environment on a different node in the cluster, in a separate cluster, or on a remote system. For a decoupled database installation, the OVO 8.11 patches or superseding must be installed during the management server installation. These patches are recommended for all installations as they contain some general improvements.

For more information about setting up OVO/UNIX with an independent database server in a clustered or non-clustered environment, see also the *OVO/UNIX Independent Database Server Whitepaper*.

There are three different installation possibilities:

Basic management server configuration

The OVO/UNIX management server *and* the Oracle database server are installed on the *same system* or are part of the *same HA resource group* in a cluster environment.

Independent database server configuration

The Oracle database server can be independently configured:

- On a remote system or on an different HA installation to the OVO/UNIX cluster.
- On the same cluster as the OVO/UNIX management server, but not configured as an HA resource group in OVO/UNIX.

❑ Decoupled (3-Tier) management server configuration

The OVO/UNIX management server and the Oracle database server are configured as separate HA resource groups in a single cluster environment.

Configuration Scenario	Basic		Independent		Decoupled
	Standard	HA	Standard	HA	HA
Database Installation	On OVO/UNIX Management Server System	Part of the OVO/UNIX Management Server HA resource group	On a dedicated remote system	On a dedicated remote system, preferably a remote cluster	As separate HA resource group on the OVO/UNIX Management Server system

For further information, refer to the latest version of the *HP OpenView Operations Installation Guide*, available from the following location:

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

If you want to use the new flexible database installation options, the OVO Management Server 8.11 or superseding and the appropriate Core Agent patches must be installed during the management server installation. Refer to the section entitled Installing the OVO Software on the Management Server in the *Installation Guide for the Management Server* for patch installation guidance. The Installation Guide has been updated to reflect the flexible database installation options and can be downloaded from the OpenView documentation web site:

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

Select Operations for UNIX and version 8.x.

All other functionality can be accessed by installing the appropriate patches on the OVO management server and Java GUI client system.

OVO/UNIX 8 and Independent Database Server on Different Operating Systems

HP OpenView Operations can be set up with an independent Oracle Database so that the OVO Management Server and the independent Oracle Database server systems run on different operating systems, as long as the Oracle Database version and the database server operating system are supported also by the OVO for UNIX Management Server.

Both Oracle 9i and 10g are supported in this setup with limitations for certain operating system versions.

Since OVO/UNIX 8 Management Server on HP-UX 11.23 and higher supports only Oracle 10g, the independent Oracle Database server version for OVO/UNIX on HP-UX 11.23 and higher is limited to Oracle 10g. OVO/UNIX Management Server on other supported HP-UX platforms supports both Oracle 9i and 10g in this setup.

For more information, refer to the *OVO/UNIX Independent Database Server Whitepaper*, available from the following location:

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

Oracle Real Application Clusters (RAC) Support

OVO/UNIX also offers support for Oracle Real Application Clusters (RAC) with Oracle 10g Release 2 (patch level 10.2.0.2) running as an independent database server.

Oracle RAC is a highly available, scalable and manageable solution for sharing access to a single database among managed nodes in a cluster environment.

For more information about using OVO/UNIX with an independent database server on Oracle RAC, please consult the *Oracle Real Application Clusters (RAC) Support Whitepaper*, available from the following location:

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

Oracle RAC server requirements are described in the Oracle RAC documentation available from the following location:

<http://www.oracle.com/technology/documentation/database10gR2.html>

Service Navigator

This section describes the new announcements and features available for Service Navigator.

Service Navigator Enhancements

Service Graph Navigation enhancements include:

- Navigation panel.
- Zooming.
- Service icon positioning and dragging.
- Service line selection marking.
- Lasso selection.
- Dynamic and multi-line service labels which can be set using the `opcsvcattr(1)` command line interface.
- Multi-line service labels that can also incorporate graphics.
- Auditing for Service Navigator

Figure 1-3 Service Navigator Screenshot

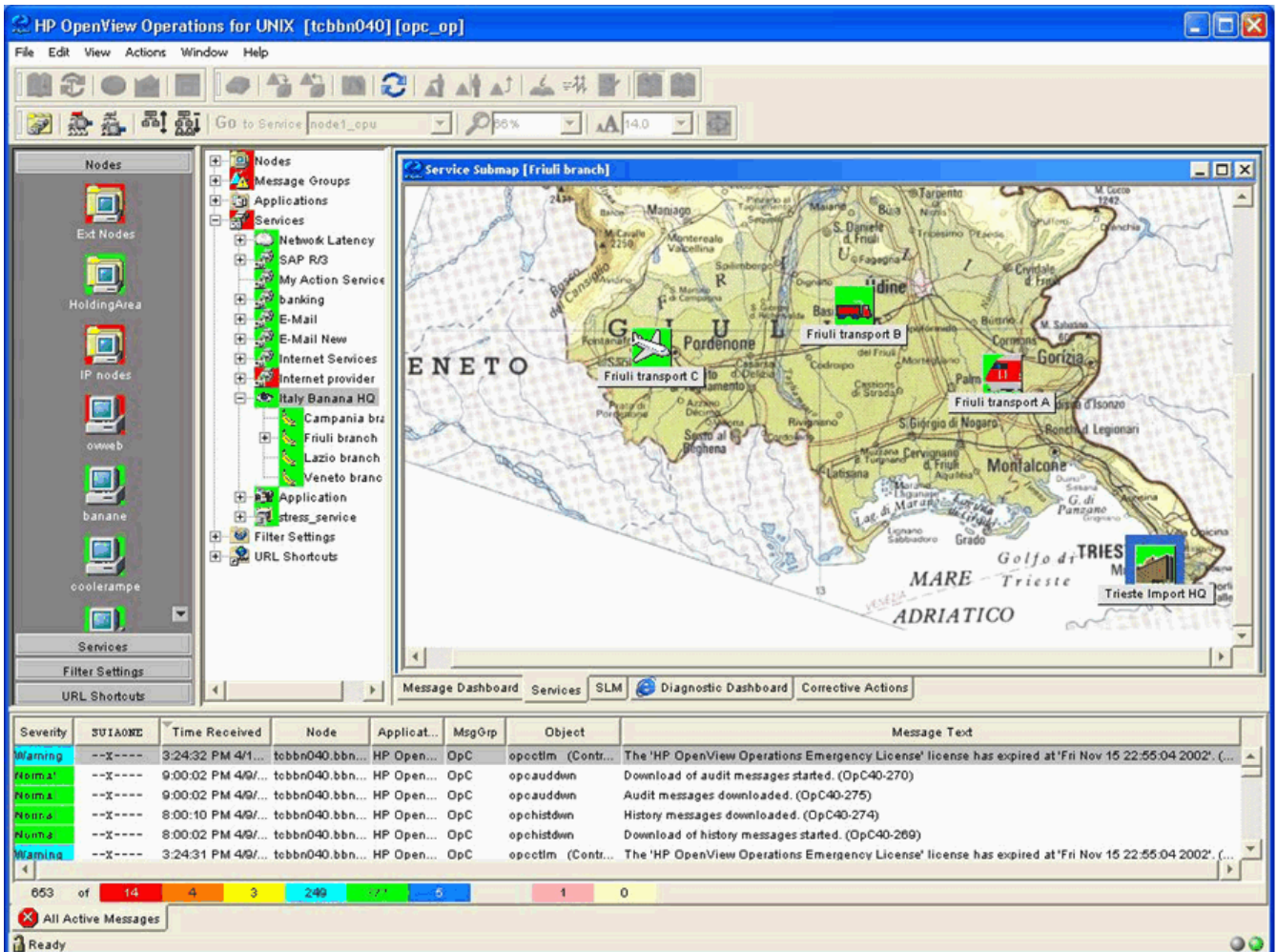
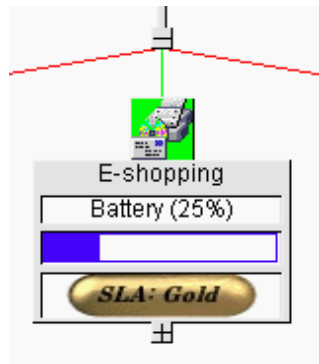


Figure 1-4 Multi-Line Service Label



Allowing Dynamic Configuration Changes in Service Navigator

It is possible to program the OVO/UNIX Service Engine to allow dynamic configuration changes, for example in Service Navigator.

For more information, refer to the *Getting Started with XML/Perl Programming for the OVO Service Engine* whitepaper, available at the following location:

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

Service Navigator Value Pack Support

Service Navigator Value Pack (SNVP) 9.0 is built for use with Service Desk version 5, patch level SD SP1. This version of the SNVP software is easier to install due to the introduction of a single step installation using HP OpenView Installer. Moreover, a new Web Console integration type, introduced with SNVP 9.0, lets you launch Service Desk Web Console from within Service Navigator. SNVP 9.0 also offers an URL support for service icons and backgrounds, copy and paste within a service hierarchy, zooming a map view of services, and so on. For more information about the SNVP 9.0 benefits, refer to the HP OpenView Service Navigator Value Pack Release Notes available for download at:

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

SNVP 8.0 and 9.0 with Oracle 10g Release 2

SNVP 8.0 supports Oracle 10g Release 2 database. The following conditions apply:

- Latest SNVP service pack must be installed; SNVP patch level 8.13 or higher.
- Only Oracle patch level 10.2.0.2 or later is supported.

SNVP 9.0 supports Oracle 10g Release 2 database. The following conditions apply:

- Only Oracle patch level 10.2.0.2 or later is supported.

HTTPS-Agents

With OVO 8, the new HTTPS-Agent software is available for highly secure communication between OVO/UNIX management servers and the managed nodes. HTTPS agent platforms and latest HTTPS agent patches are listed in Table 3-1, “OVO 8 HTTPS Agent Versions from OVO Media Kit and Latest,” on page 70.

The OVO HTTPS agents are developed on new and modern architecture, using several of the new OpenView Common Management Environment (CME) components, including HTTPS communication, control and deployment, and the standardized logging and tracing module. For further details, refer to the new *HTTPS Agent Concepts and Configuration Guide*.

Single-Port Communication

OVO/UNIX 8 allows a configurable, single-port, secure communication to and from the HTTPS agents. This restricts outside access to dedicated HTTP proxies and reduces port usage by multiplexing over HTTP proxies.

OVO/UNIX 8 can also be configured to use outbound-only communication with uni-directional secure communication between OVO management servers and OVO HTTPS agents through multiple firewalls and trust zones.

Windows Installation Server

Windows installation server for OVO HTTPS Windows agents is supported.

NOTE The agent must run as a domain administrator to allow access to the installation server functionality.

This is not as secure as running under the SYSTEM account.

Cluster Awareness for HTTPS Agents

The OVO HTTPS agent supports the concept of virtual nodes and applications running in a high-availability environment. For more details, refer to the *HTTPS Agent Concepts and Configuration Guide*.

DHCP Support for HTTPS Agents

The OVO HTTPS agent can be set up on managed nodes receiving dynamically assigned IP addresses using DHCP. For more details, refer to the *HTTPS Agent Concepts and Configuration Guide*.

SNMP Trap Interception for OVO/UNIX Agents

Most currently available OVO/UNIX agent platforms support SNMP trap interception, including Linux DCE and HTTPS agent platforms.

OVO/UNIX Agents Running as "Non-Root"

HTTPS, as well as 7 DCE¹ agents, can be run under an alternative user to the privileged user.

NOTE This feature is not available for the Windows agent, which must always be run under the SYSTEM account, except for Installation Servers which must be run as a Domain Administrator.

NOTE For both the DCE and HTTPS agent, the actual executing user for operator-launched applications will always be mapped to the current agent user, in case the OVO/UNIX agent runs as non-root.

Refer to the *HP OpenView Operations HTTPS Agent Concepts and Configuration Guide* for further details.

Multiple OVO/UNIX Configuration Servers

The HTTPS agents are able to intercept configuration data from multiple OVO/UNIX 8 management servers. For example, a dedicated OVO server acting as SAP competence center deploys *only* SAP-related policies and instrumentation, while another OVO server is responsible for other tasks. For details refer to the *HTTPS Agent Concepts and Configuration Guide*.

-
1. The OVO/UNIX 7 agents are generically referred to as DCE agents in this document. This usually includes all non-HTTPS OVO/UNIX agents, including those using the following protocols:
 - Distributed Computing Environment (DCE)
 - Network Computing System (NCS)
 - SunRPC

SNMP Trap Interception on Linux DCE Nodes

SNMP Trap Interception is supported on Linux nodes running the OVO 7.1x agent. This support is available with the OVO 7.29 agent patch or superseding.

Common Criteria EAL-2 Certification

OVO/UNIX is certified to comply with the Common Criteria EAL-2 guidelines. For an overview of the security aspects of OVO, refer to Chapter 11, “About OVO Security”, in the *OVO Administrator's Reference* and the OVO/UNIX Security Advisory Guide, available through <http://support.openview.hp.com/news.jsp>.

For more details about OVO/UNIX and Common Criteria, refer to the following link:

http://niap.bahialab.com/cc-scheme/st/ST_VID10011.cfm

opcdelmsg Troubleshooting Utility

opcdelmsg utility removes a single message out of the OVO database without accessing the database directly.

The following is the opcdelmsg syntax:

```
opcdelmsg [ -help ] | [-o] [ -u <user_name> ] <msg_id> [<msg_id>...]
```

Where msg_id (message id) is used for message identification.

See opcdelmsg man page for more details on this utility.

Handling IP node and non-IP node with the same node name

A new configuration parameter OPC_NEW_NAMERES has been introduced to handle IP nodes and non-IP nodes with the same name as a single node. If the parameter is set to TRUE, the following behavior is activated:

- OVO treats the IP node and the non-IP nodes with the same name as a single node.
- Non-IP node names are also converted to lowercase if the OPC_USE_LOWERCASE parameter is set to TRUE.
- `opcdbidx -lower` converts non-IP nodes to lowercase.
- A new configuration parameter OPC_NEW_NAMERES_NO_LOOKUP: if set to TRUE, dblink (and opcmsgm) will not contact the name service for any node. The node name and IP address from the agent are taken as they are.

Changed Features

This section lists existing functionality that has changed from OVO 7.1x.

Installation of OVO Management Server

It is much easier to install the OVO management server. The `ovinstall` utility guides you through the entire installation process.

NOTE Do *NOT* install OVO using the Software Distributor UI or directly through the `swinstall` command line.

On HP-UX, the concept of a central depot server is no longer supported. However, you can use NFS-mounted file systems to install the OVO/UNIX software, provided that your network has fast NFS response times.

Configuration Settings on the OVO Management Server

The OVO management server no longer uses the `opcsvinfo` configuration file.

Management server configuration is based on the new OpenView Common Management Environment (CME) components using `ovconfget(1)` and `ovconfchg(1)`.

For example to set the limit of messages that are acknowledged directly to 1, you use:

```
ovconfchg -ovrg server -ns opc -set OPC_DIRECT_ACKN_LIMIT 1
```

Configuration Settings on HTTPS Managed Nodes

The OVO HTTPS agents no longer use the `opcinfo` and `nodeinfo` configuration files. The local HTTPS agent configuration is based on the new OpenView Common Management Environment (CME) components using `ovconfget(1)` and `ovconfchg(1)`. For details, refer to the *HP OpenView Operations HTTPS Agent Concepts and Configuration Guide*.

In case a variable is not explicitly set in a node's configuration, the command:

```
opcragt -get_config_var <name_space>:<variable_name> <node>
```

will return empty.

The node will still use default values if available. If the node is a DCE node, the same command will show the used default setting.

If you want to set specific values for a selected process, the `opcragt` syntax is different for HTTPS and DCE agents.

For example, for HTTPS agents:

```
opcragt -set_config_var eaagt.opcacta:MAX_NBR_PARALLEL_ACTIONS=100 <nodename>
```

This value is set for the action agent `opcacta` alone in namespace `eaagt.opcacta`.

The syntax for DCE managed nodes is:

```
opcragt -set_config_var 'MAX_NBR_PARALLEL_ACTIONS(opcacta)=100' <nodename>
```


OVO Message Variables Passed into Instruction Text Parameter

The default behavior of the handling of message variables that are passed as parameters to an instruction interface has been changed.

The old behavior was that the variables were replaced by the attributes of the original message. For example, if you call:

```
opcmsg msg_t=hello
```

<MSG_MSG> is replaced by the value that has been specified in the `set` area of the condition, for example, "This is a hello message."

The new behavior can be changed back to the old behavior by setting `OPC_SET_MSGVARS_FROM_ORIGMSG` to `TRUE`.

Examples

Change to the old behavior for all agent processes:

```
ovconfchg -ns eaagt -set OPC_SET_MSGVARS_FROM_ORIGMSG TRUE
```

Change to the old behavior for the `opcmsgi` process only:

```
ovconfchg -ns eaagt.opcmsgi -set OPC_SET_MSGVARS_FROM_ORIGMSG TRUE
```

Remote Actions Authorization

OVO 8 has improved remote action execution authorization. By default, remote automatic actions from HTTPS nodes are allowed, but remote automatic actions from DCE managed nodes are disabled. In order for SPI discovery to work, you must explicitly enable that the managed DCE node or all nodes in the SPI node group are allowed to execute actions on the OVO management server system.

By default all remote actions from DCE nodes are denied on the OVO 8 management server. This also includes operator-initiated actions where the target node and the node which sends the message are the same. If needed, this restriction can be weakened by using the "self-rule". It allows in particular "local" operator-initiated actions.

In general: the security check is successful, if message sender and action target are identical. The "self-rule" is only useful for DCE nodes. The rule is sufficient, to run most of the SPIs for DCE agents (all except the ones which require an action to be executed on the management server).

Here an example for such a rule:

```
<rule>
  <doc>allow DCE local operator action</doc>
  <if>
    <target>
      <self/>
    </target>
    <certified>>false</certified>
  </if>
  <allow/>
</rule>
```

For details see the *Remote Action Authorization* section in the *HTTPS Agent Concepts and Configuration Guide*.

HTTPS Managed Nodes Policies

Policies are no longer encrypted, but signed. As superuser, you can read them directly. All templates of the same type are stored in one directory instead of one file.

There is a file for the policy header in XML (<UUID>_header.xml) and the policy body (<UUID>_data). The header basically contains information that is also in the body. To view the template as it would have been in OVO 7, just view the UUID_data file. The policies are stored under following directories:

nodeinfo Templates	\$OvDataDir/datafiles/policies/configsettings/
Logfile Templates	\$OvDataDir/datafiles/policies/le/
MoM Templates	\$OvDataDir/datafiles/policies/mgrconf/
Monitor Templates	\$OvDataDir/datafiles/policies/monitor/
opcmmsg Templates	\$OvDataDir/datafiles/policies/msgi/
SNMP trap Templates	\$OvDataDir/datafiles/policies/trapi/

No Remote Access to the Service Engine

By default, remote access to the service engine is disabled.

To allow remote access to the service engine, make the following configuration changes:

1. Enter the following line in the `/etc/services` file:

```
opcsvcterm 7278/tcp # Service engine remote access
```

2. Enter the following line in the `/etc/inetd.conf` file:

```
opcsvcterm stream tcp nowait root /opt/OV/bin/OpC/opcsvcterm opcsvcterm
```

3. Restart the `inetd` process:

```
inetd -c
```

Locally Managed Tablespaces

OVO creates the database using Oracle locally managed tablespaces instead of dictionary managed tablespaces.

Error Logging

OVO 8 uses the common OpenView logging. The errors are no longer logged to the `opcerror` file, but to the following log files:

Binary \$OvDataDir/log/System.bin

ASCII \$OvDataDir/log/System.txt

The HTTPS agent and management server use the same location.

Tracing

OVO 8 uses the common OpenView tracing. For further information about common OpenView tracing, refer to the *Tracing Concepts and User's Guide*. For OVO-related tracing details, refer to the latest *HTTPS Agent Concepts and Configuration Guide*, which can be downloaded from the following website:

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

OVO-SunMC Integration Kit

OVO-SunMC integration kit is shipped with the OVO/UNIX SPI CD and is no longer part of the management server depot.

Refer to OVO/UNIX SPI CD Release Notes for details about the OVO-SunMC integration kit.

The OVO/SunMC Instegration Kit is not yet available for OVO/UNIX on HP-UX Itanium.

Default Templates for AIX, HP-UX, Linux, Sun Solaris, Tru64, and Microsoft Windows

The default templates for AIX, HP-UX, Linux, Sun Solaris, Tru64, and Windows are no longer shipped with OVO 8. This functionality is replaced by the Smart Plug-ins for Operating Systems, which are regularly updated and shipped on the frequently-released OpenView SPI CD.

NOTE The OS-SPI includes a dedicated Release Notes document. Read this document before installing.

NOTE Instrumentation for the remaining supported OVO 7 DCE platforms - such as Novell Netware, MPE/iX, ptx, Reliant and IRIX- are unchanged and shipped as part of OVO/UNIX.

For consistency and to avoid duplication, names and grouping of the policies and applications has been adapted to the SPI standard.

Where possible, the OS-SPIs provide the same instrumentation for both the HTTPS and DCE agents.

NOTE In cases where the OS-SPI has already provided similar functionality or a superset of the OVO functionality, the existing OS-SPI version is used. In these cases, the actual template conditions, and command line parameters may not be 100% identical.

Table 0-1 maps the new OS-SPI instrumentation names to the names previously used by OVO/UNIX 7.

Table 0-2 maps the new OS-SPI policy names to the template names previously used by OVO/UNIX 7.

Table 1-10 maps the new OS-SPI application names to the names previously used by OVO/UNIX 7.

Make sure that you change the names of your existing instrumentation and any copies of the original files on your system to match the names used by the OS-SPI as shown in Table 1-8, Table 1-9, and Table 1-10.

Table 1-8 OS-SPI Instrumentation Mapping

Platform	Type	Instrumentation Name used in OVO/UNIX 7	OS-SPI Instrumentation Name
AIX	Actions	mailq_pr.sh	osspi_mailqpr.sh
		ana_disk.sh	osspi_anadisk.sh
		sh_procs.sh	osspi_shprocs.sh
	Commands	opcdf	osspi_df.sh
		opclpst	osspi_lpst.sh
		opcps	osspi_ps.sh
	Monitors	cpu_mon.sh	osspi_cpuutil.sh
		disk_mon.sh	osspi_diskutil.sh
		errpt_fmt.sh	osspi_errptfmt.sh
		opcfwtmp	osspi_fwtmp
		proc_mon.sh	osspi_pcntmon.sh
	HP-UX	Actions	mailq_pr.sh
ana_disk.sh			osspi_anadisk.sh
sh_procs.sh			osspi_shprocs.sh
Commands		opcdf	osspi_df
		opclpst	osspi_lpst
		opcps	osspi_ps
OVPA Commands		anycmd.sh	osspi_anycmd.sh
		perfcmd.sh	osspi_perfcmd.sh
		cfgfile.sh	osspi_cfgfile.sh
Monitors		cpu_mon.sh	osspi_cpuutil.sh
		disk_mon.sh	osspi_diskutil.sh
		opcfwtmp	osspi_fwtmp
		opcnprcs	osspi_nprcs
		proc_mon.sh	osspi_pcntmon.sh
Linux		Actions	mailq_pr.sh
	ana_disk.sh		osspi_anadisk.sh
	sh_procs.sh		osspi_shprocs.sh
	Commands	opcdf	osspi_df.sh
		opclpst	osspi_lpst.sh
		opcps	osspi_ps.sh
	Monitors	cpu_mon.sh	osspi_cpuutil.sh
		disk_mon.sh	osspi_diskutil.sh
		opcfwtmp	osspi_fwtmp
		proc_mon.sh	osspi_pcntmon.sh

Table 1-8 OS-SPI Instrumentation Mapping (Continued)

Platform	Type	Instrumentation Name used in OVO/UNIX 7	OS-SPI Instrumentation Name
Solaris SPARC	Actions	mailq_pr.sh	osspi_mailqpr.sh
		ana_disk.sh	osspi_anadisk.sh
		sh_procs.sh	osspi_shprocs.sh
	Commands	opcdf	osspi_df.sh
		opclpst	osspi_lpst.sh
		opeps	osspi_ps.sh
	OVPA Commands	anycmd.sh	osspi_anycmd.sh
		perfcmd.sh	osspi_perfcmd.sh
		cfgfile.sh	osspi_cfgfile.sh
	Monitors	cpu_mon.sh	osspi_cpuutil.sh
		disk_mon.sh	osspi_diskutil.sh
		opcfwtmp	osspi_fwtmp
		proc_mon.sh	osspi_pcntmon.sh
		vcs_monitor.sh	osspi_vcsmon.sh
Tru64 UNIX	Actions	mailq_pr.sh	osspi_mailqpr.sh
		ana_disk.sh	osspi_anadisk.sh
		sh_procs.sh	osspi_shprocs.sh
	Commands	opcdf	osspi_df.sh
		opclpst	osspi_lpst.sh
		opeps	osspi_ps.sh
	Monitors	cpu_mon.sh	osspi_cpuutil.sh
		disk_mon.sh	osspi_diskutil.sh
		opcfwtmp	osspi_fwtmp
		proc_mon.sh	osspi_pcntmon.sh
Windows	Actions	None	
	Commands	itodiag.exe	winosspi_windiag.exe
		itouuser.exe	winosspi_winuser.exe
		itokill.exe	winosspi_prockill.exe
		itosdown.exe	winosspi_shutdown.exe
		itoreg.exe	winosspi_winreg.exe
		opcprfls.exe	winosspi_perfobj.exe
		itoreg.cfg	winosspi_winreg.cfg
		itomserv.exe	winosspi_confserv.exe
	mf_app.bat	winosspi_mf_app.bat	
Monitors	None		

NOTE The itoprocs.exe binary is not longer shipped as part of the OVO Windows Agents. This binary was previously included in the OVO default instrumentation.

Table 1-9 OS-SPI Template/Policy Mapping

Template Name	OS-SPI Policy Name
NOTE: To find the template groups which have a dedicated policy assigned, use the OVO report <code>Template Summary</code> and search for the policy name in the report output. Most policies are assigned to more than one template group. This OVO report can be found in the OVO Administrator's GUI selecting: <code>Actions -> Utilities -> Reports...</code>	
AIX	
opcmsg(1 3)	OSSPI-opcmsg_3
Audit Log (AIX)	OSSPI-AIX-AuditLog_1
Bad Logs (AIX)	OSSPI-AIX-BadLogs_1
Kernel Logs (AIX)	OSSPI-AIX-KernelLogs_2
Logins (AIX)	OSSPI-AIX-Logins_1
Su (AIX)	OSSPI-AIX-Su_1
Syslog (AIX)	OSSPI-AIX-syslog_1
Inetd	OSSPI-inetdproc_1
MailQueueLength	OSSPI-mailqueue_2
Sendmail	OSSPI-mailproc_1
Syslogd	OSSPI-syslogproc_1
cpu_util	OSSPI-cpuutil_1
disk_util	OSSPI-diskutil_1
proc_util	OSSPI-procutil_1
swap_util	OSSPI-swapmon_2
AIX with HACMP	
opcmsg(1 3)	OSSPI-opcmsg_3
Audit Log (AIX)	OSSPI-AIX-AuditLog_1
Bad Logs (AIX)	OSSPI-AIX-BadLogs_1
HACMP logfile (AIX)	OSSPI-HACMP_Log_1
Kernel Logs (AIX)	OSSPI-AIX-KernelLogs_2
Logins (AIX)	OSSPI-AIX-Logins_1
Su (AIX)	OSSPI-AIX-Su_1
Syslog (AIX)	OSSPI-AIX-syslog_1
Inetd	OSSPI-inetdproc_1
MailQueueLength	OSSPI-mailqueue_2
Sendmail	OSSPI-mailproc_1
Syslogd	OSSPI-syslogproc_1
cpu_util	OSSPI-cpuutil_1
disk_util	OSSPI-diskutil_1
proc_util	OSSPI-procutil_1
swap_util	OSSPI-swapmon_2
Debian Linux	
opcmsg(1 3)	OSSPI-opcmsg_3
Auth (Debian Linux)	OSSPI-Linux-authlog_1
Kernel (Debian Linux)	OSSPI-linux-debian_kernellog_1
Logins (Linux)	OSSPI-Linux-Logins_2
Syslog (Debian Linux)	OSSPI-Linux-syslog_2
Inetd	OSSPI-Linux_inetdproc_2
MailQueueLength	OSSPI-mailqueue_2

Table 1-9 OS-SPI Template/Policy Mapping (Continued)

Template Name	OS-SPI Policy Name
Debian Linux continued	
Sendmail	OSSPI-mailproc_2
Syslogd	OSSPI-syslogproc_2
cpu_util	OSSPI-cpuutil_1
disk_util	OSSPI-diskutil_1
swap_util	OSSPI-swapmon_2
HP-UX	
opcmsg(1 3)	OSSPI-opcmsg_3
Bad Logs (10.x/11.x HP-UX)	OSSPI-HPUX-BadLogs_1
Boot (10.x/11.x HP-UX)	OSSPI-HPUX-Boot_1
Cron (10.x/11.x HP-UX)	OSSPI-HPUX-Cron_1
Kernel Logs (10.x/11.x HP-UX)	OSSPI-HPUX-Dmesg_2
Logins (10.x/11.x HP-UX)	OSSPI-HPUX-Logins_1
Mailqueue (10.x/11.x HP-UX)	OSSPI-mailqueue_2
Su (10.x/11.x HP-UX)	OSSPI-HPUX-Su_1
Syslog (10.x/11.x HP-UX)	OSSPI-HPUX-syslog_2
Syslog (ServiceGuard)	OSSPI-MCSG-Syslog_1
Inetd	OSSPI-inetdproc_1
MailQueueLength	OSSPI-mailqueue_2
Sendmail	OSSPI-mailproc_1
Syslogd	OSSPI-syslogproc_1
cpu_util	OSSPI-cpuutil_1
disk_util	OSSPI-diskutil_1
proc_util	OSSPI-procutil_1
swap_util	OSSPI-swapmon_2
Management Server	
opcmsg(1 3)	OSSPI-opcmsg_3
Cron (10.x/11.x HP-UX)	OSSPI-HPUX-Cron_1
Su (10.x/11.x HP-UX)	OSSPI-HPUX-Su_1
disk_util	OSSPI-diskutil_1
proc_util	OSSPI-procutil_1
swap_util	OSSPI-swapmon_1
SNMP Traps (NNM 7.01) SNMP ECS Traps	Replaced by corresponding versions for NNM 7.01. Provided by OVO Platform.
Su (Solaris)	OSSPI-SOL-Su_1
Syslog (Solaris)	OSSPI-SOL-syslog_2
Inetd	OSSPI-inetdproc_1
MailQueueLength	OSSPI-mailqueue_2
Sendmail	OSSPI-mailproc_1
Syslogd	OSSPI-syslogproc_1
cpu_util	OSSPI-cpuutil_1
swap_util	OSSPI-swapmon_2

Table 1-9 OS-SPI Template/Policy Mapping (Continued)

Template Name	OS-SPI Policy Name
MC/SG Physical Management Server	
opcmsg(1 3)	OSSPI-opcmsg_3
Cron (10.x/11.x HP-UX)	OSSPI-HPUX-Cron_1
Su (10.x/11.x HP-UX)	OSSPI-HPUX-Su_1
disk_util	OSSPI-diskutil_1
proc_util	OSSPI-procutil_1
swap_util	OSSPI-swapmon_2
MetaFrame	
System Log (MetaFrame)	WINOSSPI-MF_FwdAllSysInformation
	WINOSSPI-MF_FwdAllSysWarnError
MF_ICA_Browser	WINOSSPI-MF_ICA_Browser
MF_Prog_Neighborhood	WINOSSPI-MF_Prog_Neighbourhood
TS_Licensing	WINOSSPI-WTS_TermServLicensing
TS_Service	WINOSSPI-WTS_TermService
SC/HA Physical Management Server	
opcmsg(1 3)	OSSPI-opcmsg_3
Bad Logs (Solaris)	OSSPI-SOL-BadLogs_1
Cron (Solaris)	OSSPI-SOL-Cron_1
Logins (Solaris)	OSSPI-SOL-Logins_1
Su (Solaris)	OSSPI-SOL-Su_1
Syslog (Solaris)	OSSPI-SOL-syslog_2
Inetd	OSSPI-inetdproc_1
MailQueueLength	OSSPI-mailqueue_2
Sendmail	OSSPI-mailproc_1
Syslogd	OSSPI-syslogproc_1
cpu_util	OSSPI-cpuutil_1
disk_util	OSSPI-diskutil_1
proc_util	OSSPI-procutil_1
swap_util	OSSPI-swapmon_2
Solaris SPARC	
opcmsg(1 3)	OSSPI-opcmsg_3
Bad Logs (Solaris)	OSSPI-SOL-BadLogs_1
Cron (Solaris)	OSSPI-SOL-Cron_1
Engine Log (SC)	OSSPI-SC-EngineLog_1
Engine Log (VCS)	OSSPI-VCS-EngineLog_1
Engine Notify Log (VCS)	OSSPI-VCS-EngineNotifyLog_1
Logins (Solaris)	OSSPI-SOL-Logins_1
Su (Solaris)	OSSPI-SOL-Su_1
Syslog (Solaris)	OSSPI-SOL-syslog_2
Inetd	OSSPI-inetdproc_1
MailQueueLength	OSSPI-mailqueue_2
Sendmail	OSSPI-mailproc_1
Syslogd	OSSPI-syslogproc_1
cpu_util	OSSPI-cpuutil_1

Table 1-9 OS-SPI Template/Policy Mapping (Continued)

Template Name	OS-SPI Policy Name
Solaris continued	
disk_util	OSSPI-diskutil_1
proc_util	OSSPI-procutil_1
swap_util	OSSPI-swapmon_2
SuSE Linux	
opcmsg(1 3)	OSSPI-opcmsg_3
Kernel Messages (SuSE)	OSSPI-linux-suse_kernellog_1
Logins (Linux)	OSSPI-Linux-Logins_2
Messages (SuSE)	OSSPI-linux-suse_messages_1
Inetd	OSSPI-Linux_inetdproc_2
MailQueueLength	OSSPI-mailqueue_2
Sendmail	OSSPI-mailproc_2
Syslogd	OSSPI-syslogproc_2
cpu_util	OSSPI-cpuutil_1
disk_util	OSSPI-diskutil_1
swap_util	OSSPI-swapmon_2
Terminal Server	
System Log (Terminal Server)	WINOSSPI-WTS_FwdAllInformation
	WINOSSPI-WTS_FwdAllSysWarnError
TS_Licensing	WINOSSPI-WTS_TermServLicensing
TS_Service	WINOSSPI-WTS_TermService
Tru64 UNIX	
opcmsg(1 3)	OSSPI-opcmsg_3
Cron (Digital Unix)	OSSPI-cronproc_1
Logs (Digital Unix)	OSSPI-Tru64-Logins_1
Lplog (Digital Unix)	OSSPI-Tru64-printlog_1
OS Msgs (Digital Unix)	OSSPI-Tru64_messages_1
SIA Log (Digital Unix)	OSSPI-Tru64-BadLogs_1 and OSSPI-Tru64-Su_1
Inetd	OSSPI-inetdproc_1
MailQueueLength	OSSPI-mailqueue_2
Sendmail	OSSPI-mailproc_1
Syslogd	OSSPI-syslogproc_1
cpu_util	OSSPI-cpuutil_1
disk_util	OSSPI-diskutil_1
swap_util	OSSPI-procutil_1
VCS Physical Management Server	
opcmsg(1 3)	OSSPI-opcmsg_3
Application (VCS)	OSSPI-VCS-ApplicationServiceLog_1
Bad Logs (Solaris)	OSSPI-SOL-BadLogs_1
Cron (Solaris)	OSSPI-SOL-Cron_1
Disk (VCS)	OSSPI-VCS-DiskServiceLog_1
DiskGroup (VCS)	OSSPI-VCS-DiskGroupLog_1
DiskReservation (VCS)	OSSPI-VCS-DiskReservationLog_1
ElifNone (VCS)	OSSPI-VCS-ElifNoneServiceLog_1

Table 1-9 OS-SPI Template/Policy Mapping (Continued)

Template Name	OS-SPI Policy Name
VCS Physical Management Server continued	
Engine	OSSPI-VCS-EngineLog_1
Engine Shadow	OSSPI-VCS-EngineShadowLog_1
Engine Shadow Error	OSSPI-VCS-EngineShadowErrorLog_1
FileNone (VCS)	OSSPI-VCS-FileNoneServiceLog_1
FileOnOff (VCS)	OSSPI-VCS-FileOnOffServiceLog_1
FileOnOnly (VCS)	OSSPI-VCS-FileOnOnlyServiceLog_1
IP (VCS)	OSSPI-VCS-IPServiceLog_1
IPMultiNIC (VCS)	OSSPI-VCS-IPMultiNICServiceLog_1
Logins (Solaris)	OSSPI-SOL-Logins_1
Mount (VCS)	OSSPI-VCS-MountServiceLog_1
MultiNICA (VCS)	OSSPI-VCS-MultiNICAServiceLog_1
NFS (VCS)	OSSPI-VCS-NFSServiceLog_1
NIC (VCS)	OSSPI-VCS-NICServiceLog_1
Phantom (VCS)	OSSPI-VCS-PhantomServiceLog_1
Process (VCS)	OSSPI-VCS-ProcessServiceLog_1
Proxy (VCS)	OSSPI-VCS-ProxyServiceLog_1
ServiceGroupHB (VCS)	OSSPI-VCS-ServiceGroupHBSERVICELog_1
Share (VCS)	OSSPI-VCS-ShareServiceLog_1
Su (Solaris)	OSSPI-SOL-Su_1
Syslog (Solaris)	OSSPI-SOL-syslog_2
Volume (VCS)	OSSPI-VCS-VolumeServiceLog_1
Inetd	OSSPI-inetdproc_1
MailQueueLength	OSSPI-mailqueue_2
Sendmail	OSSPI-mailproc_1
Syslogd	OSSPI-syslogproc_1
cpu_util	OSSPI-cpuutil_1
disk_util	OSSPI-diskutil_1
had	OSSPI-VCS-had_1
hashadow	OSSPI-VCS-Hashadow_1
proc_util	OSSPI-procutil_1
swap_util	OSSPI-swapmon_2
vmsa_server	OSSPI-vmsa-server_1
vxconfigd	OSSPI-vxconfigd_1
Windows 2000/2003	
opcmsg(1 3)	WINOSSPI-opcmsg
dflt_AppLEvLog (2000)	WINOSSPI-Logon_ApplInfo
	WINOSSPI-NetworkConfig_ApplInfo
	WINOSSPI-ADS_Replication_ApplInfo
dflt_DNSEvLog (NT)	WINOSSPI-ADS_DNSServ_FwdAllInformation
	WINOSSPI-ADS_DNSServ_FwdAllWarnError
dflt_DirectoryEvLog (2000)	WINOSSPI-ADS_FwdAllInformationDS
	WINOSSPI-ADS_FwdAllWarnErrorDS
	WINOSSPI-ADS_ReplcationActivites

Table 1-9 OS-SPI Template/Policy Mapping (Continued)

Template Name	OS-SPI Policy Name
dflt_FileReplicationEvLog (2000)	WINOSSPI-ADS_FwdAllInformationFRS
	WINOSSPI-ADS_FwdAllWarnErrorFRS
dflt_SecEvLog (NT)	WINOSSPI-Logon_SecInfo
	WINOSSPI-Process_SecInfo
	WINOSSPI-SecEvLog_Operations
	WINOSSPI-ADS_PrivilegedObjects
dflt_SysEvLog (NT)	WINOSSPI-SCM_Sysinfo
	WINOSSPI-NetLogon_SysInfo
dflt_cpu_util_NT	WINOSSPI-SysMon_CpuSpikeCheck_Win2k_PrivilegedTime
	WINOSSPI-SysMon_CpuSpikeCheck_Win2k_ProcessorTime
	WINOSSPI-SysMon_CpuSpikeCheck_Win2k_UserTime
Windows NT^a	
opcmsg(1 3)	WINOSSPI-opcmsg
dflt_ApplEvLog (NT)	WINOSSPI-Logon_ApplInfo
	WINOSSPI-NetworkConfig_ApplInfo
	WINOSSPI-ADS_Replication_ApplInfo
dflt_SecEvLog (NT)	WINOSSPI-Logon_SecInfo
	WINOSSPI-Process_SecInfo
	WINOSSPI-SecEvLog_Operations
	WINOSSPI-ADS_PrivilegedObjects
dflt_SysEvLog (NT)	WINOSSPI-SCM_Sysinfo
	WINOSSPI-NetLogon_SysInfo
dflt_cpu_util_NT	WINOSSPI-SysMon_CpuSpikeCheck_NT4_PrivilegedTime
	WINOSSPI-SysMon_CpuSpikeCheck_NT4_ProcessorTime
	WINOSSPI-SysMon_CpuSpikeCheck_NT4_UserTime
dflt_disk_util_NT	WINOSSPI-SysMon_DiskBusyCheck_AvgDiskQueue
	WINOSSPI-SysMon_DiskBusyCheck_DiskTime
	WINOSSPI-SysMon_DiskFullCheck_FreeMB
	WINOSSPI-SysMon_DiskFullCheck_PercentageFreeSpace

a. Microsoft Windows NT operating system is no longer supported by Microsoft. The Windows OS-SPI currently delivers these policies with no further commitment to continue development.

Table 1-10 OS-SPI Application Mapping

OVO/UNIX 7 Application Name	OS-SPI Application Group	OS-SPI Application Name
GlancePlus		
Start gpm	Unix OS SPI\HP Performance Products\HP Glance	GPM (Motif)
Start glance		Glance (Ascii)
List Processes	Unix OS SPI\HP Performance Products\ Common Applications	List processes
List Versions		List Versions
Tail Status Files		Tail Status Files
Config ttd.conf		Configure ttd.conf
MetaFrame Tools		
Sessions	Windows OS SPI\MetaFrame Tools	Sessions
Users		Users
Servers		Servers
Auditlog		Audit Log
ACL Info		ACL Info
Disconnect		Disconnect
Flush		Flush
Send Message		Send Message
Processes		Processes
License		License
NT Tools		
Cancel Reboot	Windows OS SPI\Microsoft Windows Core\System	Cancel Shutdown
CPU Load		CPU Load
LM Sessions		List Sessions
Process Kill		Kill Process
Reboot		Shutdown
Reg Viewer		Show Registry Key
Show Services		List Services
Start Service		Start Service
Stop Service		Stop Service
Diagnosics		Windows OS SPI\Microsoft Windows Core\ Information
Installed Software	Installed Software	
Job Status	Job Status	
Local User	Local User	
Memory Load	Memory Information	
PerfMon Objs	Perfmon Objects	
Shares	Shares	
Server Config	Server Config	
Server Stats	Server Stats	
Show Drivers	Show Drivers	
Show Users	User List	
Used Shares	Used Shares	
Workst Stats	Workst Stats	

Table 1-10 OS-SPI Application Mapping (Continued)

OVO/UNIX 7 Application Name	OS-SPI Application Group	OS-SPI Application Name
NetBios Sessions	Windows OS SPI\Microsoft Windows Core\ Networking	NetBios Sessions
TCP/IP Status		Show TCP/IP Connections
OV Performance		
Start Perf Agt	Unix OS SPI\HP Performance Products\HP OVPA	Start OVPA
Stop Perf Agt		Stop OVPA
Restart Perf Agt		Restart Perf Agt
Restart PA Servers		Restart PA Servers
Reactivate alarmdef		Reactivate alarmdef
Config parm		Configure parm
Check parm		Check parm
Config perflbd.rc		Configure perflbd.rc
Config alarmdef		Configure alarmdef
Check alarmdef		Check alarmdef
Start extract		Start extract
Start utility		Start utility
Config ttd.conf		Unix OS SPI\HP Performance Products\ Common Applications
List Versions	List Versions	
Tail Status Files	Tail Status Files	
List Processes	List Processes	
Start pv	Unix OS SPI\HP Performance Products\HP OVPM	OVPM Console
Start pvalarmd		Start pvalarmd
Stop pvalarmd		Stop pvalarmd
Tools		
Disk Space	"OS Tools" for every platform's Admin and Operator groups	Disk Space
Processes	"OS Tools" for every platform's Admin and Operator groups	Processes
UN*X Tools		
SMIT (AIX)	Unix OS SPI\AIX\AIX Admin Tools\OS Tools	SMIT (AIX)
ASCII SAM	Unix OS SPI\HPUX\HPUX Admin Tools\OS Tools	ASCII SAM
Motif SAM		Motif SAM
Print Status	"OS Tools" for every platform's Admin and Operator groups	Print Status
VERITAS		
VERITAS CSCM	Unix OS SPI\Veritas\Veritas Admin Tools	VERITAS CSCM
VERITAS VMSA		VERITAS VMSA

Changed Features

The following Application Groups have been replaced and are obsolete:

- GlancePlus
- Jovw
- MetaFrame Tools
- OV Performance
- Reports
- VERITAS

In addition to the applications in the obsolete application groups, the following applications are no longer provided:

Application	Label

/Net Activity/Interface Statistics	: Interface Statistics
/OV Services/OV CDP View	: CDP View

The following applications are renamed and enhanced:

Application	New Label

/Net Config/Addresses	: Addresses(Node) Addresses(Interface)
/Net Config/Routing Table	: Routing Table(Node) Routing Table(Interface)
/Net Config/ARP Cache	: ARP Cache(Node) ARP Cache(Interface)

Changed Features with HP OpenView Operations for UNIX Developer's Toolkit

This section lists existing functionality that has changed from the HP OpenView Operations for UNIX Developer's Toolkit version 7.1x.

Server API `opcapp_start()` Function Behavior Changed with OVO 8

The function `opcapp_start()` is obsolete since VPO 6.0 and is only included for compatibility reasons. It is strongly recommended that you use the function `opcappl_start()` instead. Note the added 'l' in the function name.

The behavior of the function `opcapp_start()` has been changed and is forced to check the execution user name and password on the target node before the execution of the application. This is because execution user name could have been changed and is different from the execution user name of the application stored in the database. This was not the case with OVO/UNIX 7 and earlier versions and has been changed to improve security.

This change also introduces a new configuration parameter:

```
OPC_OMIT_PWD_CHECK_FOR_APP_START
```

Setting this parameter to `TRUE` will switch the behavior back to the pre- OVO/UNIX 8 and less secure model. This is NOT recommended, but implemented so that it is still possible to work with applications that require it.

To set the `OPC_OMIT_PWD_CHECK_FOR_APP_START` parameter only for the one application that needs it, enter the following command:

```
ovconfchg -ovrg server -ns opc.<appl_name> -set OPC_OMIT_PWD_CHECK_FOR_APP_START TRUE
```

Alternatively, use the function `opcappl_start()`, particularly for newer integrations.

In general it is NOT necessary to set the user name and password as long as it is not required to execute the application as different user. The execution user that is specified in the database will be used to execute applications on the target node, as long as the execution user in the `OPCDTYPE_APPL_CONFIG` structure is not changed. If it is changed, then the user will be checked and it is also necessary to specify the password.

Obsolete Features

This section lists the obsolete features of this release of OVO:

❑ **Obsolete Management Server Platforms**

- HP-UX 11.0
- HP-UX 10.20
- Sun Solaris 7

❑ **Obsolete OVO Agent Platforms**

- HP-UX 11.0
- HP-UX 10.20
- Linux Kernel 2.2 all derivatives
- Novell NetWare 4.x
- Tru64 UNIX 4.0x (excluding 4.0 F/G)
- Microsoft Windows NT 4.0
- HP MPE/iX

NOTE HP plans to obsolete all DCE- and NCS-based OVO 7 agents as part of the OVO/UNIX 7 obsolescence by end of CY2007.

❑ **Obsolete Java UI Platforms**

- HP-UX 11.0
- HP-UX 10.20
- Sun Solaris 7
- Microsoft Windows NT and 98

❑ **opcinfo and nodeinfo Configuration Files**

The OVO HTTPS agents no longer use the `opcinfo` and `nodeinfo` configuration files. The local HTTPS agent configuration is based on the new OpenView Common Management Environment (CME) components using `ovconfget(1)` and `ovconfchg(1)`. For details, refer to the *HP OpenView Operations HTTPS Agent Concepts and Configuration Guide*.

❑ **opcsvinfo Configuration File**

The OVO management server no longer uses the `opcsvinfo` configuration file. The management server configuration is based on the new OpenView Common Management Environment (CME) components using `ovconfget(1)` and `ovconfchg(1)`.

❑ **opcerror**

OVO uses the common OpenView logging. The errors are no longer logged to the `opcerror` file, but to the `$OvDataDir/log/System.bin (binary)` and `$OvDataDir/log/System.txt (ASCII)` log files. The HTTPS agent and management server use the same location.

❑ **OV Advanced Security**

The OV Advanced Security (OVAS) is not offered for this version of OVO. OVO/UNIX 8 itself provides most of the OVAS functionality, since HTTPS communication can be used for the OVO agents and for the OVO Java UI - OVO/UNIX management server communication.

Before migrating from OVO/UNIX 7.1x, you must switch off the OVAS functionality completely for the Java UI and all DCE agents.

❑ **opcdbreorg**

The Oracle database maintenance program `opcdbreorg` is no longer necessary, since the Database Extend Management is switched to `local`.

❑ **Virtual Terminal Application to Connect to HTTPS Agent for Windows**

There is no standard application delivered with OVO/UNIX to provide a virtual terminal connection to the HTTPS Windows managed nodes.

There are several 3rd party applications available designed specifically to achieve such connections.

What's Not Yet Supported

❑ **Internet Services (OVIS)**

Internet Services (OVIS) cannot co-exist with the HTTPS agent on HP-UX 11.23 Itanium.

❑ **UTF8 Character Set**

OVO/UNIX 8 does not support UTF8 as the character set used for the Oracle database and the OVO management server. The supported encoding and character sets are detailed in Table 2-5, "Certified Encoding and Character Sets," on page 63.

However, UTF8 character set is supported for the OVO Agent platforms. The supported encoding and character sets are detailed in Table 7-1, "OVO/UNIX Agent Platform Character Sets and Locales," on page 178.

❑ **User Provided Certificate Authority**

OVO/UNIX does not support the use of any external or custom Certificate Authority.

❑ **Hostnames Maximum Character Length is 256**

OVO/UNIX does not yet support hostnames longer than 256 characters.

What's Not Supported

❑ HTTP Proxy Limitations

In case the OVO/UNIX management server does not talk directly to an HTTPS agent, but via an HTTP proxy, be aware of the following limitations:

— HTTP Proxy with USER/PASSWD Authorization

One of the following alternatives can be used:

- HTTP Proxy must accept non-authorized requests from specific IP address or domain ranges with specified destination ports.
- An additional HTTP Proxy must be used, which accepts non authorized requests from the OVO Application but then contacts the main HTTP Proxy with USER/PASSWD.

— Fail-Over, Fallback, and Alternative HTTP Proxies

OVO supports only one HTTP proxy per HTTPS agent, but different HTTP proxies can be specified for different HTTPS agents.

❑ Running the HTTPS Windows Agent under Account other than System

The `ovswitchuser` command is not supported by the HTTPS agent for Windows. The HTTPS agent for Windows must run under the `SYSTEM` account. One exception is for managed nodes that are used as installation servers.

❑ OVPA 4.5 on Tru64 DCE Nodes

OVPA 4.5 cannot coexist with OVO DCE agent on Tru64 on English and localized systems. It is not possible to run both products in parallel. Either keep OVPA 3.x or upgrade to OVO Tru64 HTTPS agent.

❑ HTTPS to DCE Agent Conversion

OVO 8 HTTPS agents cannot be directly downgraded to DCE agents. You must completely deinstall the HTTPS agent and install the DCE agent.

Upgrading DCE agents to HTTPS agents, however, offers the following advantages:

- The installation procedure automatically deinstalls the DCE agent.
- `opcinfo` settings are rescued and converted automatically.
- The Embedded Performance database settings are rescued and converted automatically.
- ECS data and fact stores are rescued automatically.

❑ ECS Designer

ECS Designer is not supported running on HP-UX 11.23 Itanium, HP-UX 11.23 PA-RISC and on Solaris 10. If you would like to use ECS Designer in conjunction with OVO/UNIX, you will have to create ECS circuits and data/fact stores on a operating system platform supported by ECS Designer, for example HP-UX 11.11, Solaris 8 or Solaris 9.

After creating the circuits, data and fact stores on another system, transfer them to the OVO/UNIX management server. Detailed instructions are available in the *Using ECS Designer Remotely* whitepaper that can be downloaded from the following location:

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

Obsolescence Announcements for the Next Major OVO Release

The following features may no longer be supported with the next major release of OVO/UNIX. The next major release of OVO/UNIX is planned for mid 2008.

NOTE HP appreciates your feedback. Contact your HP sales or support representative if you would like HP to continue supporting the features listed in this section with the next major release.

❑ **Management Server Platform**

HP plans to obsolete the following management server versions:

- HP-UX PA-RISC all versions
- HP-UX Itanium 11.23 (HP-UX 11.31 will be supported only)
- Sun Solaris 8 and 9 (Solaris 10 will be supported only)

❑ **Managed Node Platform**

HP plans to obsolete all DCE- and NCS-based OVO 7 agents as part of the OVO/UNIX 7 obsolescence by end of CY2007.

❑ **Java UI**

The Java UI may no longer be supported on the following platforms:

- HP-UX PA-RISC all versions
- HP-UX Itanium 11.23
- Sun Solaris 8 and 9
- Windows 2000
- Red Hat 8

❑ **Motif UI**

The Motif UI will no longer be further developed and enhanced with the next releases of OVO. This means that new features will only be implemented for the Java UI. The Motif Operator and Administrator UIs are in version mature mode and may become obsolete with a future release of OVO.

❑ **Backward Compatibility with Previous OVO Agents**

OVO/UNIX 9 will no longer support backward compatibility with OVO 7 DCE agents. Only OVO 8 HTTPS agents will be supported.

❑ **OVO DCE and HTTPS Compatibility Wrappers**

HP plans to obsolete the DCE compatibility wrappers on the HTTPS agents. These include:

- `opcagt` (to be replaced by `ovc`)
- `optemplate` (to be replaced by `ovpolicy`)

In addition, wrappers on the OVO management server, such as `opcdeploy`, will also be obsoleted.

❑ **Miscellaneous**

HP plans to obsolete the following features:

- *CD-ROM as Installation Media*

The next major release of OVO may no longer be shipped on CD-ROMs as installation media, but on Digital Versatile Disks (DVDs).

- *Expressions <S> and <nS>*

The pattern-matching expressions <S> and <nS> used in templates may be obsoleted with future releases.

What's in This Version

Obsolescence Announcements for the Next Major OVO Release

2 Management Server and Java UI Installation Requirements

Management Server Hardware and Software Requirements

Table 2-1 Supported Management Server Platforms

Management Server Platform	Requirements	
HP-UX 11.11	ovo.info.HP-UX.B.11.11.txt	See “NNM 7.51 CD-ROM Installation Important Update” on page 112
HP-UX 11.23 PA-RISC	ovo.info.HP-UX.B.11.23.txt	See Installation Guide for the Management Server, requires NNM 7.51.
HP-UX 11.23 Itanium	ovo.info.HP-UX.B.11.23.txt	Requires NNM 7.51.
Solaris 8	ovo.info.SunOS.5.8.txt	
Solaris 9	ovo.info.SunOS.5.9.txt	
Solaris 10	ovo.info.SunOS.5.10.txt	See Installation Guide for the Management Server, requires NNM 7.51.

For more details on installation requirements, refer to the OVO/UNIX installation requirements info file applicable to your operating system version. Installation requirements info files are located in the `Required_OS_Patch_Lists` directory on the OVO/UNIX CD1.

Before installing OVO, make sure that the system you select as the management server meets the hardware and software requirements listed in Chapter 1 of the *Installation Guide for the Management Server*. In particular, make sure that all required additional software packages and operating system patches are installed.

Table 2-2 Latest Management Server Patch

Patch Name	Management Server Platform		
	HP-UX PA-RISC	HP-UX Itanium	Solaris
OVO8 consolidated server 8.24	PHSS_35526	PHSS_35525	ITOSOL_00538

NOTE If you are using Oracle 10g and NNM 7.5, refer also to the Oracle 10g and NNM 7.5 installation documentation for other requirements.

Refer to Chapter 2 of the *Installation Guide for the Management Server* for detailed instructions on how to install OVO, as well as chapter 7 of this Release Notes document for known problems and their workarounds.

The following readme file describes the OVO/UNIX media CD contents and layout and help you to locate products and documentation:

/READMEHPUX_PA-RISC.txt

WARNING **An HTTPS agent must be installed on the OVO/UNIX 8 management server system. Do not install a DCE/NCS agent on the OVO/UNIX 8 management server system. Installing the DCE/NCS agent on the OVO management server system could damage your installation!**

Do not install the HTTPS agent on an OVO/UNIX 7 management server system. OVO/UNIX 7 cannot communicate with the HTTPS agent and attempting to install the HTTPS agent could damage your installation!

WARNING **Edit the `/etc/MANPATH` file and set the `MANPATH` variable to include the following OVO directory:**

`/opt/OV/man/`

NOTE It can be very helpful to set the `PATH` variable to include the following OVO/UNIX directories on the Management Server: `/opt/OV/bin`, `/opt/OV/bin/OpC`, `/opt/OV/bin/Perl/bin` and `/opt/OV/bin/OpC/Utils`.

IMPORTANT If you plan to use the HTTPS Java GUI, make sure that you copy the `opcuihttps` file from `/opt/OV/contrib/OpC/` to `/opt/OV/bin/OpC/` after the OVO/UNIX installation. To get updated the `opcuihttps` binary automatically after OVO management server patch installation, use a symbolic link instead of copying it to the required location.

In case you have management server in a cluster environment copy this file on each cluster node. For more details, refer to `/opt/OV/contrib/OpC/opcuihttps.readme` file located on the OVO management server.

High Availability Environments

Table 2-3 lists the High Availability environments supported on the OVO/UNIX management server.

Table 2-3 Supported High Availability Environments

Management Server Platform	High Availability Application	Supported Versions
HP-UX 11.11	HP Serviceguard	11.14, 11.15, and 11.16
	Veritas Cluster	3.5
HP-UX 11.23 PA-RISC	HP Serviceguard	11.16, 11.17
	Veritas Cluster	4.1
HP-UX 11.23 Itanium	HP Serviceguard	11.16, 11.17
	Veritas Cluster Server	4.1 ^a
Solaris 8	Sun Cluster	3.0 and 3.1
	Veritas Cluster	3.5, 4.0
Solaris 9	Sun Cluster	3.0 and 3.1
	Veritas Cluster	3.5, 4.0, 4.1
Solaris 10	Sun Cluster	3.1
	Veritas Cluster	4.1

a. See “Installing OVO/UNIX on VERITAS Cluster Server 4.1 on HP-UX 11.23 Itanium” on page 118

Cluster Awareness Support

Table 2-4 Cluster Awareness Supported Platforms (HP-UX PA-RISC)

Cluster Awareness Supported Platforms	Agent ^a	Server ^b		Cluster Awareness Supported Platforms	Agent ^c
		HP-UX 11.11	HP-UX 11.23 PARISC		
HP Serviceguard				HP Serviceguard	
11.13	DCE agents only			11.13	DCE agents only
11.14	✓	✓		11.14	✓
11.15	✓	✓		11.15	✓
11.16	✓	✓	✓	11.16	✓
11.17	✓		✓	11.17	✓
Sun Cluster				Sun Cluster	
3.0	✓			3.0	✓

- a. Agent runs on each physical node in a cluster.
- b. OVO management server is able to switch as package.
- c. Agent runs on each physical node in a cluster.

OVO 8 HTTPS and 7 DCE agents can be used to run on and to manage High Availability environments.

Certified Encoding and Character Sets on OVO/UNIX Management Servers

Table 2-5 details the certified encoding and character sets that need to be set for the OVO/UNIX management server and Oracle database host systems.

Table 2-5 Certified Encoding and Character Sets

Language Variables / Character Sets	Encoding OVO/UNIX Node Character Set	HP-UX Language Variable LANG	Solaris Language Variable LANG and LC_ALL	Oracle Database Code Set NLS_LANG
English	ISO-885915	C, en_US.iso88591, en_US.iso885915@euro, en_GB.iso88591, en_US.iso885915@euro	C, en_US.iso88591, en_US.iso885915@euro, en_GB.iso88591, en_US.iso885915@euro	WE8ISO8859P15
Spanish	ISO-885915	es_ES.iso885915@euro	es_ES.iso885915-euro	WE8ISO8859P15
Japanese	Shift-Jis	ja_JP.SJIS	ja_JP.PCK	JA16SJIS
Korean	EUC	ko_KR.eucKR	ko, korean, ko_KR.EUC	KO16KSC5601
Simplified Chinese	GB2312	zh_CN.hp15CN	zh, zh_CN.EUC	ZHS16CGB231280
Traditional Chinese	BIG5	zh_TW.big5	zh_TW.BIG5	ZHT16BIG5

Other locales are also supported, for example, German, and French.

NOTE OVO/UNIX 8 is internationalized and supports most of the common languages. It has been explicitly certified for English, Japanese, Korean, Simplified Chinese, Traditional Chinese and Spanish. Please check also the Oracle documentation, which character sets are available.

Please note, the UTF-8 character set is NOT supported by OVO/UNIX 8 as the Oracle database character set.

Java UI Supported Platforms

Table 2-6 JavaGUI Client Patch 8.24

	Management Server Platform		
Patch Name	HP-UX PA-RISC	HP-UX Itanium	Solaris
JavaGUI client 8.24	PHSS_35791	PHSS_35790	ITOSOL_00541

OVO/UNIX bundles JRE for all MS Windows platforms.

For all other platforms the required Java Runtime version must be available.

Table 2-7 Support Matrix - Java UI

Java Runtime	JRE	JRE Plug-in	JRE Plug-in	JRE Plug-in
TYPE	as Application	Internet Explorer 5.5, 6	Safari 1.2.3	Mozilla 1.7
Linux Red Hat 9.0	1.4.2_13 ^a	N/A	N/A	1.4.2_13a
Windows 2000	1.4.2_13	1.4.2_13	N/A	1.4.2_13
Windows 2003	1.4.2_13	1.4.2_13	N/A	1.4.2_13
Windows 2003 for Itanium	N/A	1.4.2_13	N/A	1.4.2_13
Windows XP	1.4.2_13	1.4.2_13	N/A	1.4.2_13
HP-UX 11.11, 11.23 (PA-RISC), 11.23 (IPF)	1.4.2_11	N/A	N/A	1.4.2_11
Solaris 8, 9, 10	1.4.2_13	N/A	N/A	1.4.2_13
MacOs	1.4.2_09	N/A	1.4.2_09	1.4.2_09

a. Sun's JRE.

NOTE If the default JRE version installed with the operating system is not the same as the one required by OVO/UNIX, install the supported Java Runtime Environment JRE from the following location:

<http://www.hp.com/products1/unix/java/>

Set the location of the installed JRE directory to the `JAVA_DIR` environment variable, for example.:

```
export JAVA_DIR=/opt/java1.4/jre
```

3 HTTPS Agent Installation Requirements

This chapter provides prerequisite information for HTTPS agents:

- HTTPS Agent Hardware Requirements
- HTTPS Agent Software Requirements

Before installing OVO, make sure the hardware appropriate for your HTTPS managed node platform is available. The hardware requirements are detailed in “HTTPS Agent Hardware Requirements” on page 72.

Before installing OVO, make sure the software appropriate for your HTTPS managed node platform is installed. The software requirements are detailed in the following tables:

- “HP-UX HTTPS Agent Software Requirements” on page 73
- “Solaris HTTPS Agent Software Requirements” on page 74
- “Linux HTTPS Agent Software Requirements” on page 75
- “Microsoft Windows HTTPS Agent Software Requirements” on page 76
- “AIX HTTPS Agent Software Requirements” on page 77

HTTPS Agent Supported Platforms

NOTE OVO/UNIX Product Support Matrix with the latest patch levels available for the supported platforms is available through:

http://support.openview.hp.com/sc/support_matrices.jsp

or by following the HP OpenView Support Matrix > HP OpenView Support Matrix - Part 1 - Operations and Service Navigator Value Pack links at:

http://partners.openview.hp.com/ovcw/pricing/config_matrix.jsp

With OVO 8, the new HTTPS-Agent software is available for highly secure communication between OVO management servers and the following managed nodes:

Table 3-1 OVO 8 HTTPS Agent Versions from OVO Media Kit and Latest

Managed Node Platform	HTTPS Agent Version							
	Core Agent		EventAction		Embedded Performance		OVO Accessories	
	OVO CD	Latest	OVO CD	Latest	OVO CD	Latest	OVO CD	Latest
HP-UX PA-RISC 11.11, 11.23	8.10	8.16	8.10	8.14.1	8.10	8.10	8.10 05.06.01 3	8.11
HP-UX Itanium IA64 11.22, 11.23	8.10	8.16	8.10	8.14.1	8.10	8.10	8.10 8.10 05.06.01 3	8.11
Solaris 8, 9, 10 for SPARC	8.10	8.16	8.10	8.14	8.10	8.10	8.10 8.10 05.06.01 3	8.11
Solaris 10 for x86/x64	N/A	8.16	N/A	8.14	N/A	8.10	N/A	8.11
Microsoft Windows 2000, XP Professional, 2003	8.10	8.16	8.10	8.14.1	8.10	8.10	8.10 8.10 05.06.01 3	8.11
Linux (Kernel2.4) Refer to Table 3-4	8.10	8.16	8.10	8.14	8.10	8.11	8.10 8.10 05.06.01 3	8.12

Table 3-1 OVO 8 HTTPS Agent Versions from OVO Media Kit and Latest

Managed Node Platform	HTTPS Agent Version							
	Core Agent		EventAction		Embedded Performance		OVO Accessories	
	OVO CD	Latest	OVO CD	Latest	OVO CD	Latest	OVO CD	Latest
Linux (Kernel2.6) Refer to Table 3-4	N/A	8.16	N/A	8.15	N/A	8.11	N/A	8.12
IBM AIX 5.1, 5.2, 5.3	N/A	8.16	N/A	8.14	N/A	8.10	8.10 8.10 05.06.01 3	8.11
Tru64 5.1, 5.1A, 5.1B	N/A	8.10.160	N/A	8.10.160	N/A	8.10.160	N/A	N/A
Tru64 Cluster 5.1A, 5.1B	N/A	8.10.160	N/A	8.10.160	N/A	8.10.160	N/A	N/A

NOTE The OVO HTTPS agent for Tru64 with Cluster Awareness, the OVO HTTPS agent for AIX, and the OVO HTTPS agent for Solaris x86/x64 are available. Although these are not included in the OVO/UNIX media kit, the agents can be downloaded from the following site:

<http://support.openview.hp.com/patches/ito/ito.jsp>

The OVO HTTPS agent for Linux kernel 2.6 is available through OVO Agent patches.

NOTE It is strongly recommended that you download and apply the latest Openview software patches after installing the OVO/UNIX Management Server. The latest software patches are available at the following location:

<http://openview.hp.com/sso/ecare/getsupportdoc?docid=OVO-PATCHES>

Please check the above web location quarterly for the latest OVO/UNIX software patches.

HTTPS Agent Hardware Requirements

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

Disk Space

Up to 100 MB depending on platform.

(Up to 200 MB is required during the initial software installation).

HTTPS Agent Software Requirements

Before installing OVO, make sure the software appropriate for your HTTPS managed node platform is installed. The requirements are detailed in the following tables:

- Table 3-2, “HP-UX HTTPS Agent Software, Settings and Operating System Patches,” on page 73
- Table 3-3, “Solaris HTTPS Agent Software, Settings and Operating System Patches,” on page 74
- Table 3-4, “Linux HTTPS Agent Software, Settings and Operating System Patches,” on page 75
- Table 3-5, “Microsoft Windows HTTPS Agent Software, Settings and Operating System Patches,” on page 76
- Table 3-6, “AIX HTTPS Agent Software, Settings and Operating System Patches,” on page 77

HP-UX HTTPS Agent Software Requirements

Table 3-2 HP-UX HTTPS Agent Software, Settings and Operating System Patches

HP-UX Supported Platforms	
<ul style="list-style-type: none"> • HP-UX PA-RISC: 11.11, 11.23 • HP-UX Itanium IA64: 11.23 	
Required Software	
<input type="checkbox"/> Internet Services SD package: InternetSrvcs.INETSRVCS-RUN	
<input type="checkbox"/> LAN/9000 SD package: Networking.NET-RUN	
<input type="checkbox"/> SNMP Agent for MIB Monitoring (optional) SD Package for HP-UX 11.x and higher: OVSNMPAgent	
<input type="checkbox"/> Native Language Support (NLS) Package (optional) SD package: OS-Core.NLS-AUX	
<input type="checkbox"/> MIB-I or MIB II The MIB monitoring functionality of OVO requires SNMP-based, MIB-I (RFC 1156) or MIB-II (RFC 1158) compliant agent software.	
Kernel Settings	
No specific settings required; default settings are acceptable.	
Supported High-Availability Environments	
<ul style="list-style-type: none"> • HP Serviceguard 11.14, 11.15, 11.16, 11.17. • Veritas Cluster 3.5, 4.0, 4.1 	
Operating System Patches	
HP-UX 11.11 PA-RISC	
HWEnable11i	Hardware Enablement version B.11.11.0306.4 (June 2003) or higher
GOLDBASE11i	Gold Base Patch for HP-UX 11.i version B.11.11.0306.4 (June 2003) or higher
PHSS_26946	HP aC++ -AA runtime libraries (aCC A.03.37)
PHSS_28871	ld(1) and linker tools cumulative patch.
PHNE_28568	s700_800 11.11 ONC/NFS General Release/Performance Patch
PHCO_27950	tbl(1) cumulative patch (optional in case of man page formatting issues)
HP-UX 11.23 IA64	
The OVO HTTPS agent for HP-UX 11.23 runs as a native 32-bit application on IA64. There are no 64-bit APIs offered.	
PHSS_31086	libunwind Library Cumulative patch

Solaris HTTPS Agent Software Requirements

Table 3-3 Solaris HTTPS Agent Software, Settings and Operating System Patches

<p>Solaris SPARC Supported Platforms</p> <p>Solaris 7, 8, 9, 10</p> <p>Solaris x86/x64 Supported Platforms</p> <p>Solaris 10</p>											
<p>Sun Solaris Required Software</p> <p><input type="checkbox"/> MIB</p> <p>The MIB monitoring functionality of OVO requires the snmpd of the HP OpenView platform, or SNMP-based, MIB-I (RFC 1156) or MIB-II (RFC1158) compliant agent software.</p> <p><input type="checkbox"/> MIB-I or MIB II</p> <p>The MIB monitoring functionality of OVO requires SNMP-based, MIB-I (RFC 1156) or MIB-II (RFC 1158) compliant agent software.</p> <p><input type="checkbox"/> Solaris x86/x64</p> <p>At least a minimal installation of OVO/UNIX Management Server version 8.22 is required..</p>											
<p>Kernel Settings</p> <p>No specific settings required for Solaris 8; default settings are acceptable.</p> <p>Set the following minimum kernel parameter values for Solaris 9:</p> <pre>semsys:seminfo_semmni=30 semsys:seminfo_semmns=200 semsys:seminfo_semmns1=100</pre>											
<p>Supported High-Availability Environments</p> <ul style="list-style-type: none"> • Sun Cluster 3.0, 3.1. • Veritas Cluster 3.5, 4.0, 4.1 											
<p>Operating System Patches</p>											
<p>Solaris 8</p> <table border="1"> <tr> <td>108434-13</td> <td>SunOS 5.8: 32-Bit shared library patch for C++</td> </tr> <tr> <td>108528-23</td> <td>SunOS 5.8: Kernel update patch</td> </tr> <tr> <td>108993-25</td> <td>SunOS 5.8: LDAP2 client, libc, libthread and libnsl libraries patch</td> </tr> <tr> <td>109147-25</td> <td>SunOS 5.8: Linker patch</td> </tr> <tr> <td>111293-04</td> <td>SunOS 5.8: /usr/lib/libdevinfo.so.1</td> </tr> </table>		108434-13	SunOS 5.8: 32-Bit shared library patch for C++	108528-23	SunOS 5.8: Kernel update patch	108993-25	SunOS 5.8: LDAP2 client, libc, libthread and libnsl libraries patch	109147-25	SunOS 5.8: Linker patch	111293-04	SunOS 5.8: /usr/lib/libdevinfo.so.1
108434-13	SunOS 5.8: 32-Bit shared library patch for C++										
108528-23	SunOS 5.8: Kernel update patch										
108993-25	SunOS 5.8: LDAP2 client, libc, libthread and libnsl libraries patch										
109147-25	SunOS 5.8: Linker patch										
111293-04	SunOS 5.8: /usr/lib/libdevinfo.so.1										
<p>Solaris 9</p> <p>No patches are required.</p>											
<p>Solaris 10</p> <ul style="list-style-type: none"> • SPARC <p>No patches are required for SPARC.</p> <ul style="list-style-type: none"> • x86/x64 <p>SunOS5.10 GA 01/06 for x86/x64.</p>											

Linux HTTPS Agent Software Requirements

Table 3-4 Linux HTTPS Agent Software, Settings and Operating System Patches

<p>Linux Supported Platforms (Intel x86)</p> <ul style="list-style-type: none">• Debian: 3.0, 3.0r1, 3.0r2, 3.1• Mandrake 9.2• RedFlag Professional Server 4.0• Red Hat: RHEL-AS/ES/WS 2.1, 3, 3 U3 on AMD64/EM64T, RHEL 3 U6• SuSE: 8.0, 8.1, 8.2, 9, SuSE 9.1 on x86, SUSE Enterprise Server 8 <p>No patches are required for the supported distribution versions.</p>
<p>Linux Required Software</p> <ul style="list-style-type: none"><input type="checkbox"/> Red Hat Package Manager (RPM) <i>Must</i> be installed on Debian systems.<input type="checkbox"/> SNMP Daemon (optional) Ensure that the SNMP daemon (<code>snmpd</code>) is running when you install the software remotely from the OVO management server. This allows the OVO management server to automatically determine the node type of the Linux managed node. The SNMP daemon must also be running if you want to use MIB variable monitoring.<input type="checkbox"/> MIB-I or MIB II The MIB monitoring functionality of OVO requires SNMP-based, MIB-I (RFC 1156) or MIB-II (RFC 1158) compliant agent software.
<p>Kernel Settings</p> <p>No specific settings required; default settings are acceptable.</p>
<p>Supported High-Availability Environments</p> <ul style="list-style-type: none">• Red Hat Enterprise Linux – Advanced Server 2.1 / 3.0.
<p>RH AS/ES/WS 3.0</p> <p>An updated RPM package that addresses possible RPM database issues must be installed. The package is <code>rpm-4.2.1-4.4.i386.rpm</code> or a superseding one.</p> <p>In addition, the <code>RPM_FORCE_NPTL</code> environment variable must be set for the root user.</p> <p>Refer to the following document for more information: https://rhn.redhat.com/errata/RHEA-2004-010.html</p>

Microsoft Windows HTTPS Agent Software Requirements

Table 3-5 Microsoft Windows HTTPS Agent Software, Settings and Operating System Patches

<p>Microsoft Windows Supported Platforms (Intel x86)</p> <p>Windows 2000 including SP3-SP6 XP Professional including SP1 and SP2 2003 Server including SP1</p>	
<p>Software Requirements</p> <p><input type="checkbox"/> FTP</p> <p>FTP Service must be running (required during “FTP Agent Package” installation). The FTP service must have read/write permission for the FTP home directory and must not allow anonymous FTP access if the Administrator account is used.</p> <p><input type="checkbox"/> SNMP Services</p> <p>SNMP services must be running if you plan to use discovery and other SNMP features of OVO.</p> <p><input type="checkbox"/> MIB-I or MIB II</p> <p>The MIB monitoring functionality of OVO requires SNMP-based, MIB-I (RFC 1156) or MIB-II (RFC 1158) compliant agent software.</p>	
<p>Supported High-Availability Environments</p> <ul style="list-style-type: none"> MS Cluster Server. 	
<p>Operating System Patches</p>	
<p>Windows 2000</p>	
Service Pack	Service Pack 3 or higher supported Service Pack
msvcp60.dll	Often installed by another Microsoft product. If this is not the case, you can install this DLL from the MS installation CD under the support/tools section.
<p>Windows XP Professional</p> <p>No patches are required.</p>	
<p>Windows 2003</p> <p>No patches are required.</p>	

AIX HTTPS Agent Software Requirements

Table 3-6 AIX HTTPS Agent Software, Settings and Operating System Patches

AIX Supported Platforms	
<ul style="list-style-type: none"> <input type="checkbox"/> AIX: 5.1, 5.2, 5.3 English and Japanese Locales <input type="checkbox"/> POWER 5 hardware with 64-bit Kernel running AIX5.3 OS <input type="checkbox"/> HACMP 5.2 (64 bit) with ClAw feature certified for AIX 5.1 and 5.2 (including OSSPI) 	
Required Software	
<p>The OVO HTTPS agent for AIX is available. Although it is not included in the OVO/UNIX media kit, it can be downloaded from the following site: http://support.openview.hp.com/cpe/patches/ito/ito.jsp</p> <p>NOTE: Make sure you have installed a depot on the OVO management server before you begin with the AIX HTTPS agent patch installation.</p> <p>The following file provided along with the depot needs to be replaced on the management server in /opt/OV/bin/OpC/agtinstall for the successful deployment of the AIX agent from the OVO 8.1 management server:</p> <p>Source file name: opcxinst_bbc.hpux</p> <p>Target file name: opcxinst_bbc</p> <p>Execute the following command:</p> <pre>cp opcxinst_bbc.hpux /opt/OV/bin/OpC/agtinstall/opcxinst_bbc</pre>	
<ul style="list-style-type: none"> <input type="checkbox"/> SNMP Daemon (optional) <p>Ensure that the SNMP daemon (snmpd) is running when you install the software remotely from the OVO management server. This allows the OVO management server to automatically determine the node type of the managed node. The SNMP daemon must also be running if you want to use MIB variable monitoring.</p> <input type="checkbox"/> MIB-I or MIB II <p>The MIB monitoring functionality of OVO requires SNMP-based, MIB-I (RFC 1156) or MIB-II (RFC 1158) compliant agent software.</p> 	
Kernel Settings	
No specific settings required; default settings are acceptable.	
Supported High-Availability Environments	
HACMP 5.1, 5.2 and 5.3 (64 bit)	
OS-SPI Support	
Required patches	PHSS_33106
Operating System Patches	
AIX 5.1	
Patch Level 7	
AIX 5.2	
Patch Level 4	
AIX 5.3	

Table 3-6 AIX HTTPS Agent Software, Settings and Operating System Patches

Patch Level 2	
Additional Requirements	
Performance Statistics filesets	bos.perf.libperfstat bos.perf.perfstat bos.perf.perfstat
POWER 5 with 64-bit Kernel running AIX 5.3	Xlc.Aix50.rte.7.0.0.5 fileset or greater

4 DCE Agent Installation Requirements

This chapter provides prerequisite information for the OVO 7 DCE agents:

- “DCE Agent Hardware Requirements”
- Software Requirements

Before installing OVO, make sure the hardware appropriate for your DCE¹ managed node platform is available. The hardware requirements are detailed in “DCE Agent Hardware Requirements” on page 83.

Before installing OVO, make sure the software appropriate for your DCE managed node platform is installed. The software requirements are detailed in the following tables:

- “HP-UX PA-RISC DCE Agent Software Requirements” on page 85
- “HP-UX Itanium DCE Agent Software Requirements” on page 87
- “Sun Solaris (SPARC) DCE Agent Software Requirements” on page 88
- “Linux DCE Agent Software Requirements” on page 90
- “Microsoft Windows DCE Agent Software Requirements” on page 92
- “AIX DCE Agent Software Requirements” on page 96
- “Tru64 UNIX DCE Agent Software Requirements” on page 98
- “Novell NetWare DCE Agent Software Requirements” on page 99
- “SGI IRIX DCE Agent Platforms” on page 100
- “IBM/Sequent ptx DCE Agent Software Requirements” on page 101
- “OpenVMS DCE Agent and Smart Plug-In Software Requirements” on page 103
- “SINIX RM/Reliant DCE Agent Platforms” on page 102

NOTE

In case you have IBM zSeries (s/390) systems running zOS (OS/390, MVS) or AS/400 systems running OS/400, you can use the OVO/UNIX add-on products "OS/390 Management" and "OS/400 Management". These products provide OVO agent-like capabilities including default instrumentation. For further information, refer to http://ovweb.external.hp.com/lpe/doc_serv/.

1. The OVO 7.xx agents are generically referred to as DCE agents in this document. This usually includes all non-HTTPS OVO agents, including those using the following protocols:
 - Distributed Computing Environment (DCE)
 - Network Computing System (NCS)
 - SunRPC
 - EZRPC

DCE Agent Versions

WARNING If you have already installed newer DCE agent patch levels on the OVO/UNIX 7.1x management server, do NOT install the DCE agent packages that are delivered with the OVO/UNIX 8 Media Kit.

During an upgrade to OVO/UNIX 8, the DCE agent versions installed on the OVO/UNIX 7.1x installation are retained, even if they are an earlier version than those provided with OVO/UNIX 8.

There are newer OVO 7.xx DCE agent patches available than those shipped with the OVO/UNIX 8 Media Kit. To obtain the newer patches, follow the link below.

NOTE You may apply the SAME OVO 7.xx DCE agent patches for OVO/UNIX 7.xx and OVO/UNIX 8 management servers.

Unless you have upgraded from OVO/UNIX 7.10, the Software Distributor Installed Products Database will not have a record of the actual DCE agent versions (patch levels). Therefore you must make sure that you do not downgrade your agents by installing a patch with a lower version than the installed one (as displayed by the `opcversion -a` command).

The latest agent component patches are available from the following web site. Refer to this information to ensure that you have the latest agent patch levels:

<http://openview.hp.com/sso/ecare/getsupportdoc?docid=OVO-PATCHES>

The DCE agent versions (patch levels) provided with OVO/UNIX 8.1x and the latest available patch levels are listed in Table 4-1, “OVO 7 DCE Agent Versions from OVO 8.1x HP-UX Media Kit and Latest,” on page 82.

The DCE agent version currently installed on the OVO management server can be checked with the `opcversion` utility.

Example:

```
/opt/OV/bin/OpC/agtinstall/opcversion -a
```

The output takes the following form:

```
dec/alpha/unix51A+:  
07.10V5.1, P5.1, 5.1  
opc_version: 07.23  
comm_version: 2.6.5.0  
perf_version: 07.21  
  
hp/ia64/hp-ux11_32:  
07.10 11.22, 11.23  
opc_version: 07.23  
comm_version: 2.6.5.0  
perf_version: 07.21
```

NOTE The agent version on the managed node for all platforms can be checked with the command:
`opcragt -agent_version <node_name>`

NOTE OVO/UNIX Product Support Matrix with the latest patch levels available for the supported platforms is available through:

http://support.openview.hp.com/sc/support_matrices.jsp

or by following the HP OpenView Support Matrix > HP OpenView Support Matrix - Part 1 - Operations and Service Navigator Value Pack links at:

http://partners.openview.hp.com/ovcw/pricing/config_matrix.jsp

Table 4-1 OVO 7 DCE Agent Versions from OVO 8.1x HP-UX Media Kit and Latest

Managed Node Platform	DCE Agent Version					
	Message/Action		Communication		Embedded Performance	
	OVO 8.1x CD	Latest	OVO 8.1x CD	Latest	OVO 8.1x CD	Latest
HP-UX PA-RISC 11.11, 11.23	07.25	7.32	7.14 2.6.5.0	7.16	07.21	7.27
HP-UX Itanium IA64 11.22, 11.23	07.25	7.32	7.14 2.6.5.0	7.17	07.21	7.27
Solaris 2.6, 7, 8, 9, 10	07.25	7.32	7.14 2.6.5.0	7.17	07.21	7.27
Microsoft Windows 2000, XP Professional, 2003	07.25	7.32	7.14 2.6.5.0	7.17	07.21	7.27
Linux (Kernel 2.4) Refer to Table 4-9	07.25	7.32.1	7.14 2.6.5.0	7.16	07.21	7.27
IBM AIX 4.3.1, 4.3.2, 4.3.3, 5.1, 5.2, 5.3	07.25	7.32	7.14 2.6.5.0	7.17	07.21	7.27
Tru64 Tru64 4.0F, 4.0G, 5.1A, 5.1B	07.23	7.32	7.14 2.6.5.0	7.17	07.21	7.27
Novell NetWare 5.1, 6.0, 6.5	07.12	7.13	Not Applicable			
SGI IRIX 6.2, 6.4, 6.5	07.10	7.10	Not Applicable			
IBM/Sequent ptx 4.4.10, 4.5.3	07.10	7.10	Not Applicable			
SINIX RM/Reliant 5.43C20, 5.44, 5.45	07.10	7.10	Not Applicable			
OpenVMS for Alpha	N/A	7.23.1	Not Applicable			
OpenVMS for Integrity	N/A	7.23.1	Not Applicable			

DCE Agent Hardware Requirements

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

Table 4-2 Disk Space for OVO DCE Agents

Platform	Required Disk Space ^a
HP-UX PA-RISC	28 MB
HP-UX Itanium	47 MB
Sun Solaris (SPARC)	65 MB <ul style="list-style-type: none"> • NCS - 10 MB • DCE - 20 MB <ul style="list-style-type: none"> — 10 MB for OVO agent — 10 MB for HP Lightweight DCE software
Linux	33 MB
Microsoft Windows Installation Server	<p>Local Drive 35 MB free disk space must be temporarily available on the drive that contains the FTP directory during installation.</p> <p>NTFS Disk A total of 65 MB of free disk space must be available on the NTFS-formatted disk:</p> <ul style="list-style-type: none"> • 50 MB for the installed agent files. • 15 MB for the agent packages to be transferred to the managed nodes.
Microsoft Windows Managed Node	<p>Local Drive 35 MB free disk space must be temporarily available on the drive that contains the FTP directory during installation.</p> <p>NTFS Disk 50 MB of space must be free for the installed agent files on the first NTFS-formatted disk (usually c:\).</p>
AIX	60 MB
Novell Netware	<ul style="list-style-type: none"> • <i>NetWare Server</i> 10 MB on each NetWare server in the SYS: volume • <i>Software Depot</i> 20 MB disk space for the software depot on the Windows 95/98/NT/2000 server.
SGI IRIX	10 MB
SINIX RM/Reliant ^b	14 MB
Tru64 UNIX	35 MB For TruCluster systems, this disk space is required on each node.

Table 4-2 Disk Space for OVO DCE Agents (Continued)

Platform	Required Disk Space ^a
IBM/Sequent ptx ^b	10 MB OVO agent must be installed on an HPFS partition. FAT partitions are not supported for OVO agent operation.
OpenVMS Alpha	18 MB
OpenVMS Integrity	35 MB

a. Approximately double the specified disk space is required during the software installation.

Table 4-3 Additional RAM Required by OVO DCE Agents

Platform	Required Additional Ram
Linux	20 MB
Microsoft Windows	15 MB
Sequent DYNIX	4 MB
Novell Netware	<p><i>NetWare Server</i> 7 MB additional free RAM on the NetWare server:</p> <ul style="list-style-type: none"> • 4 MB for the OVO agent • 1 MB for TIRPC • 0.5 to 2 MB for the NetWare Management Agent and XCONSOLE (<i>optional</i>) <p>At least 32 MB of server RAM is suggested for fair performance (depending on the OS version). <i>OVO Agent</i> 16 MB additional free RAM for the OVO agent if using NetWare SFT III file servers.</p>

HP-UX PA-RISC DCE Agent Software Requirements

Table 4-4 HP-UX PA-RISC DCE Agent Software, Settings and Operating System Patches

HP-UX Supported Platforms	
HP-UX 11.11, 11.23, 11.23PI	
HP-UX Required Software	
<input type="checkbox"/> Internet Services SD package: InternetSrvcs.INETSRVCS-RUN	
<input type="checkbox"/> LAN/9000 SD package: Networking.NET-RUN	
<input type="checkbox"/> Native Language Support (NLS) Package (optional) SD package: OS-Core.NLS-AUX	
<input type="checkbox"/> SNMP Agent for MIB Monitoring (Required for HP-UX 11.11 only) SD Package for HP-UX 11.x and higher: OVSNMPAgent	
Kernel Settings	
NOTE: If monitoring performance metrics with the embedded performance component, increase the value of the kernel parameter <code>max_thread_proc</code> to: <code>min + (Number_of_Templates * 2)</code> .	
Supported High-Availability Environments	
<input type="checkbox"/> HP Serviceguard 11.11 - 11.17 <input type="checkbox"/> Veritas Cluster 3.5, 4.0, 4.1	
Operating System Patches	
HP-UX 11.11 PA-RISC	
GOLDBASE11i	Gold Base Patches for HP-UX 11.i, June 2003, version B.11.11.0306.4
PHSS_26946	HP aC++ -AA runtime libraries (aCC 03.37)
PHSS_26560	ld(1) and linker tools cumulative patch.
PHNE_28568	s700_800 11.11 ONC/NFS General Release/Performance Patch

Table 4-5 Important Kernel Parameters for Managed Nodes

Parameter	Description	Minimum Value
<code>nfile</code>	Maximum number of open files.	20 ^a
<code>semms</code>	Required semaphores.	20
<code>shmmax</code>	Maximum shared memory.	None required.
<code>msgmni</code>	Message queues.	None required.
<code>nlocks</code>	File locks.	10

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

HP-UX Itanium DCE Agent Software Requirements

Table 4-6 HP-UX Itanium DCE Agent Software, Settings and Operating System Patches

<p>HP-UX Supported Platforms</p> <p>HP-UX 11.22, 11.23</p>
<p>HP-UX Required Software</p> <p>HP-UX Itanium DCE agent software is not part of the OVO 7.10 media kit but can be downloaded.</p> <ul style="list-style-type: none"> <input type="checkbox"/> DCE RPC DCE RPC version 1.7 or higher. SD package: DCE-Core.DCE-CORE-RUN NOTE: OVO supports DCE versions supplied with the HP-UX 11.x operating system. Although the HP-UX operating system includes DCE, you must install DCE separately as an optional product. <input type="checkbox"/> Internet Services SD package: InternetSrvcs.INETSRVCS-RUN <input type="checkbox"/> LAN/9000 SD package: Networking.NET-RUN <input type="checkbox"/> Native Language Support (NLS) Package (optional) SD package: OS-Core.NLS-AUX
<p>Kernel Settings</p> <p>NOTE: If monitoring performance metrics with the embedded performance component, increase the value of the kernel parameter <code>max_thread_proc</code> to: <code>min + (Number_of_Templates * 2)</code>.</p>
<p>Supported High-Availability Environments</p> <ul style="list-style-type: none"> <input type="checkbox"/> HP Serviceguard 11.14.01 for HP-UX 11.22, and 11.15-11.17 for HP-UX 11.23. Application package monitoring (opcapm) is not supported. <input type="checkbox"/> Veritas Cluster 3.5, 4.0, 4.1

Table 4-7 Important Kernel Parameters for Managed Nodes

Parameter	Description	Minimum Value
<code>nfile</code>	Maximum number of open files.	20 ^a
<code>semms</code>	Required semaphores.	20
<code>shmmax</code>	Maximum shared memory.	None required.
<code>msgmni</code>	Message queues.	None required.
<code>nlocks</code>	File locks.	10

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

Sun Solaris (SPARC) DCE Agent Software Requirements

Table 4-8 Sun Solaris (SPARC) DCE Agent Software, Settings and Operating System Patches

<p>Sun Solaris Supported Platforms</p> <p>Solaris 2.6, 7, 8, 9, 10</p>							
<p>Sun Solaris Required Software</p> <p><input type="checkbox"/> Communication Software</p> <ul style="list-style-type: none"> • <i>NCS</i> <p>If NCS is chosen as the <code>Communication Type</code> in the OVO GUI, and NCS version 1.5.1 is <i>not</i> found on the managed node, OVO installs <code>11bd</code> and <code>1b_admin</code> during the OVO agent software installation.</p> <ul style="list-style-type: none"> • <i>DCE</i> <p>Supported DCE packages: IBM DCE 3.1, HPLwdce 1.1.x, DASCOM DCE 1.1.x.</p> <p>If the communication type is set to DCE RPC (TCP or UDP) and none of the supported DCE packages is installed (or running) on the managed node, then the HPLwdce (HP Lightweight DCE runtime version 1.1) is installed and configured.</p> <p><input type="checkbox"/> ARPA/Berkeley Services</p> <p><input type="checkbox"/> MIB</p> <p>The MIB monitoring functionality of OVO requires the <code>snmpd</code> of the HP OpenView platform, or SNMP-based, MIB-I (RFC 1156) or MIB-II (RFC1158) compliant agent software.</p> <p>Kernel Settings</p> <p>Set the following minimum kernel parameter values:</p> <pre>semsys:seminfo_semmni=30</pre> <pre>semsys:seminfo_semmmap=15 (If available on platform).</pre> <pre>semsys:seminfo_semmns=200</pre> <pre>semsys:seminfo_semmsl=100</pre> <p>You can check and change the kernel parameters by editing the <code>/etc/system</code> file.</p>							
<p>Supported High-Availability Environments</p> <p><input type="checkbox"/> Sun Cluster 3.0, 3.1</p> <p><input type="checkbox"/> Veritas Cluster 3.5, 4.0, 4.1</p>							
<p>Operating System Patches</p> <p>The following patches are required for the OVO Sun Solaris managed nodes. They are available from the www.sunsolve.sun.com web site.</p> <p>See also the section “Problems with OS Patches for Sun Solaris” below for information about patches that must not be installed on Sun Solaris managed nodes.</p>							
<p>Solaris 2.6</p> <table border="1"> <tr> <td>107733-09</td> <td>SunOS 5.6: Linker patch</td> </tr> <tr> <td>105591-11</td> <td>SunOS 5.6: Shared library patch for C++</td> </tr> <tr> <td>106429-02</td> <td>SunOS 5.6: /kernel/drv/mm patch</td> </tr> </table>		107733-09	SunOS 5.6: Linker patch	105591-11	SunOS 5.6: Shared library patch for C++	106429-02	SunOS 5.6: /kernel/drv/mm patch
107733-09	SunOS 5.6: Linker patch						
105591-11	SunOS 5.6: Shared library patch for C++						
106429-02	SunOS 5.6: /kernel/drv/mm patch						

Table 4-8 Sun Solaris (SPARC) DCE Agent Software, Settings and Operating System Patches (Continued)

105181-29	SunOS 5.6: Kernel update patch
105210-38	SunOS 5.6: libaio, libc & watchmalloc patch
105568-23	SunOS 5.6: /usr/lib/libthread.so.1 patch
105633-59	OpenWindows 3.6: Xsun patch
106841-01	OpenWindows 3.6: Keytables patch
106842-09	SunOS 5.6: Feature patch for Euro currency support in Solaris 2.6
105181-16 105210-24 105568-14	For multi-processor systems which use the DCE communication type, make sure you that have these patches installed.
Solaris 7	
106950-15	SunOS 5.7: Linker patch
106327-10	SunOS 5.7: 32-Bit Shared library patch for C++
107544-03	SunOS 5.7: /usr/lib/fs/ufs/fsck patch
106541-17	SunOS 5.7: Kernel update patch
106980-17	SunOS 5.7: libthread patch
Solaris 8	
109147-09	SunOS 5.8: Linker patch
108434-03	SunOS 5.8: Shared library patch for C++
108827-11	SunOS 5.8: libthread patch
Solaris 9 No patches are required.	
Solaris 10 No patches are required.	
Problems with OS Patches for Sun Solaris	
101327-04 101327-05	<p>If version -04 or -05 of patch 101327 is installed, the OVO installation fails on Sun Solaris managed nodes with the following message:</p> <pre>tar xof...core dump</pre> <p>To solve this problem, do one of the following:</p> <ul style="list-style-type: none"> • De-install the old patch • Install patch version -06 (or later) <p>To check which patches are currently installed on Sun Solaris systems, enter:</p> <pre>showrev -p</pre>

Linux DCE Agent Software Requirements

Table 4-9 Linux DCE Agent Software, Settings and Operating System Patches

Linux Supported Platforms (Intel x86)				
Refer to the detailed listing later in this table.				
Linux Pentium Required Software				
<input type="checkbox"/> DCE RPC Delivered with the OVO DCE agent packages.				
<input type="checkbox"/> General Packages The following packages <i>must</i> be installed on every platform: <ul style="list-style-type: none"> • bash and gawk 				
<input type="checkbox"/> Red Hat Package Manager (RPM) <i>Must</i> be installed on Debian systems.				
<input type="checkbox"/> SNMP Daemon (optional) Ensure that the SNMP daemon (<code>snmpd</code>) is running when you install the software remotely from the OVO management server. This allows the OVO management server to automatically determine the node type of the Linux managed node. The SNMP daemon must also be running if you want to use MIB variable monitoring.				
Language	OS and Version	Packages	Kernel	glibc
English	Red Hat EL 2.1 ^a	compat-libstdc++ glibc	2.4.x (x ≥ 9)	2.2.4
	Red Hat EL 3 ^b		2.4.21	2.3.2
	SuSE 7.2	compat glibc	2.4.x (x ≥ 4)	2.2.2
	SuSE 7.3		2.4.x (x ≥ 10)	2.2.4
	SuSE 8.0		2.4.x (x ≥ 18)	2.2.5
	SuSE 8.1x, 8.2	compat-2002 glibc	2.4.x (x ≥ 19)	2.2.5-161
	SuSE Enterprise Server 8.0		2.4.x (x ≥ 19)	2.2.5
	SuSE 9.0		2.4.x (x ≥ 21)	2.3.x (x ≥ 2)
English	Debian 3.0	libstdc++2.9-glibc2.1 libc6	2.4.x (x ≥ 18)	2.2.5
	Debian 3.0 r1, 3.0 r2		2.4.x (x ≥ 18)	2.2.5
	Mandrake 9.2	libstdc++2.10	2.4.x (x>=22)	2.3.2
	RedFlag Professional Server 4.0	libstdc++-3.2-2.96.110 libgcc-3.2-7	2.4.x (x >=20-8)	2.2.93-5

Table 4-9 Linux DCE Agent Software, Settings and Operating System Patches

<p>Supported High-Availability Environments</p> <p>❑ Red Hat Enterprise Linux – Advanced Server 2.1 / 3.0.</p> <p>No patches are required for the supported distribution versions.</p>
<p>Linux Itanium</p> <p>The OVO DCE agent runs in emulation mode on IA64 Linux.</p> <p>NOTE Kernel versions 2.4.18-e.47 - e.54 will hinder the functionality of the RHEL 2.1 agent on Itanium. Please use kernel patch 2.4.18-e.56 available from RedHat.</p>
<ul style="list-style-type: none">• RH EL-AS 2.1, RH EL-AS 3 (with U2 and U3* patch) <p>*An operating system issue prevents the installation of OVO agent on Red Hat Enterprise Linux 3 Update 3 for Itanium. Please read https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=137452 and follow the instructions for resolving this issue. A 32-bit bash is also required. The media kit contains the bash-2.05b-29.0.3.i386.rpm package.</p> <ul style="list-style-type: none">• RedHat Enterprise Linux 4 on x86 RedHat Enterprise Linux 4 on AMD64/EM64T RedHat Enterprise Linux 3 update 4 on Itanium• SUSE 9.1 on x86 SUSE Enterprise Server 9 on AMD64/EM64T SUSE Enterprise Server 9 on Itanium

- a. Red Hat Enterprise Linux AS, ES and WS 2.1
- b. Red Hat Enterprise Linux AS, ES and WS 3.0

Microsoft Windows DCE Agent Software Requirements

Table 4-10 Windows DCE Agent Software, Settings and Operating System Patches

<p>Windows Supported Platforms Microsoft Windows 2000, XP Professional, 2003 Server.</p>
<p>Requirements for the OVO Management Server Make sure your OVO management server meets the following requirements:</p> <ul style="list-style-type: none"><input type="checkbox"/> Kernel Parameter Maxfiles Use the following settings for kernel parameter maxfiles:<ul style="list-style-type: none">• <i>35 or Less Windows Managed Nodes</i> If your installation includes 35 or less Windows managed nodes, use the setting for the kernel parameter maxfiles described in the <i>Installation Guide for the Management Server</i>.• <i>36 or More Managed Nodes</i> If your installation includes 36 or more Windows managed nodes, increase the setting of maxfiles by the following: $3 * \text{Number_of_additional_NT_nodes} + 15$
<p>Requirements for the Windows Installation Server If you are using a Windows Installation Server, make sure that it is a domain controller.</p>
<p>Requirements for the Windows Managed Node Make sure your OVO managed nodes meet the following requirements: NOTE: For information about software requirements for a combination of Windows NT Terminal Server Edition and Citrix MetaFrame, see “About Citrix MetaFrame Integration” in the <i>HP OpenView Operations DCE Agent Concepts and Configuration Guide</i>.</p>
<p>Software Requirements</p> <ul style="list-style-type: none"><input type="checkbox"/> FTP FTP Service must be running (required during “FTP Agent Package” installation). The FTP service must have read/write permission for the FTP home directory and must not allow anonymous FTP access if the Administrator account is used.<input type="checkbox"/> Name of Management Server The name of the management server must be known to the managed node. You can verify this by using the ping command.<input type="checkbox"/> Schedule Service Schedule service may <i>not</i> be disabled (required during installation)<input type="checkbox"/> TCP/IP Services TCP/IP services must be running and started automatically.
<p>Software Requirements (continued)</p> <ul style="list-style-type: none"><input type="checkbox"/> RPC Services RCP services (that is, the Remote Procedure Call Service must be running and started automatically.<input type="checkbox"/> SNMP Services SNMP services must be running if you plan to use discovery and other SNMP features of OVO.<input type="checkbox"/> DHCP Service DHCP (dynamic address service for Windows clients) may <i>not</i> be used because OVO relies on the IP address to identify the managed nodes.

Table 4-10 Windows DCE Agent Software, Settings and Operating System Patches

Supported High-Availability Environments	
<input type="checkbox"/> MS Cluster Server.	
Operating System Patches, Service Packs and Requirements	
Windows 2000 Pentium	
Service Pack	No Service Pack, Service Pack 1, 2, 3 or 4
msvcp60.dll	Often installed by another Microsoft product. If this is not the case, you can install this DLL from the MS installation CD under the support/tools section.
Windows XP Pentium	
Service Pack	No Service Pack, Service Pack 1, 2
Windows XP Service Pack 2 Firewall Settings	<p>The following steps are required when adding a node running Windows XP SP2 to the VPO Node Bank:</p> <ol style="list-style-type: none"> 1. Open the "Modify Node..." dialog of the node. 2. Open the "Communication Options..." dialog. 3. Change the "Communication Type" entry from "DCE RPC (UDP)" to "DCE RPC (TCP)" <p>The following steps are required for an agent installation via Installation Server on a node running Windows XP SP2:</p> <ol style="list-style-type: none"> 1. Open the Windows Firewall on the node. 2. Go to the tab "Exceptions". 3. Select the "File and Printer Sharing" option. <p>After the agent has been installed, the installation procedure adds some additional entries to the "Exceptions" tab:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> HP OpenView Black Box Communication Broker <input checked="" type="checkbox"/> HP OpenView Control Agent RPC Server <input checked="" type="checkbox"/> HP OpenView Performance Collector <p>For the agent to work correctly, these settings must remain assembled.</p> <p>These step will also be published in future versions of the OVO Unix Firewall Whitepaper.</p>
Windows 2003 Pentium	
Service Pack	No Service Pack, Service Pack 1
	No patches are required.
Windows 2003 64-bit Itanium.	
Service Pack	No Service Pack, Service Pack 1
	No patches are required
	The Virtual Term (PC) application has to run as user "HP ITO account" when started on an IA64 system. You can also use a fully qualified user login (username and password). The IA64 system doesn't allow a passwordless switch user.

Table 4-10 Windows DCE Agent Software, Settings and Operating System Patches

	The HP Installation Server method for installing agents is not supported on IA64 systems (for the Installation Server as well as for the node).
Windows 2003 64-bit AMD64/EM64T	
	Supported in x86 mode with Windows 2003 server Pentium running on AMD64/EMT64T processors.

Table 4-10 Windows DCE Agent Software, Settings and Operating System Patches

Windows 2003 Itanium

The Windows OVO DCE agent supports the 64 Bit version of Microsoft Windows Server 2003 but runs in emulation mode on IA64 Windows.

An additional Hotfix from Microsoft is required to stop memory leaks.

The following limitations that apply during the runtime of the agent:

Virtual Term (PC)

Virtual Term (PC) application has to run as user "HP ITO account" when started on an IA64 system, or you use a fully qualified user login (username and password). In general, the IA64 system doesn't allow a passwordless switch user!

HP Installation Server

The HP Installation Server method for installing agents is not supported on IA64 systems.

Files

The agent is not able to process files that are bigger than 2 GB. This mainly affects the Logfile Encapsulator, which is not able to read those files. In case a logfile exceeds this size, the following error is displayed:

Cannot seek file <...> System Error Number: 131(83) - (OpC20-70)

Registry

The registry entries for the agent are located under:

HKLM\SOFTWARE\Wow6432Node\Hewlett-Packard\...

In order to access the registry while using the original path:

HKLM\SOFTWARE\Hewlett-Packard\...

the application that is accessing the registry must also run in 32 bit emulation mode.

This applies, for example, to the VisualBasic script mgmt_sv.vbs.

The script should be executed by using the script engine located under:

%SYSTEMROOT%\SysWOW\64

You may use wscript.exe or cscript.exe.

The script will fail when using the standard script engine that is located in the PATH.

See the Microsoft Article Q305097, *How to View the System Registry By Using 64-Bit Versions of Windows*, for further information.

[http://support.microsoft.com/default.aspx?scid=kb; \[LN\]; 305097](http://support.microsoft.com/default.aspx?scid=kb;[LN];305097)

Microsoft Windows 2003 64 bit problems that affect the OVO agent

The agent processes may show a memory increase while starting external processes.

This problem is documented and fixed with the Microsoft article 822961, *A 32-bit process calls the CreateProcess function but does not successfully start another 32-bit process*:

[http://support.microsoft.com/default.aspx?scid=kb; \[LN\]; 822961](http://support.microsoft.com/default.aspx?scid=kb; [LN]; 822961)

HP strongly recommends that you install this HotFix prior to installing the OVO agent on Windows 2003 64 Bit installations.

AIX DCE Agent Software Requirements

Table 4-11 AIX DCE Agent Software, Settings and Operating System Patches

<p>AIX Supported Platforms AIX 4.3.1, 4.3.2, 4.3.3, 5L 5.1, 5L 5.2, 5L 5.3</p>	
<p>AIX Before installing OVO, make sure the following software is installed on AIX systems:</p> <p><input type="checkbox"/> Communication Software OVO supports the NCS RPC and DCE RPC communication types:</p> <p>Requirements for DCE RPC on AIX Managed Nodes For DCE RPC communication type, you must install the following software:</p> <ul style="list-style-type: none"> • <i>DCE on AIX</i> DCE is supplied with the AIX operating system up to version 4.2.x. With version 4.3 or newer, DCE is a standalone product and must be purchased separately. • <i>Filesets on AIX 4.3</i> On AIX 4.3 DCE RPC, you must install <i>one</i> of the following filesets: <pre>dce.client.core.rte 2.1 dce.client.rte 2.1 dce.client.core.rte.admin 2.1</pre> <p>Requirements for NCS RPC on AIX Managed Nodes For NCS RPC communication type, you must install the NCS Runtime package <code>bos.net.ncs</code>. You can verify and install NCS with the following commands: <pre>lslpp -l <package> installp -s <package></pre></p> <p><input type="checkbox"/> ARPA/Berkeley Services</p> <p><input type="checkbox"/> MIB-I or MIB II The MIB monitoring functionality of OVO requires SNMP-based, MIB-I (RFC 1156) or MIB-II (RFC 1158) compliant agent software.</p>	
<p>Supported High-Availability Environments HACMP 4.3.3, 4.4.1, 4.5, 4.5 ES, 5L 5.1, 5.2 (32 and 64 bit)</p>	
<p>Operating System Patches The following patches are required for AIX 4.3.1 managed nodes. Contact IBM support to obtain these patches</p>	
PTF: U455996	<pre>bos.up version 4.3.1.1 Base Operating System Uniprocessor Runtime</pre>

Table 4-11 AIX DCE Agent Software, Settings and Operating System Patches

PTF: U453884	bos.mp version 4.3.1.1 Base Operating System Multiprocessor Runtime
NOTE: To resolve monitor agent (opcmna) crashes in the mbstowcs() subroutine, at least the following revisions of OS patches should be installed on the system:	
4.3.3.89 (AIX 4.3)	bos.rte.libc
4.3.3.80 (AIX 4.3)	bos.rte.libpthreads
5.x (AIX 5L)	ML-03
NOTE: To collect the performance data, the following AIX OS filesets must be installed on the system: bos.perf.libperfstat [Performance Statistics Library Interface] and bos.perf.perfstat [Performance Statistics Interface]. Make sure that the filesets are installed prior to starting the OpenView performance tools. The latest version information for these filesets is available at: https://techsupport.services.ibm.com/server/aix.fdc The patch level of these filesets for each of the applicable OS versions are as follows:	
AIX 4.3.3	bos.perf.libperfstat 4.3.3.4 bos.perf.perfstat 4.3.3.1
AIX 5.1	bos.perf.libperfstat 5.1.0.52 bos.perf.perfstat 5.1.0.51
AIX 5.2	bos.perf.libperfstat 5.2.0.12 bos.perf.perfstat 5.2.0.12

Tru64 UNIX DCE Agent Software Requirements

Table 4-12 Tru64 UNIX DCE Agent Software, Settings and Operating System Patches

Tru64 UNIX Supported Platforms Tru64 4.0F, 4.0G, 5.1A, 5.1B
Kernel settings No specific settings required; default settings acceptable. You can verify and change the kernel parameters using the <code>setup</code> tool. NOTE: If monitoring performance metrics with the embedded performance component, and agent runs as non-root user, increase the value of the kernel parameter <code>max_threads_per_user</code> to: <code>default + (Number_of_Templates * 2)</code> .
Required Software Before installing OVO, make sure the following software is installed on Tru64 UNIX managed nodes: <ul style="list-style-type: none"><input type="checkbox"/> Required Patch for the Tru64 UNIX Managed Nodes The <code>CXXREDIST632V11.tar</code> patch is required for the Tru64 UNIX managed nodes. Check if the installed <code>libcxx</code> is earlier than <code>V60300001</code>: <pre>nm /usr/lib/comp1rs/cxx/libc*.so grep libc*_V</pre> If the symbol <code>_libc*_V60300001</code> exists in the image on your system, then you do <i>not</i> need to install this patch. You can download the latest version from the following ftp patch site: <code>ftp://ftp.compaq.com/pub/products/c-cxx/tru64/cxx/</code><input type="checkbox"/> Basic Networking Services OSFCLINET4xxx Basic Networking Services. The operating system determines the value of <code>xxx</code>.
<ul style="list-style-type: none"><input type="checkbox"/> DCE Runtime Kit NOTE: DCE Runtime Kit software is required only if you choose DCE as communication type. NOTE: The OVO DCE agent installed on Tru Cluster nodes must use the DCE communication Type. NCS is not supported on Tru Cluster OVO 7 managed nodes. NOTE: OVO supports DCE versions supplied with the Tru64 UNIX operating system. However, although the Tru64 UNIX operating system includes DCE on the layered product CD up to version 5.0A, DCE has to be installed separately as an optional product.<input type="checkbox"/> Package: OSFINCLUDExxx OSFINCLUDExxx Standard Header Files package is required for building executables on Tru64 UNIX nodes. The operating system determines the value of <code>xxx</code>.
Supported High-Availability Environments TruCluster 4.0F, 4.0G, 5.1A, 5.1B

Novell NetWare DCE Agent Software Requirements

Table 4-13 Novell NetWare DCE Agent Software, Settings and Operating System Patches

<p>Novell NetWare Supported Platforms Novell NetWare 5.1, 6.0, 6.5</p>
<p>Kernel settings No specific settings required; default settings acceptable.</p>
<p>Software Requirements for the Depot Server Before installing OVO, make sure the following software is installed on Novell NetWare depot server system:</p> <ul style="list-style-type: none"><input type="checkbox"/> Microsoft Windows Microsoft Windows 2000 Operating System.<input type="checkbox"/> Novell Client Novell Client 32 for Windows must be installed on the system to be used as the depot server.<input type="checkbox"/> FTP server (<i>optional</i>) It is recommended that the depot server runs FTP server so the OVO agent package can be easily transferred from the OVO management server to the depot server.<input type="checkbox"/> TIRPC If it is not already present on the system, TIRPC is supplied with the OVO agent software. It is installed during OVO agent installation. NOTE: On NetWare 6, PKERNEL service and TIRPC <i>cannot</i> run concurrently. This means that NFS and NDPS services will be unavailable while OVO Agent is running. The OVO Agent installation will disable starting of PKERNEL in AUTOEXEC.NCF file if it is present.
<ul style="list-style-type: none"><input type="checkbox"/> TCP/IP Services TCP/IP services must be configured (including name resolution), running, and started automatically.<input type="checkbox"/> Network FRAMING Types Network FRAMING types must be configured. Ethernet II frame type is required.<input type="checkbox"/> CLIB.NLM CLIB.NLM version 4.10 or higher must be installed.<input type="checkbox"/> SNMP Daemon (<i>optional</i>) SNMP daemon must be configured, running, and started automatically if monitoring and trap interception is required.<input type="checkbox"/> XCONSOLE (<i>optional</i>) XCONSOLE.NLM must be installed and configured on each server only if you want remote access from the Management Server. XCONSOLE is part of Novell products like Flex-IP and NetWare/IP. XCONSOLE must be configured and running. Remote console access (through telnet) must be allowed.<input type="checkbox"/> Novell NMA (<i>optional</i>) If Novell NMA is installed and configured on the NetWare server, it is recommended that Trap Interceptor templates from group NetWare are deployed on the NetWare managed node. Those templates will take advantage of information provided by NMA and forward the events detected by it to the management server message browser. In this case, it is recommended that Monitor Agent templates are <i>not</i> deployed on the managed node.<input type="checkbox"/> DSEVENT.NLM Default OVO instrumentation (VENDOR.NLM) requires the presence of DSEVENT.NLM on the system in order to catch events raised by the NDS system. This module is distributed by default with the operating system and should <i>not</i> be removed from the system.

SGI IRIX DCE Agent Platforms

Table 4-14 SGI IRIX DCE Agent Software, Settings and Operating System Patches

SGI IRIX Supported Platforms IRIX 6.2, 6.4, 6.5
Kernel settings No specific settings required; default settings acceptable. You can check and change the system parameters using the <code>sysmgr</code> tool.
Required Software Before installing OVO, make sure the following software is installed on SGI IRIX managed nodes: <ul style="list-style-type: none"><input type="checkbox"/> NCS For SGI IRIX 6.2 or higher, install the following NCS 1.5.1 package: <code>license_eoe.sw.netls_server</code> If neither NCS nor DCE are found on the managed node, OVO installs <code>llbd</code> and <code>lb_admin</code> during OVO software installation.<input type="checkbox"/> NFS For diskless operations, install SGI IRIX NFS on a cluster server.

IBM/Sequent ptx DCE Agent Software Requirements

Table 4-15 IBM/Sequent ptx DCE Agent Software, Settings and Operating System Patches

IBM/Sequent ptx Supported Platforms ptx 4.4.10, 4.5.3
Kernel settings No specific settings required; default settings acceptable. You can check and change the system parameters using the menu tool.
Software Requirements Before installing OVO, make sure the following software is installed on managed nodes: <ul style="list-style-type: none"><input type="checkbox"/> Sequent LAN Sequent local area network product ptx/LAN version 4.0.1. or higher.<input type="checkbox"/> Sequent TCP/IP Sequent TCP/IP product ptx/TCP/IP version 4.0.3 or higher.<input type="checkbox"/> Gradient NCS 1.5.1 NckNidl If NCS is not found on the managed node, OVO installs 11bd and 1b_admin during the OVO agent software installation.

SINIX RM/Reliant DCE Agent Platforms

Table 4-16 SINIX RM/Reliant DCE Agent Software, Settings and Operating System Patches

<p>SINIX RM/Reliant Supported Platforms SINIX 5.4320, 5.44, 5.45</p>
<p>Kernel settings No specific settings required; default settings acceptable. You can check and change the system parameters using the <code>sysadm</code> tool.</p>
<p>Required Software Before installing OVO, make sure the following software is installed on SINIX RM/Reliant managed nodes:</p> <ul style="list-style-type: none"><input type="checkbox"/> System Parameters You can check and change the system parameters using the <code>sysadm</code> tool.<input type="checkbox"/> Siemens-Nixdorf Networking Packages (5.43)<ul style="list-style-type: none">• <code>tcp</code>• <code>SImac596</code><input type="checkbox"/> Communication Software<ul style="list-style-type: none">• <i>NCS 1.5.1</i> If NCS is chosen as the <code>Node Type</code> in the OVO GUI, and NCS 1.5.1 is not found on the managed node, OVO installs <code>l1bd</code> and <code>l1b_admin</code> during the OVO agent software installation.• <i>DCE-CLNT 2.0</i> If the communication type is set to DCE RPCS (TCP or UDP), DCE-CLNT must be installed on the managed node. NOTE: You can purchase DCE at additional cost for SINIX/Reliant platforms from the platform vendor or from a third-party supplier.<input type="checkbox"/> Package: <code>atcmd</code>
<p>Package: <code>SIsnmpd</code> This package is necessary if you want to run the OVO monitoring agent. The 64-bit version of SINIX 5.45 includes this software package only for version V5.45A30 or higher. If you have a 64-bit SINIX 5.45 system with a lower version, you can either upgrade, take this package from the V5.45A30 release, or take the following files from a 32-bit SINIX 5.45 system:</p> <ul style="list-style-type: none">• <code>/opt/lib/snmpd/snmpplib/libsnmp.so</code>• <code>/opt/lib/snmpd/snmpplib/libsnmpio.so</code>• <code>/opt/lib/snmpd/snmpplib/libsnmpuser.so</code>• <code>/opt/snmp/lib/libsnmpapi.so</code> <p>and copy them to their original locations in <code>/opt/lib/snmpd</code> and <code>/opt/snmp/lib</code> directories. Before starting the OVO agent, export the <code>LD_LIBRARY_PATH</code> path to the SNMP product library directories using the following commands:</p> <pre>LD_LIBRARY_PATH=\$LD_LIBRARY_PATH:/opt/snmp/lib:/opt/lib/snmpd/snmpplib export LD_LIBRARY_PATH.</pre>

OpenVMS DCE Agent and Smart Plug-In Software Requirements

Table 4-17 **OpenVMS DCE Agent Software, Settings and Operating System Patches**

<p>OpenVMS Supported Platforms OpenVMS Alpha versions 7.3-2, 8.2 OpenVMS Integrity versions 8.2-1, 8.3</p>
<p>Required Software</p> <ul style="list-style-type: none">❑ OpenVMS Alpha Version 7.3-2 DEC AXPVMS VMS732_UPDATE V6.0 DEC AXPVMS VMS732_SYS V8.0 DEC AXPVMS VMS732_PCSI V3.0❑ OpenVMS Alpha Version 8.2 DEC AXPVMS VMS82A_SYS V2.0 DEC AXPVMS VMS82A_UPDATE V1.0❑ OpenVMS Integrity Version 8.2 HP I64VMS VMS821I_SYS V3.0 HP I64VMS VMS821I_UPDATE V 3.0❑ OpenVMS Integrity Version 8.3 No patches required
<ul style="list-style-type: none">❑ DCE Runtime Kit NOTE: DCE Runtime Kit software is required only if you choose DCE as communication type. The DCE Runtime kit is bundled with the OpenVMS Operating System and must be started for the OpenVMS OVO Agents to function.❑ SNMP SNMP must be enabled and started for the OpenVMS OVO Agents to recognize the Operating System.

5 HTTPS Agent Resource Requirements and Performance

This section highlights some operating differences between the HTTPS and DCE agents and explains the points you should consider when installing agents.

Some new shared OpenView components have been introduced to work with the OVO HTTPS agent. Therefore, the system requirements for the HTTPS agents are higher than for the DCE agent. However, it is normally not required to change any system parameters from the operating system defaults to higher values for the HTTPS agent on any platform.

For further information, also refer to the *HP OpenView Operation HTTPS Agent Concepts and Configuration Guide* and *HP OpenView Operations for UNIX Performance Guide*, both available for download at the following location:

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

Comparison Between HTTPS and DCE Agents

❑ Disk Space

The HTTPS agent needs approximately twice the disk space used by the DCE agent. However, additional OpenView products installed on the same system use the already present shared components.

❑ Main Memory Usage

The HTTPS agent needs approximately 2 to 3 times more main memory than the DCE agent at agent startup. During runtime, the difference in additional memory consumption between DCE and HTTPS agent is negligible.

Known Problem

The `ovconfd` process can grow and eventually exceed the HP-UX operating system default of 64 MB main memory per process. This depends on the amount of configuration data to be installed and on the number of configuration transfers.

If large amounts of configuration data are distributed frequently, for example 5 MB deployed each day, the `maxdsiz` kernel parameter on HP-UX systems should be increased to a minimum of 128 MB.

❑ Number of Open File Handles, Number of Semaphores, Shared Memory

No significant difference between DCE and HTTPS agents.

❑ Number of Processes

The HTTPS agent has one more process than the DCE agent. The differences are:

- DCE: `rpcd` (DCE daemon), `opcctl1a`.
- HTTPS: `ovbbccb` (replaces `rpcd`), `ovconfd` and `ovcd` (replace `opcctl1a`).

❑ CPU Usage and Overall Performance

There is no significant difference in the throughput of the interceptor processes, including `opcmona`, `opc1e`, `opcmsgi`, between DCE and HTTPS agents.

Message transfer of the HTTPS agent is slower, for example, due to the default usage of SSL encryption. However, optimizations have been implemented to reduce the peak demands, for example by using a block mode transfer when sending many messages in a short period of time.

Configuration deployment to an HTTPS agent is slower than to a DCE agent. In particular the transfer of instrumentation (previously referred to as actions/commands/monitors) can take a noticeable amount of time, in the range of a few minutes. Improvements are planned as part of the next releases.

Installation of the HTTPS agent binaries takes longer than for the DCE agent. This is due to the installation of the new, shared OpenView components. However, additional OpenView products benefit, as the shared components are only installed once by the first product but used by the additional products.

Comparison Between OVO 7.x and OVO 8 Agent-Related Management Server Components

❑ Main Memory Usage

The OVO/UNIX 8 management server requires approximately 2 to 3 times more main memory than the OVO/UNIX 7.x management servers. The increase is mainly caused by some additional processes (ovcd, ovbbccb, opcbbcdist, opcmsgrb, opccsad, ovcs), and the extra requirements of Oracle 9.2 compared with Oracle 8.1.7.

❑ Number of Open File Handles, Number of Semaphores, Shared Memory

No significant difference between OVO/UNIX 7.x and OVO/UNIX 8 with regards to common processes. However, there is a higher requirement by Oracle 9.2 compared with 8.1.7, and due to a number of new processes in OVO/UNIX 8.

❑ Number of Processes

The OVO/UNIX 8 management server has some new processes dedicated to work with HTTPS agents: ovcd, ovbbccb, ovcs, opcbbcdist, opcmsgrb, opccsad. All other processes are common between OVO/UNIX 7.x and 8.

❑ CPU Usage and Overall Performance

The processing of messages from HTTPS agents and the deployment of configuration data to HTTPS agents by an OVO/UNIX 8 management server leads to a moderate increase in CPU utilization compared to OVO/UNIX 7.x. This is mainly caused by the usage of SSL encryption for data transfer.

6 Last-Minute Changes to Documentation

IMPORTANT Always check the latest available versions of OVO/UNIX manuals, available from the following location:

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

New Java GUI Enhancements

The following OVO/UNIX Java GUI enhancements are not documented, yet.

Introduction of R Flag for Read-Only Messages in Java UI Message Browser

OVO/UNIX distinguishes between two subtypes of read-only messages:

- Notification
In MoM environments, a message can be forwarded to or from management servers as a notification (as opposed to a controlled message)
- Read-Only
Messages, that would normally not be shown to the operator because of their responsibility matrix settings if the service attribute of the message is a service that is assigned to that operator. The `OPCUIWWW_NORESP_SVCMSG` configuration variable on the management server must be set to `READONLY`.

OVO/UNIX Java UI now also distinguishes between these two different read-only message types by setting the `S` flag to:

- `N` for `NOTIFICATION` messages (these messages can be (un)acknowledged and annotations can be added)
- `R` when message is operator level `READ-ONLY` (no operations are allowed on these messages)

Full Support for INFORM Own Mode in Java UI

The concept of ownership, as set by the OVO/UNIX administrator by selecting one of the default ownership modes, is replaced with that of marking and unmarking. A marked message indicates that an operator has taken note of a message.

Use the option `OPC_OWN_MODE INFORM`. Informational mode does not restrict or alter operations on the message.

Support for Daylight Saving Time Change in Year 2007

OVO/UNIX Java UI now offers support for daylight saving time changes in year 2007 with the following enhancements:

- A new JRE is bundled with the 08.24 patch for the OVO/UNIX Java UI application on Windows platforms.

- For other platforms, users must install the recommended JRE, listed in Table 2-7, “Support Matrix - Java UI.”
- For users that do not want to migrate to a newer versions of JRE and are using a Sun's JVM, a tool is available that modifies the time zone data within the installed version on JRE. For more information see: <http://java.sun.com/developer/technicalArticles/Intl/USDST/index.html>
- The time zone for OVO/UNIX Java UI can also be manually configured

Java GUI Timezone Adjustments

Java GUI always uses the time zone of the local client. If the Java GUI runs in a time zone different from the mgmt sv time zone, the messages display a different time. You can force the Java GUI to use a specified time zone by editing the `ito_op.bat` script for Windows clients.

Timezone Settings in `ito_op.bat`

The Java GUI displays time-related information in the local timezone of the client. If the Java GUI and the OVO management server are located in different timezones, you can force the Java GUI to use the timezone of the management server by setting the `-Duser.timezone=<time_zone>` switch in the `ito_op.bat` file.

For example, to use the timezone Australia/Sydney, add the text `-Duser.timezone=Australia/Sydney` to the `ito_op.bat` file (example extract):

```
:: Starting JavaGUI
for %%p in (true TRUE on ON yes YES) do if "%%p"=="%TRACE%" echo on
for %%p in (true TRUE on ON yes YES) do if "%%p"=="%PLUGIN%" goto :PLUGIN
%START% .\j2re1.4.2\bin\%JAVA% -Duser.timezone=Australia/Sydney -Xmx128m
com.hp.ov.it.ui.OvEmbApplet initial_node=%ITOSERVER% user=%USER% passwd=%PASSWD%
trace=%TRACE%
display=%DISPLAY% locale=%LOCALE% max_limited_messages=%MAX_LIMITED_MESSAGES%
refresh_interval=%
REFRESH_INTERVAL% apiport=%APIPORT% apisid=%APISID% https=%HTTPS% %BBCPARM%
goto END
```

Valid timezones are listed in the directory `<JRE_HOME>\lib\zi`, for example GMT, Asia/Singapore, or Europe/Warsaw. If you specify an invalid timezone, GMT is used.

Customized Message Group Icons

Previously, the message groups icon with certain severity colors was hard to distinguish from the message group icon itself. Message group icons can now be customized through the `OPC_JGUI_MSGGRP_ICON` server-side variable in one of the following ways:

- the default icon can be set to be displayed in black and white:
`OPC_JGUI_MSGGRP_ICON=BW`
- a custom image can be loaded (in the second example the image will be loaded from default OVO image path `/opt/OV/www/htdocs/ito_op/images`):
`OPC_JGUI_MSGGRP_ICON=http://<server>:3443/ITO_OP/images/juke.32.gif`
`OPC_JGUI_MSGGRP_ICON=africa.32.gif`
- an empty image can be loaded, so only the severity color is visible:
`OPC_JGUI_MSGGRP_ICON=nonexisting_image`

Application HTML Output as an Internal Webpage

Java GUI can show OVO Application responses differently if they are plain text, valid HTML text (content is redirected to the web browser), or both (window application output and web browser).

HTML content redirection to the browser is disabled by default. To enable it, add the following parameter to `itopr`:

```
"web_browser_html_appl_result" "true"
```

Java GUI Connection Port Setting

Beside setting the port for non-secure socket communication using the `itopr` file or by directly editing the `ito_op` startup script, you can now also specify the port number as a parameter of the `ito_op` startup script or as part of the server name, passed as parameter to the `ito_op` startup script or in the login dialog.

The port number can thus be set in one of the following ways:

- in `itopr`: `port=<port_number>`
- with `ito_op ... -port <port_number> ...`
- with `ito_op hostname:<port_number> ...` or `ito_op ... -server hostname:<port_number> ...`
- at login dialog in the Management Server field: `hostname:<port_number>`
- in `ito_for_activator.html`: add `<PARAM NAME = port VALUE = port_number">`

Improved Cluster Error Handling and Logging

- When the HARG start, stop or monitor script returns an error and the HARG tracing was not switched on, it was extremely difficult to find out why the HARG script failed since the errors from these scripts were not logged anywhere.

Errors from failed HARG scripts are now logged into the `/var/opt/OV/hacluster/<HARG>/error.log` file.

- HARG `trace.log` file size is limited. When the maximum file size is reached, `trace.log` is moved into `trace.log.old` and new information is written into a new `trace.log` file.

Max size of `trace.log` file can be changed by editing the following file:

```
/var/opt/OV/hacluster/<HARG name>/settings
```

and adding the following line:

```
TRACING_FILE_MAX_SIZE=<maximum size in kBytes>
```

Below is an example with a maximum size of 7MB:

```
TRACING_FILE_MAX_SIZE=7000
```

opccmachg CLI Tool

opccmachg is a command-line tool for handling Custom Message Attributes, making it possible to add, modify, remove and list Custom Message Attributes.

The opccmachg utility resides in /opt/OV/bin/OpC. For more information refer to the opccmachg man page.

NNM 7.51 CD-ROM Installation Important Update

The NNM 7.5 CD-ROMs use a new format that is somewhat different from older formats.

As a result, HP UX 11.11 systems require a system patch in order to read the CD-ROM properly. The CD-ROMs may appear to mount correctly on an unpatched HP UX 11.11 system. However, software installation will fail, because the system can not find certain files on the CD ROM.

Note that the issue is in reading the CD-ROM, not in the NNM installation process. Therefore the solution is to patch the system where the CD-ROM will be mounted, which is not necessarily where NNM is to be installed.

Visit <http://www4.itrc.hp.com/service/index.html> and follow the "patch database" link to download the appropriate patches for your system.

HP-UX 11.11 Prerequisites

PHKL_28025 - s700_800 11.11 Rock Ridge extension for ISO-9660

Other Dependencies:

PHCO_25841 - s700_800 11.11 Add Rock Ridge extension to mount_cdfs(1M)

PHKL_26269 - s700_800 11.11 Rock Ridge extension for ISO-9660

Installation

Apply the patches on the system where the CD-ROM will be mounted as follows:

1. Unpack the patch using this command:

```
sh <patchname>
```

2. Apply the patch using this command:

```
swinstall -s <patchname>.depot
```

NOTE This patch requires a system reboot.

IMPORTANT Long file names may be truncated when NNM CDs are mounted using the mount command as documented in the NNM CD insert and the HP-UX Quick Start Installation Guide.

Use the following mount command with the Rock Ridge extension:

```
mount -F cdfs -o rr,ro,cdcase <cd device> <mount destination>
```

Proceed with software installation as usual, according to the *NNM Release Notes* and *Quick Start Installation Guide*.

Upgrading to Oracle 10g Release 2

This section describes how to upgrade Oracle 9.2.0.6 or Oracle 10.1.0.4 to version 10.2.0.1 (Release 2). After 10.2.0.1 (Release 2), 10.2.0.2 patch level is required. For more detailed information see the "Oracle Database Upgrade Guide 10g".

The steps needed for a first-time installation of Oracle 10g are provided in the *Installation Guide for the Management Server*.

NOTE Once you start up your database with ORACLE_HOME containing the new Oracle software, do not attempt to go back to the old version, as this could result in database files being corrupted.

Check the System Requirements

Make sure your system meets the requirements stated in the Oracle documentation. There might be a difference between Oracle 10g Release 1 and Oracle 10g Release 2 required OS patches and kernel parameters.

Prepare the Database for the Upgrade

Before upgrading the Oracle software, perform the following steps:

1. Exit the OVO GUIs (motif and java) and stop the OV processes with **ovstop -c** and **ovc -kill**.
2. Stop all processes that access the Oracle database.
3. Shut down the database and, if necessary, the SQL*Net listener, as follows:
 - a. Log in as user oracle or switch to user oracle:
su - oracle
 - b. If you are using SQL*Net, shut down the SQL*Net listener using the following command:
ORACLE_HOME/bin/lsnrctl stop
 - c. Start the Oracle SQL*Plus tool and shut down the database as follows:

```
$ORACLE_HOME/bin/sqlplus /nolog
SQL> connect / as SYSDBA
SQL> shutdown
SQL> exit
```

4. Perform a full offline backup of the Oracle database or the complete system before you perform the upgrade. A full backup ensures that you can recover from errors encountered during the upgrade process.

Installation of Oracle 10.2.0.1 (Oracle 10g Release 2)

Perform the following steps in order to install Oracle Database 10.2.0.1 (Release 2) software:

1. *If you are upgrading from Oracle 10g Release 1:*

Since user `oracle`, `oinstall` (primary) and `dba` (secondary) groups were already created as prerequisites for the Oracle 10.1.0.4 installation, there is no need to create them again.

If you are upgrading from Oracle 9:

Modify the user `oracle` with the following attributes:

- a. Create a UNIX group named `oinstall`. The group ID should be greater than 100.
- b. Make the user `oracle` a member of the group `oinstall` as the primary group, and `dba` as the secondary group.

Set `umask` to allow users to access the Oracle binaries:

```
umask 022
```

2. Create the Oracle home directory `ORACLE_HOME`:

```
mkdir /opt/oracle/product/10.2.0
```

You can also choose a different directory for `ORACLE_HOME` but you must use it consistently in all subsequent steps.

3. Change the ownership of the directories to `oracle:oinstall` by entering:

```
chown -R oracle:oinstall /opt/oracle/product/10.2.0
```

4. Change the following Oracle environment variables in the `/home/oracle/.profile` of user `oracle`:

```
export ORACLE_HOME=$ORACLE_BASE/product/10.2.0
```

This variable determines the location and the version of the Oracle installation. This is the recommended setting. You can choose a different setting, if needed.

5. As user `oracle`, start the Oracle Universal Installer.
6. After the Oracle Universal Installer is started, follow the instructions for installing the Oracle Database software provided by Oracle. After exiting the Oracle Universal Installer, run the Oracle Database Upgrade Assistant to upgrade the database software.

Configuring OpenView Products to Use the New Oracle Version

Perform the following steps as user `oracle`:

1. Since the upgrade of Oracle database was done by Oracle Database Upgrade Assistant, there is no need to manually move the parameter file of the `ORACLE_SID` database instance to the new location. This is usually a symbolic link to `/opt/oracle/admin/<ORACLE_SID>/pfile/init<ORACLE_SID>.ora`.
2. Copy the `SQL*Net` files from the old `ORACLE_HOME` to the new location, for example:

```
cd /opt/oracle/product/9.2.0/network/admin/  
cp listener.ora /opt/oracle/product/10.2.0/network/admin/listener.ora  
cp tnsnames.ora /opt/oracle/product/10.2.0/network/admin/tnsnames.ora  
cp sqlnet.ora /opt/oracle/product/10.2.0/network/admin/sqlnet.ora  
cp tnsnav.ora /opt/oracle/product/10.2.0/network/admin/tnsnav.ora
```

3. As user root, replace all occurrences of the old ORACLE_HOME value with the new value in the following files. You have to change variable assignments as well as directory names containing this value. Replace the following:

```
-ORACLE_HOME in /etc/opt/OV/share/conf/ovdbconf  
-DB_RELEASE in /etc/opt/OV/share/conf/ovdbconf  
-ORACLE_HOME in /opt/oracle/product/10.2.0/network/admin/listener.ora  
-LOG_DIRECTORY_LISTENER in /opt/oracle/product/10.2.0/network/admin/listener.ora  
-TRACE_DIRECTORY_CLIENT in /opt/oracle/product/10.2.0/network/log/sqlnet.ora  
-LOG_DIRECTORY_CLIENT in /opt/oracle/product/10.2.0/network/log/sqlnet.ora  
-ORA_CRS_HOME in /sbin/init.d/init.cssd
```

4. Change the symbolic links used by HP OpenView Operations. Change the following symbolic links:

```
libclntsh.sl, libclntsh.sl.1.0, libclntsh.sl.8.0, libclntsh.sl.9.0, libclntsh.sl.10.1,  
libopcora.sl
```

These point to the Oracle shared libraries. Remove them and recreate new links that point to the Oracle shared libraries in the new ORACLE_HOME, for example:

```
ln -s /opt/oracle/product/10.2.0/lib32/libclntsh.sl libclntsh.sl  
ln -s /opt/oracle/product/10.2.0/lib32/libclntsh.sl libclntsh.sl.1.0  
ln -s /opt/oracle/product/10.2.0/lib32/libclntsh.sl libclntsh.sl.8.0  
ln -s /opt/oracle/product/10.2.0/lib32/libclntsh.sl libclntsh.sl.9.0  
ln -s /opt/oracle/product/10.2.0/lib32/libclntsh.sl libclntsh.sl.10.1  
ln -s /opt/oracle/product/10.2.0/lib32/libclntsh.sl libopcora.sl
```

5. To find the missing files and to avoid starting the database with the wrong ORACLE_HOME value, it is recommended you rename the old ORACLE_HOME directory.

6. Start the database and the SQL*Net listener as follows:

- a. Log in as user oracle or switch to user oracle.

- b. If you are using SQL*Net, start up the SQL*Net listener:

```
$ORACLE_HOME/bin/lsnrctl start
```

- c. Start the Oracle SQL*Plus tool and start the database, for example:

```
$ORACLE_HOME/bin/sqlplus /nolog  
SQL> connect / as SYSDBA  
SQL> startup  
SQL> exit
```

7. If you no longer need the old Oracle version and after you verified that the new Oracle version works, you can remove the old Oracle version to gain disk space.
8. You can start the OVO/UNIX Management Server and other OV component processes.

Mixed Flexible Management with OVO 7 and OVO 8

In general, message forwarding from OVO 8 to 7 and OVO 7 to 8 works in the same way as message forwarding from OVO 7 to 7 and OVO 8 to 8.¹

However, the HTTPS communication mechanism, which is new with OVO 8, is not entirely compatible with DCE-based communication in a mixed flexible management environment:

- ❑ HTTPS-based managed nodes cannot communicate with an OVO 7 management server directly, only through an OVO 8 server.
- ❑ Actions and applications cannot be started on HTTPS-based managed nodes.

To receive messages from OVO 8 HTTPS-based managed nodes on an OVO 7 management server, the HTTPS-based managed nodes must first send their messages to an OVO 8 server, who will then forward them to the OVO 7 server. In addition, the OVO 8 HTTPS-based nodes must be added as **message-allowed** or **external nodes** to the node bank of the OVO 7 management server.

Refer to the chapter titled *MOM Environments* in the *OVO HTTPS Agent Concepts and Configuration Guide* for more information about migrating the flexible management configuration of OVO 7 DCE environments to OVO 8 HTTPS environments.

Assessing Your System Vulnerability with ovprotect

OVO/UNIX provides a new utility, called `ovprotect`, that helps you to determine and minimize the vulnerability risks of your systems from the HP OpenView perspective. It tests and disables unused services on the OVO/UNIX management server or on the OVO HTTPS agent platforms. In addition, it checks local file permissions, and can perform some corrective actions on the local systems.

The `ovprotect` tool is modular. More extensions, as well as modules for other HP OpenView products, are expected to be released on a regular basis. You can always download the latest version of the `ovprotect` tool from the OVO/UNIX web site:

`ftp://ovweb.external.hp.com/pub/ovprotect`

For details and usage options, refer to the `ovprotect(1m)` man page and the Security Advisory guide.

1. Patch levels 7.24 and 8.11 are required on the management server for full message text and severity synchronization.

Message Counter Feature: Severity and Message Text Updates

When suppressing/counting duplicate messages, the severity and the message text of the message that has first arrived to the browser was retained. When the new incoming OVO message has a different severity or message text, these new values can be displayed instead of the previous data.

Two new variables have been introduced to facilitate updating message text and severity:

`OPC_UPDATE_DUPLICATED_SEVERITY`

`OPC_UPDATE_DUPLICATED_MSGTEXT`

If these variables are set to `LAST_MESSAGE`, the appropriate value will be changed in the browser.

To test these two variables, use the following commands:

```
ovconfchg -ovrg server -ns opc -set OPC_UPDATE_DUPLICATED_SEVERITY LAST_MESSAGE
```

```
ovconfchg -ovrg server -ns opc -set OPC_UPDATE_DUPLICATED_MSGTEXT LAST_MESSAGE
```

ovoinstall Hangs if NNM 7.51 is Installed

The following note is missing in the OVO/UNIX Installation Guides for HP-UX PARISC and HP-UX Itanium, in the Chapter 2, “Installing OVO on the Management Server”.

NOTE If NNM 7.51 is installed, `ovoinstall` hangs at the point where `ovoinstall.log` says it is entering the `PostM10iPatch` function. To avoid this, edit `ovoinstall` and comment out the `PostM10iPatch` shell function before running the installation script.

Installing OVO/UNIX on VERITAS Cluster Server 4.1 on HP-UX 11.23 Itanium

During the OVO Management Server installation, the `ov-server` HA resource group is not started. To start the OVO Management Server as an HA resource group manually, execute the following commands immediately after the installation:

```
/opt/OV/bin/ovharg_config ov-server -add_node <local hostname>
```

```
/opt/OV/bin/ovharg_config ov-server -start <local hostname>
```

Command Line Utilities `opcinstrumdwn` and `opcpkgdwn`

Two new utilities have been introduced on the OVO/UNIX Management Server:

- `opcpkgdwn` is an OVO/UNIX Management Server utility that copies all software packages together which are needed to install an OVO HTTPS agent.

Utility location: `/opt/OV/bin/OpC/opcpkgdwn`

- `opcinstrumdwn` is an OVO/UNIX Management Server utility that copies all instrumentation files together which would be deployed to an OVO HTTPS agent.

Utility location: `/opt/OV/bin/OpC/opcinstrumdwn`

These tools are helpful for generating the generic HTTPS agent packages, which allow you easy mass deployments. For further details refer to the *HTTPS Agent Clone Imaging* whitepaper available for download from the following website:

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

opcdelmsg Troubleshooting Utility

opcdelmsg utility removes a single message out of the OVO database without accessing the database directly.

The following is the opcdelmsg syntax:

```
opcdelmsg [ -help ] | [-o] [ -u <user_name> ] <msg_id> [<msg_id>...]
```

Where msg_id (message id) is used for message identification.

See opcdelmsg man page for more details on this utility.

dtterm Default for Agent Installation

hpterm is replaced with dtterm as the default terminal for the installation of the OVO Agent. However, if you prefer to use hpterm, you can change the default installation window to hpterm using the following command:

```
# ovconfchg -ovrg server -ns opc -set OPC_TERMINAL /usr/bin/X11/hpterm
```

For more information about the default window for the agent installation, refer to the README file provided with the 8.21 server patch.

Security Advisory Guide

A dedicated document providing you with a summary of security-relevant information about OVO/UNIX 8 can be obtained through <http://support.openview.hp.com/news.jsp>.

Message Attribute Synchronization between OVO Management Servers in MoM Environments

Changes of OVO message attributes, for example message severity, message text, and custom message attributes can be synchronized with other OVO management servers.

Separating Message Fields with Tabs

With Java GUI 7.20 and later, when copying one or more messages using Ctrl+C and Ctrl+V commands, message fields were separated using a space as a separator, which commonly happens with Edit -> Copy to clipboard functionality.

The old functionality is restored, where the fields of the message are separated with tabs. This makes possible organising messages into Excel spreadsheets, where the each field of each message is a separate column in the row.

Command Line Utility `opcfcguser`

A new utility have been introduced on the OVO/UNIX Management Server. The command `opcfcguser` configures OVO/UNIX operators and is used for assigning and unassigning user profiles.

Changed Behavior of the Java GUI ‘Lock’ Feature

When viewing old messages in the Java GUI, the arrival of new messages may cause that the messages you are currently viewing become invisible in the message browser.

To make sure that the messages you currently work on remain visible in the message browser while new messages are arriving, you can disable an autoscroll feature by clicking the `Lock` checkbox placed at the bottom of message browser. For more information, refer to the *OVO Java GUI Operator’s Guide*.

According to the old behavior of this feature, disabling an autoscroll feature resulted also in not being able to see any changes to the messages in the browser while it is locked.

The message browser shows the changes in the messages that are already visible and the acknowledged messages disappear from the browser, while the new messages are still stopped from showing. Changing sorting, clicking on the column header, or moving scroll slider unlocks the message browser while scrolling inside the message browser with keys does not unlock it, which makes possible to navigate through messages while the message browser is locked.

Moreover, an appropriate information is displayed in a locked message browser’ status bar to indicate its status.

Auditing for Service Navigator

The auditing for Service Navigator (`opcsvcn`) should be documented in the OVO Administration Reference Guide. In the “Table 12-1: Audit Areas of the Administrator Audit Level” on page 505, a new table row should be added with the following details:

Service Navigator

- Add, remove, replace operations
- Assign, deassign operations

NOTE OVO creates an audit entry when the action is carried out in the Service Navigator (opcsvcm)

Interoperability with OVO for Windows

On page 243 of the *OVO Administrator's Reference*, information about the new server-based message forwarding capabilities of OVO for Windows version 7.50 and higher is not available. To learn more about the improved interoperability with OVO for Windows, refer to the OVO for Windows 7.50 online help:

HP OpenView Operations for Windows
Administering Your Environment
Scalable Architecture for Multiple Management Servers
Server-based Flexible Management

Obtaining Automatically Updated opcuhttps After Patch Installation

The following note should be documented in the section “Configuring the opcuhttps Process” on page 359 of the OVO Administration Reference Guide:

NOTE The opcuhttps binary is by default installed in the `/opt/OV/contrib/OpC` directory, while a prerequisite for successfully using the HTTPS Java GUI is having opcuhttps located in the `/opt/OV/bin/OpC` directory. To get updated the opcuhttps binary automatically after OVO management server patch installation, use a symbolic link instead of copying it to the required location.

Problems with Database Startup After Oracle 10.2.0.2 Patch Installation

The following note should be added in the OVO Installation Guides, in the “Installing an Oracle Database” section:

NOTE If you encounter problems with starting the database after the Oracle 10.2.0.2.0 patch installation, check the upgrade information in the 10.2.0.2 patchnote.htm file located on the Oracle patch depot (under doc). Additionally check the Oracle documentation.

Enhanced Auditing for the Java GUI

When logging into the OVO Java GUI, multiple records are recorded in the audit report because the Java GUI uses three connections for each session. This makes the audit reports difficult to read and understand.

Auditing for the Java GUI has now been enhanced such that each connection from the Java GUI to the OVO management server is clearly marked with the acronym `JUI`. In addition, the hostname of the Java GUI client, the process ID of the connected Java GUI console, and the session ID of the currently connecting Java GUI console are listed.

Disabling Data Collection for the Embedded Performance Component

You may want to disable metric collection for the embedded performance component if you have HP OpenView Performance Agent (OVPA) on the same node, since OVPA collects a superset of the metrics available through the embedded performance component data source.

With data collection disabled, the process `coda` continues to run and remains under OVO control. It then acts as a data communication layer for OVPA.

To disable data collection for the embedded performance component on HTTPS-based managed nodes or on DCE-based managed nodes with OVPA 4.5 installed, use the following command:

```
ovconfchg -ns coda -set DISABLE_PROSPECTOR false
```

Set the parameter `DISABLE_PROSPECTOR` to `true` to enable data collection again.

SQL *Plus Missing for Independent Database Server Installation

In OVO/UNIX Installation Guides, in the “Setting Up an Independent Database-Server System” section, the following bullet should be added in the step 2 (Install the following Oracle products on the OVO management server):

- SQL *Plus 9.2.0.1.0 or SQL *Plus 10g (10.1.0.2.0 or 10.2.0.1.0)

7 Known Problems and Workarounds

This section describes problems with the OVO software that are already known and could *not* be fixed until now. Where necessary, recommended workarounds are provided.

IMPORTANT The workarounds documented in these Release Notes reflect the status of the latest patch level. It is strongly recommended to install the most recent patches to ensure that you have the latest functionality and fixes.

It is also recommended to review the following sections before searching for a specific problem workaround:

- “Changed Features” on page 36.
- “What’s Not Yet Supported” on page 54.
- “What’s Not Supported” on page 55
- “Obsolete Features” on page 52.

NOTE **Before you install OVO/UNIX, read this section in its entirety.**

NOTE The latest OVO/UNIX known problems and workarounds are accessible from the following location:

<http://support.openview.hp.com/support/>

Oracle Database Installation and Configuration

NOTE All Oracle 9 versions from 9.2.0.2 are supported. However, some problems have been experienced with version 9.2.0.4. If you have this version installed, it is recommended that you update to version 9.2.0.6.

1. Symptom QXCR1000206911 ovoinstall: Local Agent Installation Fails With ORA-12500 Message

During or after the installation the following error message occurs on the command line or in the log file:

```
/var/opt/OV/log/System.txt
```

```
"Database: ORA-12500: TNS:listener failed to start a dedicated server process (OpC50-15)".
```

Solution

Take one of the following actions:

- Upgrade your Oracle installation to Oracle 9.2.0.3 or above.
- Increase the parameter PROCESSES in the file initopenview.ora as follows:

```
set PROCESSES = 200
```

If increasing the PROCESSES parameter does not help, also set the following parameter in initopenview.ora:

```
_attach_count_slack = 2000
```

2. Symptom QXCR1000200753 Too many 'ORA-00054 resource busy messages' in System.txt

There are several error messages that appear in the file System.txt repeatedly containing text ORA-00054 resource busy, such as:

```
0: INF: Fri May 20 15:44:49 2005: opcannoadd (5307/1): [chk_sqlcode.scp:95]: Dat  
abase: ORA-00054: resource busy and acquire with NOWAIT specified  
0: INF: Fri May 20 15:45:29 2005: opcannoadd (6591/1): [chk_sqlcode.scp:95]: Dat  
abase: ORA-00054: resource busy and acquire with NOWAIT specified  
0: INF: Fri May 20 15:45:51 2005: opcannoadd (6644/1): [chk_sqlcode.scp:95]: Dat  
abase: ORA-00054: resource busy and acquire with NOWAIT specified
```

Solution

This text states that the process cannot access the Database resource, but it will retry again after a while. In case that several of such messages appear repeatedly, check the status of commands or processes (especially these mentioned in the error message).

3. Symptom QXCR1000323835

ovcs aborted after performing full restore from a backup file

After a full restore is performed from a backup file, Oracle, OVO server and OV agent processes should be started. However, when checking the status of the OV Control Core components, the OV Certificate Server ovcs is in state aborted.

Solution

Restart the OVO server and component processes.

Management Server Upgrade/Migration

WARNING An HTTPS agent must be installed on the OVO/UNIX 8 management-server system. Do not attempt to install a DCE/NCS agent on the OVO/UNIX 8 management server system. Installing the DCE/NCS agent on the OVO/UNIX 8 management server system could damage your installation!

Do not install the HTTPS agent on an OVO/UNIX 7 management server system. OVO/UNIX 7 cannot communicate with the HTTPS agent and attempting to install the HTTPS agent could damage your installation!

NOTE When installing OVO/UNIX in a Japanese environment, the underlying Network Node Manager installation and UNIX OS-SPI installation dialogues are in English.

Uploading Upgrade Data

The handling of uploading the upgrade data has changed significantly from OVO/UNIX 7 to OVO/UNIX 8. With OVO/UNIX 7, after loading the initial defaults, the customer data was uploaded with the command:

```
opccfgupld -replace -subentity
```

The OVO/UNIX 8 upgrade procedure now documents to upload the downloaded data with the command:

```
opccfgupld -add -subentity.
```

This means, that for some configurations, the OVO/UNIX 8 defaults are not be replaced by the previously downloaded configuration, but only not previously existing subentities are added.

This means, that the following configuration that was changed in OVO/UNIX 7 will be present with the OVO/UNIX 8 default and not the downloaded customer data:

- Application Group data (label and description - assignments are preserved).
- The management server managed node (this is by intention, since it is now an HTTPS agent).
- Message groups (label and description).
- Node defaults.
- Node Group data (only the label and descriptions).
- NodeBank Node Hierarchy. Note, that the command `opccfgupld add -subentity` will upload all nodes that are not yet in the node bank into the correct node layout group. So the node bank hierarchy is retained except for the management server node.
- Template defaults and existing conditions.
- Core data of the default users (`opc_adm`, `opc_op`, `netop` and `itop`).

NOTE The home directory of `opc_op` is always `.`

- Database maintenance settings are reset (no audit and history download).
- Management Server Configuration is reset (audit settings, duplicate suppression settings, Server MSI settings and parallel distributions).
- Trouble Ticket Call is reset to no trouble tickets.

The Required Approach

The data that would cause problems when uploaded with the `-replace` option is the management server node and all cluster nodes. Therefore, after uploading the data with `-add -subentity`, you can upload the data with `-replace -subentity` if you exclude the managed nodes:

1. Copy the index file of the download (download-directory/\$LANG/*.idx). For example:

```
cp /tmp/cfgdwn/C/cfgdwn.idx /tmp/cfgdwn/C/nonodes.idx
```

2. Modify the copied index file. Remove the node bank section from the index file. This is everything from the line:

```
ENTITY NODE_BANK
```

To the semi colon (;) before the node defaults:

```
;  
ENTITY NODE_DEFAULTS *
```

and the `CONTENTS *` line if it exists.

3. Now upload your configuration data using the command:

opccfgupld -replace -subentity with the -index option

For example:

```
opccfgupld -replace -subentity -configured -index \  
/tmp/cfgdwn/C/nonodes.idx /tmp/cfgdwn
```

Workarounds

1. Symptom QXCR1000196910

MoM: respmgrs File Must be Updated After OVO/UNIX Server and Agent Upgrade to OVO/UNIX 8

After upgrading a MoM environment from OVO/UNIX 7 to OVO/UNIX 8 and converting some agents to HTTPS, the following must be taken into consideration. OVO/UNIX 8 managed nodes cannot communicate with an OVO/UNIX 7 management server and therefore you might get errors.

Solution

If you have a mixed environment with OVO/UNIX 7 and OVO/UNIX 8 servers, you may need to deploy two flavors of `allnodes` files:

- The `allnodes` file that contains OVO/UNIX 7 and OVO/UNIX 8 management servers.
- The `allnodes.bbc` file that contains only OVO/UNIX 8 management servers.

The essential thing is that no OVO/UNIX 7 management servers are mentioned in a responsible-manager file which is deployed to an HTTPS agent, because the OVO/UNIX 7 server cannot handle HTTPS traffic from the agent.

In addition, all management servers that are mentioned in responsible-manager templates, for example:

```
/etc/op/OV/share/conf/OpC/mgmt_sv/resmgrs/allnodes.bbc
```

- a. Must be added to the Node Bank
- b. Must be HTTPS-capable (not OVO/UNIX 7 or lower)
- c. Their core ID must be present in the node bank

For more information, check for term `allnodes.bbc` in the *HTTPS Agent Concepts and Configuration Guide*.

2. Symptom QXCR1000200001

ovoremove does not Remove Some Filesets on Upgraded Systems

After running `ovoremove` on a system which was upgraded from OVO/UNIX 7.xx to 8.xx some filesets are still present.

Solution

Perform deinstallation using the command `ovoremove -f`. If you already encountered this problem use `ovoremove -f` from OVO CD1.

To remove left-over from OVO/UNIX 7.10 system run the following commands:

```
swlist -l | grep -i -e ITO -e OVO  
swremove <product1> <product2> ...
```

3. Symptom

Nodes with Unknown Agent Type Skipped During Configuration Upload

When uploading configuration data to an OVO/UNIX management server, errors are displayed for managed nodes with agent platforms types that are not installed on the management server, for example, DCE agents.

Solution

This is the intended behavior.

However, to avoid losing node configurations of these managed node platforms, make sure that you have the corresponding OVO/UNIX agent fileset installed on the OVO/UNIX management server before running `opccfgupld(1m)` again. The current DCE agent platforms can be found on CD2:

```
/OV_DEPOT/HPOvOrpcClients.depot
```

To install the depot, mount CD2 and enter the following command as user `root`:

```
swinstall -x mount_all_filesystems=false -s <mount point>/\
OV_DEPOT/HPOvOrpcClients.depot \*
```

4. Symptom NSMbb70296

Obsolete Application Groups Still Visible After Upgrading from OVO/UNIX 7.1x to OVO/UNIX 8

After the upgrade from OVO 7.10 to OVO 8, some obsolete application groups are still visible in the Application Bank. For example `MetaFrame Tools`. In general, these application groups have been replaced with new ones. The OVO applications in these obsolete groups might not work. If no customizations have been made, these application groups can be removed. However, if you have added applications to these groups, please move them to an appropriate OVO 8 application group before deleting the obsolete groups.

For a detailed mapping of the new application groups used by the OS-SPIs, refer to Table 0-1, “OS-SPI Instrumentation Mapping,” on page `HIDDEN`.

The following Application Groups have been replaced and are obsolete:

- GlancePlus
- Jovw
- MetaFrame Tools
- OV Performance
- Reports
- VERITAS

The following applications are also no longer provided:

Application	Label
/Net Activity/Interface Statistics	: Interface Statistics
/OV Services/OV CDP View	: CDP View

Solution

To remove an application, execute the following steps:

- a. Right-click the application or application group.
- b. Select `Delete...`

5. Symptom NSMbb70285

VPO Status Application Visible After Upgrading from OVO/UNIX 7.1x to OVO/UNIX 8

After the upgrade from OVO/UNIX 7.1x to OVO/UNIX 8, in the Application Bank you see one `OVO Status` application and one `VPO Status` application.

Solution

To remove the `VPO Status` application, execute the following steps:

- a. Right-click the `VPO Status` application.

b. Select Delete.

6. Symptom QXCR1000196891

Service Navigator Value Pack Requirements for Migration from OVO/UNIX 7 to OVO/UNIX 8

The listed parameters in the `opcsvinfo` file of an OVO/UNIX 7.xx installation are used by the Service Navigator Value Pack and must be migrated to `OVconf`, `ovrg server`, namespace `opc` for OVO/UNIX 8.xx.

Solution

Recreate the two required parameters:

```
OPCSVCM_MSGSVSNAME_DEFAULT
```

```
OPCSVCM_FILESYSTEM_SOCKET
```

using the following commands:

```
cadmactivate -d
```

```
cadmactivate
```

7. Symptom QXCR1000139398

OVwModifySubmap: Submap Permission Denied

After the upgrade from OVO/UNIX 7.1x to OVO/UNIX 8, when you start the Motif GUI for the first time, the following error message is displayed on `stderr` of the shell from which you started the Motif GUI:

```
OVwModifySubmap: Submap permission denied.
```

Solution

This error message can be safely ignored.

New Installation of the OVO/UNIX Management Server

WARNING An HTTPS agent must be installed on the OVO/UNIX 8 management-server system. Do not attempt to install a DCE/NCS agent on the OVO/UNIX 8 management server system. Installing the DCE/NCS agent on the OVO management server system could damage your installation!

Do not install the HTTPS agent on an OVO 7 management server system. OVO 7 cannot communicate with the HTTPS agent and attempting to install the HTTPS agent could damage your installation!

NOTE DO NOT run `ovoinstall` from the CD mount point.

NOTE Before migrating from OVO/UNIX 7.1x to OVO/UNIX 8, you must switch off the OVAS functionality completely for the Java UI and all DCE agents.

NOTE When installing OVO/UNIX in a Japanese environment, the underlying Network Node Manager installation and UNIX OS-SPI installation dialogues are in English.

NOTE If you are using Hummingbird Exceed, XDMCP should be set to `Exceed XDMCP Query`.

Installation Workarounds

1. **Symptom QXCR1000363029**
ovoinstall Hangs if NNM 7.51 is Installed

`ovoinstall` hangs at the point where `ovoinstall.log` says it is entering the `PostM10iPatch` function.

Solution

Edit `ovoinstall` and comment out the `PostM10iPatch` shell function, then run `ovoinstall` again.

2. **Symptom QXCR1000288952**
Error During Database Configuration - ORA-00942: table or view does not exist

During the database configuration section of the installation of the OVO/UNIX management server the following error is written into `System.txt`:

```
ORA-00942: table or view does not exist
```

Solution

You can safely ignore this error.

3. Symptom QXCR1000294562**Errors During when Deinstalling OVO/UNIX with a Remote Database**

When deinstalling the OVO management server using a remote database server with `ovoremove`, the following errors and warnings are displayed:

```
ERROR: Error occurred calling sqlplus.
ERROR: Error occurred while trying to get ORACLE tablespaces and data files
WARNING: Couldn't remove the opc tablespaces.
WARNING: Please remove these files manually in the index and data directory.
WARNING: If these files aren't removed a later installation can fail.

WARNING: Net listener configuration files left untouched
WARNING: Please remove the entries for ov_net/openview manually.
```

Solution

You can safely ignore these errors and warnings. After `ovoremove` has finished, remove the database on the remote database server manually. As user `oracle` execute the following commands:

```
sqlplus /nolog
SQL> connect system/manager
SQL> shutdown abort
SQL> quit
```

Manually delete all files in the Oracle index and data directory on the database server , for example `/u01/oradata/openview/`.

Remove SID (for example, `openview`) entries on both the management server and the database server from the following configuration files:

```
/etc/oratab
<ORACLE_HOME>/network/admin/listener.ora
<ORACLE_HOME>/network/admin/sqlnet.ora
<ORACLE_HOME>/network/admin/tnsnames.ora
<ORACLE_HOME>/network/admin/tnsnv.ora
```

Delete the following files on the management server:

```
/etc/opt/OV/share/conf/ovdbconf
/opt/OV/conf/ovdbora ( on OVO server)
```

Delete the following files on the database server:

```
<ORACLE_HOME>/dbs/init<SID>.ora
<ORACLE_HOME>/dbs/spfile<SID>.ora
```

4. Symptom QXCR1000289820**ovcs Aborts after Deinstalling and Installing OVO/UNIX**

After de-installing OVO and installing it again with `ovinstall`, `ovcs` keeps aborting, even after stopping and starting all processes.

Solution

The deinstallation of OVO/UNIX also removed the certificate server (CS) including the root CA, but could not remove the certificate client (CC) with old certificates if other installed OpenView products use the CC component. The old certificates are now not accepted by the new C

First, remove the old certificates. Here is an example of commands used:

```
COREID=`ovcoreid`  
ovcert -remove $COREID  
ovcert -remove $COREID -ovrg server
```

You also have to remove the old CA certificate in the agent section:

```
ovcert -remove CA_${COREID}
```

Now export the trusted CA certificate (the CA certificate that was created during the installation):

```
ovcert -exporttrusted -file /tmp/trustedcertif -ovrg server  
ovcert -importtrusted -file /tmp/trustedcertif
```

Issue a new certificate:

```
ovcm -issue -file /tmp/certif -name $(hostname) -pass mypwd -coreid $(ovcoreid)
```

Import the new certificate for the local agent:

```
ovcert -importcert -file /tmp/certif -pass mypwd
```

Import the new certificate for the management server. The needed steps depend on whether you use a cluster or not.

a. Non-clustered environment:

```
ovcert -importcert -file /tmp/certif -pass mypwd -ovrg server
```

b. Clustered environment:

```
rm -f /tmp/certif  
ovcm -issue -file /tmp/certif -name $(hostname) -pass mypwd -coreid \  
$(ovcoreid -ovrg server)  
ovcert -importcert -file /tmp/certif -pass mypwd -ovrg server
```

Remove the temporary files:

```
rm -f /tmp/trustedcertif /tmp/certif
```

Remove the templates in the OVO template cache that were signed with the old certificate:

```
find /etc/opt/OV/share/conf/OpC/mgmt_sv/templates -type f -exec rm -f {} \;
```

5. Symptom QXCR1000213326

ovinstall: wrong text for NLS proposal for Taiwanese

During the installation of the OVO/UNIX management server in Taiwanese, the proposed `NLS_LANG` is `traditional chinese_taiwan.ZHS16GBK` but the message text recommends using `traditional chinese_taiwan.ZHT16BIG5`.

Solution

Use the proposed `NLS_LANG` of `traditional chinese_taiwan.ZHS16GBK` and ignore the message text.

6. Symptom QXCR1000202026

expr Error During ovinstall with CC Mounts

During disk space check of `ovinstall` `expr` error is displayed.

Solution

This problem is caused by local filesystem mounts (`lofs`). Except bad disk space calculation for the file systems in questions and aesthetic problems this error output can be safely ignored.

7. Symptom QXCR1000195500
OVO/UNIX Management Server Installation Fails if /var/opt is a Symbol Link

If the directory `/var/opt/OV` or `/var/opt` is a symbolic link, the OVO/UNIX management server installation fails.

Solution

`/var/opt/OV` and `/var/opt` must be local directories.

8. Symptom QXCR1000135085
swverify Error Messages

`swverify` reports many errors about the existing installation.

Solution

These error messages can be safely ignored.

9. Symptom QXCR1000199175
OVO/UNIX Installation Fails in NIS Environments

It is possible that when `ypbind` (NIS binder process) is running but the NIS environment is not configured, the `opcgrp` group is not created and OVO/UNIX server installation fails.

Solution

If you are using NIS or NIS+, make sure that the NIS or NIS+ environment is correctly configured and all NIS or NIS+ processes are running on the system where OVO/UNIX server is to be installed. Otherwise, all NIS or NIS+ processes, for example, `ypbind` or `rpc.nisd`, must be stopped before starting the OVO/UNIX management server installation.

10. Symptom QXCR1000225221
ovoinstall script Fails to Install Local Agent on HP-UX 11.23 PA-RISC system

During the OVO/UNIX Server installation on HP-UX 11.23 PA-RISC system, the local agent is not automatically installed.

Solution

After OVO/UNIX Server installation, the local agent must be installed manually using the OVO Administrator's GUI.

New HA Installation of the OVO/UNIX Management Server

TIP Before installing the OVO/UNIX management server in a cluster environment, refer to the chapter titled *Administration of the OVO Management Server in a Cluster Environment* in the *OVO Administrator's Reference Guide* for information on cluster concepts, and how to use and troubleshoot OVO/UNIX installed in cluster environments.

NOTE OVO/UNIX 8 can only be installed on clean systems or migrated from OVO/UNIX 7.1x and later versions. If any other previous version of OVO/UNIX was installed on the system chosen to host the OVO/UNIX 8 management server, ensure that this installation is completely removed and that the `openview` database instance is also removed.

NOTE DO NOT run `ovoinstall` from the CD mount point.

WARNING **An HTTPS agent must be installed on the OVO/UNIX 8 management-server system. Do not attempt to install a DCE/NCS agent on the OVO/UNIX 8 management server system. Installing the DCE/NCS agent on the OVO management server system could damage your installation!**

Do not install the HTTPS agent on an OVO/UNIX 7 management server system. OVO/UNIX 7 cannot communicate with the HTTPS agent and attempting to install the HTTPS agent could damage your installation!

NOTE Before migrating from OVO/UNIX 7.1x to OVO/UNIX 8, you must switch off the OVAS functionality completely for the Java UI and all DCE agents.

NOTE When installing OVO/UNIX in a Japanese environment, the underlying Network Node Manager installation and UNIX OS-SPI installation dialogues are in English.

1. Symptom AutoPass License Password Installation in Server HA Environments

The OVO AutoPass component is integrated into OVO/UNIX 8 to manage its licenses. This component installs, checks and manages the license passwords and stores the passwords in a location that is typically not shared in HA environments. In addition, AutoPass uses the local IP-Address and not on the virtual IP-Address. This makes it necessary to get OVO license passwords for all cluster nodes and install them on each cluster node.

Solution

Request your OVO license passwords for all cluster nodes in a HA environment with its physical IP-Address and install these passwords on the according cluster nodes.

2. Symptom QXCR1000237219**Failover problems with OVO 8.10 on VCS 3.5**

Users of OVO 8.10 without the 8.11 management server patch or superseding installed during the OVO configuration phase in VERITAS Cluster 3.5 environments with Maintenance Pack 1 or 2 may experience failover problems.

Solution

If no server patch was installed during OVO management server installation and configuration, the following procedure must be executed to avoid failover problems:

- a. Stop the OVO management server as a HA resource group by using the following command:

```
/opt/OV/bin/ovharg_config ov-server -stop <hostname>
```

In a decoupled management server configuration, also execute:

```
/opt/OV/bin/ovharg_config ov-oracle -stop <hostname>
```

- b. Open the configuration utility:

```
/opt/VRTSvcs/bin/haconf -makerw
```

- c. Modify Resource:

```
/opt/VRTSvcs/bin/hares -modify ov-application CleanProgram"/opt/OV/lbin/ovharg -stop ov-server"
```

In a decoupled management server configuration, also execute:

```
/opt/VRTSvcs/bin/hares -modify ov-oracle-application CleanProgram  
"/opt/OV/lbin/ovharg -stop ov-oracle"
```

- d. Close the configuration utility:

```
/opt/VRTSvcs/bin/haconf -dump -makero
```

- e. Start the OVO management server as a HA resource group:

```
/opt/OV/bin/ovharg_config ov-server -start <hostname>
```

In a decoupled management server configuration, execute:

```
/opt/OV/bin/ovharg_config ov-oracle -start <hostname>
```

NOTE

The above procedure needs to be followed only if you haven't installed any OVO 8 management server patches at the time `opccconfig` was run. If you have installed the 8.11 or superseding management server patch while executing `opccconfig`, following the procedure is not necessary. However, installing a management server patch after running `opccconfig` will not resolve this issue.

Upgrade of the OVO/UNIX Management Server Running in an HA Environment

TIP Before installing the OVO/UNIX management server in a cluster environment, refer to the chapter titled *Administration of the OVO Management Server in a Cluster Environment* in the *OVO Administrator's Reference Guide* for information on cluster concepts, and how to use and troubleshoot OVO/UNIX installed in cluster environments.

NOTE OVO/UNIX 8 can be installed *only* on clean systems or migrated from OVO/UNIX 7.1x and later patch versions. If any other previous version of OVO/UNIX was installed on the system chosen to host the OVO/UNIX 8 management server, ensure that this installation is completely removed and that the `openview` database instance is also removed.

WARNING **An HTTPS agent must be installed on the OVO/UNIX 8 management-server system. Do not attempt to install a DCE/NCS agent on the OVO/UNIX 8 management server system. Installing the DCE/NCS agent on the OVO management server system could damage your installation!**

Do not install the HTTPS agent on an OVO/UNIX 7 management server system. OVO/UNIX 7 cannot communicate with the HTTPS agent and attempting to install the HTTPS agent could damage your installation!

NOTE DO NOT run `ovoinstall` from the CD mount point.

NOTE Before migrating from OVO/UNIX 7.1x to OVO/UNIX 8, you must switch off the OVAS functionality completely for the Java UI and all DCE agents.

NOTE When installing OVO/UNIX in a Japanese environment, the underlying Network Node Manager installation and UNIX OS-SPI installation dialogues are in English.

1. Symptom QXCR1000139026 Node Type (DCE or HTTPS) Must be Changed on All Cluster Nodes

Using virtual nodes in OVO/UNIX 8 requires that all nodes (physical and virtual) are of the same platform type (DCE / HTTPS).

Upgrade of the OVO/UNIX Management Server Running in an HA Environment

Changing the agent type when upgrading from DCE to HTTPS must be done in a very short time frame for all nodes (minutes!).

NOTE All agent types must be of the same type also after the migration.

Management Server Runtime

1. Symptom QXCR1000361388 Inaccessible OVO URLs When NNM 7.51 Installed

Management Server URLs are inaccessible when NNM 7.51 patch is installed.

Solution

- a. Stop all OVO processes including httpd. Enter the following:

```
ovstop
```

- b. Modify /opt/OV/httpd/conf/httpd.conf file on your management server. Add the following lines:

```
<Directory /opt/OV/www/htdocs/ito_doc>Options Indexes FollowSymLinks
AllowOverride None
order allow,deny
allow from all
</Directory>
```

```
<Directory /opt/OV/www/htdocs/ito_op>
```

```
Options +MultiViews
```

```
Options +MultiViews
```

```
Options +MultiViews
```

```
Options +MultiViews
</Directory>
```

```
<Directory /opt/OV/www/htdocs/ito_op/>
```

```
ErrorDocument 404 /ITO_MAN/itoman_error.htm
</Directory>
```

```
Alias /ITO_OP /opt/OV/www/htdocs/ito_op/
```

```
Alias /ITO /opt/OV/www/htdocs/ito/
```

```
Alias /ITO_DOC /opt/OV/www/htdocs/ito_doc/
```

```
Alias /ITO_JDOC_AGT /opt/OV/www/htdocs/jdoc_agent/
```

```
Alias /ITO_MAN /opt/OV/www/htdocs/ito_man/
```

```
ScriptAlias /ITO_SVC /opt/OV/www/htdocs/ito_svc/opcsvcweb
```

- c. Start all OVO processes. Enter the following:

```
ovstart
```

2. Symptom QXCR1000291336 Templates are not distributed to the Managed Nodes

Templates for the OVO managed node are not successfully distributed after changing the communication port ranges for the OVO managed node

Solution

Before distributing the templates to the OVO managed node once the communication ports for it had been changed, create a symbolic link on the OVO management server using the following command:

```
ln -s /opt/OV/bin/OpC/utils/opcsv_reinit /opt/OV/lbin/xpl/config/update/opcsv_reinit
```

3. Symptom QXCR1000289933

Error in System.txt: Cannot open pipe svcengmsgadptp

When restarting the management server using `opcsv -stop` and `opcsv -start`, the following error is logged in `System.txt`:

```
Cannot open pipe svcengmsgadptp
```

Solution

This error message can safely be ignored.

4. Symptom QXCR1000289718

Critical Errors in Message Browser and System.txt after Disabling OvoDceDistmMsgrd

If the `OvoDceDistmMsgrd` service is disabled with `ovprotect`, critical messages and errors occur in the Message browser and `System.txt`.

Solution

Do not disable the `OvoDceDistmMsgrd` service. If the service is already disabled, enabled it using `ovprotect`.

5. Symptom QXCR1000289120

Deleting a Node with Software Already Deinstalled

When deleting a node within the OVO GUI, from which OVO software has already been deinstalled, the following question is displayed nonetheless:

```
Do you want to automatically deinstall software from managed nodes?
```

Solution

If the OVO software has already been removed from the specified node, you can safely ignore this question.

6. Symptom QXCR1000229432

Error when Deploying an OVO/UNIX 8 to OVO/UNIX 7 Message Forwarding Policy

When a message forwarding policy for forwarding messages from an OVO/UNIX 8 to an OVO/UNIX 7 management server is created, the OVO/UNIX 7 management server is added to the OVO/UNIX 8 management server's Node bank as a DCE node . When this policy is deployed on the OVO/UNIX 8 management server, the following error appears:

```
Node testnode from responsible-manager file must have communication type HTTPS. Can't convert / distribute responsible-manager file needed on HTTPS nodes therefore. For details see instruction text. (OpC20-3182)
```

When OVO/UNIX 7 nodes without `OVCoreID` are defined in the `mgrconf` file on an OVO/UNIX 8 management server., converting the `mgrconf` policy will fail. On an OVO/UNIX 8 management server, only OVO/UNIX 8 nodes are expected in the `mgrconf` file.

Solution

Create an empty or limited `mgrconf` file on the OVO/UNIX 8 management server named `allnodes.bbc` beside the existing `allnodes` file. For HTTPS nodes, the `allnodes.bbc` file will be used, and for the DCE nodes, the `allnodes` will be used. When all management servers are upgraded to use HTTPS communication the `allnodes.bbc` file will become obsolete.

7. Symptom QXCR1000214318
ovpolicy Fails to List Remote Policies from an OVO/UNIX Management Server Running on an High Availability Cluster

When attempting to list the policies on a remote node from a clustered management server, the remote node returns an illegal CoreID error message.

For example, when entering a command of the following form on the OVO management server:

```
ovpolicy -list -node <remote node>
```

the remote node replies with the following error:

```
ERROR: (conf-570) The policy operation was not authorized from the Configuration server on host 'rzhptest'. Check if the local host is allowed to execute the requested operation.
```

```
(conf-143) Policy listing is not allowed on host 'rzhptest'.
```

```
(conf-176) Sender with id '9208ee9e-f934-7508-1947-f2ee7dfab937' is not authorized to execute policy list operation.
```

Solution

Query the installed policies locally on the remote node.

8. Symptom QXCR1000200633
Logfile Entries Cannot be converted from eucJP to SJIS

The following message appears in the OVO Message Browser:

```
(OpC30-138)  
Can't convert logfile entry.  
(OpC20-274)  
Bad input character converting string from "eucJP" to "SJIS".  
Incorrect byte sequence.
```

Solution

The character set for all Logfile Templates must be changed to reflect the current locale character set. This can be done using Message Source Templates window from the Motif GUI. Redistribute modified templates, if they were previously distributed.

9. Symptom QXCR1000138782
Identical Cron Messages Are Generated From Two Templates

Two identical Cron messages are generated each time, (one in English and the other Japanese) from the following message source templates:

Message in Japanese:

```
Cron (Solaris) under Default: Solaris template group:  
fetch 'cron|at|batch command failed
```

Message in English:

Management Server Runtime

OSSPI-SOL-Cron_1 under "Operating System SPIs: SOLARIS: QuickStart Solaris Policies template group:

```
fetch 'cron|at|batch command failed.
```

Solution

Write a multiple-source ECS correlator such that only one of these messages hits the browser.

Or,

Suppress the conditions from either template, if both templates are deployed to all nodes.

Management Server Deinstallation

1. Symptom QXCR1000138928 OS-SPI Scripts Remain after ovoremove

After removal of the OS-SPI, many OS-SPI scripts remain in the directory tree:

```
/var/opt/OV/share/databases/OpC/mgd_node/customer/...
```

Solution

Execute the following command to remove all OS-SPI related programs:

```
find /var/opt/OV/share/databases/OpC/mgd_node/customer -name \
osspi_* -type f | xargs rm
```

HTTPS Managed Nodes Installation

NOTE If you are using the ‘certificate installation using install-key’ method (refer to the *HTTPS agents concepts and configuration guide* for details about this method), always use a new installation key for each new managed node installation. Reuse of a previously used installation keys can result in lack of connection to the managed node without any error messages being displayed.

1. Symptom QXCR1000381360

Cannot install 8.10.160 AIX Agent on HP-UX 11.23 PA-RISC

The installation of the HP OpenView OVO A.08.10.160 AIX Agent on OVO Management Server for HP-UX 11.23 PA-RISC fails.

Solution

Install the agent using the `allow_incompatible=true` option:

```
swinstall -x allow_incompatible=true
```

2. Symptom QXCR1000344595

Windows agent installation unregisters RegObj.dll

The installation of the HTTPS agent software unregisters the shared library RegObj.dll. This causes problems with other applications that use this DLL.

Solution

Reregister RegObj.dll using the following command:

```
C:\WINDOWS\system32\regsvr32.exe /s "<path_to_regobj>\regobj.dll"
```

3. Symptom QXCR1000202565

Modifying Type/Platform of a Node Retains Previous Parameters

After modifying the machine type/platform of a node in the Node Bank, parameters valid for the original type/platform remain. For example, Interval and Installation user. This can cause installations to fail, for example, when you modify from UNIX to Windows node types and the Installation user field is not changed from root to Administrator.

Solution

After modifying Machine type/platform from UNIX to Windows in the Motif GUI, modify the Installation user field from root to Administrator.

4. Symptom QXCR1000204686

Communication Broker does not Register with Windows Firewall on Windows XP SP2

When installing the OVO HTTPS agent on a Windows XP SP 2 system, the certificate installation fails because the Communication Broker (ovbbccb) is not registered at the Windows Firewall. The result is that all HTTPS communication fails.

This can be verified by running the following command on the OVO/UNIX Management Server system:

```
bbcutil -ping <node>
```

Solution

Register the Communication Broker (ovbbccb) manually:

- a. Open the Control Panel -> Windows Firewall.
- b. Open the Exceptions tab.
- c. Click Add Program ...
Browse and select `<OV InstallDir>/bin/ovbbccb.exe`
- d. Click OK.

The `bbcutil -ping <node>` command should now succeed.

NOTE If SNMP trap interception is desired and `SNMP_SESSION_MODE` is set to `NNM_LIBS`, SNMP trap reception must also be enabled in the firewall.

- a. Select `<OVO installDir>/lbin/eaagt/opctrapi.exe` in the Exceptions tab.
 - b. Click OK.
-

5. Symptom QXCR1000135982

Windows Agent Install using an Installation Server Completes Asynchronously

When installing an HTTPS agent to a Windows system via an installation server, the installation window on the OVO/UNIX Management Server shows the following output:

```
[...]  
PHASE III: (de)-installing Agent Packages to Managed Nodes.  
=====  
  
---- <Name of target node> ----
```

After this, no progress is visible to the installing user but the installation is actually running in the background. The installation script on the OVO/UNIX Management Server will eventually either successfully contact the OVO/UNIX Agent after being started on the target system or time out.

Solution

Wait until either of these two events occurs. Additionally, you may check the installation progress on the target node by watching for `msiexec` processes or viewing the OVO/UNIX Agent installation log file in `%SystemRoot%\Temp\opc_inst.log`.

6. Symptom QXCR1000135861

Path Problem in New Shell after Windows Agent Install using an Installation Server

After installing a Windows agent using an Installation Server, there is a path-related problem when opening a new shell, and none of the OV commands are found.

During the installation, the system environment is extended by <InstDir>/bin and <InstDir>/bin/OpC.

When opening the Control Panel -> System -> Advanced -> Environment Variables... these are present for the system variable PATH but due to a Windows problem, the modification of the PATH does not get propagated to other programs.

To verify this particular behavior, open a new command shell and enter the command:

```
ovc
```

If this command is found and works normally, everything is OK. If the command is not found, verify the system PATH in the control panel, follow the described workaround and try again.

Solution

Open the Control Panel -> System -> Advanced -> Environment Variables... and modify the system path to include <InstDir>/bin and <InstDir>/bin/OpC and click OK.

This will trigger the propagation of the PATH change to other programs. If the OVO/UNIX path components are already in place, perform some other minor modification, for example, add a semicolon.

7. Symptom QXCR1000134895

Unexpected Pop Up Window During HTTPS Agent Installation (opcnodetimestamp)

After distributing a new agent to a remote machine, a message window displays the following message:

The configuration of the Node Bank has changed. Please restart your session.

Solution

This message can be safely ignored. There are no changes in the Node Bank to refresh.

8. Symptom QXCR1000203378

Replacing Windows HTTPS Agent with DCE Agent Retains HTTPS Installation Directory

When changing the platform type of a managed node from IP Network Intel x86 (HTTPS) MS Windows to IP Network Intel x86 MS Windows, that is from HTTPS to DCE, if non-default installation directory is set, it will not be handled correctly and the subsequent installation of the OVO/UNIX Agent software will fail with the following error:

```
C:\Inetpub\ftproot\temp>opc_inst
I-> Setup program started (preinit).
T-> Tracing information: Tracing to C:\WINDOWS\temp\inst.log .
I-> Setup program started at 10/26/2004 09:34:10. It may need some time.
T-> Tracing information: The installation of the user will not be forced.
T-> Tracing information: Installing agent version: 07.25 .
I-> Specified destination drive is not NTFS. Setup will now abort.
E-> Error from FindSetupDrive.
E-> Setup program aborted.
E-> INSTALLATION ABORTED
```

Then the file <ftp root>\temp\opcsetup.inf on the Windows system contains:

```
[Setup Drive]
<install directory configured for HTTPS>
```

For example:

```
[Setup Drive]
C:/ovo-agt
```

Solution

Clear the install directory in the `Communication Options` window before **before** switching from HTTPS to DCE. This will update the database correctly. Then, the install drive field can be set and changed normally.

Alternatively, correct the setting in the `opcsetup.inf`, for example:

```
[Setup Drive]
C:
```

9. Symptom QXCR1000131758 and 1000132001 Manual Installation of HTTPS Agents: Agent is not Activated if OVO/UNIX Management Server is not Reachable

During manual agent installation, the following lines are displayed:

```
NOTE: Starting opcactivate utility
ERROR: Server ... and/or BBC CB on server not reachable
```

Solution

The management server to which the agent should report must be running when making either of the following calls:

- `opc_inst -s <mgmt server>`
- `opcactivate -s <mgmt server>`

10. Symptom QXCR1000139502 Problems While Running the OS-SPI Service Discovery on Non-Root Agents

The directory `/var/opt/OV/SPISvcDisc` is not present when a SPI is distributed to the agent and, as a result, the permissions of this directory are not changed when `ovswitchuser.sh` is called. This can cause problems while running the SPI Service Discovery on non root https agents.

Solution

A script is provided to solve this problem and must be called before `ovswitchuser.sh` is used to change the user under which the OVO/UNIX agent runs. Before `ovswitchuser.sh` is called on an HP-UX, Solaris or Linux HTTPS managed node, enter the command:

```
/var/opt/OV/bin/instrumentation/ovcreatedirs.sh
```

It is not necessary to call that script more than once on a node, even when `ovswitchuser.sh` is used to subsequently switch the agent to another user.

11. Symptom QXCR1000137734

Some OS-SPI Tools do Not Work on Linux Red Hat Advanced Server 2.1

The following error message is displayed when attempting to launch the following applications on Red Hat Advanced Server 2.1 HTTPS managed nodes:

- Disk Space
- Print Status
- Processes

```
Warning opcacta (Action Agent)(29597) : Cannot change the current working directory to  
/home/opc_op for user opc_op.  
Permission denied (OpC20-53).
```

The home directory may be assigned permissions of 0700 in place of 0755 (which is the default on most UNIX systems).

Solution

Check on the Red Hat Advanced Server 2.1 HTTPS managed node, if it is possible to change the user to `opc_op` from the command line:

```
su opc_op
```

If it fails due to permission problems, run the following command as user root:

```
chmod -R 755 /home/opc_op/
```

The applications should now run as designed.

12. Symptom QXCR1000136922

Agent Installation Fails on Turbolinux ES 8J

Agent installation fails on Turbolinux ES 8J systems because only manual installation is supported.

Solution

Copy packages, package descriptors, and the `opc_inst` script to the managed node.

Execute the following commands:

```
chmod +x opc_inst  
opc_inst -s <mgmt_server>
```

HPOvXpl package is installed but postinstall script fails.

```
opc_inst -s <mgmt_server>
```

HPOvCtrl package is installed but postinstall script fails.

```
cp <inst_dir>/HPOvCtrl.xml /var/opt/OV/installation/inventory
```

```
opc_inst -s <mgmt_server>
```

13. Symptom QXCR1000103186

Error OpC60-800 Displayed After Agent Deinstallation Using Motif GUI

After deinstallation of an agent from the Motif GUI, the following error message maybe displayed:

```
Can't deinstall Agent Software on Node <node> (OpC60-0800)
```

Solution

Provided that no other errors were reported during deinstallation, this message can safely be ignored.

14. **Symptom QXCR1000133707**

Removing Physical Nodes from Virtual Node Does Not Remove Its Policies

When removing a node from the list of physical nodes belonging to a virtual node, the policies assigned to the virtual node are not removed with the next deployment to the virtual node. After removing the physical node from this list, information about the linked (virtual) policies in the database is also removed from the configuration stored on the management server, but requires an explicit deployment to the physical node.

Solution

You must redistribute the policies to the physical node itself to enforce an update of all policies on the managed node.

15. **Symptom QXCR1000103060**

Agent Upgrade or Patch Installation and Deinstallation

Agent upgrade (patch installation) and deinstallation is performed using the deployment component and no password is required. As a result, when OpenView core components are stopped during deinstallation or when upgrading core components, the connection to the remote node is lost.

Agent Deinstallation

It is reported that deinstallation was started, then the connection is lost and status of deinstallation is not known.

Agent Upgrade

If an error is encountered during the upgrade, processes do not start and errors are reported.

Solution

Agent Deinstallation

To check if deinstallation was successful, login to remote node and check the log file:

```
$Datadir/log/opc_inst.log
```

Agent Upgrade

If an error was reported during upgrade, open the log file `$DataDir/log/opc_inst.log` on the managed node and check whether the packages were correctly installed.

If the packages were properly installed but there was a problem with the starting of components, try to start the processes with the command:

```
opcagt -start
```

Check if all processes were started with the command:

```
ovc -status
```

If there is a problem with installation of upgraded components, reinstall the agent using the `force` mode.

HTTPS Managed Nodes Runtime

1. Symptom QXCR1000217165

Cannot Change Root Directories After ovswitchuser is Run

When `ovswitchuser` is run on a UNIX managed node where the `suid-bit` is not set for `ovbbccb` the following error might be entered in the `System.txt` file and the OVO message browser at each startup of `ovbbccb`:

```
ovbbccb (16577/1): (bbc-188) Cannot change the root directory for the current process.  
See chroot man page for additional detail.
```

Solution

Enter the following configuration command on any UNIX managed node that exhibits this behavior:

```
ovconfchg -ns bbc.cb -set CHROOT_PATH /
```

2. Symptom QXCR1000216143

Output of Application with Japanese Paramaters is Garbled with HTTPS Agent on AIX

Output of an application with Japanese paramaters from an HTTPS agent on AIX systems is garbled.

Solution

Use Ksh as a login shell on the managed node system.

3. Symptom QXCR1000189469

opcmsg and opcmon Java API Wrappers do not work on Linux Platforms

The `opcmsg` and `opcmon` Java API wrappers do not work on Linux platforms.

Solution

No workaround is currently available.

4. Symptom QXCR1000103564

ovconfd Sends Error Regular Message When Veritas Cluster Server is Down

`ovconfd` continuously sends error messages when the Veritas Cluster server is down on a cluster node.

Solution

- Create a message interceptor template with a suppress-condition for:

```
application = "OpenView", message group = "OpenView", object = "ovconfd"
```

The message text must contain the string "`(conf-336)`".

- Deploy this template to the concerned Veritas cluster node(s).

5. Symptom QXCR1000197215

Applications do Not Work if Executed as `opc_op` User on Windows

If applications, for example `Broadcast`, are started under the user `opc_op` on a Windows system, the following error is displayed:

```
Application started, please wait.
```

```
Error: Process could not be started in the specified user account.
```

```
Please check the agent's logfile for more information.
```

The HTTPS Windows agent does not create the `opc_op` user. Recommending administrator is somewhat different, because `opc_op` used to be a non-admin user.

Solution

Configure \$AGENT_USER or administrator or any other existing user account and execute applications on Windows systems under this account.

6. Symptom QXCR1000138209 Control Kills ovconfd if the Initialization Hook Times Out

On slow or busy systems, ovconfd may take longer than 30 seconds to initialize. In such cases it is not possible to start ovconfd using ovctrl because any processes that ovctrl has invoked which do not initialize within the configured time period are killed by ovctrl. In such a situation, the OVO HTTPS agent is NOT started at all. For example, this problem may be experienced if tracing is activated.

Solution

Increase the ACTION_TIMEOUT parameter of ctrl.ovcd namespace in the configuration settings, for example to 120 seconds, with the command:

```
ovconfchg -ns ctrl.ovcd -set ACTION_TIMEOUT 120
```

7. Symptom QXCR1000139256 opcragt -set_config_var 'var(procname)=value' Syntax is Not Valid on HTTPS Nodes

In order to set a variable specifically for one process, the command used for DCE agents fails. When the following command is entered:

```
opcragt -set_config_var 'MAX_NBR_PARALLEL_ACTIONS(opcacta)=100' <nodename>
```

The result on the managed node is:

```
[eaagt]
MAX_NBR_PARALLEL_ACTIONS=opcacta)
```

The expected result is:

```
[eaagt.opcacta]
MAX_NBR_PARALLEL_ACTIONS=100
```

Solution

The name space of the process must also be specified as follows:

```
opcragt -set_config_var eaagt.opcacta:MAX_NBR_PARALLEL_ACTIONS=100 <nodename>
```

This value is now set for the process opcacta alone in namespace eaagt.opcacta.

8. Symptom QXCR1000136133 Immediate-Linked API Program Crashes with Missing Symbols

Custom OVO API programs built with OVO/UNIX 7.xx do not run on OVO/UNIX 8 HTTPS HP-UX managed nodes, if the executable is built with immediate binding.

The program crashes with the following error:

```
# ./<program_name>
/usr/lib/dld.sl: Unresolved symbol: U_TRAP_STACK_TRACE (code) from
/usr/lib/libcl.2
/usr/lib/dld.sl: Unresolved symbol: U_STACK_TRACE (code) from
/usr/lib/libcl.2
Memory fault(coredump)
```

Solution

Change the program to deferred binding (the missing symbols will never be used):

```
# chatr -B deferred <program>
```

Alternatively you may also use nonfatal binding or re-link your application.

OS patches with an updated libcl will be available in December 2004:

11.11 PA PHSS_32226

11.22 PA PHSS_32227

11.23 PI (IPF/PA) PHSS_32228

9. Symptom QXCR1000136222

Virtual Terminal is Not Supported for HTTPS Agents

It is not possible to use a PC Virtual Terminal (DCE) application on an HTTPS Windows node.

Solution

The *OVO DCE Agent Concepts and Configuration Guide* contains information on software you could use to achieve the same result.

Symptom QXCR1000203203

Remote Action Security Rule is Still Provided for Deleted Node Group

If you delete a node group that is under the control of remote action authorization rules from the OVO Node Group Bank, those rules will still applied to the nodes which were in this group.

Remote action authorization rules are defined in the configuration file:

```
/etc/opt/OV/share/conf/OpC/mgmt_sv/remactconf.xml
```

Solution

Do not delete the node group. Only remove nodes from this node group. Now, rules which applied to nodes in this node group will have no effect on the nodes deleted from this node group.

10. Symptom QXCR1000140673

ovconfd Exits on Linux Nodes

ps output on Linux shows an ovconfd zombie process (defunct).

Solution

This situation can be safely ignored.

11. Symptom QXCR1000197467

ComponentMatrix.cfg & DependenciesMatrix.cfg Contain OvDepl After Deinstalling Agent

Files `/var/opt/OV/conf/ComponentMatrix.cfg` and `/var/opt/OV/conf/DependencyMatrix.cfg` still contain an entry for OvDepl after deinstalltion of an OVO HTTPS agent from the OVO/UNIX management server system using the Administrator's GUI.

Solution

This situation can be safely ignored.

12. Symptom QXCR1000285220

coda Daemon Stops on an HTTPS OVO/UNIX 8.10.160 Agent on AIX 5.1

The coda daemon stops on an HTTPS OVO/UNIX 8.10.160 agent on AIX 5.1.

Solution

No workaround is currently available.

HTTPS Managed Nodes and Proxies

1. Symptom QXCR1000133276

Change in ovconf: PROXY Setting is Not Processed without Restart

Changing of PROXY settings takes no effect on the management server system or on a managed node system.

Solution

If you changed the PROXY configuration settings, all processes must be restarted with the following commands:

On managed node: **ovc -kill**

ovc -start

On management server: **ovstop ovoacomm**

opcsv -start

HTTPS Managed Nodes and NAT Environments

1. Symptom QXCR1000136801

NAT (Server IP Address): Windows Agent Installation Hangs

In a NAT environment (server IP address is translated on agent side) the HTTPS agent installation may hang. This is caused by ftp which is used during installation. The ftp connection to Windows 2000 itself hangs.

Solution

Install the HTTPS Agent software manually. It is very likely that FTP does not work, so another file transport mechanism must be used.

2. Symptom QXCR1000136802

NAT (Node IP Address): Broadcast Application does Not Start on HP-UX Agent

In a NAT Environment (node system IP addresses translated on the OVO/UNIX management server side), the execution of applications and actions may immediately return a communication error.

Solution

Check if the corresponding agent is reachable using `ping` and other commands. For help on how to do this, refer to *Troubleshooting HTTPS-based Communication* in the *HTTPS Agent Concepts and Configuration Guide*.

If it is reachable the communication error message is obviously wrong. Restart the server processes and retry.

This behavior is seen very infrequently after adding and installing a Node in an NAT environment. If an application can be executed, the error message will not be displayed again, as long as the agent remains reachable.

DCE Managed Nodes

NOTE NCS RPC on TruCluster DCE Managed Nodes

Tru64 UNIX managed nodes support both DCE RPC and NCS RPC as communication types. TruCluster managed nodes support only DCE RPC communication. Before installing the OVO/UNIX agent software on Tru64 UNIX managed nodes, make sure to set up and configure DCE RPC or NCS RPC correctly.

1. Symptom QXCR1000102576 Support for HACMP 5.1 for AIX Managed Nodes

HACMP 5.1 is now supported for AIX managed nodes. Some template changes are required, which will be delivered with the corresponding OS-SPI.

Solution

Modify the template to use the new location of the logfile. If the HACMP logfile template is assigned to the node, an error message is reported about missing logfile. This happens because location of the logfile is different in HACMP ES:

```
/usr/es/adm/cluster.log
```

2. Symptom QXCR1000287213 Continuous Alert Messages for the BBC Local Location Broker with OVPA 4.5 Installed

The DCE agent continuously sends the following alert message to the OVO management server:

```
BBC Local Location Broker of subagent 0 aborted; process did an exit 77.  
The process has been started for '6' times in the last '0 d 00:00:50' already.  
(OpC30-1198).
```

Solution

OVPA 4.5 installs a newer version of BBC, causing the BBC Local Location Broker that was delivered with the DCE agent to stop.

After installing OVPA 4.5, restart the DCE agent using the following commands:

```
opcagt -kill  
opcagt -start
```

3. Symptom QXCR1000296158 SNMP Trap Templates could not be Distributed to Linux Nodes

For Linux managed nodes, `opctrapi` cannot be used nor can the SNMP Trap templates distributed.

Solution

To enable `opctrapi` on linux/intel/linux24 nodes, do the following:

- a. Add the linux24 node to the Node Bank.
- b. Edit the following file :

```
/var/opt/OV/share/databases/OpC/mgd_node/vendor/linux/intel/linux24/AgentPlatform
```

The AgentPlatform file must contain the following line:

```
TEMPLATE_TYPES
```

```
LOGFILE MONITOR OPCMSG TRAP SCHEDULE
```

c. Assign and distribute the SNMP Trap templates.

4. Symptom QXCR1000200007

DCE Agent on Windows does not Install from the Management Server after OVO/UNIX Management Server Upgrade

After upgrading an OVO/UNIX management server from OVO/UNIX 7.xx to OVO/UNIX 8, Windows DCE agents could not be installed using the GUI or the `inst.sh` script.

Solution

Near the end of upgrade when you are asked:

```
Do you want to remove old agent software from managed node (y|n=default)?
```

in a separate terminal, execute the command:

```
touch /opt/OV/bin/OpC/install/opcsvinfo
```

After the command has executed, confirm the deinstallation of the old agent.

When the upgrade has completed, remove the file:

```
/opt/OV/bin/OpC/install/opcsvinfo
```

An alternative method is to reinstall the `HPovOrpcClients.depot depot` from the `OV OCD2/OV_DEPOT` directory after the OVO/UNIX management server upgrade has completed.

5. Symptom QXCR1000102576

Support for HACMP 5.1 for AIX Managed Nodes

HACMP 5.1 is now supported for AIX managed nodes. Some template changes are required, which will be delivered with the corresponding OS-SPI.

Solution

Modify the template to use the new location of the logfile. If the HACMP logfile template is assigned to the node, an error message is reported about missing logfile. This happens because location of the logfile is different in HACMP ES:

```
/usr/es/adm/cluster.log
```

6. Symptom QXCR1000112735

MAX_NBR_PARALLEL_ACTIONS Setting

On a node with many monitors distributed, the monitor agent `opcmona` may raise the following type of error messages:

```
08/13/03 12:23:32 WARNING opcmona (Monitor Agent)(16907)
[genmonc:5154]: Can't retrieve value for monitor 'r3monwpa'.
Suppressing further error messages. (OpC30-608)
```

This may be caused by the value of `MAX_NBR_PARALLEL_ACTIONS` having been set too low.

Solution

The `MAX_NBR_PARALLEL_ACTIONS` setting is applied separately to the following processes:

- `opcmona`
- `opcle`
- `opcacta`

Example

If you have 50 monitor templates and all are started at the same time and all 50 execute a monitor script, then `MAX_NBR_PARALLEL_ACTIONS` should be 50.

The default setting is 10, but will be increased to 25 with OVO/UNIX 8.1x.

To set the `MAX_NBR_PARALLEL_ACTIONS` value, enter the command appropriate for the type of agent installed.

On HTTPS Managed Nodes:

```
opcragt -set_config_var eaagt.opcacta:MAX_NBR_PARALLEL_ACTIONS=100 <nodename>
```

On DCE Managed Nodes:

```
opcragt -set_config_var 'MAX_NBR_PARALLEL_ACTIONS(opcacta)=100' <nodename>
```

7. Symptom QXCR1000126783

Monitor Agent opcmona Size can be Large

When using a high number of CODA templates/policies, the monitor agent size is large.

Solution

There is currently no workaround for this situation.

8. Symptom QXCR1000103609

Agent Installation on IRIX Platform Error in Local ovoinstall.log

During agent installation on IRIX platform the following error may be found in the `/var/opt/OV/log/OpC/mgmt_sv/install.log` file:

```
ERROR: Cannot open /opt/OV/bin/OpC/install/opcinfo: No such file or directory.
```

Solution

This error can be safely ignored.

Embedded Performance Component (EPC, also known as CODA)

1. Symptom QXCR1000139054

OVPM 4.05 and OV Reporter 3.5 Require that EPC Runs in HTTP Mode

If the Embedded Performance Component (EPC) is configured to use the HTTPS protocol, OpenView Performance Manager 4.05 (OVPM) and OpenView Reporter 3.5 (OV Reporter) fail to make a connection to the Embedded Performance Component on OVO HTTPS agents and are unable to collect performance metrics.

However, these applications can connect to and collect performance metrics, if the Embedded Performance Component is configured to use the HTTP protocol.

To determine if the EPC is configured to use the HTTP protocol or the HTTPS protocol, run the command:

```
<OV_DIR>/bin/ovconfget coda SSL_SECURITY
```

where <OV_DIR> is the directory where EPC is installed.

If the output is `ALL` or `REMOTE`, then EPC is configured to use the HTTPS protocol.

If the output is `NONE`, then EPC is configured to use the HTTP protocol.

Solution

To configure EPC to use the HTTP protocol, run the command:

```
<OV_DIR>/bin/ovconfchg -ns coda -set SSL_SECURITY NONE
```

Deployable Performance Agent (OVPA)

1. Symptom QXCR1000314580

Deployment of OVPA fails on OVO/U 8.21

Deployment of OVPA/HP-UX C.04.50.00 from a 8.21 OVO/U Management Server fails if higher versions of shared components (HPOvLcore.*, HPOvPerf.*) are already installed on the node.

Solution

As a higher version of shared components are already installed on the node, OVPA installation will complete, although the deployment reports that a failure has occurred. OVPA will not be running on the node after the deployment.

To start the OVPA on node, execute the following command

```
/opt/perf/bin/ovpa start
```

Motif UI

1. Symptom QXCR1000136788

Changing IP Address Of Node Creates Errors When Starting Applications

When a node in the Node Bank is changed to use a different IP-Address or Node Name, an error occurs when starting an application on that node using the Motif GUI. The error is:

```
Unable to get node information of <oldnodename>.
```

Solution

Apply one of the following workarounds:

- Do not use the `Modify Node` window to change the IP-Address or the node name of a node. Delete the node and add a new one instead.
- When the IP-Address or the node name has been changed using the `Modify Node` window, restart the Motif GUI.

2. Symptom QXCR1000135741 and QXCR1000139344

Setting Times in OVO/UNIX

In OVO/UNIX there are a number places where times must be specified, for example, scheduled outages, time templates, and notification. The time format is `hh:mm`.

Solution

OVO time inputs are interpreted as `hh:mm:00`.

For example, if you want to specify a 24 hour time period ending at midnight, enter:

```
00:00-24:00
```

Specifying a notification time period of `00:00 - 23:59` for every day would mean that any message being received after `23:59:00` and before `00:00:00` would not create notification.

When setting values in time fields of the `Scheduled Action Template` window, any time fields that are left blank are interpreted as a wildcard and the scheduled action is executed continually at one minute intervals. Wildcard characters themselves are not recognized.

3. Symptom QXCR1000144554 & QXCR1000211752

English OVw Starts When Starting OVw in X-OVw Application Group

When starting the `Start OVw` application from the `X-OVw` application group, OVw is always started in locale C (English) even on a Japanese, Simplified Chinese or Korean system.

Solution

If you always want to start OVw in a language other than English, you can modify the `Start Ovw` application as follows:

- a. Right click the application symbol and select `Modify`.
- b. In the `Application Call` edit text, at the very beginning, add the required `LANG`:

HP-UX	Japanese:	<code>LANG=ja_JP.SJIS</code>
	Simplified Chinese:	<code>LANG=zh_CN.hp15CN</code>
	Korean:	<code>LANG=ko_KR.eucKR</code>
Solaris	Japanese:	<code>LANG=ja_JP.PCK</code>

Simplified Chinese: `LANG=zh_CN.EUC`

Korean: `LANG=ko_KR.EUC`

c. Insert a space after the `LANG=*` entry and before `opcctrloww`.

4. Symptom QXCR1000139221 NNM-ET View Application IPv6 Network

Applications in application group `NNM-ET Views` do not work and a Java error message is displayed. Some of the `NNM-ET` views require additional configuration to work correctly.

Solution

For `NNM-ET` applications to work, you must run the `NNM-ET` setup script to enable `NNM-ET` on the management server system.

For more details on `NNM` Extended Topology and how to enable it, refer to the `NNM` release notes under:

```
/opt/OV/www/htdocs/<language>/ReleaseNotes
```

5. Symptom QXCR1000113589 XmScrollBar Warning Opening Message Detail Window for Long Messages

When a message detailed window containing a long message text is opened, a Motif warning message of the following form is displayed in the terminal window:

```
&#129;@[W: X Toolkit Warning:
```

```
\012
```

```
Name: HorScrollBar\012
```

```
Class: XmScrollBar\012
```

```
The specified scrollbar value is greater than the maximum\012 scrollbar value minus the scrollbar slider size.\012].
```

Solution

This warning message can be safely ignored.

Java UI

1. Symptom QXCR1000199105

Issues starting two Java UI applets in two Mozilla web browsers on Windows

Two Java UI applets cannot be started on the same machine within two Mozilla web browsers.

Solution:

When each Mozilla web browser uses its own profile, it is possible to use two Java UI applets on the same machine within two Mozilla web browsers. To allow Mozilla to start with a different profile, set the environment variable using the following command:

```
set MOZ_NO_REMOTE=1
```

To add a new profile, start mozilla with the following command:

```
mozillexe -p
```

2. Symptom QXCR1000211752 & QXCR1000144554

The Interface Traffic Net Activity Tool Cannot be Started from the Java UI

When running NNM tools from the Java GUI, some characters may be garbled. When running NNM tools from Java GUI, characters are garbled or are launched in English on Japanese, Korean or S-Chinese management servers.

Solution

The LANG environment variable should be added to the operator (opc_op) profile. For example, on a Japanese management server, Add the following LANG environment statement appropriate to the operating system of your management server in the opc_op .profile file:

HP-UX	Japanese:	LANG=ja_JP.SJIS
	Simplified Chinese:	LANG=zh_CN.hp15CN
	Korean:	LANG=ko_KR.eucKR
Solaris	Japanese:	LANG=ja_JP.PCK
	Simplified Chinese:	LANG=zh_CN.EUC
	Korean:	LANG=ko_KR.EUC

3. Symptom QXCR1000198864

Non-Graphical Applications (cmd.exe and telnet) Cannot be Started from the Java UI

Non graphical applications, such as cmd.exe and telnet, do not work when started as local applications from the Java UI.

Applications that are not GUI based, such as cmd.exe or telnet, are not correctly started as local applications from the Java UI. The input/output window of the application is not visible.

Solution

In order to open a terminal, and start application in that window, the application must be defined in the following way:

Syntax for Windows:

```
cmd /c start <application>
```

Example: telnet application call: cmd /c start telnet \$OPC_NODES
cmd application call: cmd /c start

Syntax for UNIX:

```
dtterm -e <application>
```

```
Example:      telnet application call: dtterm -e telnet $OPC_NODES
              dtterm application call: dtterm
```

4. Symptom QXCR1000197155

Example XML File for Non-English Environments (opcservice)

In order to successfully upload the service definition file, you need to specify the correct encoding in the header of the xml definition file. It is currently not documented in the manuals how to write multi-byte service definition files. An example is given in the solution below.

Solution

Here are the examples how the header should look like for different languages.

```
Japanese      <?xml version="1.0" encoding="Shift_JIS"?>
```

```
Korean        <?xml version="1.0" encoding="EUC-KR"?>
```

```
Simplified Chinese <?xml version="1.0" encoding="GB2312"?>
```

For further information, refer to the chapter titled *The Service Configuration File Syntax* in the *Service Navigator Concepts and Configuration Guide*.

Example

A complete XML file for Korean:

```
<?xml version="1.0" encoding="EUC-KR"?>
<!-- this file was generated by opcsvcconv(1m) -->
<Services xmlns="http://www.hp.com/OV/opcsvc"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.hp.com/OV/opcsvc /etc/opt/OV/share/conf/OpC/mgmt_
sv/dtds/service.xsd">
<Service>
<Name>localsvc</Name>
<Label>Some Korean text</Label>
</Service>
</Services>
<!-- end of file -->
```

5. Symptom QXCR1000202126

Java Null Pointer Error with NNM Views in ICE Browser

When using the ICE Browser to display an NNM View, a window is sometimes opened that contains a java null pointer exception message. However, the NNM View usually also displayed.

Solution

In order to successfully launch applications in NNM Views group, you need to use external browser as your default browser.

See support matrix for recommended web browser.

6. Symptom QXCR1000237264

When Exiting or Logging off from the OVO/UNIX Java UI, an Error Message is Displayed

When Java UI is running in the HTTPS communication mode, the following error message is displayed, when exiting or logging off from Java UI:

```
ERROR MSG, 7:42:47 AM,
com.hp.ov.it.comm.OvEmbHttpsClient:
https status - InternalServerError:text/html,
Message = HTTP/1.1 500 Internal Server Error
Date: Wed, 11 May 2005 05:41:57 GMT
Transfer-Encoding: chunked
Server: BBC 05.20.010; opcuhttps 01.00.000
senderid: e6979118-aca1-750b-1f6a-de6eb9cfe391
Cache-Control: no-cache
Content-Type: text/html
```

Solution

This message can be safely ignored.

**7. Symptom QXCR1000309412
Exceptions in the Java GUI Console Window**

Sometimes the following exception is shown in the console window of the Java UI:

```
javlang.ClassCastException
at com.klg.jclass.chart.BarChartDraw.recalc(BarChartDraw.java:95)
at com.klg.jclass.chart.JCChartArecalcGraphExtents(JCChartArejava:2376)
at com.klg.jclass.chart.JCChartArerecalc(JCChartArejava:1124)
at com.klg.jclass.chart.JCChartAresetBounds(JCChartArejava:1266)
at com.klg.jclass.util.DefaultComponentLayout.layoutContainer(DefaultComponentLayout.java:59 4)
at javawt.Container.layout(Container.java:1020)
at javawt.Container.doLayout(Container.java:1010)
at com.klg.jclass.chart.JCChart.performLayout(JCChart.java:843)
at com.klg.jclass.chart.JCChart.doLayout(JCChart.java:785)
at javawt.Container.validateTree(Container.java:1092)
at javawt.Container.validateTree(Container.java:1099)
at javawt.Container.validateTree(Container.java:1099)
...
```

Solution

This exception can be safely ignored.

**8. Symptom QXCR1000329118
JRE 1.4.2_11 causing failure of a Java GUI applet**

When opening URLs in an ActiveX Internet Explorer control workspace the Java Virtual Machine (JVM) fails. The affected version of JRE is 1.4.2_11. The problem usually occurs when operators open URLs (hyperlink, applet, and so on) in the workspace that supports showing content in an ActiveX IE control. JVM and Internet Explorer fails while opening or closing the web browser window. The result of this is closure of all IE web browser windows and failure of JVM.

Solution

Please use the supported JRE version.

ECS/OV Composer

1. Symptom QXCR1000187583, QXCR1000128343, QXCR1000134617, QXCR1000193526, QXCR1000009281, QXCR1000009282 and QXCR1000199714 ECS Designer Does Not Work

It is not possible to use ECS Designer 03.20 after installation. For example, after clicking one of the ECS Agent policies in the Message Source Templates window and selecting Circuit. ., instead of the OV HP ECS window opening for verifying the policies, the following error messages maybe displayed:

```
ITO Modules not found.
```

```
OpC60-0973
```

```
The ECS GUI returned an unknown exit-code.
```

If you can reproduce this problem then please contact HP support with the exact details.

Solution

Copy ITO module files to the required location using the following steps:

```
OV_CONF="/etc/opt/OV/share/conf"
ITO_MODULES="/etc/opt/OV/share/conf/OpC/mgmt_sv/ecs/modules"
rm -f $OV_CONF/ecs/modules.newconfig/ito 2>/dev/null
mkdir -p $OV_CONF/ecs/modules.newconfig/ito 2>/dev/null
if [ -d $ITO_MODULES ]
then
  for MODULE in `ls $ITO_MODULES/*.ecs`
  do
    cp $MODULE $OV_CONF/ecs/modules.newconfig/ito 2>&1
  done
fi
```

The ECS Designer should now work. However, the following error message is also displayed and can be ignored:

```
/etc/opt/OV/share/conf/ecs/modules.newconfig/ito/*.ecs not found.
```

2. Symptom QXCR1000134910 Launching ovcomposer on HP-UX Does Not Work

The ovcomposer script on HP-UX has an error.

The workaround is fully documented in the OV Composer release notes.

Solution

Edit the /opt/OV/bin/ovcomposer script.

Replace:

```
java
```

with

```
java -Xint
```

3. **Symptom QXCR1000140462 and QXCR1000131660**
Disabling the Event Correlation Template does not Stop Event Correlation

Event correlation is still working even if all event correlation templates are disabled.

Solution

Stop OVO Event Correlation (opceca) manually with the following command:

```
ovc -stop opceca
```

Reporting

1. **Symptom QXCR1000138530**
Service History Status Reports (SN Report Pack) Limit ID and Name Length

With OVO/UNIX 8, it is possible to specify service names or service labels that exceed 253 characters in length. Problems occur with these long names since the Crystal runtime engine used in Reporter 03.50 has a limitation for string lengths of 254 characters. The OVO/UNIX Service Status History reports Version 03.50 do not support service names or service labels that are longer than 253 characters.

If service names exceed the 253 character limit, the name is truncated. The status history data may be incorrectly calculated if the service names are not unique within the first 253 characters.

Solution

Do not use service names that are longer than 253 characters. The support for service names longer than 253 characters has been added to the OV Reporter 03.60 release, and the corresponding Service Navigator Report Package.

Service Navigator Value Pack

1. Symptom QXCR1000107875

Pointer Shadow Problems on Windows 2000 Installations

There are GUI problems when using a mouse configured to use the "pointer shadow". In a Windows 2000 standard installation the "pointer shadow" is enabled as default. The GUI problems are typically small rectangular trails of inverse color left by mouse when moving across menu items.

The GUI problems occur around the mouse pointer especially when:

- Selecting a service hierarchy with the mouse in the drop-down menu in the upper right corner.
- Selecting a menu item with the mouse.

Solution

If possible, avoid using remote desktop solutions such as VNC. Always use the latest version of Windows certified graphic drivers.

2. Symptom QXCR1000192982

Rules and Actions Cannot be Deleted Without A Service Hierarchy

If no service hierarchies exist, it is not possible to delete calculation rules, propagation rules, actions, child object rules, and parent-and-child object rules. In some cases, an exception message is displayed.

Solution

Create a dummy service hierarchy with one root object. Delete the rules and actions that you no longer need, and finally delete the dummy hierarchy.

3. Symptom QXCR1000192582

Obsolete Statement in OLH Topic Copy and Paste Between Service Hierarchies

The online help topic Copy and Paste between Service Hierarchies contains the following incorrect text:

If one of the copied objects already exists in that hierarchy, you can either cancel the paste operation or overwrite the existing object(s).

Solution

It is not possible to paste an object into the same hierarchy more than once. The note below the incorrect text explains what happens if you try to do this.

4. Symptom QXCR1000192582

Inverted Results for Weight is Empty

Using the Find in Service Hierarchy dialog box with the criteria Parent objects;Weight is empty or Message weight is empty, produces an unexpected set of results.

Solution

Only user defined weightings are stored in the database, default weightings are not. Therefore, searching with the criteria weight is empty returns a list of objects for which the default weighting has not been changed.

Network Node Manager

For Network Node Manager specific problems, refer to the HP OpenView Network Node Manager 7.5 Runtime Release Notes appropriate for your operating system:

<http://ovweb.external.hp.com/ovnsmdps/pdf/nnm750rn/HPUX/README.html>

<http://ovweb.external.hp.com/ovnsmdps/pdf/nnm750rn/Solaris/ReadmeAll.html>

WARNING By default, the file:
`OVNNMgr.OVNNM-RUN: /opt/OV/bin/ovtraceroute`
has the **setuid** bit set for root:
`-r-sr-xr-x 1 root bin`
Security concerned customers should change the permissions as follows:
`chmod 555 /opt/OV/bin/ovtraceroute`

1. Symptom QXCR1000295810 and QXCR1000295800

Inappropriate Entries in `/etc/services` for `ito-e-gui` in NIS+ Environments

If the `ito-e-gui` service is managed by NIS+, the service should not be listed in `/etc/services`.

You can check if the `ito-e-gui` service is managed by NIS+ using the following command:

```
niscat services.org_dir | grep ito-e-gui
```

Solution

If the `ito-e-gui` service is managed NIS+, remove `ito-e-gui` service configuration line from `/etc/services`. The following is an example of the configuration line that should be removed:

```
ito-e-gui      2531/tcp      # OpenView Operations Java Console
```

2. Symptom QXCR1000297690

OVO/UNIX Management Server cannot be Started

After shutting down the management server you may not be able to start it again.

Solution

The system shutdown sequence is missing a link to `/sbin/rc2.d/` for the NNM and OVO/UNIX processes.

Create a link manually before shutting down your system using the following command:

```
ln -s /sbin/init.d/ov500 /sbin/rc2.d/K060ov500
```

3. Symptom QXCR1000217223

NNM license key Installation Using `ovnnmInstallLic` is not Documented

NNM license key installation using the `ovnnmInstallLic` tool not documented.

Solution

A second, NNM, license key must be installed using the NNM license key installation tool `ovnnmInstallLic`, otherwise is this license key ignored and not installed.

Use the following command to add NNM license passwords:

```
/opt/OV/bin/ovnmInstallLic /tmp/save710/.license
```

4. Symptom QXCR1000205834

X-OVw Requires a Home Directory that may not Exist

After successfully installing NNM 7.5, an OVO HTTPS agent, and the OVO/UNIX 8.1x Remote NNM package on an HP-UX system, `opcctrlow` runs correctly.

However, when attempting to run the X-OVw application `Start OVw`, the following error message is displayed:

```
Warning opcacta (Action Agent) (22960 : Cannot change the current working directory to /home/opc_op for user opc_op.  
No such file or directory (OpC20-53)
```

At this point, `/home/opc_op` does not exist.

Solution

To correct the problem, create the directory `/home/opc_op`.

5. Symptom QXCR1000206586

Applications Using `opcctrlow` are hard to use with Windows Java GUI

Applications, such as Net Activity, sometimes do not start in the Windows Java GUI, when using `opcctrlow`. Instead, error messages are printed in OVO Communication Status window.

Solution

When the OVO Java GUI is run on a Windows system, these error messages are sometimes displayed when some applications are started. The applications that may trigger this problem are those that display an `ovw` session to the Windows box.

Error Message 1

```
Command: opcctrlow -display 15.2.118.164:0.0 -user "opc_adm" -action "IP Tables"  
AddressesForIface" produced the following output error:  
Error: Can't open display: <IP Address>:0.0  
with Exit Code: 3
```

Solution 1:

An X-Windows emulator such as Reflection X or Hummingbird Exceed must be running on the Windows system.

Error Message 2

```
INTERNAL ERROR at: CWfong.cpp:264.  
Contact your HP Support representative.  
Could not conver "-*-medium-f-normal-*-12-*-*-*-*m-*-*-*" to XFontSet.  
Try changing your "*.cwFont" resource.
```

Solution 2

The X-Windows emulator is not able to find the correct font. In this case you need to configure a font server, for example, on the OVO/UNIX Management Server: `xfs -port 7100` and then configured Reflection X to use this font server.

6. Symptom QXCR1000196492

HA Environments should be in Maintenance Mode when `setupExtTopo.ovpl` is Run

If you run `setupExtTopo.ovpl` to enable ET in a high availability environment, there is a possibility that some monitored processes could be restarted, triggering a failover.

When performing actions on an OVO/UNIX management server installed in a cluster environment that result in the stopping of OVO/UNIX management server processes, for example when installing patches, upgrading, or doing maintenance, it is necessary to first disable the OVO/UNIX management server HA resourcegroup and stop the OVO/UNIX management server.

Solution

Switch the HA system to mainenance mode before running `setupExtTopo.ovpl`.

How to switch the OVO/UNIX management server to and from maintenance mode is described in the section titled *Stopping the OVO Management Server in a Cluster Environment for Maintenance* for the appropriate cluster type in the *HP OpenView Operations Installation Guide*. This section describes how the OVO/UNIX management server can be stopped without causing failover of the OVO/UNIX management server HA resource group.

When this script has run successfully, start the OVO/UNIX management server and check that the OVO/UNIX processes are up and running, and then enable OVO/UNIX management server monitoring.

7. Symptom QXCR1000193099

Ovcd is not yet Started Message after installing NNM on System with HTTPS Agent

If NNM 7.5 is installed on a UNIX system where an OVO HTTPS agent is running, the `ovcd` process is stopped.

Entering the command `opcagt -status` results in the following error message being displayed:

```
Ctrl-1111 Ovcd is not yet started.
```

Solution

Enter the following command to restart the agent:

```
opcagt -start
```

8. Symptom QXCR1000188382

OSPF View in NNM-ET Views Stops Working if RAMS is Enabled

RAMS functionality is supported with NNM 7.5, and can be easily enabled or disabled.

When RAMS is disabled, the application call for OSPF View NNM-ET Views is:

```
http://<$OPC_MGMTSV>:7510/topology/ospfView?viewInBrowser=true
```

In this case, application OSPF View works correctly.

If RAMS is enabled, OSPF View stops working because the following application call is still used:

```
http://<$OPC_MGMTSV>:7510/topology/ospfView?viewInBrowser=true
```

Solution

If RAMS is enabled, modify the application and change the application call for OSPF View NNM-ET Views to:

```
http://<$OPC_MGMTSV>:7510/topology/rexView?viewInBrowser=true
```

9. Symptom QXCR1000187416

Net Activity/Network Polling requires OV Services/MIB Grapher

When creating new user or using `opc_op`, and assigning the Net Activity application group, the MIB Grapher must also be assigned from OV Services. If this is not assigned, the following error is displayed next time you log on to the Motif GUI as the new user or as `opc_op`:

```
Error: Application "Network Monitor Statistics": parent "mibgraph" undefined.
```

```
Error: Application "mibgraph" undefined.
```

OpC-0830

Application(s) in the Application Desktop may not be started because application Network Monitor Statistics is not registered.

When selecting Net Activity -> Network Polling, the following error is displayed:

OpC60-010

OVw Error with OVwCheckAction(netmonStatus): Application not found.

A related error is also displayed in the OVO Error Information window.

Solution

Assign the OV Services group, or at least the MIB Grapher application, in addition to Net Activity to the opc_op user or when creating a new user.

10. Symptom QXCR1000211829 Applications in Jovw (old) Group may Fail

When trying to start applications such as Highlight In IPMap and Jovw from the Jovw (old) group in the Application Bank window, error messages are displayed:

Highlight In IPMap error:

```
Cannot find an ovw on host <hostname> with map named default using session ID  
<hostname>:0.
```

Jovw error:

```
Cannot find an ovw on host <hostname> with map named default using session ID  
<hostname>:0.
```

Solution

In order for these applications to work, an ovw session with the default map must be running on the host.

On the system <hostname> enter the command:

```
/opt/OV/bin/ovw
```

Make sure that default is displayed in the lower left corner.

To change to the default map, choose Map -> Open and select default.

It is recommended that NNM Dynamic Views be used rather than Jovw. The NNM Dynamic Views are available from the application group NNM Views.

11. Symptom QXCR1000213132 Wrong Japanese Name for [OV Extended Topology] Tool

The OV Extended Topology tool in the OV Services application group is labeled Node View in a Japanese environment, resulting in two Node View tool icons in this application group.

Solution

Open the Modify window of the application with the incorrect label and enter the correct name.

12. Symptom QXCR1000209866 The Interface Traffic Net Activity Tool Cannot be Started from the Java UI

The Net Activity tool Interface Traffic does not work when started directly from the Java UI.

Solution

You can start an NNM dynamic view, for example, a Neighbor view, and select a node in that view. The Interface Traffic tool is available under the menu options:

Performance -> Network Activity

The Interface Traffic tool can also be started from the Internet submap or from the Application Bank in the Motif UI, again using the menu options:

Performance -> Network Activity

**13. Symptom QXCR1000200666
ovuispmd Fails to Start if Port 7777 is Already in Use**

The ovuispmd process may fail to start if it is not able to use the port 7777.

The following error messages may be displayed:

```
ovuispmd FILED to start.  
Unable to get port 7777.  
Address already in use.
```

Solution

Restart the system. All NNM processes, including ovuispmd, should now be running.

**14. Symptom QXCR1000199438
xnmevents is Killed by SIGSEGV when Starting ovw**

After upgrading from OVO 7.1x to 8.1x on a Japanese HP-UX 11.11 system, xnmevents is killed with the signal SIGSEGV (11) if ovw is started.

Solution

Install the following patches:

- PHSS_30627
- PHSS_31930

**15. Symptom QXCR1000194785
NNM S-Chinese Online Help unusable on Solaris 8 via Hummingbird Exceed**

NNM online help in Simplified Chinese installations is unusable on Solaris 8 via Hummingbird Exceed. Some of Chinese characters are not readable. This is because Hummingbird Exceed does not support the Song family fonts on Solaris 8.

Solution

You can use one of the following alternatives:

- Directly log on to the Solaris console
- Start the font server on the machine where fonts are installed and set the server path in Reflection-X.

**16. Symptom QXCR1000134547
NNM and MC/ServiceGuard White Paper is Not Updated**

The white paper *Network Node Manager 7.xx and MC/ServiceGuard* available on the OVO management server at the following location does not match the NNM version installed on the system:

```
/opt/OV/doc/WhitePapers/MC/ServiceGuard.doc
```

It is for NNM 6.x and MC/ServiceGuard.

Solution

The *Network Node Manager 7.xx and MC/ServiceGuard* white paper is available from the HP OpenView web page:

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

Select operations for unix and version 8.xx, and the list of available documents is displayed.

17. **Symptom QXCR1000281147**

Could not install remote pkg for NNM on HPUX 11.23 PARISC

Could not install remote pkg for NNM on HPUX 11.23 PARISC with instructions provided in the OVO/UNIX installation guide.

Solution

Use the following command to install the remote pkg for NNM on HPUX 11.23 PA-RISC systems:

```
swinstall -x allow_incompatible=true -s \  
../OVOCD2/OV_DEPOT/HPOvOServer.depot OVORemoteOVw,a=HP-UX_B.11.11_32/64,r=08.10.160
```

Network Diagnosis Add-On Module

CAUTION For a complete list of NDAOM-related problems, refer to the NDAOM Release Notes document.

NDAOM

Tracing is centrally controlled by the `ndaom.cfg` configuration file present under the location:

```
/etc/opt/OV/ndaom/conf/ndaom.cfg
```

Trace areas are defined for bigger modules, such as the `ovnwlinkmon` or the `ovnwmonitor`. These modules read the configuration file, check whether tracing is enabled and whether the trace area is set.

Trace areas are: `ovnwmonitor`, `ovnwlinkmon`, `ALL`.

Trace levels are : 0 - 9 with increasing order of trace information.

NDAOM trace can be enabled by adding the following lines in `ndaom.cfg` file:

```
TRACE_AREA=[ovnwmonitor|ovnwlinkmon]  
TRACE_LEVEL=[0 - 9]
```

NDAOM trace information file `ndaom.trc` can be found on the management server at:

```
/var/opt/OV/ndaom/log
```

Problem Diagnosis Probe

Tips for working with the Problem Diagnosis Probe:

- If the GUI applet is not working, check the java console for exceptions.
- If `pd central` will not start via `ovstart`, try using `ovstop pd`, then running the PD manually with the command:

```
pdcentral.sh -start or pdcentral.bat -start
```

Also, try an `ovstop` then `ovstart` on UNIX systems for the `ovspmd` problem.

- Use `<DEBUG>true</DEBUG>` in the `pdconfig.xml` file to generate debug output in the `pd.log` file. This option should only be used briefly because it can generate large amounts of data
- To verify that the probe is running and responding properly, use the command:
`http://probe_name:8067/netpath/netpath.req?destination=sometarget .`
- To verify that the central application is running and responding properly, use the command:
`http://nmsserver:8068/central/central.req?destination=probe_name|sometarget`
- To see the L2 data being returned by ET for an IP address pair, use the command:
`http://nmsserver:7510/topology/NMTopoApi?api=getL2BetweenNodes&begin=ipaddress
&end=ipaddress`
- To get a UI that allows SQL queries on the PD databases, use the commands:

```
pdcentral.sh -dbmgr or pdcentral.bat -dbmgr
```

Internet Services (OVIS)

1. Symptom QXCR1000089414

OVIS Integration does not work with OVO/UNIX 8

OVIS 5.20 integration for OVO/UNIX on OVO/UNIX 8 installation fails.

For more details, refer to the following Ecare document:

<http://openview.hp.com/sso/ecare/getsupportdoc?docid=QXCR1000089414>

Solution

A patch is available on the Openview support web site for OVIS 5.20 to integrate with OVO Unix 8:

<http://support.openview.hp.com/cpe/patches/is/is.jsp>

2. Symptom QXCR1000214514

OVIS 5.20 Integration Does not Work %OvDataDir/datafiles Permissions Changed

The integration of OVIS and OVO/UNIX no longer works after upgrading the OVO 7 DCE agents to OVO 8 HTTPS agents because the file permission of the directory %OvDataDir/datafiles has been changed. Therefore OVIS can no longer access its dat

Solution

When installing the OVO 8 HTTPS agent AFTER installing OVIS, the permissions of the %OvDataDir/datafiles directory and all its current content are changed to only include full permissions for local Administrators. IIS requires IUSR_MACHINE permissions to access the IopsTraceTable.mdb file stored in % OvDataDir/datafiles.

Add this permission manually.

WARNING **The permissions get reset EVERY TIME that the OVO HTTPS agent is started by "ovc -start". Therefore the permissions must be adapted after EVERY "ovc - start".**

NOTE Internet Services (OVIS) cannot co-exist with OVO HTTPS agent on an HP-UX Itanium IA64 node, since the OVIS Probe uses Aries dynamic translation. Install the OVIS Probe on a different system.

Tracing and Troubleshooting

1. Symptom QXCR1000133724

TraceMon Cannot be Used on DHCP or NAT Nodes to Access Trace Server

The TraceMon GUI on a system using DHCP or NAT cannot connect to a Trace Server if there is no name resolution of the GUI station possible.

The Trace Server attempts to verify the validity of the connection request from the TraceMon GUI system by checking the name with DNS. If it cannot be resolved, the connection is refused.

Solution

Configure Trace Server to write to a file and copy the file to the TraceMon System.

Localization

NOTE The OVO agent software for Novell is NOT supported in any type of multi-byte locales.

1. Symptom QXCR1000214400
New Menu Items in Java GUI are in English Only

Some new functionalities introduced with newer versions of JavaGUI come with new menu entries but they are all in english only.

Solution

These will be translated with a future update of OVO/UNIX.

2. Symptom QXCR1000190998
Input/Output and Virtual Terminal Applications Show Garbled Text

On Spanish, Japanese, Simplified Chinese or Korean management servers, Input/Output and Virtual Terminal applications show garbled text instead of correct non-ASCII characters.

Solution

`xterm` and `hpterm` are not able to display non-ASCII characters, so for Input/Output and Virtual Terminal applications for the aforementioned languages, you must use `dtterm`. You may want to set `dtterm` as the default for those platforms where you want to use Input/Output and Virtual Terminal applications.

To do this:

- a. Select [Actions] -> [Set Defaults].
- b. Open a Node Bank window.
- c. In the listbox, select the agent platform for which you want to change the default value.
- d. Click Advanced Options and change the setting for Virtual Terminal Emulator.
- e. Save your change by clicking OK.

After this change, adding a new node of this platform type will automatically have Virtual Terminal Emulator set to `dtterm`. For nodes that you have configured before changing the default, you must change this value manually from the Advanced Options for the node.

In addition, the Character Set for the agent platform and already configured node must match a locale that is already installed on the node, as listed in Table 7-1 on page 178.

Table 7-1 OVO/UNIX Agent Platform Character Sets and Locales

Agent Platform	Management Server Language	Character Set	Locale
HP-UX	Japanese	Shift-JIS	ja_JP.SJIS
		Japanese EUC	ja_JP.eucJP
		UTF-8	ja_JP.utf8
	Spanish	ISO 8859-15	es_ES.iso885915@euro
		UTF-8	es_ES.utf8
	Simplified Chinese	GB-2312	zh_CN.hp15CN
		UTF-8	zh_CN.utf8
	Traditional Chinese	ZHT16BIG5	zh_TW.big5
	Korean	Korean EUC	ko_KR.eucKR
		UTF-8	ko_KR.utf8
Solaris	Japanese	Shift-JIS	ja_JP.PCK
		Japanese EUC	ja_JP.eucJP ja japanese
		UTF-8	ja_JP.UTF-8
	Spanish	ISO 8859-15	es.ISO8859-15
		UTF-8	es.UTF-8
	Simplified Chinese	GB-2312	zh_CN.EUC zh.GBK zh_CN.GBK
		UTF-8	zh_CN.UTF-8
	Traditional Chinese	ZHT16BIG5	zh_TW.big5
	Korean	Korean EUC	ko_KR.EUC ko korean
		UTF-8	ko.UTF-8 ko_KR.UTF-8

Table 7-1 OVO/UNIX Agent Platform Character Sets and Locales (Continued)

Agent Platform	Management Server Language	Character Set	Locale
Linux	Japanese		
		Japanese EUC	ja_JP.EUC-JP
		UTF-8	ja_JP.UTF-8
	Spanish	ISO 8859-15	es_ES@euro
		UTF-8	es_ES.UTF-8
	Simplified Chinese	GB-2312	zh_CN
		UTF-8	zh_CN.UTF-8
	Traditional Chinese	ZHT16BIG5	zh_TW.big5
	Korean	Korean EUC	ko_KR.EUC-KR
		UTF-8	ko_KR.UTF-8

Japanese Version Issues

1. Symptom QXCR1000293835 Message Garbled on Win2003J

Japanese messages, generated by `opcmsg` are garbled on a Win2003J managed node.

Solution

Do the following on the managed node:

- a. Change the `OPC_NODE_CHARSET` to `acp932` using the following command:

```
ovconfchg -ns eaagt -set OPC_NODE_CHARSET acp932
```

- b. Restart the agent using the following commands:

```
opcagt -stop  
opcagt -start
```

2. Symptom QXCR1000298137 DCE Agent is not Running with ja Locale on Solaris 10

Agent does not appear to be running on Solaris 10 with Japanese locale `ja_JP.eucJP`.

Solution

Go to the `/opt/OV/locale/ja/LC_MESSAGES` directory and rename the `opcagt.mo` file to `opcagt.mo.ORIG`.

Run the following command:

```
ln -s ../../ja_JP.PCK/LC_MESSAGES/opcagt.mo
```

3. Symptom QXCR1000193802 RH9.0 Hangs or Fails to Install Certificates from a Japanese/Korean Management Server

Agent may be experiencing problems with Japanese locale `ja_JP.eucJP`.

Solution

Change default locale to `ja_JP.utf8`.

To verify that locales are set correctly, perform an `rlogin` to the Linux node and execute the command:

```
locale
```

The locale `ja_JP.utf8` should be displayed.

4. Symptom QXCR1000194960 ovc -start Hangs on Linux During Installation

During the installation of certificates on Linux systems during installation, the `ovc -start` command hangs. This problem occurs if the locale on the managed node is set to `ja_JP.eucjp`.

Using the `top` command, it can be seen that the `ovbbccb` process is consuming almost 100% of CPU.

Solution

To avoid this problem set `ja_JP.utf8` as a default locale:

For example, in the `/etc/profile` file, enter the following lines:

```
export LANG=ja_JP.utf8
```



```
export LC_ALL=ja_JP.utf8
```

5. Symptom NSMbb69079
Logfile Entry Cannot Be Converted From eucJP to SJIS

There is Logfile Characterset option available in the Add/Modify Logfile window. If you have selected a character set that is different from the current locale, the logfile conversion from one character set to another fails and a critical message is displayed in the message browser.

Solution

Select Logfile Characterset to match the current locale.

6. Symptom NSMbb68102
Japanese Text on Title Bar of Output Window is Unintelligible (hpterm)

Japanese text on title bar of output window opened by either Issue Certificate or Issue Install Key for Certificate tool is unintelligible.

Solution

Modify HP-UX management server node to use dtterm for Virtual Terminal Emulator.

7. Symptom QXCR1000137593
Cannot Convert String to Type Font Structure Warning Message

Motif Administrator and Operator GUI: When starting a Motif GUI, some font-related messages may appear on the command line:

```
Warning: cannot convert string ... to type Font struct.
```

Solution

Every X application requests fonts from the application defaults files or from the code. The Xserver then searches all of the known fonts to locate the font request. If the Xserver does not find the requested font, it reverts back to the system font, and the warning message is displayed:

```
owv:xt warning missing charsets in string to font setconversion.
```

This is an Xtool kit warning from the remote system. Use your Xserver documentation to find the correct procedure for creating a permanent search path in an Xserver environment.

Check also this document:

<http://openview.hp.com/sso/ecare/getsupportdoc?docid=OV-EN004584>.

Korean Version Issues

1. Symptom QXCR1000194960 ovc -start Hangs on Linux During Installation

During the installation of certificates on Linux systems during installation, the `ovc -start` command hangs. This problem occurs if the locale on the managed node is set to `ko_KR.euckr`.

Using the `top` command, it can be seen that the `ovbbccb` process is consuming almost 100% of CPU.

Solution

To avoid this problem set `ja_JP.utf8` as a default locale:

For example, in the `/etc/profile` file, enter the following lines:

```
export LANG=ja_JP.utf8
export LC_ALL=ja_JP.utf8
```

2. Symptom QXCR1000192730 HTTPS Agent Installation on Red Hat Fails During opactivate (ko_KR.euckr)

Problems may be experienced with the Korean locale `ko_KR.euckr`.

Solution

Change default locale to `ko_KR.utf8`.

To verify if locales are set correctly, perform `rlogin` to the system and execute the `locale` command. It should display `ko_KR.utf8`.

3. Symptom QXCR1000204232 Heartbeat Polling Messages do not Acknowledge Each Other on Solaris 9 Systems

On Simplified Chinese and Korean OVO management server installations running on Solaris 9 systems, heartbeat polling messages do not acknowledge each other.

For example, a red *node down* message is not acknowledged by a following green *node up again* message.

Solution

This is planned to be fixed with the next OVO UNIX server patch.

4. Symptom QXCR1000102961 & NSMbb68636 Solaris Korean: ovw Warnings of Duplicate Definitions

For both the Motif Administrator and Operator GUIs, when starting a Motif GUI in Korean locale (ko) on Solaris 8, many warnings appear on the command line:

```
Duplicate define has been ignored.
```

Solution

These warning messages can safely be ignored.

5. Symptom QXCR1000137218 Cannot Display Alphanumeric Labels in Motif UI in Korean Environments

Alphanumeric labels are not displayed correctly in Korean environments.

Solution

- a. Create a link under `/usr/lib/X11`:

```
cd /usr/lib/X11
```

```
ln -s /usr/openwin/lib/locale/ko_KR.EUC ko_KR.EUC
```

- b. Modify the /usr/lib/X11/ko_KR.EUC/app-defaults/OVw file as follows:

Original:

```
OVw*size30Font: *-gothic-medium-r-normal--16-160-*-*-*--ksc5601.1987-0
OVw*size20Font: *-gothic-medium-r-normal--16-160-*-*-*--ksc5601.1987-0
OVw*size10Font: *-gothic-medium-r-normal--16-160-*-*-*--ksc5601.1987-0
OVw*smallFont: *-gothic-medium-r-normal--16-160-*-*-*--ksc5601.1987-0
```

Updated:

```
OVw*size30Font: -adobe-times-medium-r-normal--*-*-*-*--iso8859-15, \
-*gothic-medium-r-normal--16-160-*-*-*--ksc5601.1987-0
OVw*size20Font: -adobe-times-medium-r-normal--*-*-*-*--iso8859-15, \
-*gothic-medium-r-normal--16-160-*-*-*--ksc5601.1987-0
OVw*size10Font: -adobe-times-medium-r-normal--*-*-*-*--iso8859-15, \
-*gothic-medium-r-normal--16-160-*-*-*--ksc5601.1987-0
OVw*smallFont: -adobe-times-medium-r-normal--*-*-*-*--iso8859-15, \
-*gothic-medium-r-normal--16-160-*-*-*--ksc5601.1987-0
```

Modify the /usr/lib/X11/ko_KR.eucKR/app-defaults/OVw file as follows:

Original:

```
OVw*size30Font: -hp-batang-medium-r-normal--*-*-*-*--ksc5636.1989-0
OVw*size20Font: -hp-batang-medium-r-normal--*-*-*-*--ksc5636.1989-0
OVw*size10Font: -hp-batang-medium-r-normal--*-*-*-*--ksc5636.1989-0
OVw*smallFont: -hp-batang-medium-r-normal--*-*-*-*--ksc5636.1989-0
```

Updated:

```
OVw*size30Font: -adobe-times-medium-r-normal--*-*-*-*--iso8859-15, \
-hp-batang-medium-r-normal--*-*-*-*--ksc5636.1989-0
OVw*size20Font: -adobe-times-medium-r-normal--*-*-*-*--iso8859-15, \
-hp-batang-medium-r-normal--*-*-*-*--ksc5636.1989-0
OVw*size10Font: -adobe-times-medium-r-normal--*-*-*-*--iso8859-15, \
-hp-batang-medium-r-normal--*-*-*-*--ksc5636.1989-0
OVw*smallFont: -adobe-times-medium-r-normal--*-*-*-*--iso8859-15, \
-hp-batang-medium-r-normal--*-*-*-*--ksc5636.1989-0
```

Traditional Chinese Version Issues

1. Symptom QXCR1000214444

Cannot Display Alphanumeric Labels in Motif UI in Traditional Chinese Environments

Alphanumeric labels are not displayed correctly in Traditional Chinese environments.

Solution

- a. Create a link under `/usr/lib/X11`:

```
cd /usr/lib/X11
ln -s /usr/openwin/lib/locale/zh_TW.big5 zh_TW.big5
```

- b. Modify the `/usr/lib/X11/zh_TW.big5/app-defaults/OVw` file as follows:

Original:

```
OVw*size30Font: *-medium*-normal---*---*---*---big5-1
OVw*size20Font: *-medium*-normal---*---*---*---big5-1
OVw*size10Font: *-medium*-normal---*---*---*---big5-1
OVw*smallFont: *-medium*-normal---*---*---*---big5-1
```

Updated:

```
OVw*size30Font: -adobe-times-medium-r-normal---*---*---*---iso8859-15, \
*-medium*-normal---*---*---*---big5-1
OVw*size20Font: -adobe-times-medium-r-normal---*---*---*---iso8859-15, \
*-medium*-normal---*---*---*---big5-1
OVw*size10Font: -adobe-times-medium-r-normal---*---*---*---iso8859-15, \
*-medium*-normal---*---*---*---big5-1
OVw*smallFont: -adobe-times-medium-r-normal---*---*---*---iso8859-15, \
*-medium*-normal---*---*---*---big5-1
```

Modify the `/usr/lib/X11/zh_TW.big5/app-defaults/OVw` file as follows:

Original:

```
OVw*size30Font: -hp-sung-medium-r-normal---*---*---*---tchinesebig5
OVw*size20Font: -hp-sung-medium-r-normal---*---*---*---tchinesebig5
OVw*size10Font: -hp-sung-medium-r-normal---*---*---*---tchinesebig5
OVw*smallFont: -hp-sung-medium-r-normal---*---*---*---tchinesebig5
```

Updated:

```
OVw*size30Font: -adobe-times-medium-r-normal---*---*---*---iso8859-15, \
-hp-sung-medium-r-normal---*---*---*---tchinesebig5
OOVw*size20Font: -adobe-times-medium-r-normal---*---*---*---iso8859-15, \
-hp-sung-medium-r-normal---*---*---*---tchinesebig5
OVw*size10Font: -adobe-times-medium-r-normal---*---*---*---iso8859-15, \
-hp-sung-medium-r-normal---*---*---*---tchinesebig5
OVw*smallFont: -adobe-times-medium-r-normal---*---*---*---iso8859-15, \
-hp-sung-medium-r-normal---*---*---*---tchinesebig5
```

2. **Symptom QXCR1000192091**

Traditional Chinese Locale, Core Agent Uses Simplified Chinese Catalog Instead of English

When running some command line commands, such as `ovc`, `ovpolicy`, and `ovcert`, some Traditional Chinese characters in the output of the command are not readable.

Solution

On Traditional Chinese systems, the following will make sure that the strings are displayed in English.

Move the catalog files in the directory `/opt/OV/msg/zh` to `/opt/OV/msg/zh_CN`.

NOTE On Solaris systems, if the locale is `zh`, moving the catalogs will also cause the help strings to be displayed in English.

Spanish Version Issues

1. Symptom QXCR1000198059

English Welcome Message After Installing Spanish OVO/UNIX

When installing in a Spanish environment, the welcome message text is displayed in English.

Solution

This is a language issue and does not affect any other functionality. You may safely ignore this, you can upload your own customized welcome message text, or disable it. For further information on how to work with the welcome message, refer to the `opcuistartmsg` manpage.

2. Symptom QXCR1000285811

A number of NNM 7.5 AE/SE filesets not removed by the `ovoremove` script

After deinstallation of NNM 7.5 AE/SE (published in July 2005) using the NNM remove script or `ovoremove` script, the following NNM filesets could still be found on the system:

Name	Version	Description
HPOv3ComAgt	2.50.000	HP Openview NNM Advanced Edition Device Support for 3Com
HPOvAlcatelAgt	2.50.000	HP Openview NNM Advanced Edition Device Support for Alcatel
HPOvBayAgt	3.00.000	HP Openview NNM Advanced Edition Device Support for Nortel Bay
HPOvCDPAgt	2.50.000	HP Openview NNM Advanced Edition Device Support for CDP
HPOvCentilAgt	1.50.000	HP Openview NNM Advanced Edition Device Support for Centillion
HPOvCiscoAgt	2.60.000	HP Openview NNM Advanced Edition Device Support for Cisco
HPOvEDPAgt	2.51.000	HP Openview NNM Advanced Edition Device Support for EDP
HPOvExtremeAgt	2.50.000	HP Openview NNM Advanced Edition Device Support for Extreme
HPOvFoundryAgt	2.51.000	HP Openview NNM Advanced Edition Device Support for Foundry
HPOvPassAgt	3.00.000	HP Openview NNM Advanced Edition Device Support for Nortel Passport
HPOvProAgt	2.50.000	HP Openview NNM Advanced Edition Device Support for HP Procurve

Solution

Manually deinstall all remaining NNM filesests with `swremove` tool.