

# **HP Operations Manager on Linux**

## **Security Advisory**

**Software Version: 9.01**



**Manufacturing Part Number: None**

**September 2009**

© Copyright 2005-2009 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 at DFARS 252.227-7013.

Hewlett-Packard Company  
United States of America

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

### **Copyright Notices.**

©Copyright 2005-2009 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.

### **Trademark Notices.**

Adobe® is a trademark of Adobe Systems Incorporated.

Intel®, Itanium®, and Pentium® are trademarks of Intel Corporation in the U.S. and other countries.

Java™ is a US trademark of Sun Microsystems, Inc.

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

Oracle® is a registered trademark of Oracle Corporation and/or its affiliates.

UNIX® is a registered trademark of the Open Group.



---

## Support

### 1. Introduction

Document Overview . . . . .	12
Document Audience . . . . .	13

### 2. HPOM Security Overview

Security Risks . . . . .	16
Key to Table Values . . . . .	18
Key to Risk Table Values . . . . .	18
Key to Service Table Values . . . . .	18

### 3. Protecting HPOM Components

Securing the HPOM Management Server . . . . .	21
HTTPS-based HPOM Server-to-Server Communication . . . . .	21
Securing Sockets . . . . .	22
Changing Permissions for the Sockets Directory . . . . .	22
Securing the Java GUI . . . . .	23
Running the Java GUI as a Web Applet . . . . .	23
Restricting Java GUI Privileges . . . . .	23
Restricting Java GUI Communication . . . . .	27
Changing the Default Port of opcuwww . . . . .	29
Changing the Default Port of opcuhttps . . . . .	30
Providing Certificates for Full Authentication Mode . . . . .	30
Protecting the Java GUI against Denial of Service Attacks . . . . .	32
Restricting the Number of Simultaneous Connections to opcuhttps . . . . .	34
Changing Permissions for the Agent Installation Trace File . . . . .	35
Securing APIs . . . . .	36

### 4. Protecting the IT Environment

Securing the Operating System . . . . .	41
Reviewing OS Security Documents . . . . .	41
Installing OS Security Patches . . . . .	41
Preventing Stack Execution . . . . .	41
Preventing Stack Execution on HP-UX . . . . .	43
Preventing Stack Execution on Sun Solaris . . . . .	43

---

Securing the Oracle Database . . . . .	45
Changing Oracle Database Default Passwords . . . . .	45
Changing the Oracle Database Password for OPC_OP . . . . .	46
Running the Oracle Database on HPOM . . . . .	47
Restricting Remote Access to the Oracle Database . . . . .	48
Restricting Access to the Oracle Listener . . . . .	50
Restricting Access to Oracle User Passwords . . . . .	50
Securing the Network Node Manager . . . . .	51
Changing Permissions for the ECS Directory . . . . .	51
Changing Permissions for the SNMP Trap Interceptor and Daemon . . . . .	52
Changing Permissions for the OVSPMD_MGMT Socket . . . . .	53
Securing SNMP and NNM . . . . .	54
Changing the SNMP Community String . . . . .	54
Verifying Access to NNM Shared Memory . . . . .	54
Securing the HP Web Server . . . . .	55
Securing the HPOM Agent . . . . .	57
Installing the HPOM Agent . . . . .	57
Switching to the HPOM HTTPS Agent . . . . .	58
Single-Port Communication . . . . .	59
Running Non-Root HPOM HTTPS Agents on UNIX Platforms . . . . .	59
Securing the IT Infrastructure . . . . .	61

## **5. Configuring HPOM in a Secure Way**

Assigning Rights to Users . . . . .	65
Assigning Applications . . . . .	66
Assigning Applications to Generic Users . . . . .	66
Assigning Applications to User Profiles . . . . .	66
Assigning Broadcast and Virtual Terminal Applications . . . . .	66
Assigning URL Applications . . . . .	67
Restricting Operator Access to Node and Message Groups . . . . .	67
Restricting Operator Access to Services . . . . .	67
Changing Default Operator Passwords . . . . .	68
PAM - Pluggable Authentication Module . . . . .	70
Auditing Users . . . . .	71
Auditing Administrator Activities . . . . .	71
Protecting Audit and History Download Files . . . . .	72
Locking Administrator Audit Levels . . . . .	73

---

Protecting Machine and Account Names . . . . .	74
Securing Remote Actions . . . . .	75
Securing the Certificate Server . . . . .	78
Securing Local Actions . . . . .	79
Configuring the Managed Nodes as “Monitored Only” . . . . .	80
Avoiding Unattended Configuration Deployment . . . . .	81
Denial of Configuration Deployment . . . . .	81
Digitally Signed Configuration . . . . .	82

## **6. Protecting HPOM Services**

Assessing Your System Vulnerability with ovprotect . . . . .	85
Services on HPOM . . . . .	88
Services Not Required by HPOM . . . . .	88
Services Required by HPOM . . . . .	92
Services for HPOM HTTPS Windows Agents . . . . .	95
Services Required by HPOM HTTPS Windows Agents . . . . .	95
Start or Stop Services on Microsoft Windows . . . . .	98

### **A. Checking HPOM Versions**

Check the HP Operations Management Server . . . . .	101
Check the Java Operator GUI Client . . . . .	102
Check Core Agent Components . . . . .	103
Check OpenSSL . . . . .	104
Check the EventAction Component of the HTTPS Agent . . . . .	105
Check Non-HPOM Components . . . . .	107





---

## Support

Please visit the HP Operations support web site at:

[www.hp.com/go/hpsoftwaresupport](http://www.hp.com/go/hpsoftwaresupport)

This web site provides contact information and details about the products, services, and support that HP Operations offers.

HP Operations online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valuable support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit enhancement requests online
- Download software patches
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and log on. Many also require a support contract.

To find more information about access levels, go to:

[http://www.hp.com/managementsoftware/access\\_level](http://www.hp.com/managementsoftware/access_level)

To register for an HP Passport ID, go to:

<http://www.managementsoftware.hp.com/passport-registration.html>



---

# **1 Introduction**

## Document Overview

This document provides you with a summary of security information related to HP Operations Manager on Linux (HPOM).

To provide security, HPOM strictly controls the functionality and information provided to users by the system.

The recommendations listed in this document are based on certifying HPOM for the National Information Assurance Partnership (NIAP) Common Criteria Evidence Assurance Level 2 (EAL-2) in 2005. These recommendations are updated periodically.

NIAP is a program driven by the National Institute of Standards and Technology (NIST) and National Security Agency (NSA) in the U.S.A. to evaluate IT product conformance to international standards, especially with regards to security.

The Common Criteria are the result of many decades of effort to develop practical and measurable criteria for evaluating IT security that are broadly useful within the international community. Common Criteria predecessors are the Orange Book, ITSEC, and many country-specific security guidelines.

NIAP acts as the U.S. oversight body for the Common Criteria.

For more information about the Common Criteria, see the following web site:

<http://niap.nist.gov>

For detailed information about the HPOM Common Criteria EAL-2 certification, see the following web site:

[http://niap.nist.gov/cc-scheme/st/ST\\_VID10011.html](http://niap.nist.gov/cc-scheme/st/ST_VID10011.html)

---

### NOTE

There is a utility called `ovprotect` that helps you to address several of the outlined security risks automatically. For more information about `ovprotect`, see *OvProtect User Manual* located on the HPOM management server at the following location:

```
/opt/OV/contrib/OpC/OvProtect
```

## **Document Audience**

This document is intended primarily for the following audience:

- HPOM administrator
- Security expert in your company
- System and application administrators monitored by HPOM

Introduction

**Document Audience**

---

## **2** **HPOM Security Overview**

## Security Risks

HPOM is a powerful IT service management solution used to manage networks, systems, applications, and the Internet from a service-driven operations perspective.

For almost all software products, potential vulnerability risks need to be assessed carefully in your actual IT environment. This risk assessment is particularly important for applications like HPOM, a multiple-component, distributed software product to which many users can have access.

Depending on your software usage paradigm, your company security policies, and so on, some of the security risks of HPOM outlined below may or may not apply.

This document categorizes security risks to an HPOM implementation as follows:

- **HPOM Components**

- HPOM Java GUI
- HPOM Service Navigator
- HPOM management server
- HPOM HTTPS agent

For details, see Chapter 3, “Protecting HPOM Components,” on page 19.

- **Services Providing Remote Access/Query Capabilities**

For details, see Chapter 6, “Protecting HPOM Services,” on page 83.

- **IT Environment**

- Operating system  
(for example, HP-UX, Solaris, Linux, and so on)
- Oracle Database
- Network Node Manager (NNM)<sup>1</sup>

---

1. NNM is treated as an IT environment component.



- Embedded APIs or hooks  
(for example, OpenSSL, Java API, PAM, and so on)
- Specific run-time environments  
(for example, Java Virtual Machine, libc, and so on)
- Other IT infrastructure components  
(for example, firewall, routers, and so on)

For details, see Chapter 4, “Protecting the IT Environment,” on page 39.

- **HPOM Configuration**

- User configuration
- Auditing
- HPOM agent type and run level
- Remote action execution
- And so on

For details, see Chapter 5, “Configuring HPOM in a Secure Way,” on page 63.

Some of these security risks are exposed in the entire IT infrastructure, and some only on the local system.

This document provides a comprehensive list of actual and potential security risks for each category, and the corresponding steps to minimize or eliminate them.

---

**NOTE**

The impact, relevance, and risk level for the different security concerns have been determined by HP for typical customer environments. The actual risk, impact, and relevance may be different in your environment.

---

## Key to Table Values

This document contains many risk and service tables.

### Key to Risk Table Values

Many sections in this document contain risk tables with the following levels:

**Relevance** High, Medium, or Low. Damage that could occur to your HPOM installation, managed environment, or both if someone gained access to them.

**Risk Level** High, Medium, or Low. Likelihood that someone could access or misuse the outlined vulnerability.

These levels are just assessments by HP. The actual relevance and risk level may vary significantly for your environment.

### Key to Service Table Values

“Services on HPOM” on page 88 contains two service tables with the following headings:

**Port** Port that is used by the service.

**Service** Name of the service. This name could be different for HP-UX, Solaris, AIX, and Linux.

**Required** Yes or No. Service is required to run HPOM.

**Comment** Description and recommendation.

---

# **3**      **Protecting HPOM Components**

HPOM software components could be exposed to a wide variety of security risks.

HPOM provides powerful mechanisms for service-driven operations management. System and network security requires reasonable usage (or even limitation) of optional HPOM features, based on the least permissions paradigm.

## Securing the HPOM Management Server

The standard installation of the HP Operations management server is suitable for most customers. Nevertheless, you should check carefully, on a regular basis, to make sure that none of the security risks listed in this section could potentially impact your managed environment.

### HTTPS-based HPOM Server-to-Server Communication

HPOM uses HTTPS-based communication for forwarding events to other HP Operations management servers. The HTTPS protocol establishes a higher level of security for the communication between management servers. HTTPS-based message forwarding between management servers is enabled by default.

To successfully use HTTPS-based forwarding, a trust relationship must be established between all HP Operations management servers that communicate with each other. For more information about setting up trust relationships, see the *HPOM HTTPS Agent Concepts and Configuration Guide*.

---

## Securing Sockets

This section describes vulnerabilities in sockets used by the HPOM management server.

### Changing Permissions for the Sockets Directory

To prevent non-root users from removing socket files, you can change permissions for the sockets directory.

<b>Vulnerability</b>	The directory <code>/var/opt/OV/sockets</code> is world writable.
<b>Impact</b>	It is possible for a non-root user to remove socket files in the <code>/var/opt/OV/sockets</code> directory. These files are important for inter-process communication.
<b>Relevance</b>	High
<b>Risk Level</b>	High
<b>Solution</b>	<p>Run <code>ovprotect</code> or follow these steps:</p> <ol style="list-style-type: none"><li>1. Change the permissions for the <code>/var/opt/OV/sockets</code> directory to <code>0770</code>: <pre># chmod 0770 /var/opt/OV/sockets</pre></li><li>2. Create an entry in <code>/etc/opt/OV/share/conf/ovperms.conf/files</code> to permanently change this file permission: <pre>/var/opt/OV/sockets file bin bin 0770</pre></li></ol> <p>For more information about <code>ovprotect</code>, see <i>OvProtect User Manual</i> located on the HPOM management server at the following location: <code>/opt/OV/contrib/OpC/OvProtect</code></p>

---

## Securing the Java GUI

This section describes vulnerability risks in the HPOM Java GUI.

### Running the Java GUI as a Web Applet

To prevent unauthorized persons from tampering with the Java GUI shar file, you can run the Java GUI as an applet in your web browser.

<b>Vulnerability</b>	If you run the Java GUI as an application, its digital signature is <i>not</i> verified.
<b>Impact</b>	An unauthorized person could tamper with the Java GUI jar file.
<b>Relevance</b>	Medium
<b>Risk Level</b>	Medium
<b>Solution</b>	Run the Java GUI as an applet in your web browser. In this case, its digital signature is verified.

### Restricting Java GUI Privileges

To prevent unauthorized persons from reading or writing operator-specific Java GUI settings, you can give user preference files the lowest possible level of privileges.

<b>Vulnerability</b>	Java GUI users can store their preferences in local files, which could be tampered with by other users.
<b>Impact</b>	Depending on the default privileges, it is possible for unauthorized persons to read or write operator-specific Java GUI settings (for example, filter settings, refresh rate, and so on).
<b>Relevance</b>	Medium
<b>Risk Level</b>	Medium

<b>Solution</b>	<p>Give user preference files the lowest possible level of privileges.</p> <p>To set the <i>SAME</i> preferences for all Java GUI sessions, you can also place the preferences files on the HP Operations management server.</p> <p>You move three files to a global location:</p> <ul style="list-style-type: none"><li>• <code>Itoopbrw</code> Stores message browser settings (layout, position, size).</li><li>• <code>Itooprc</code> Stores general Java GUI settings. Most of the properties can be configured in the Preferences dialog of the Java GUI.</li><li>• <code>HP_OV_consoleSettings_mgmtServerName_operator</code> Stores all GUI layouts (for example, browser column layout).</li></ul> <p>Example:</p> <pre>HP_OV_consoleSettings_chita.hermes.si_opc_op</pre> <p>The following files remain on the user <code>.home</code> directory:</p> <ul style="list-style-type: none"><li>• <code>OV_JGUI_portRepository</code> Used for Java API discovery.</li></ul> <p>To set up a global location for preference files, use the following variables:</p> <pre>OPC_JGUI_GLOBAL_SETTINGS_WIN OPC_JGUI_GLOBAL_SETTINGS_UNIX</pre> <p>Example:</p> <pre># ovconfchg -ovrg server -ns opc -set \ OPC_JGUI_GLOBAL_SETTINGS_WIN \ X:\Shared\javau\</pre>
-----------------	---



<b>Solution</b>	<p>Give user preference files the lowest possible level of privileges.</p> <p>To set the <code>SAME</code> preferences for all Java GUI sessions, you can also place the preferences files on the HP Operations management server.</p> <p>You move three files to a global location:</p> <ul style="list-style-type: none"><li>• <code>Itoopbrw</code> Stores message browser settings (layout, position, size).</li><li>• <code>Itooprc</code> Stores general Java GUI settings. Most of the properties can be configured in the Preferences dialog of the Java GUI.</li><li>• <code>HP_OV_consoleSettings_mgmtServerName_operator</code> Stores all GUI layouts (for example, browser column layout).</li></ul> <p>Example:</p> <pre>HP_OV_consoleSettings_chita.hermes.si_opc_op</pre> <p>The following files remain on the user <code>.home</code> directory:</p> <ul style="list-style-type: none"><li>• <code>OV_JGUI_portRepository</code> Used for Java API discovery.</li></ul> <p>To set up a global location for preference files, use the following variables:</p> <pre>OPC_JGUI_GLOBAL_SETTINGS_WIN OPC_JGUI_GLOBAL_SETTINGS_UNIX</pre> <p>Example:</p> <pre># ovconfchg -ovrg server -ns opc -set \ OPC_JGUI_GLOBAL_SETTINGS_WIN \ X:\Shared\javau\</pre>
-----------------	---

<p><b>Solution</b> (continued)</p>	<p><b>To set up the share:</b></p> <ol style="list-style-type: none"><li>1. Log on as the user who has write permission to this directory.</li><li>2. Set all defaults within the Java GUI as needed.</li><li>3. Save the session and log out.</li><li>4. Rename the <code>consoleSettings</code> file with a more global name.</li></ol> <p>For example, you could change the <code>HP_OV_consoleSettings_ligety.bbn.hp.com_opc_op</code> file to <code>HP_OV_consoleSettings</code>.</p> <p>To do so, you would input the following:</p> <pre>f:\JGUI_share&gt; rename \ HP_OV_consoleSettings_ligety.bbn.hp.com_opc_op \ HP_OV_consoleSettings</pre> <ol style="list-style-type: none"><li>5. Make the share read only.</li></ol>
--	--

## Restricting Java GUI Communication

By default, the proprietary communication protocol (except for the log-on data) between the HP Operations management server and the Java GUI is unencrypted.

The communication protocol contains sensitive data. For this reason, it must be protected in the IT environment. The Java GUI communication can be switched to HTTPS, which provides authentication and encryption.

---

**NOTE**

Only the HTTPS-based Java GUI has been evaluated as part of the Common Criteria EAL-2 evaluation.

---

<b>Vulnerability</b>	<p>The <code>opcuiwww</code> socket on the HP Operations management server accepts incoming connection requests from any system. For each Java GUI session, a dedicated <code>opcuiwww</code> process is launched.</p> <p>The connection protocol requires a valid authentication process, and therefore provides reasonable protection against misuse.</p> <p>During the connection initiation and validation phase (that is, until the logon is granted or denied), <code>opcuiwww</code> already consumes system resources (for example, memory, CPU, and file handles).</p>
<b>Impact</b>	Opening too many connections to the <code>opcuiwww</code> service may consume all available system resources.
<b>Relevance</b>	High
<b>Risk Level</b>	High

<b>Solution</b>	<p>Run the <code>ovprotect</code> utility or do one of the following:</p> <ul style="list-style-type: none"><li>• Switch on HTTPS communication between the Java GUI and the HP Operations management server. To find out how to configure the HP Operations management server and the Java GUI, see the corresponding documentation.</li></ul> <p>Detailed configuration and usage instructions are available in the <i>HPOM Java GUI Operator's Guide</i>, available for download from the following web site:</p> <p><a href="http://support.openview.hp.com/selfsolve/manuals">http://support.openview.hp.com/selfsolve/manuals</a></p> <ul style="list-style-type: none"><li>• Do not allow all systems in the network to access the HP Operations management server, especially the <code>opcuiwww</code> port (for example, by protecting it with a firewall, by changing <code>/var/adm/inetd.sec</code> on HP-UX, or by changing the corresponding file on other OS platforms).</li></ul> <p>For example, if you want to allow the local system and the system with IP address 15.1.2.3, you would use the following:</p> <pre><b>ito-e-gui allow 127.0.0.1 15.1.2.3</b></pre> <p>For details, refer to the <i>inetd.sec(4)</i> man page.</p> <p>Monitor the number of started <code>opcuiwww</code> processes to ensure that it is consistent with the maximum number of concurrent Java GUI operators you expect.</p> <p>For more information about <code>ovprotect</code>, see <i>OvProtect User Manual</i> located on the HPOM management server at the following location:</p> <pre>/opt/OV/contrib/OpC/OvProtect</pre>
-----------------	---

## Changing the Default Port of opcuiwww

<b>Vulnerability</b>	The default port number (2531) of the opcuiwww process is known and might therefore be a target of attack.
<b>Impact</b>	If opcuiwww is attacked through the default port, the system may stop responding.
<b>Relevance</b>	Medium
<b>Risk Level</b>	Medium
<b>Solution</b>	<p>The configuration setting OPCUIWWW_PORT holds the opcuiwww port number as defined in /etc/services (ito-e-gui entry). It is used by opcuihttps to start opcuiwww processes.</p> <p>It is recommended to change the default port 2531 to another port:</p> <pre>ovconfchg -ovrg server -ns opc.opcuihttps -set OPCUIWWW_PORT &lt;new port&gt;</pre> <p>You can also use the ovprotect utility to change the default port. For more information, see Table 6-2, “Services and Ports Required by HPOM,” on page 92.</p> <p>For more information about configuration variables for the management server, see the <i>HPOM Server Configuration Variables</i> guide.</p>

## Changing the Default Port of opcuhttps

<b>Vulnerability</b>	The default port number (35211) of the opcuhttps process is known and might therefore be a target of attack.
<b>Impact</b>	If opcuhttps is attacked through the default port, the system may stop responding.
<b>Relevance</b>	Medium
<b>Risk Level</b>	Medium
<b>Solution</b>	<p>The default port number on which opcuhttps listens for incoming HTTPS connections from Java GUI clients is 35211.</p> <p>It is recommended to change the default port 35211 to another port:</p> <pre>ovconfchg -ovrg server -ns opc.opcuhttps -set SERVER_PORT &lt;new port&gt;</pre> <p>For more information about configuration variables for the management server, see the <i>HPOM Server Configuration Variables</i> guide.</p>

## Providing Certificates for Full Authentication Mode

<b>Vulnerability</b>	The opcuhttps server accepts anonymous connections from clients by default. Clients are usually HTTPS-based Java GUI consoles, but can also be web browsers.
<b>Impact</b>	If opcuhttps is attacked through anonymous connections, the system may stop responding.
<b>Relevance</b>	Medium
<b>Risk Level</b>	Medium

<b>Solution</b>	<p>If <code>SSL_CLIENT_VERIFICATION_MODE</code> is set to <code>RequireCertificate</code>, clients require the certificate for (full) authentication. To provide the certificates for the full authentication mode, perform the following steps:</p> <ol style="list-style-type: none"><li>1. Enable full authentication mode for <code>opcuihttps</code>:<ol style="list-style-type: none"><li>a. Configure <code>opcuihttps</code>:<pre>ovconfchg -ovrg server -ns opc.opcuihttps -set SSL_CLIENT_VERIFICATION_MODE RequireCertificate</pre></li><li>b. Restart the <code>opcuihttps</code> process.</li></ol><p>For more information about configuring <code>opcuihttps</code> parameters, see the <i>HPOM Administrator's Reference</i>.</p></li><li>2. Ensure that the client certificate is installed on the client system. If an HP Operations agent is installed on the Java GUI client system, you can use its client certificate for authentication. If no agent is installed, install the client certificate manually as described in the <i>HPOM Java GUI Operator's Guide</i>.</li><li>3. Set the Java GUI startup parameter <code>lcore_defaults</code> to <code>yes</code>, so that Java GUI uses the default Core functionality. The Core functionality is installed with the HP Operations agent if it exists on the Java GUI client. If no agent is installed, install the Core functionality manually as described in the <i>HPOM Java GUI Operator's Guide</i>.</li></ol> <p>For more information about configuration variables for the management server, see the <i>HPOM Server Configuration Variables</i> guide.</p>
-----------------	--

## Protecting the Java GUI against Denial of Service Attacks

Denial of Service (DoS) functionality provides protection against attacks to the opcuwww process. The protection includes:

- Limitation of the number of connections to the Java GUI
- Limitation of the number of connections from one system
- Limitation of input buffer size
- Time out of input stream inactivity before the first request is served

<b>Vulnerability</b>	Multiple Java GUIs may open too many sockets to opcuwww and keep them open.
<b>Impact</b>	Such attack or situation may occupy all available memory after some time and the system may stop responding.
<b>Relevance</b>	Medium
<b>Risk Level</b>	Medium



<b>Solution</b>	<ol style="list-style-type: none"><li>1. Enable basic DoS protection for the <code>opcuiwww</code> process. Set the configuration variable <code>DOS_ENABLED</code> to <code>TRUE</code>: <pre>ovconfchg -ovrg server -ns opc -set DOS_ENABLED TRUE</pre></li><li>2. <i>Optional.</i> Configure the following DoS settings according to your security needs:<ol style="list-style-type: none"><li>a. Set the size of the input buffer on the <code>opcuiwww</code> socket. If the size exceeds the buffer limit, an error is reported to <code>System.txt</code>, and the connection (<code>opcuiwww</code> process) is closed. The default value is 4096. Example: <pre>ovconfchg -ovrg server -ns opc -set OPCUIWWW_INPUT_BUFFER_LIMIT 512</pre></li><li>b. Set the maximum number of simultaneous connections to <code>opcuiwww</code> (Java GUIs). The default value is 100. Example: <pre>ovconfchg -ovrg server -ns opc -set OPCUIWWW_MAX_CONNECTION 5</pre></li><li>c. Set the number of connections to <code>opcuiwww</code> from a single system. The default value is 30. Example: <pre>ovconfchg -ovrg server -ns opc -set OPCUIWWW_ONE_CONNECTION 2</pre></li><li>d. Set the time out for inactivity on the <code>opcuiwww</code> socket. A valid request must arrive at the socket within the specified time (measured from the initial connection), otherwise <code>opcuiwww</code> logs an error and exits. The default value is 5 (seconds). Example: <pre>ovconfchg -ovrg server -ns opc -set OPCUIWWW_TIMEOUT 3</pre></li></ol></li></ol> <p>For more information about configuration variables for the management server, see the <i>HPOM Server Configuration Variables</i> guide.</p>
-----------------	--

## Restricting the Number of Simultaneous Connections to opcuhttps

<b>Vulnerability</b>	Multiple Java GUIs may open too many sockets to opcuhttps and keep them open.
<b>Impact</b>	Such attack or situation may occupy all available memory after some time and the system may stop responding.
<b>Relevance</b>	Medium
<b>Risk Level</b>	Medium
<b>Solution</b>	<p>Limit the maximum number of simultaneous connections to opcuhttps. Clients are usually HTTPS-based Java GUI consoles, but can also be web browsers. The default value is 100. Example:</p> <pre>ovconfchg -ovrg server -ns opc.opcuhttps -set MAX_CONNECTIONS 10</pre> <p>For more information about configuration variables for the management server, see the <i>HPOM Server Configuration Variables</i> guide.</p>

---

## Changing Permissions for the Agent Installation Trace File

To prevent non-root users from reading the agent installation trace file, you can change permissions for the file.

<b>Vulnerability</b>	The file <code>/tmp/inst.sh.2</code> may be world readable when agent installation tracing is set up.
<b>Impact</b>	It is possible for a non-root user to read the agent installation trace file. This file may contain node passwords. The file is created when the agent installation tracing is set up. For details, see the man page for <code>inst_debug</code> .
<b>Relevance</b>	Medium
<b>Risk Level</b>	Medium
<b>Solution</b>	Change the permission of the trace file to 0600: <pre># chmod 0600 /tmp/inst.sh.2</pre> <p><b>NOTE:</b> The name of the file depends on the configuration of the variable <code>OPC_DEBUG_FILE</code> in the file <code>/var/opt/OV/share/tmp/OpC/mgmt_sv/inst_debug.conf</code>.</p>

## Securing APIs

HPOM provides a rich set of APIs on the management server and the HP Operations agents. This section describes only the APIs that expose security-related risks.

<b>Problem</b>	The HPOM API <code>opcapp_start()</code> on the management server has a potential security problem, which is fixed by <code>opcapp1_start()</code> . For backward compatibility, <code>opcapp_start()</code> is still offered, but should <i>not</i> be used.
<b>Impact</b>	Some existing applications that use <code>opcapp_start()</code> may not run as expected.
<b>Relevance</b>	Low
<b>Risk Level</b>	Low

<b>Solution</b>	<p>Do one of the following:</p> <ul style="list-style-type: none"><li>• <b>Recommended</b> Replace the function call <code>opcapp_start()</code> with <code>opcappl_start()</code> in all of your applications.</li><li>• <b>Workaround</b> If the recommended solution is not immediately possible, you can set the variable <code>OPC_OMIT_PWD_CHECK_FOR_APP_START</code> in the namespace <code>opc</code> and the resource group <code>server</code> to <code>TRUE</code>:<ol style="list-style-type: none"><li>1. Stop your application: <pre># &lt;stop your application&gt;</pre></li><li>2. Enter the following: <pre># ovconfchg -ovrg server -ns opc \ OPC_OMIT_PWD_CHECK_FOR_APP_START \ TRUE</pre><p><b>CAUTION:</b> Setting the <code>OPC_OMIT_PWD_CHECK_FOR_APP_START</code> configuration variable partially re-introduces the security problem.</p></li><li>3. Start your application: <pre># &lt;start your application&gt;</pre></li></ol></li></ul>
-----------------	--



---

# **4            Protecting the IT Environment**

The HP Operations Manager for UNIX (HPOM) IT environment includes security for the operating system (OS), Oracle Database, and Network Node Manager (NNM).



## Securing the Operating System

This section contains information about OS security. It outlines only a few of the currently known potential security risks. Review the security announcements of your OS vendors on a regular basis.

### Reviewing OS Security Documents

For more information about OS security, refer to the following documents:

- *UNIX Security Checklist v2.0*  
[http://www.cert.org/tech\\_tips/AUSCERT\\_checklist2.0.html](http://www.cert.org/tech_tips/AUSCERT_checklist2.0.html)
- *HP-UX 11i Security* (web site)  
<http://www.hp.com/products1/unix/operating/security/>
- *HP-UX 11i Security* (book by Chris Wong)  
[http://www.hp.com/hpbooks/prentice/ptr\\_0130330620.html](http://www.hp.com/hpbooks/prentice/ptr_0130330620.html)

For other operating systems, consult the corresponding web pages and announcements of their vendors on a regular basis.

### Installing OS Security Patches

At all times, make sure that the latest available OS and product patches are installed on all systems. Regularly review OS vendor web sites for updates.

### Preventing Stack Execution

The Stack Execution Prevention, also known as Non-Stack Execution (NX), is a feature of modern processors that prevents or at least limits the risk of the execution of code on the stack. This feature increases security by preventing some types of buffer overflows. It is safe to enable this feature. Newer applications do not execute any code on the stack.

HPOM has been tested to run with this feature switched on.

Overview of Stack Execution Prevention Support by platform:

- **Windows XP SP2**

By default, NX is switched on for the following CPU types: AMD 64, AMD Opteron, Intel Itanium, and most recent Pentium and Xeon.

- **Windows Server 2003 SP1**

By default, NX is switched on for the following CPU types: AMD 64, AMD Opteron, Intel Itanium, and most recent Pentium and Xeon.

- **Solaris 9 and higher (SPARC)**

NX is available. By default, NX is switched *off*.

- **HP-UX 11i v3 on Integrity**

NX is available. By default, NX is switched *on*.

- **Red Hat Enterprise Linux 3 and higher**

NX is available. By default, NX is switched *on*.

- **SuSE Professional 9.2, SuSE Linux Enterprise Server and higher**

NX is available. By default, NX is switched *off*.

---

**CAUTION**

---

There may be some applications that require stack execution by design.

You can determine which applications require stack execution by reading technical application descriptions. If these descriptions do not contain the information you need, you can monitor the appropriate logfiles (for example, `syslog` on Solaris).

## Preventing Stack Execution on HP-UX

To prevent stack execution, HP-UX 11i v3 provides a kernel parameter that can be set through the SMH tool:

```
executable_stack = 0
```

Default. Causes stacks to be non-executable. This setting is strongly preferred from a security perspective. If a program attempts to execute code from its stacks after this setting is chosen, the HP-UX 11.31 Itanium kernel immediately terminates the program (sends a SIGKILL signal), and logs the apparent stack buffer overflow attack.

```
executable_stack = 1
```

Causes all program stacks to be executable. This setting is *not* recommended. Change the setting in the SMH tool, and generate a new kernel.

```
executable_stack = 2
```

Same as a setting of 0, except that it gives non-fatal warnings instead of terminating the process. Think of this setting as a kind of “trial mode.”

## Preventing Stack Execution on Sun Solaris

Solaris 9 and higher include a built-in feature that prevents stack execution. This feature can be enabled or disabled, as needed.

For details, see the following web sites:

<http://www.sun.com/software/solaris/ds/ds-security/>

<http://www.sun.com/software/solaris/9/ds/ds-sol9oe/index.html>

With Solaris 9 or higher, you can modify the `/etc/system` file to disable the stack execution.

To disable the stack execution, add the following two lines to `/etc/system`:

```
set noexec_user_stack=1  
set noexec_user_stack_log=1
```

The second line adds an entry to `syslog` every time code is executed on the stack.

---

## Securing the Oracle Database

This section contains information about Oracle Database security. For further details, check the appropriate Oracle security news regularly.

### Changing Oracle Database Default Passwords

After the installation of the Oracle Database, the default database users are set up to accept default passwords. These default passwords could be used by intruders to access the database and change data.

---

#### CAUTION

It is strongly recommended that you change the passwords of the default Oracle Database users immediately after installation of Oracle software.

---

#### To change Oracle Database user passwords:

1. Log on to the Oracle Database as the user `oracle`.
2. Enter the following:

```
# sqlplus /nolog
SQL# connect / as sysdba;
SQL# select username from dba_users;

USERNAME
-----
SYS
SYSTEM
OUTLN
DBSNMP
SD
OPC_OP
OPC_REPORT
7 rows selected.
```

`SYS`, `SYSTEM`, `OUTLN`, and `DBSNMP` are the default users created by Oracle itself. `OPC_OP` and `OPC_REPORT` are additional default users created by HPOM during the `ovoinstall` phase. The `SD` user is added if you use the HP Service Desk (HPSD) products.

3. For each default user created by Oracle and OPC\_REPORT, enter the following:

```
SQL# alter user <username> identified by <newpasswd>;
```

```
User altered.
```

In this command, *<username>* is the name of the default user (for example, *sys*), and *<newpasswd>* is the new, unique password.

---

**CAUTION**

During the HP Operations management server installation, the `ovoinstall` script requires that the Oracle user `SYSTEM` have its default password. Otherwise, the HPOM database table creation fails.

---

## Changing the Oracle Database Password for OPC\_OP

The only Oracle Database user for which you may *not* change the password using the SQL `alter` statement is `OPC_OP`.

This password is also stored (encrypted) by HPOM internally in the file:

```
/etc/opt/OV/share/conf/OpC/mgmt_sv/.opcdbpwd.sec.
```

### To change the OPC\_OP database user password:

1. Log on to the Oracle Database as the user `root`.
2. Enter the following:

```
# opcdbpwd -s
```

```
New password of database user opc_op: *****
```

```
Please retype the password: *****
```

---

**NOTE**

The OPC\_REPORT password is used by applications such as HP Reporter. It needs to be adapted in HP Reporter accordingly in the **File→Configure→Databases** menu.

---

<b>Vulnerability</b>	A local user who is not authorized to access the database may run HPOM command-line tools with public execute permissions or from another system to access the database.
<b>Impact</b>	The local user could see and modify data in the database through HPOM command-line tools.
<b>Relevance</b>	Medium
<b>Risk Level</b>	Medium
<b>Solution</b>	To change the permission of the HPOM password file, enter the following:  <pre># chmod 0440 /etc/opt/OV/share/conf/OpC/mgmt_sv/.opcdbpwd.sec</pre>

## Running the Oracle Database on HPOM

If the HP Operations management server and the Oracle Database are not running on the same system, communication between the two is more vulnerable to security threats.

The communication protocol is defined and implemented by the database API (using Oracle SQL\*Net).

---

**NOTE**

As part of the Common Criteria EAL-2 evaluation, the Oracle Database was running on the HP Operations management server.

---

If you need to use a remote database for HPOM, you should consider using optional Oracle products (for example, Oracle Advanced Security). For details, refer to the Oracle documentation.

## Restricting Remote Access to the Oracle Database

If the Oracle Database is running on the same system as the HP Operations management server, remote access to the database is not needed for normal operation of the HP Operations management server (other than running database reports through Crystal reports).

<b>Vulnerability</b>	Remote access to the Oracle Database is possible by default.
<b>Impact</b>	An unauthorized person may be able to access the Oracle Database from a remote system, or access the operating system through the Oracle Database.
<b>Relevance</b>	High
<b>Risk Level</b>	High



<b>Solution</b>	<ol style="list-style-type: none"><li>1. Update the Oracle Database to the latest version.</li><li>2. Limit remote access to the Oracle Database by applying a password.</li><li>3. Disable remote access to the Oracle Database entirely, if not needed. To disable remote access, follow these steps:<ol style="list-style-type: none"><li>a. Stop HPOM and Oracle processes. <pre># opcsv -stop</pre> <pre># /sbin/init.d/ovoracle stop</pre></li><li>b. Edit the corresponding <code>tnslister.ora</code> file.</li><li>c. Remove the following lines from the Listener Address Sections: <pre>(ADDRESS =           (PROTOCOL = TCP)           (HOST = &lt;YOUR_HOSTNAME&gt;)           (PORT = 1521)         )</pre></li><li>d. Restart Oracle and HPOM for UNIX processes: <pre># /sbin/init.d/ovoracle start</pre> <pre># opcsv -start</pre></li></ol></li></ol> <p><b>NOTE:</b> If Oracle runs on a cluster system, you need to add the option <code>force</code> when starting and stopping the database.</p>
-----------------	--

## Restricting Access to the Oracle Listener

To prevent unauthorized access to the Oracle listener, you can apply a password to it.

<b>Vulnerability</b>	Unauthorized access to the Oracle listener.
<b>Impact</b>	An unauthorized user may stop the listener.
<b>Relevance</b>	Medium
<b>Risk Level</b>	Medium
<b>Solution</b>	Apply a password to the listener: <pre>\$ lsnrctl next line: # set password</pre> <p><b>NOTE:</b> This password also prevents the HPOM scripts (<code>opc_backup</code>, <code>/sbin/init.d/ovoracle</code>) from stopping the Oracle listener. Afterwards, when the scripts try to start the Oracle listener, they return an error because the listener is already running. These errors can be ignored.</p>

## Restricting Access to Oracle User Passwords

To prevent unauthorized access to Oracle user passwords, you can run `ovprotect` or change permissions for the `/opcdbsetup.log` logfile.

<b>Vulnerability</b>	The logfile <code>/opcdbsetup.log</code> on the HP Operations management server contains the password settings in clear text to access the Oracle database.
<b>Impact</b>	Unauthorized people could learn the Oracle user passwords.
<b>Relevance</b>	High
<b>Risk Level</b>	Medium
<b>Solution</b>	Run <code>ovprotect</code> or manually change the file permission for <code>/opcdbsetup.log</code> so that only root has read/write privileges: <pre># chmod 400 /opcdbsetup.log:</pre>

---

## Securing the Network Node Manager

Network Node Manager (NNM) software can be installed on the same system as an HP Operations agent, but not on the same system as the HP Operations management server.

This section describes a few aspects of NNM security. For further information, refer to the appropriate NNM documentation.

---

### NOTE

NNM is part of the IT environment from the HP Operations Common Criteria evaluation perspective.

---

## Changing Permissions for the ECS Directory

To prevent non-root users from removing socket files, you can change permissions for the ECS directory.

<b>Vulnerability</b>	The directories <code>/var/opt/OV/sockets/ecs/1</code> and <code>/var/opt/OV/sockets/ecs/1/socket</code> are world writable.
<b>Impact</b>	It is possible for a non-root user to remove socket files in the two ECS directories. The files are important for ECS inter-process communication.
<b>Relevance</b>	Medium
<b>Risk Level</b>	Medium
<b>Solution</b>	Change the permission of the directories to 0770: <pre># chmod 0770 /var/opt/OV/sockets/ecs/1 # chmod 0770 /var/opt/OV/sockets/ecs/1/socket</pre>

## Changing Permissions for the SNMP Trap Interceptor and Daemon

To prevent non-root users from removing or changing the NNM event specification and configuration, you can change permissions for the `trapd.conf` and `trapd.socket` files.

<b>Vulnerability</b>	The <code>/etc/opt/OV/share/conf/*/trapd.conf</code> file is world writable.
<b>Impact</b>	It is possible for a non-root user to remove or change the <code>trapd.conf</code> file. Removing or changing the file would remove or change the configuration of the SNMP trap daemon.
<b>Relevance</b>	Medium
<b>Risk Level</b>	Medium
<b>Solution</b>	<p>Change the permission of the <code>trapd.conf</code> file to 0664:</p> <ul style="list-style-type: none"><li>• <i>HP-UX</i><pre># chmod 664 \ /etc/opt/OV/share/conf/*/trapd.conf  # addgroup ovnmm  # chgrp ovnmm \ /etc/opt/OV/share/conf/*/trapd.conf</pre></li><li>• <i>Solaris</i><pre># chmod 664 \ /etc/opt/OV/share/conf/*/trapd.conf  # groupadd ovnmm  # chgrp ovnmm \ /etc/opt/OV/share/conf/*/trapd.conf</pre></li></ul> <p><b>IMPORTANT:</b> Other consumers (for example, your network administrator, HP integrations such as Network SPIs) need to be members of the group “<code>ovnmm</code>”.</p>

To prevent non-root users from removing or changing the SNMP trap daemon, you can change permissions for the `trapd.socket` file.

<b>Vulnerability</b>	The socket file <code>/var/opt/OV/sockets/trapd.socket</code> is world writable.
<b>Impact</b>	It is possible for a non-privileged user to write into this socket, and cause non-predictable behavior of the SNMP trap daemon.
<b>Relevance</b>	Medium
<b>Risk Level</b>	Medium
<b>Solution</b>	Change the permission of the <code>trapd.socket</code> file to 0660:  <pre># chmod 0660 \ /var/opt/OV/sockets/trapd.socket</pre>

### Changing Permissions for the `OVsPMD_MGMT` Socket

To prevent non-privileged users from causing non-predictable behavior in NNM and HPOM, you can change permissions for the `OVsPMD_MGMT` file.

<b>Vulnerability</b>	The socket file <code>/var/opt/OV/sockets/OVsPMD_MGMT</code> is world writable.
<b>Impact</b>	It is possible for a non-privileged user to write into this socket, and cause non-predictable behavior in NNM and HPOM.
<b>Relevance</b>	Medium
<b>Risk Level</b>	Medium
<b>Solution</b>	Change the permission of the <code>OVsPMD_MGMT</code> file to 0600:  <pre># chmod 0600 \ /var/opt/OV/sockets/OVsPMD_MGMT</pre>

## Securing SNMP and NNM

This section describes SNMP community string and NNM shared memory usage.

### Changing the SNMP Community String

Typically, when NNM is installed on a clean Solaris machine, the native Solaris `snmpdx` agent runs on port 161. NNM installs the `emanate` agent onto port 161, and moves the native `snmpx` agent to port 50161.

NNM sets up the `emanate snmpd.conf` file (`/etc/SnmpAgent.d/snmpd.conf`) with the community get string of `public`, regardless of what is in the native Solaris `snmpdx conf` file (`/etc/snmp/conf/snmpd.conf`). This setup does not allow change access, but does allow read access.

---

#### TIP

Change the community string to a non-default string, which may already be set in `/etc/snmp/conf/snmpd.conf`. Also, verify on *all* other systems that the SNMP community string is no longer set to its default value.

---

Because the community string is in clear text in the `snmpd.conf` file, you should make sure that the file is readable by the `root` user only. If the community string is changed in `snmpd.conf`, it must also be changed with `ovconfchg` for HTTPS agents. For details, see the `SNMP_COMMUNITY` variable.

---

#### CAUTION

The `SNMP_COMMUNITY` variable is stored in clear text. As a result, any user on that system could obtain its value via `ovconfget`.

---

### Verifying Access to NNM Shared Memory

For its internal communication, NNM uses shared memory.

Access privileges should be verified with the `ipcs` tool.

---

## Securing the HP Web Server

HPOM leverages a web server, which listens on port 3443, for the following tasks:

- Installing the Java operator GUI remotely
- Providing the online help for the Java operator GUI
- Starting Jovw (the Java version of ovw)

Alternately, you can omit the following from the web server:

- **Java Operator GUI**

Install manually. For example, you can use SSH (scp).

- **Java Operator GUI Online Help**

Find the same information in the corresponding PDF document:

```
/opt/OV/www/htdocs/ito_doc/C/manuals/JavaOperatorGuide.pdf
```

There are a number of different ways to disable and enable the HP web server.

### To disable the HP web server:

Do one of the following:

- **Perform Manual Steps**

Perform the following manual steps:

```
# ovc -stop ovtomcatB  
# ovcreg -del ovtomcatB
```

- **Run ovprotect**

To automatically disable the HP web server, you can run the `ovprotect` utility. For details, see “Assessing Your System Vulnerability with `ovprotect`” on page 85.

For more information about `ovprotect`, see *OvProtect User Manual* located on the HPOM management server at the following location:

```
/opt/OV/contrib/OpC/OvProtect
```

- **Block Firewall Port**

Block port 3443 with your firewall.

**To re-enable the HP web server:**

Enter the following:

```
# ovcreg -add  
/opt/OV/newconfig/DataDir/conf/dma/ovtomcatB.xml  
# ovc -start ovtomcatB
```

Make sure that port 3443 is *not* blocked by your firewall.



## Securing the HPOM Agent

You can secure the HP Operations agent by doing the following:

- “Installing the HPOM Agent” on page 57
- “Switching to the HPOM HTTPS Agent” on page 58
- “Running Non-Root HPOM HTTPS Agents on UNIX Platforms” on page 59

## Installing the HPOM Agent

The core functionality of HPOM depends to a significant degree on reliable and trustworthy communication between the HP Operations management server and the HP Operations agent. This communication requires high attention.

The communication between the HP Operations management server and the HP Operations agent can be categorized as follows:

- Software installation
- Standard operations (for example, sending HPOM messages, deploying configuration, and launching remote actions)
- Software de-installation

HPOM provides an `inst.sh` script for installing the HP Operations agent. For details on HP Operations agent installation, see the *HPOM Administrator's Reference*.

### To install the HPOM agent:

1. Transfer the HPOM agent software to the target node.
2. Install and configure the HPOM agent software, and start its processes.

---

### CAUTION

It is *strongly recommended* that you use only a secure IT infrastructure for installing the HPOM agent software. The installation process is *vulnerable* in insecure IT environments. It should *not* be used there.

3. *HTTPS agent only:*

- Generate a certificate for the node.
- Transfer the certificate to the node.

Each step can be performed manually using secure mechanisms (for example, using a CD to install the HPOM agent software or to transfer the certificate using a removable medium, such as a floppy disk, CD, or USB stick). For details, refer to the *HTTPS Agent Concepts and Configuration Guide*.

---

**NOTE**

If you use the installation debug functionality (see the *inst\_debug(5)* man page), be aware that the passwords of the systems on which the software is installed appear in the debug file. Make sure that the debug output file is in a directory to which non-root users have no write access, and that it is read/write for root only.

For example, for the logfile location in *inst\_debug.conf*, use this:

```
OPC_DEBUG_FILE=/var/opt/OV/tmp/OpC/inst.sh.log
```

Change the permissions:

```
# chmod 600 /var/opt/OV/tmp/OpC/inst.sh.log
```

If you do not need it anymore, empty the file after the agent installation:

```
# > /var/opt/OV/tmp/OpC/inst.sh.log
```

```
# chmod 600 /var/opt/OV/tmp/OpC/inst.sh.log
```

---

## Switching to the HPOM HTTPS Agent

As a general rule, communication between the HPOM management server and the HTTPS agent uses an HTTPS-based protocol. This protocol ensures authentication, authorization, and encryption of the communication. An HTTP-based protocol is used only for Heartbeat Polling, where few or none of these features are required.

OpenSSL is used for implementing the HTTPS protocol.

The HTTPS agent software upgrade (for example, patch installation) and de-installation uses the same security mechanisms as the standard operation (HTTPS and OpenSSL).

Although the HTTPS agent uses HTTPS as its means of communication, there are a few exceptions:

- At installation time, when no certificates are yet available, the certificate request is sent via HTTP.
- The HPOM heartbeat polling is based on HTTP and ICMP (normal ping). The ICMP part can be switched off. Typically, firewalls block ICMP packages. When “RPC only” is chosen for a managed node, only HTTP requests are sent to perform heartbeat polling. The usage of HTTP instead of HTTPS is not a security problem in this case.

## Single-Port Communication

In addition to the HTTPS communication, HPOM provides a “single port” communication model.

By default, all HPOM-generated network traffic is sent to port 383 of the target node. Because there is no single-port model implemented for the source node, every communication partner (for example, the HPOM management server as well as the HPOM HTTPS agents) opens its own source port. Typically, this is not seen as a security risk.

---

### NOTE

If you want, you can restrict the source port range in a granular manner.

For details, refer to the *Firewall Concepts and Configuration Guide*, which is available for download on the following web site:

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

---

The “outbound only” functionality opens all communication from the HPOM management server and/or the HPOM HTTPS agent from the more secure side only. This will allow you to completely close firewalls from the less secure side for HP BTO Software-related network traffic. For that purpose, a new concept — called “Reverse Channel Proxy” — will be introduced.

## Running Non-Root HPOM HTTPS Agents on UNIX Platforms

Whenever possible, run the HPOM agent under a non-administrative account (that is, as “non-root”). This non-administrative account limits the privileges of the HPOM agent, and increases system security.

The `ovswitchuser` command enables you to run HPOM processes under a non-administrative account.

---

**NOTE**

The HPOM agent on the HPOM management server must be an HTTPS agent.

---

The `ovswitchuser` command has the following limitations:

- **HPOM Agent**

The HPOM agent must be always running as root on the HPOM for UNIX management server.

- **SPIs**

Some SMART Plug-ins (SPIs) require you to run the HPOM agent as the user `root`. Verify that the SPIs you use do, in fact, require root privileges. If the SPIs do require root privileges, do *not* distribute them to such nodes.

- **Applications**

Some applications in the HPOM for UNIX application bank require root privileges. Do not assign these applications to users who are responsible only for managed nodes, which run “non-root” HPOM HTTPS agents. At the very least, do not execute the applications on these nodes.

- **Microsoft Windows**

The non-root agent feature is currently not supported on Microsoft Windows nodes. By default, the HPOM HTTPS Windows agents run on Microsoft Windows using the system account. The system user is an administrator user, but has limited network access (compared to a full administrator).

---

**CAUTION**

The network access rights may differ, based on the Microsoft Windows release.

---

## Securing the IT Infrastructure

The security risks in your IT infrastructure are primarily related to communication between the HPOM management server and the following:

- Oracle Database (if not installed locally)
- HTTPS agents
- Java GUI

In general, there are three major security risks for HPOM communication:

- Analysis of the communication protocol
- Modification of the communication protocol
- Partial or complete interruption of communication

Other IT security risks are beyond the scope of this document.



---

  

---

# 5

# Configuring HPOM in a Secure Way

HPOM offers a wide variety of powerful features. Decide which features to use, based on your company security policies. Decide which features to assign to different HPOM users, based on their skills and responsibilities.



## Assigning Rights to Users

HPOM users can have different capabilities and privileges, based on their skill sets, trust relationships, and responsibilities. To limit your security risk, assign these rights carefully.

When assigning rights to HPOM users, keep the following assumptions and guidelines in mind:

- **Guidelines**

Make sure that the HPOM administrator and operators are not hostile, are trained appropriately, and follow all administrative guidance, including guidelines for setting passwords. Of course, the HPOM administrator and operators are capable of making errors.

- **Passwords**

Make sure that the HPOM administrator regularly remind other HPOM users *not* to share their individual passwords or company-specific security guidelines.

- **Log-on Messages**

Make sure that the HPOM GUI log-on message (see *opcuistartupmsg(1m)*) contains appropriate security guidelines.

- **Root System Administrator**

Make sure that the HPOM administrator is a root system administrator on the operating system underlying the HP Operations management server. Normally the HP Operations management server is a dedicated management system used to manage your IT environment controlled by HP Software.

- **Super User**

Make sure that the operating system super user on each HP Operations agent system is a trusted user who has the necessary administrative knowledge of local super users of HP Operations agent systems.

The users `root` and `opc_adm` can be used as synonyms. The `root` user can do everything that the `opc_adm` user can do. The `opc_adm` user can easily become `root` by using the local `mgmtsv` agent for that purpose.

## Assigning Applications

The applications assigned to operators influence, to a high degree, the “power” of these users. Therefore, plan carefully, and assign only those applications that are actually required by operators.

### Assigning Applications to Generic Users

---

**TIP**

---

Provide a dedicated HPOM user logon for each employee.

If generic HPOM users (for example, `shift1_operator`, `weekend_op`) are required, make sure that a unique mapping table to the real users is available for your organization.

### Assigning Applications to User Profiles

In the application bank, you can define applications to be executed, by default, with super user or administrator privileges on the target system. This definition allows a normal HPOM operator to execute selected applications on assigned nodes with super user permissions.

---

**CAUTION**

---

Do *not* assign highly privileged applications to user profiles. Assign these applications directly to operators.

It is possible for highly privileged applications to be assigned implicitly to an operator through a user profile, even when this assignment is not intended. As a result, a non-privileged HPOM operator may get more rights than necessary.

---

**NOTE**

---

Applications requiring root/administrator privileges cannot be executed on HPOM agents running as “non-root.”

### Assigning Broadcast and Virtual Terminal Applications

Make sure to assign operators to “Broadcast” and “Virtual Terminal” applications with super user rights (root, administrator) very carefully. Super user rights provide full power over the assigned managed nodes.

### **Assigning URL Applications**

Make sure not to use \$OPC\_USER and \$OPC\_PASSWD variables for URL application launch commands unless the commands are used (started) in a secure (intranet) environment. Variables are resolved on the GUI client and passed as URLs to the web browser.

### **Restricting Operator Access to Node and Message Groups**

Carefully decide which node groups and message groups need to be assigned to operators. These assignments determine which HPOM messages operators can see and work on.

### **Restricting Operator Access to Services**

Carefully decide which services need to be assigned to operators. These assignments determine which HPOM messages operators see and can work on.

## Changing Default Operator Passwords

You can change default user passwords to prevent unauthorized persons from hijacking HPOM with default user passwords.

<b>Vulnerability</b>	<p>The HP Operations management server installation automatically creates several HPOM users (<code>opc_adm</code>, <code>opc_op</code>, <code>netop</code>, and <code>itop</code>) with default passwords.</p> <p>The passwords must be changed by each of these users at the first logon. Some default HPOM users (operators), such as <code>netop</code> and <code>itop</code>, may not be used for quite some time. As a result, their default passwords may not get changed soon enough.</p> <p>The vulnerability exists between installation and the first logon for each of these users.</p>
<b>Impact</b>	<p>An unauthorized person with knowledge of the default passwords could log on and modify the default passwords to unknown passwords.</p> <p>The unauthorized person could access all default functionality of the contaminated HPOM users.</p>
<b>Relevance</b>	High
<b>Risk Level</b>	High

<b>Solution</b>	<p>Change the default passwords of all default HPOM users to private passwords immediately after the HP Operations management server installation.</p> <p>You can change the default passwords in two ways:</p> <ul style="list-style-type: none"><li>• <b>Individually by User</b> Log on to the Java GUI as each of the default HPOM users, and change their passwords manually.</li><li>• <b>Using <code>opccfguser</code></b> As an HPOM administrator, you can change the passwords of HPOM users using the following command: <pre>#opccfguser -modify &lt;user_name&gt; -password &lt;password&gt;</pre></li></ul> <p>As a second step, you might consider using a PAM integration to get centralized user administration with special features (for example, password length and format checking, as well as password aging).</p> <p>Once you switch on the PAM integration, you can no longer change passwords through HPOM, but must change passwords directly in the currently used authentication system (for example, <code>/etc/passwd</code>, OpenLDAP, ADS, Kerberos).</p>
-----------------	--

### **PAM - Pluggable Authentication Module**

You can get details about the PAM configuration in the *HPOM Administrator's Reference*.

---

**NOTE**

HPOM has been evaluated using the PAM integration for local `/etc/passwd` (`pam_unix`), as well as for OpenLDAP (`pam_ldap`) running on a remote Linux system. Other PAM integrations (for example, ADS) are possible as well.

Only the HPOM – PAM client interface was part of the Common Criteria evaluation. All other PAM components belong to the IT environment.

---

## Auditing Users

You can configure HPOM to audit the activities of the HPOM administrator and HPOM operators.

### Auditing Administrator Activities

You can configure HPOM to audit administrator activities.

<b>Vulnerability</b>	The default audit level is “Operator.”
<b>Impact</b>	Configuration activities of HPOM administrators are not audited.
<b>Relevance</b>	High
<b>Risk Level</b>	Medium
<b>Solution</b>	<p>After the installation, do one of the following:</p> <ul style="list-style-type: none"> <li>• If strict auditing of administrator activities is required, run <code>opc_audit_secure</code>.</li> </ul> <p><b>CAUTION:</b> If you use <code>opc_audit_secure</code>, there is no way to reset the audit level. Also, <code>opc_audit_secure</code> changes the audit and history download directories. After this change, it is impossible to change the directory locations in HPOM for UNIX. For details, see the <code>opc_audit_secure(1m)</code> man page.</p> <ul style="list-style-type: none"> <li>• If strict auditing of administrator activities is <i>not</i> required, change the audit level to <b>Administrator</b>. After this change, the administrator can easily change the audit level.</li> </ul>

## Protecting Audit and History Download Files

You can change download directories to prevent unauthorized persons from getting HPOM information.

<b>Vulnerability</b>	Audit and history download files may be readable by unauthorized persons.
<b>Impact</b>	An unauthorized person could get HPOM information.
<b>Relevance</b>	Medium
<b>Risk Level</b>	Medium
<b>Solution</b>	<p>Change the download directories in the HPOM Admin UI to a dedicated path. Protect this path by setting strict access permissions.</p> <p><b>CAUTION:</b> Once you lock directory path definitions, there is no way to change them. Also, <code>opc_audit_secure</code> changes the auditing level to “Administrator.” For details, see the <code>opc_audit_secure(1m)</code> man page.</p>



## Locking Administrator Audit Levels

You can lock the audit level to ensure that the activities of HPOM administrators and HPOM template administrators are audited.

<b>Vulnerability</b>	The HPOM administrator can change the audit level.
<b>Impact</b>	If the audit level is not “Administrator,” the activities of HPOM administrators and HPOM template administrators are not audited.
<b>Relevance</b>	High
<b>Risk Level</b>	Medium
<b>Solution</b>	You can lock the audit level to the “Administrator” level by calling the command <code>opc_audit_secure</code> . <b>CAUTION:</b> The utility <code>opc_audit_secure</code> changes the audit and history download directories. After this change, it is impossible to change the directory locations in HPOM. For details, see the <code>opc_audit_secure(1m)</code> man page.

## Protecting Machine and Account Names

You must set up individual HPOM users because the audit event “Logon” does not yet indicate machine or local system account names.

<b>Vulnerability</b>	The audit event “Logon” does not include the machine name or the local system account name.
<b>Impact</b>	HPOM tracks the activities of HPOM users on the user name level only. It does not indicate from which system or account the user comes.
<b>Relevance</b>	High
<b>Risk Level</b>	Medium
<b>Solution</b>	HPOM users may not share their HPOM accounts. You must set up individual HPOM users for each person. If you are running shift operations, or if you have special rotating HPOM user duties, make sure each HPOM user has a unique HPOM account. This is especially important if multiple HPOM users run Java GUI sessions with the same logon.

---

## Securing Remote Actions

As part of the policy configuration, you can configure the system so that automatic actions, operator-initiated actions, or both are executed remotely. These actions are then executed on a different system from that on which the HPOM message has been intercepted. Carefully assign such policies to the HPOM HTTPS agents. The HP Operations management server provides a powerful configuration file to enable and disable such remote actions, depending on node names, node groups, agent types, and so on.

---

### NOTE

It is a vital security requirement that the private keys and certificates of the HPOM certificate authority and management server are protected as well as possible.

For details, refer to the *HPOM HTTPS Agent Concepts and Configuration Guide*, which is available for download on the following web site:

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

---

<b>Vulnerability</b>	A malicious user could attack other systems through manipulated remote actions defined as parts of HPOM policies.
<b>Impact</b>	Action definitions and the target system could be manipulated.
<b>Relevance</b>	High
<b>Risk Level</b>	Medium

<b>Solution</b>	<p>Use HPOM enhancements:</p> <ul style="list-style-type: none"><li>• Action-definitions in policies are specially signed with the private key of the management server that deployed the policy to an HTTPS agent. Be aware that the signature refers only to the fix part of an action string, but not to the variable parts. (For example, <code>&lt;MSG_TEXT&gt;</code> would be a variable part if used in an action string, but “abcd” would be a fix.) If you want to prevent the use of executable parts (for example, backticks) in the variable part of the action, you can prefix the action with “_NO_SHELL: ” (the blank after the colon is necessary). That way, no shell is used, and backticks are not evaluated.</li><li>• Remote action configuration file (<code>remactconf.xml</code>).</li></ul> <p>In HPOM, the following is true by default:</p> <ul style="list-style-type: none"><li>• Allows all remote actions from HTTPS nodes (certified nodes).</li><li>• Always provides action string signature verification for remote actions for HTTPS agents.</li></ul> <p>Example 5-1 shows the HPOM remote action configuration file:</p> <pre>/etc/opt/OV/share/conf/OpC/mgmt_sv/ remactconf.xml</pre> <p><b>NOTE:</b> You can switch off agent access capabilities remotely. As part of the Common Criteria evaluation, the default behavior for access control is fully supported by HPOM. However, if needed (for example, in an outsourcing environment), you can restrict remote access.</p> <p><b>CAUTION:</b> Avoid variables in action strings. If you cannot avoid variables in action strings, use the “_NO_SHELL: ” prefix before action strings.</p>
-----------------	---

## Example 5-1

## Remote Action Configuration File

```
<config xmlns="http://openview.hp.com/xmlns/Act/Config/2002/08">
<!--
*****
The following rule is active and allows all remote actions, if originating
from a HTTPS node.
*****
-->
<rule>
  <doc>Allow ALL certified actions</doc>
  <allow />
</rule>
<!--
*****
Here are some examples showing how to configure the various filter elements
*****
-->
<rule>
  <doc>Actions from Group2 to Group1 allowed for HTTPS nodes</doc>
  <if>
    <source> <nodegroup>Group2</nodegroup> </source>
    <target> <nodegroup>Group1</nodegroup> </target>
  </if>
  <allow/>
</rule>
<rule>
  <doc>Execution on MgmtSrv OK, if sender in Group 3 and certified.
    The certified tag is actually NOT needed, since it's default.</doc>
  <if>
    <target> <mgmtsrv/> </target>
    <source> <nodegroup>Group3</nodegroup> </source>
    <certified>true</certified>
  </if>
  <allow/>
</rule>
<rule>
  <doc>Actions from Group4 are okay - even if not certified</doc>
  <if>
    <source> <nodegroup>Group4</nodegroup> </source>
    <certified>false</certified>
  </if>
  <allow/>
</rule>
```

## Securing the Certificate Server

<b>Vulnerability</b>	<p>The private keys of the HP Operations management server and its corresponding certificate authority (CA) are the heart of the public key infrastructure.</p> <p>The key store is located in the following directory: <code>/var/opt/OV/shared/server/datafiles/sec</code></p> <p>These keys could be lost or compromised.</p>
<b>Impact</b>	<p>Lost private keys, or even compromised CA or server private keys, can lead to enormous damage. The worst case is a stolen private key for the CA. With such a key, any type of certificate in your HPOM environment could be faked.</p>
<b>Relevance</b>	High
<b>Risk Level</b>	High
<b>Solution</b>	<p>Make sure that no unauthorized persons with root privileges have access to the management server.</p> <p>Make sure that no unauthorized persons have access to backup tapes from the management server.</p> <p>Make sure that the key store mentioned above can be restored easily in case of corruption or deletion. (Also, see the <code>/opt/OV/bin/OpC/opcsvcertbackup</code> utility, which can be used to generate a backup copy of the critical pieces.)</p>

## Securing Local Actions

By default, all actions executed on the node where the HPOM message has been generated are not signature-checked on the HP Operations management server.

You can enable this check by setting the variable  
`OPC_DO_ACTION_SIGNATURE_CHECK_FOR_ALL_NODES`:

- **Advantage**  
Enabling this check provides a higher security level (for example, against debugger attacks on managed nodes).
- **Disadvantage**  
Added/changed action strings by MSI-processed HPOM messages would always be cut off because signing is not possible for MSI applications.

### To switch on the signature validation for local actions:

On the HP Operations management server, execute the following:

```
# ovconfchg -ovrg server -ns opc -set \  
OPC_DO_ACTION_SIGNATURE_CHECK_FOR_ALL_NODES TRUE
```

## **Configuring the Managed Nodes as “Monitored Only”**

If you do *not* want to allow operators to perform any kind of action on the managed node, configure the managed node as “monitored only” instead of “controlled.”



## Avoiding Unattended Configuration Deployment

To avoid unattended configuration deployment, you can deny configuration deployment or digitally sign the configuration.

### Denial of Configuration Deployment

To deny configuration deployment, you can do one of the following:

- **HTTPS Agent**

To disallow policy and instrumentation deployment, use the following settings on the HTTPS agent:

```
# ovconfchg -ns sec.core.auth.mapping.manager \  
-set conf 496 -set depl 2044  
  
# ovconfchg -ns sec.core.auth.mapping.secondary \  
-set conf 496 -set depl 2044
```

Then restart the HTTPS agent:

```
# ovc -kill  
# ovc -start
```

- **Management Server**

You can implement these settings automatically at agent installation time by inserting them into the following file on the management server:

```
/etc/opt/OV/share/conf/OpC/mgmt_sv/bbc_inst_defaults
```

---

#### TIP

If you add the settings to the `bbc_inst_defaults` file, you do not need to change settings on individual HTTPS agents. You can limit these settings to subnets, individual nodes, and so on within the `bbc_inst_defaults` file.

---

An error message is generated when a configuration distribution request is triggered accidentally (or without authorization) on the management server.

## **Digitally Signed Configuration**

With a digitally signed configuration, policies (templates) deployed to managed nodes are no longer encrypted, but are signed by the HP Operations management server:

- Policies can be easily read in a text editor (but only by the local super user “root” or “administrator”).
- Agent verifies policy signature, and detects whether a policy was tampered with or signed by an untrusted management server.
- Manual policy installation (pre-stage/ignite setup) is supported.

---

# **6** **Protecting HPOM Services**

HPOM requires several services and daemons to be operational.

Nevertheless, many of the default services provided with the operating system are not required, and can be switched off if no other application is using them.

It is recommended that you disable all unused services and daemons to minimize the vulnerability risks.

## Assessing Your System Vulnerability with ovprotect

HPOM provides an `ovprotect` utility that helps you to determine and minimize the vulnerability risks of your systems from the HPOM perspective. It tests and disables unused services on the HP Operations management server or on the HP Operations 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 Operations products, are expected to be released on a regular basis.

You can always download the latest version of the `ovprotect` tool from the HPOM web site:

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

For details and usage options, refer to the `ovprotect(1m)` man page. For more information about `ovprotect`, see *OvProtect User Manual* located on the HPOM management server at the following location:

`/opt/OV/contrib/OpC/OvProtect`

---

**NOTE**

The tool `ovprotect` is a self-extracting archive. You can run it without installing HPOM.

You can apply `ovprotect` on the HP Operations management server and on the following HTTPS agent platforms:

- HP-UX PA-RISC
- HP-UX Itanium
- RS/6000 AIX
- Solaris SPARC
- X86 Linux
- X86 MS Windows

---

<b>Vulnerability</b>	Unnecessary system services that are running on the HP Operations management server and HTTPS agent systems could be attacked remotely.
<b>Impact</b>	Several of the standard system services have at least one security risk because they expose ports to the public Internet. Attacking these services could result in performance degradation and limitation of available system resources (for example, memory, disk space, file handles, and so on). It could also result in someone with administrative privileges breaking into the system.
<b>Relevance</b>	High
<b>Risk Level</b>	High

<b>Solution</b>	<p>Disable unused services, or protect them with a firewall.</p> <p>HPOM provides the tool <code>ovprotect</code>, which detects services that are unnecessary to HPOM.</p> <p>It is strongly recommended that you use <code>ovprotect</code> and other commercial vulnerability scanning tools on a regular basis.</p> <p><b>CAUTION:</b> Running vulnerability scanning tools in your company might require a corresponding formal approval.</p>
-----------------	--

---

## Services on HPOM

This section lists services that may run on an HP Operations management server system. Many of these services can be disabled to increase system security.

This list can be also applied for the HTTPS agents running on UNIX platforms (for example, HP-UX, Solaris, AIX, and Linux). The service names, port numbers, and so on may differ somewhat.

---

### NOTE

The table provides only an overview. It cannot list all possible services. Check each system to verify whether unnecessary services are running.

---

## Services Not Required by HPOM

Table 6-1 lists the services and ports that are not provided and are *not* required by the HP Operations management server and HTTPS agent.

---

### TIP

To better understand this table, see “Key to Service Table Values” on page 18.

---

**Table 6-1** Services and Ports Not Required by HPOM

Port	Service		Required	Comment
	HP-UX	Sun Solaris		
7	echo	echo	No	Echo
9	discard	discard	No	Discard
13	daytime	daytime	No	Daytime (RFC 867)
19	chargen	chargen	No	Character Generator



**Table 6-1 Services and Ports Not Required by HPOM (Continued)**

Port	Service		Required	Comment
	HP-UX	Sun Solaris		
21	ftp	ftp	No	FTP: If an FTP server is not required on the system, close the server. It is recommended that you to use sftp or scp, and disable ftp. HPOM can use telnet/ftp, remsh/rcp, or ssh/scp for HPOM agent software deployment.
23	telnet	telnet	No	Telnet: It is strongly recommended that you disable telnet, and use ssh (22) instead. HPOM can use telnet/ftp, remsh/rcp, or ssh/scp for HPOM agent software deployment.
25	smtp	smtp	No	Simple Mail Transfer Protocol: If the system does not act as a mail server, disable SMTP. Otherwise, configure SMTP carefully.
37	time	time	No	Time Server: Not required on the system to run HPOM.
42	nameserver	nameserver	No	Host Name Server: Not required to have a name server running on the HPOM management server system. Nevertheless, many customers have a name server or caching name server on the HPOM management server. In fact, if name resolution is bad, it is recommended that you have a caching name server on the HPOM management server.
113	auth/ident	auth	No	Authentication Service: Not required to run HPOM. It should be disabled.
123	ntp	ntp	No	Network Time Protocol: Not required to run HPOM.
512	exec	biff	No	Remote Process Execution

**Table 6-1 Services and Ports Not Required by HPOM (Continued)**

Port	Service		Required	Comment
	HP-UX	Sun Solaris		
514	shell(tcp) / syslog(udp)	syslog	No	Remote Command / Remote System Logging: Not required to run HPOM.  <b>CAUTION:</b> The service shell(tcp) is used by remsh, and is as dangerous as rlogin. It is strongly recommended that you disable shell(tcp).
515	printer	printer	No	Printer: Not required. It is recommended that you disable this service.
517	talk	talk	No	Talk: Not required. It is recommended that you disable this service.
518	ntalk	ntalk	No	New Talk: Not required. It is recommended that you disable this service.
540	uucp	uucp	No	UNIX-to-UNIX Copy: Not required. It is recommended that you disable this service.
543	klogin	klogin	No	Kerberos Rlogin: Not required.
544	kshell	cmd	No	Kerberos Remote Shell: Not required.
587		submission	No	Submission: Not required.
600		pcserver	No	Sun IPC Server: Not required.
901	swat / (smpnameres)	swat / (smpnameres)	No	SWAT Samba Web Administration Tool: Not required to run HPOM.
1508	diagmond		No	Diagnostic System Manager
1712	registrar		No	Resource Monitoring Service

**Table 6-1 Services and Ports Not Required by HPOM (Continued)**

Port	Service		Required	Comment
	HP-UX	Sun Solaris		
2049	nfs		No	Network File System: Not required to run HPOM, but it might be required for the system.  <b>NOTE:</b> NFS is temporarily needed to set up HPOM with a remote database (which is not recommended, from a security perspective). After the setup, NFS is not needed.
3275	samd		No	SAM Daemon: Not required to run HPOM. It can be disabled if remote administration through SAM is not required.
4045		lockd	No	NFS Lock Daemon/Manager: Not required.
5988		wbem-http	No	WBEM-HTTP: Not required.
5989	wbem-https / cimserver		No	WBEM-HTTPS / CIM Server: Not required.
6112	dtspc	dtspc	No	Subprocess Control
7100	font-service	font-service	No	Font Server: Not required.
7815	recserv		No	SharedX Receiver Service: Not required to run HPOM. It should be disabled, if possible.
22273		wnn6	No	Wnn6 Jserver: Not required.
34042		kcms	No	Kodak Color Management System: On systems lower than Solaris 5.6, this system can enable local users to get root access.  For details, see the following:  <a href="http://www.securityfocus.com/bid/2605">http://www.securityfocus.com/bid/2605</a>  Not required to run HPOM. It should be disabled, if possible.

## Services Required by HPOM

Table 6-2 lists the services and ports that are provided or required by the HP Operations management server and HTTPS agent. The service names on other UNIX platforms (for example, AIX, Linux, and Tru64) might be different. For details, refer to your OS vendor documentation.

---

**TIP** To better understand this table, see “Key to Service Table Values” on page 18.

---

**Table 6-2 Services and Ports Required by HPOM**

Port	Services	Required by		Comment
	HP-UX, Linux Sun Solaris	HPOM Server	HPOM Agent	
22	ssh	(Yes)	No*	Secure Shell: It is strongly recommended that you use ssh instead of telnet (23) on all systems. If possible, disable telnet and use ssh. * Although ssh is not required by the agent, we recommend using ssh instead of rlogin or telnet.
161	snmp	(Yes)	(Yes)*	Simple Network Management Protocol Agent * Yes in case the HPOM agent does SNMP trap interception or MIB monitoring.
383	ovbbccb	Yes	Yes	HP BlackBox Communication Broker: This is the HTTPS communication broker. It is required to run HPOM. You may not block it, but you may change the ovbbccb port number with ovconfchg. For details, refer to the <i>HPOM HTTPS Agent Concepts and Configuration Guide</i> .
513	login(tcp)	(Yes)	(Yes)	Remote Logon: It is strongly recommended that you disable this service, and use ssh (22) instead. HPOM uses the log-on service for opening a Virtual Terminal application (through opcrlogin). If you do not use the HPOM Virtual Terminal application, you should disable this service

**Table 6-2 Services and Ports Required by HPOM (Continued)**

Port	Services	Required by		Comment
	HP-UX, Linux Sun Solaris	HPOM Server	HPOM Agent	
1521	oracle / listener	(Yes)	No	Oracle Listener: Required if the database is accessed remotely (for example, by HP Reporter). This is the default port for the listener, but you can configure Oracle to use a different port.
2531	ito-e-gui	Yes	N/A	<p>HP Operations Java Console: Required for the communication of the Java GUI clients to the HPOM management server. If you are using the HTTPS-based Java GUI, the <code>opcuihttps</code> process uses <code>inetd</code> to start the corresponding <code>opcuiwww</code> processes. The port needs to be available only locally on the management server.</p> <p>In <code>/var/adm/inetd.sec</code>, you can restrict it as follows:</p> <pre>ito-e-gui 2351/tcp \ allow 127.0.0.1</pre> <p>You can configure an alternative port as follows:</p> <pre>ovconfchg -ovrg \ server -ns \ opc.opcuihttps -set \ OPCUIWWW_PORT \ &lt;port_value&gt;</pre>

**Table 6-2 Services and Ports Required by HPOM (Continued)**

Port	Services	Required by		Comment
	HP-UX, Linux Sun Solaris	HPOM Server	HPOM Agent	
5053	ovtrcd	(Yes)	(Yes)	<p>HP Operations Trace Server: Required to get trace output. However, HPOM also runs without a running trace server. NNM uses ovtrcd for the NNM extended topology pieces only.</p> <pre># /sbin/init.d/OVTrcSrv \ stop</pre> <p>Edit the <code>/sbin/init.d/OVTrcSrv</code> script to disable startup (for example, put <code>?exit 2?</code> before the <code>?start_service?</code> entry).</p> <p>Port 5053 can be opened for local loopback only by using the command <code>ovtrcdm -disableremotetracing</code>. You can set <code>disable_remote_tracing</code> at install time for agents by adding an according statement to the <code>bbc_inst_defaults</code> agent profile template (on the management server). If set, no XPL remote tracing is possible. On the management server, the <code>ovtrcdm -disableremotetracing</code> should be performed manually.</p>
8081, 8444	ovtomcatB	Yes	No	OV Tomcat(B) Servlet Container
35211	opcuihttps	(Yes)	No	<p>If you like to run the HPOM Java GUI in HTTPS mode, this service is required.</p> <p>To changing the default port, enter the following command on the HPOM management server:</p> <pre># ovconfchg -ovrg \ server -ns \ opc.opcuihttps \ -set SERVER_PORT \ &lt;port_value&gt;</pre>

## Services for HPOM HTTPS Windows Agents

Microsoft Windows does not provide tools that display details about services, making it difficult, in some cases, to find out which service is listening on which port. These services may be required to run the system, and cannot be switched off. The Services are Security Accounts Manager, IPSEC Services, Kerberos Key Distribution Center, Net Logon, Protected Storage, and LM Security Support Provider.

### Services Required by HPOM HTTPS Windows Agents

Table 6-3 lists the services and ports that are required by HPOM HTTPS Windows agents.

**Table 6-3 Services and Ports Required by HPOM HTTPS Windows Agent**

Service	Port	tcp/udp	Required by HPOM	Service Name
ftp	21	tcp	For automatic installation using the GUI only	FTP Publishing
smtp	25	tcp	No	Simple Mail Transport Protocol (SMTP)
domain	53	tcp, udp	No	DNS Client, DNS Server
kerberos	88	tcp	No (Yes)	Microsoft Windows does not provide tools that display details about this service, making it difficult, in some cases, to find out which service is listening on which port. This service may be required to run the system, and cannot be switched off.
ntp	123	udp	No	Unknown (time service)
loc-srv	135	tcp	Windows Service	Unknown
netbios-ns	137	udp	Windows Service	N/A
netbios-ssn	139	tcp	Windows Service	N/A
snmp	161	udp	No	SNMP Service
snmptrap	162	udp	No	SNMP Trap Service

**Table 6-3 Services and Ports Required by HPOM HTTPS Windows Agent**

Service	Port	tcp/udp	Required by HPOM	Service Name
ovbbcbb	383	tcp	Yes	Not a service
ldap	389	tcp	No (Yes)	Microsoft Windows does not provide tools that display details about this service, making it difficult, in some cases, to find out which service is listening on which port. This service may be required to run the system, and cannot be switched off.
microsoft-ds	445	tcp	No	N/A
kpasswd	464	tcp	No (Yes)	Microsoft Windows does not provide tools that display details about this service, making it difficult, in some cases, to find out which service is listening on which port. This service may be required to run the system, and cannot be switched off.
http-rpc-epmap	593	tcp	No	Unknown
ldaps	636	tcp	No (Yes)	Microsoft Windows does not provide tools that display details about this service, making it difficult, in some cases, to find out which service is listening on which port. This service may be required to run the system, and cannot be switched off.
NFS or IIS (DCE)	1025	tcp	No	Unknown
COM+ Internet Service	1027	tcp	No (Yes)	Microsoft Windows does not provide tools that display details about this service, making it difficult, in some cases, to find out which service is listening on which port. This service may be required to run the system, and cannot be switched off.
ansyslmd	1055	tcp, udp	Yes	ANSYS - License Manager



**Table 6-3 Services and Ports Required by HPOM HTTPS Windows Agent**

Service	Port	tcp/udp	Required by HPOM	Service Name
DNS	1074	tcp	No	DNS Server
armi-server	3174	tcp, udp	Yes	ARMI Server
globalcatLDAP	3268	tcp	No (Yes)	Microsoft Windows does not provide tools that display details about this service, making it difficult, in some cases, to find out which service is listening on which port. This service may be required to run the system, and cannot be switched off.
globalcatLDAPssl	3269	tcp	No (Yes)	Microsoft Windows does not provide tools that display details about this service, making it difficult, in some cases, to find out which service is listening on which port. This service may be required to run the system, and cannot be switched off.
ms-term-serv	3389	tcp	No	Terminal Services
XPL Tracing	5053	tcp	No	HP Operations Shared Trace Service
vnc-http	5800	tcp	No	VNC Server
vnc	5900	tcp	No	VNC Server

## Start or Stop Services on Microsoft Windows

On Microsoft Windows, you can start and stop services from the GUI or the command prompt.

### To start or stop a service from the Windows GUI:

1. Select **Control Panel**→**Administrative Tools**→**Services**.
2. Start or stop the appropriate service.

### To start or stop a service from the Windows command prompt:

- List all running services:  
# **net start**
- Start a service:  
# **net start ?VNC Server?**
- Stop a service:  
# **net stop ?VNC Server?**

---

# **A** **Checking HPOM Versions**

HPOM consists of many different components, many of which have different versions and patch levels. As a result, it is sometimes hard to know which version of a particular component is installed.

This section provides tips that help you find the version of a specific component or part.

---

**NOTE**

Most of the commands described in this appendix must be executed from a UNIX shell. The `grep` tool is different from system to system. While the default HP-UX `grep` tool works for the described tasks, it is necessary to use `/usr/xpg4/bin/grep` on Solaris for the extended searches.

---

## Check the HP Operations Management Server

You can check the version of the HP Operations management server, as well as the version, the build date, and the source (patch level) of all installed HP Operations management server binaries and libraries.

You can run the `ovprotect` utility to automatically determine the installed HPOM versions and patch levels.

### To check the HP Operations management server version:

Enter the following:

```
# ovconfget -ovrg server opc | grep OPC_INSTALLED_VERSION
OPC_INSTALLED_VERSION=A.09.00

# ovconfget -ovrg server opc.patches
PHSS_32820=Thu May 19 10:17:05 METDST 2005
PHSS_33196=Thu May 19 10:19:03 METDST 2005
```

---

## **Check the Java Operator GUI Client**

To check the version of the HPOM Java operator GUI client, select **Help**→**About** in the client.

---

## Check Core Agent Components

Core Agent is the internal HP name for a subset of the components belonging to the Common Management Environment (CME).

To check the version of the installed Core Agent components, you can run `ovprotect` or enter the following:

```
# ovdeploy -inv
```

NAME	DESCRIPTION	VERSION
TYPE	OSTYPE	
HPOvBbc	HP OpenView HTTP Communication	
05.10.030	pkg HP-UX	
HPOvConf	HP OpenView Configuration	
01.00.121	pkg HP-UX	
HPOvCtrl	HP OpenView Process Control	
01.50.141	pkg HP-UX	
HPOvDep1	HP OpenView Deployment	
02.10.031	pkg HP-UX	
HPOvEaAgt	HP OpenView E/A Agent	
08.10.160	pkg HP-UX	
HPOvJxpl	HP OpenView Cross Platform Component Java	
02.60.030	pkg HP-UX	
HPOvPCO	HP OpenView Performance Core	
10.00.123	pkg HP-UX	
HPOvPacc	HP OpenView Performance Access	
10.00.123	pkg HP-UX	
HPOvPerlA	HP OpenView Perl 5.6.1 Package	
05.06.011	pkg HP-UX	
HPOvSecCC	HP OpenView Certificate Management Client	
01.00.121	pkg HP-UX	
HPOvSecCo	HP OpenView Security Core	
02.10.030	pkg HP-UX	
HPOvXpl	HP OpenView Cross Platform Component	
02.60.030	pkg HP-UX	

---

## Check OpenSSL

To determine the embedded version of OpenSSL, you can run the following on UNIX platforms:

```
# strings /opt/OV/lib/libOvSecCore.* | grep 'OpenSSL'
```



## Check the EventAction Component of the HTTPS Agent

You can check the version of the HPOM agent from the configuration and from the installer on HP-UX, Solaris, and Linux.

### To check the HP Operations agent version deployable from the HP Operations management server:

Enter the following:

```
# /opt/OV/bin/OpC/agtinstall/opcversion
```

### To check the HP Operations agent version from the configuration:

Enter the following:

```
# ovconfget eaagt | grep OPC_INSTALLED_VERSION
```

```
OPC_INSTALLED_VERSION=08.50.160
```

### To check the HP Operations agent version from the installer on HP-UX:

Enter the following:

```
# swlist -l fileset HPOvEa | grep HPOVEAAGT
```

```
HPOvEa.HPOVEAAGT      8.50.006      HP OpenView E/A Agent
```

```
HPOvEa.HPOVEAAGTCLTS 8.50.009      HP OpenView E/A Consolidated  
Package
```

### To check the HP Operations agent version from the installer on Solaris:

Enter the following:

```
# pkginfo -l HPOvEaAgt | grep VERSION
```

```
VERSION: 8.50.160
```

**Check the EventAction Component of the HTTPS Agent**

**To check the HP Operations agent version from the installer on Linux:**

Enter the following:

```
# rpm -q HPOvEaAgt  
HPOvEaAgt-8.50.160-1
```

**To check the HP Operations agent remotely from the management server:**

Enter the following:

```
# opcragt -agent_version <node>
```

## Check Non-HPOM Components

You can check the versions of non-HPOM components, such as the operating system and Oracle Database.

### To check the OS version on HP-UX and Solaris:

Enter the following:

```
# uname -r  
B.11.31
```

### To check the Oracle version on HP-UX and Solaris:

Enter the following:

```
# su - oracle  
$ sqlplus -v  
SQL*Plus: Release 11.1.0.7 - Production  
$ exit
```

Checking HPOM Versions

**Check Non-HPOM Components**

**A**

- access, verifying NNM shared memory, 54
- account names, protecting, 74
- actions, securing
  - local, 79
  - remote, 75–77
- administrator
  - auditing activities, 71–72,
  - changing passwords, 69
  - HPOM, 65
  - locking audit levels, 73
  - template, 65
- administrator, root system, 65
- agent
  - changing permissions for installation trace file, 35
  - installing HPOM, 57–58
  - mgmtsv, 65
  - running non-root HPOM HTTPS agents on UNIX, 59–60
  - securing HPOM, 57–60
  - services required by HPOM HTTPS Windows, 95
  - switching to HPOM HTTPS, 58
- AIX, applying OvProtect, 86
- AMD, 42
- ansyslmd service, 96
- APIs, securing, 36
- applet, running Java GUI, 23
- application bank, HPOM, 66
- applications, assigning, 66–67
- armi-server service, 97
- assessing system vulnerability, 85–86
- assigning
  - applications, 66–67
  - user rights, 65–70
- audience, document, 13
- audit event, “Logon”, 74
- auditing
  - administrator activities, 71
  - locking administrator levels, 73
  - protecting download files, 72
  - users, 71–74
- authentication
  - providing certificates, 30
- authority, certificate, 78
- avoiding unattended configuration deployment, 81–82

**B**

- bbc\_inst\_defaults file, 81
- Broadcast applications, assigning, 66
- browser, web, 23

**C**

- certificate
  - authority, 78
  - digital, 23
  - server, 78
- certificates
  - full authentication mode, 30
- changing
  - default operator passwords, 68–70
  - Oracle Database passwords
    - default, 45–46
    - OPC\_OP, 46–47
  - permissions
    - agent installation trace file, 35
    - ECS directory, 51
    - OVsPMD\_MGMT socket, 53
    - SNMP trap, 52–53
    - sockets directory, 22
    - SNMP community string, 54
- checking versions
  - Core Agent components, 103
  - EventAction component, 105–106
  - Java GUI, 102
  - management server, 101
  - non-HPOM components, 107
  - OpenSSL, 104
- CME, 103
- COM+ Internet Service, 96
- command, ovswitchuser, 59–60
- Common Criteria, 12
- Common Management Environment, 103
- communication
  - restricting Java GUI, 27
  - single-port, 59
- community string, changing SNMP, 54
- components
  - checking versions
    - Core Agent, 103
    - EventAction, 105–106
    - non-HPOM, 107
  - protecting, 19–36
  - summary, 16

---

# Index

configuration  
  deployment  
    avoiding unattended, 81–82  
    denying, 81  
    digitally signed, 82  
configuring  
  HPOM  
    details, 63–82  
    summary, 17  
  “monitored only” managed nodes, 80  
“controlled” managed nodes, 80  
Core Agent  
  checking component versions, 103

**D**

daemon, SNMP trap, 52–53  
database, securing, 45–50  
default passwords, changing  
  operator, 68–70  
  Oracle Database, 45–46  
Denial of Service  
  protecting opciuiwww, 32  
denying configuration deployment, 81  
deployment, denying configuration, 81  
digital certificate, 23  
digitally signed configuration, 82  
directory, changing ECS permissions, 51  
DNS service, 97  
document  
  audience, 13  
  summary, 12  
documents, reviewing OS security, 41  
domain service, 95  
download files, protecting, 72

**E**

EAL-2, 12  
ECS directory, changing permissions, 51  
encrypted passwords, 46  
environment, IT  
  protecting, 39–61  
  summary, 16  
EventAction  
  checking component version, 105–106  
Evidence Assurance Level 2, 12  
execution, preventing stack  
  HP-UX, 43  
  Solaris, 43–44  
  summary, 41–42

## F

files  
  agent installation trace, 35  
  bbc\_inst\_defaults, 81  
  jar, 23  
  protecting download, 72  
  remactconf.xml, 76  
  securing, 20–35  
  snmpd.conf, 54  
  trapd.conf, 52–53  
  trapd.socket, 52–53  
firewall ports, 56  
ftp service, 95

## G

generic users, assigning applications, 66  
globalcatLDAP service, 97  
globalcatLDAPssl service, 97  
groups, restricting operator access, 67  
GUI  
  Java operator  
    changing passwords, 69  
    checking version, 102  
    securing, 23–34

## H

Heartbeat Polling, 58  
history download files, protecting, 72  
HP OpenView Reporter, 47  
HP OpenView Service Desk, 45  
HP OpenView web server, 55–56  
HP Passport ID, 9  
HPOM  
  administrator, 65  
  application bank, 66  
  configuration, 17  
  passwords, 65  
  services  
    not required, 88  
    required, 92  
HPOM agent  
  installing, 57–58  
  securing, 57–60  
HPOM DCE, switching to HTTPS agent, 58  
HPOM HTTPS  
  running non-root agents on UNIX, 59–60  
  switching from HPOM DCE agent, 58  
  unused services, 85–86  
  Windows agent services, 95

HPOM management server. *See*  
management server

## HP-UX

- applying OvProtect, 86
- checking HPOM agent version, 105–106
- preventing stack execution, 43
- Stack Execution Prevention Support, 42

*HP-UX 11i Security*, 41

http-rpc-epmap service, 96

## HTTPS

- checking EventAction version, 105–106
- message forwarding, 21
- running non-root HPOM agents on UNIX,  
59–60
- switching from HPOM DCE agent, 58

## I

ICMP, 59

ID, Passport, 9

IIS service, 96

installing

- HPOM agent, 57–58

- OS security patches, 41

Intel, 42

interceptor, SNMP trap, 52–53

ipcs tool, 54

IPSEC Services service, 95

## IT

- protecting environment, 39–61

- risk summary, 16

- securing infrastructure, 61

ito-e-gui service, 93

itop user, 68

ITSEC, 12

## J

jar files, 23

Java GUI

- changing opcuhttps port, 30

- changing opcuwww port, 29

- changing passwords, 69

- checking version, 102

- full authentication mode, 30

- securing, 23–34

Jovw, 55

## K

Kerberos Key Distribution Center service, 95

kerberos service, 95

kernel parameters, 43

keys, public and private, 78

kpasswd service, 96

## L

ldap service, 96

ldaps service, 96

Linux

- applying OvProtect, 86

- checking HPOM agent version, 105–106

- Stack Execution Prevention Support, 42

listener, restricting access to Oracle, 50

LM Security Support Provider service, 95

local actions, securing, 79

locking administrator audit levels, 73

loc-srv service, 95

login(tcp) service, 92

“Logon” audit event, 74

log-on messages, 65

## M

machine names, protecting, 74

managed nodes, configuring “monitored  
only”, 80

management server

- checking version, 101

- HTTPS-based message forwarding, 21

- securing, 21

- unused services, 85–86

message forwarding

- HTTPS-based, 21

message groups, restricting operator access,  
67

messages, log-on, 65

mgmtsv agent, 65

Microsoft Windows. *See* Windows; Windows  
Server; Windows XP

microsoft-ds service, 96

“monitored only” managed nodes,  
configuring, 80

ms-term-serv service, 97

## N

National Information Assurance  
Partnership, 12

National Institute of Standards and  
Technology, 12

National Security Agency, 12

Net Logon service, 95

netbios-ns service, 95

netbios-ssn service, 95

netop user, 68

---

# Index

Network Node Manager. *See* NNM  
NFS service, 96  
NIAP, 12  
NIST, 12  
NNM  
    securing, 51–54  
    verifying access to shared memory, 54  
node groups, restricting operator access, 67  
non-HPOM components, checking versions, 107  
Non-Stack Execution, 41–42  
NSA, 12  
ntp service, 95  
NX, 41–42

## O

opc\_admin user  
    assigning rights, 65  
    changing default operator passwords, 68  
opc\_audit\_secure, 71–73  
opc\_op user, 68  
OPC\_OP, changing Oracle Database passwords, 46–47  
\$OPC\_PASSWD variable, 67  
\$OPC\_USER variable, 67  
opcapp\_start() API, 36  
/opcdbsetup.log logfile, 50  
opcuihttps service, 30, 34, 94  
opcuiwww service, 27, 29, 32  
OpenSSL  
    checking version, 104  
    implementing HTTPS protocol, 58  
operating system  
    checking version, 107  
    installing security patches, 41  
    reviewing security documents, 41  
    securing, 41–44  
operator  
    changing default passwords, 68–70  
    changing passwords, 69  
    securing preferences, 23  
Oracle Advanced Security, 47

Oracle Database  
    changing passwords  
        default, 45–46  
        OPC\_OP, 46–47  
    checking version, 107  
    restricting access  
        listener, 50  
        remote, 48  
        user passwords, 50  
    running on HPOM, 47  
    securing, 45–50  
Oracle SQL\*Net, 47  
oracle/listener service, 93  
Orange Book, 12  
ovbbccb service, 92, 96  
OvProtect  
    assessing system vulnerability, 85–86  
    checking versions  
        Core Agent, 103  
        management server, 101  
    disabling HP OpenView web server, 55  
    restricting  
        access to Oracle user passwords, 50  
        Java GUI communication, 28, 29, 30, 31, 33, 34  
        securing sockets, 22  
OVSD, 45  
OVsPMD\_MGMT socket, changing permissions, 53  
ovswitchuser command, 59–60  
ovtrcd service, 94

## P

PAM, 70  
parameters, kernel, 43  
Passport ID, 9  
passwords  
    changing default operator, 68–70  
    encrypted, 46  
    HPOM, 65  
    restricting access to Oracle user, 50  
patches, installing OS security, 41  
permissions, changing  
    ECS directory, 51  
    OVsPMD\_MGMT socket, 53  
    SNMP trap, 52–53  
Pluggable Authentication Module, 70  
ports, firewall, 56  
“power” users, 66  
preferences, operator, 23



- preventing stack execution
    - HP-UX, 43
    - Solaris, 43–44
    - summary, 41–42
  - private keys, 78
  - privileges, restricting Java GUI, 23
  - profiles, assigning applications to user, 66
  - Protected Storage service, 95
  - protecting
    - account names, 74
    - components, 19–36
    - download files, 72
    - IT environment, 39–61
    - machine names, 74
    - services, 83–98
  - public keys, 78
  - R**
  - Red Hat Enterprise Linux, 42
  - remactconf.xml file, 76
  - remote
    - access services, 16
    - action configuration file
      - example, 77
      - solution, 76
    - actions, securing, 75–77
  - Remote Procedure Call, 58
  - required services
    - HPOM, 92
    - HPOM HTTPS Windows agents, 95
  - restricting access
    - operator, 67
    - Oracle
      - listener, 50
      - user passwords, 50
    - Oracle Database, 48
  - restricting Java GUI
    - changing opcuihttps port, 30
    - changing opcuiwww port, 29
    - communication, 27
    - connections to opcuihttps, 34
    - full authentication mode, 30
    - privileges, 23
    - protecting against DoS, 32
  - reviewing OS security documents, 41
  - rights, assigning user, 65–70
  - risk table values, 18
  - risks, security, 16–17
  - root
    - system administrator, 65
    - user
      - assigning rights, 65
      - changing SNMP community string, 54
  - running
    - Java GUI as web applet, 23
    - non-root HPOM HTTPS agents on UNIX, 59–60
    - Oracle Database on HPOM, 47
  - S**
  - SAM, 43
  - securing
    - actions
      - local, 79
      - remote, 75–77
    - APIs, 36
    - certificate server, 78
    - configuration, 63–82
    - files, 20–35
    - HPOM agent, 57–60
    - IT infrastructure, 61
    - Java GUI, 23–34
    - management server, 21
    - NNM, 51–54
    - operating system, 41–44
    - Oracle Database, 45–50
    - SNMP, 54
    - sockets, 22
    - web server, 55–56
  - security
    - operating system, 41
    - risks, 16–17
    - summary, 15–18
  - Security Accounts Manager service, 95
  - server, securing certificate, 78
  - Service Navigator Value Pack, 45
  - service table values, 18
-

---

# Index

- services
    - HPOM
      - not required, 88
      - required, 92
    - HPOM HTTPS Windows agents, 95
    - protecting, 83–98
    - remote access, 16
    - restricting operator access, 67
    - Windows
      - starting, 98
      - stopping, 98
  - signed configuration, 82
  - single-port communication, 59
  - smtp service, 95
  - SNMP
    - changing
      - community string, 54
      - trap permissions, 52–53
    - securing, 54
  - snmp service
    - HPOM, 92
    - HPOM HTTPs Windows agents, 95
  - SNMP\_COMMUNITY variable, 54
  - snmpd.conf file, 54
  - snmptrap service, 95
  - snmpx agent, 54
  - SNVP, 45
  - sockets
    - changing OvsPMD\_MGMT permissions, 53
    - opcuihttps, 3, 34
    - opcuiwww, 27, 29, 32
    - securing, 22
  - Solaris
    - applying OvProtect, 86
    - checking HPOM agent version, 105–106
    - preventing stack execution, 43–44
    - Stack Execution Prevention Support, 42
  - ssh service, 92
  - Stack Execution Prevention, 41–42
  - stack execution, preventing
    - HP-UX, 43
    - Solaris, 43–44
    - summary, 41–42
  - starting and stopping services on Windows, 98
  - Sun Solaris. *See* Solaris
  - Sun SPARC, 42
  - super user
    - assigning rights, 65
    - digitally signed configuration, 82
  - support, 9
  - SuSE, 42
  - switching to HPOM HTTPS agent, 58
  - system
    - vulnerability, 85–86
- ## T
- table values, 18
  - template administrators, 65
  - tool, ipcs, 54
  - trace file, changing permissions, 35
  - trap, changing permissions for SNMP, 52–53
  - trapd.conf file, 52–53
  - trapd.socket file, 52–53
- ## U
- unattended configuration deployment,
    - avoiding, 81–82
  - UNIX Security Checklist*, 41
  - URL applications, assigning, 67
  - users
    - assigning applications
      - generic users, 66
      - user profiles, 66
    - assigning rights, 65–70
    - auditing, 71–74
    - itop, 68
    - netop, 68
    - opc\_admin
      - assigning rights, 65
      - changing default operator passwords, 68
    - opc\_op, 68
    - “power”, 66
    - restricting access to Oracle passwords, 50
    - root
      - assigning rights, 65
      - changing SNMP community string, 54
    - super
      - assigning rights, 65
      - digitally signed configuration, 82
- ## V
- values, table, 18
  - variables
    - \$OPC\_PASSWD, 67
    - \$OPC\_USER, 67
    - SNMP\_COMMUNITY, 54
  - verifying
    - access to NNM shared memory, 54

- versions, checking
  - Core Agent components, 103
  - EventAction component, 105–106
  - Java GUI, 102
  - management server, 101
  - non-HPOM components, 107
  - OpenSSL, 104
- Virtual Terminal applications, assigning, 66
- vnc service, 97
- vnc-http service, 97
- vulnerability, assessing system, 85–86

## **W**

- web
  - running Java GUI applet, 23
  - securing server, 55–56
- Windows
  - applying OvProtect, 86
  - HPOM HTTPS agent services, 95
  - starting services, 98
- Windows Server, 42
- Windows XP, 42

## **X**

- XPL Tracing service, 97

