HP Operations Manager

Security Advisory

Software Version: 9.02

for the UNIX and Linux operating systems

Manufacturing Part Number: None

February 2010

Legal Notices

6. Protecting HPOM Services

A. Checking HPOM Versions

Support

Please visit the HP Operations support web site at:

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

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 (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

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

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)[1]

---

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.

Vulnerability	The directory `/var/opt/OV/sockets` is world writable.
Impact	It is possible for a non-root user to remove socket files in the `/var/opt/OV/sockets` directory. These files are important for inter-process communication.
Relevance	High
Risk Level	High

Solution	Run `ovprotect` or follow these steps:
	
	1. Change the permissions for the `/var/opt/OV/sockets` directory to `0770`:
	
	   # **`chmod 0770 /var/opt/OV/sockets`**
	
	2. Create an entry in `/etc/opt/OV/share/conf/ovperms.conf/files` to permanently change this file permission:
	
	   `/var/opt/OV/sockets file bin bin 0770`
	
	For more information about `ovprotect`, see *OvProtect User Manual* located on the HPOM management server at the following location:
	
	`/opt/OV/contrib/OpC/OvProtect`

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.

Vulnerability	If you run the Java GUI as an application, its digital signature is *not* verified.
Impact	An unauthorized person could tamper with the Java GUI jar file.
Relevance	Medium
Risk Level	Medium
Solution	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.

Vulnerability	Java GUI users can store their preferences in local files, which could be tampered with by other users.
Impact	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).
Relevance	Medium
Risk Level	Medium

Solution	Give user preference files the lowest possible level of privileges.
	To set the SAME preferences for all Java GUI sessions, you can also place the preferences files on the HP Operations management server.
	You move three files to a global location:
	• Itoopbrw
	Stores message browser settings (layout, position, size).
	• Itooprc
	Stores general Java GUI settings. Most of the properties can be configured in the Preferences dialog of the Java GUI.
	• HP_OV_consoleSettings_*mgmtServerName_operator*
	Stores all GUI layouts (for example, browser column layout).
	Example:
	HP_OV_consoleSettings_chita.hermes.si_opc_op
	The following files remain on the user.home directory:
	• OV_JGUI_portRepository
	Used for Java API discovery.
	To set up a global location for preference files, use the following variables:
	OPC_JGUI_GLOBAL_SETTINGS_WIN
	OPC_JGUI_GLOBAL_SETTINGS_UNIX
	Example:
	# **ovconfchg -ovrg server -ns opc -set ** **OPC_JGUI_GLOBAL_SETTINGS_WIN ** **X:\Shared\javaui**

Solution (continued)	**To set up the share:**
	1. Log on as the user who has write permission to this directory.
	2. Set all defaults within the Java GUI as needed.
	3. Save the session and log out.
	4. Rename the `consoleSettings` file with a more global name.
	For example, you could change the `HP_OV_consoleSettings_ligety.bbn.hp.com_opc_op` file to `HP_OV_consoleSettings`.
	To do so, you would input the following:
	`f:\JGUI_share>` **`rename \`** **`HP_OV_consoleSettings_ligety.bbn.hp.com_opc_op \`** **`HP_OV_consoleSettings`**
	5. Make the share read only.

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.

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

Solution	Run the `ovprotect` utility or do one of the following:
	• 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.
	Detailed configuration and usage instructions are available in the *HPOM Java GUI Operator's Guide*, available for download from the following web site:
	http://support.openview.hp.com/selfsolve/manuals
	• Do not allow all systems in the network to access the HP Operations management server, especially the `opcuiwww` port (for example, by protecting it with a firewall, by changing `/var/adm/inetd.sec` on HP-UX, or by changing the corresponding file on other OS platforms).
	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:
	`ito-e-gui allow 127.0.0.1 15.1.2.3`
	For details, refer to the *inetd.sec(4)* man page.
	Monitor the number of started `opcuiwww` processes to ensure that it is consistent with the maximum number of concurrent Java GUI operators you expect.
	For more information about `ovprotect`, see *OvProtect User Manual* located on the HPOM management server at the following location:
	`/opt/OV/contrib/OpC/OvProtect`

Changing the Default Port of opcuiwww

Vulnerability	The default port number (2531) of the opcuiwww process is known and might therefore be a target of attack.
Impact	If opcuiwww is attacked through the default port, the system may stop responding.
Relevance	Medium
Risk Level	Medium
Solution	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.
	It is recommended to change the default port 2531 to another port:
	ovconfchg -ovrg server -ns opc.opcuihttps -set OPCUIWWW_PORT <*new port*>
	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.
	For more information about configuration variables for the management server, see the *HPOM Server Configuration Variables* guide.

Changing the Default Port of opcuihttps

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

Providing Certificates for Full Authentication Mode

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

Solution	If `SSL_CLIENT_VERIFICATION_MODE` is set to `RequireCertificate`, clients require the certificate for (full) authentication. To provide the certificates for the full authentication mode, perform the following steps:
	1. Enable full authentication mode for opcuihttps:
	a. Configure opcuihttps:

	ovconfchg -ovrg server -ns
	      opc.opcuihttps -set
	      SSL_CLIENT_VERIFICATION_MODE
	      RequireCertificate

	b. Restart the opcuihttps process.
	For more information about configuring opcuihttps parameters, see the *HPOM Administrator's Reference*.
	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 *HPOM Java GUI Operator's Guide*.
	3. Set the Java GUI startup parameter `lcore_defaults` to `yes`, 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 HPOM Java GUI Operator's Guide.
	For more information about configuration variables for the management server, see the *HPOM Server Configuration Variables* guide.

Protecting the Java GUI against Denial of Service Attacks

Denial of Service (DoS) functionality provides protection against attacks to the opcuiwww 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

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

Solution	1. Enable basic DoS protection for the opcuiwww process. Set the configuration variable DOS_ENABLED to TRUE:
	`ovconfchg -ovrg server -ns opc -set DOS_ENABLED TRUE`
	2. *Optional.* Configure the following DoS settings according to your security needs:
	a. Set the size of the input buffer on the opcuiwww socket. If the size exceeds the buffer limit, an error is reported to System.txt, and the connection (opcuiwww process) is closed. The default value is 4096. Example:
	`ovconfchg -ovrg server -ns opc -set OPCUIWWW_INPUT_BUFFER_LIMIT 512`
	b. Set the maximum number of simultaneous connections to opcuiwww (Java GUIs). The default value is 100. Example:
	`ovconfchg -ovrg server -ns opc -set OPCUIWWW_MAX_CONNECTION 5`
	c. Set the number of connections to opcuiwww from a single system. The default value is 30. Example:
	`ovconfchg -ovrg server -ns opc -set OPCUIWWW_ONE_CONNECTION 2`
	d. Set the time out for inactivity on the opcuiwww socket. A valid request must arrive at the socket within the specified time (measured from the initial connection), otherwise opcuiwww logs an error and exits. The default value is 5 (seconds). Example:
	`ovconfchg -ovrg server -ns opc -set OPCUIWWW_TIMEOUT 3`
	For more information about configuration variables for the management server, see the *HPOM Server Configuration Variables* guide.

Restricting the Number of Simultaneous Connections to opcuihttps

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

Solution	Limit the maximum number of simultaneous connections to opcuihttps. Clients are usually HTTPS-based Java GUI consoles, but can also be web browsers. The default value is 100. Example:
	
	`ovconfchg -ovrg server -ns opc.opcuihttps`
	`-set MAX_CONNECTIONS 10`
	
	For more information about configuration variables for the management server, see the *HPOM Server Configuration Variables* guide.

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.

Vulnerability	The file /tmp/inst.sh.2 may be world readable when agent installation tracing is set up.
Impact	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 inst_debug.
Relevance	Medium
Risk Level	Medium
Solution	Change the permission of the trace file to 0600: # **chmod 0600 /tmp/inst.sh.2** **NOTE:** The name of the file depends on the configuration of the variable OPC_DEBUG_FILE in the file /var/opt/OV/share/tmp/OpC/mgmt_sv/ inst_debug.conf.

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.

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

Solution	Do one of the following:
	• **Recommended**
	Replace the function call `opcapp_start()` with `opcappl_start()` in all of your applications.
	• **Workaround**
	If the recommended solution is not immediately possible, you can set the variable `OPC_OMIT_PWD_CHECK_FOR_APP_START` in the namespace `opc` and the resource group `server` to `TRUE`:
	1. Stop your application:
	# *\<stop your application\>*
	2. Enter the following:
	# **ovconfchg -ovrg server -ns opc \ OPC_OMIT_PWD_CHECK_FOR_APP_START \ TRUE**
	CAUTION: Setting the `OPC_OMIT_PWD_CHECK_FOR_APP_START` configuration variable partially re-introduces the security problem.
	3. Start your application:
	# *\<start your application\>*

4 Protecting the IT Environment

The HP Operations Manager (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

- *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

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: **********

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.

Vulnerability	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.
Impact	The local user could see and modify data in the database through HPOM command-line tools.
Relevance	Medium
Risk Level	Medium
Solution	To change the permission of the HPOM password file, enter the following: `# chmod 0440 /etc/opt/OV/share/conf/OpC/mgmt_sv/.opcdbpwd.sec`

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).

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

Solution	1. Update the Oracle Database to the latest version.
	2. Limit remote access to the Oracle Database by applying a password.
	3. Disable remote access to the Oracle Database entirely, if not needed.
	To disable remote access, follow these steps:
	a. Stop HPOM and Oracle processes.
	# **opcsv -stop**
	# **/sbin/init.d/ovoracle stop**
	b. Edit the corresponding tnslistener.ora file.
	c. Remove the following lines from the Listener Address Sections:
	(ADDRESS =
	(PROTOCOL = TCP)
	(HOST = *<YOUR_HOSTNAME>*)
	(PORT = 1521)
	)
	d. Restart Oracle and HPOM for UNIX processes:
	# **/sbin/init.d/ovoracle start**
	# **opcsv -start**
	NOTE: If Oracle runs on a cluster system, you need to add the option force when starting and stopping the database.

Restricting Access to the Oracle Listener

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

Vulnerability	Unauthorized access to the Oracle listener.
Impact	An unauthorized user may stop the listener.
Relevance	Medium
Risk Level	Medium
Solution	Apply a password to the listener: $ lsnrctl next line: # **set password** **NOTE:** This password also prevents the HPOM scripts (opc_backup, /sbin/init.d/ovoracle) 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.

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.

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

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.

Vulnerability	The directories `/var/opt/OV/sockets/ecs/1` and `/var/opt/OV/sockets/ecs/1/socket` are world writable.
Impact	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.
Relevance	Medium
Risk Level	Medium
Solution	Change the permission of the directories to `0770`: # **chmod 0770 /var/opt/OV/sockets/ecs/1** # **chmod 0770 /var/opt/OV/sockets/ecs/1/socket**

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.

Vulnerability	The `/etc/opt/OV/share/conf/*/trapd.conf` file is world writable.
Impact	It is possible for a non-root user to remove or change the `trapd.conf` file. Removing or changing the file would remove or change the configuration of the SNMP trap daemon.
Relevance	Medium
Risk Level	Medium

Solution	Change the permission of the `trapd.conf` file to `0664`:
	
	 • *HP-UX*
	
	     # **chmod 664 **
	     /etc/opt/OV/share/conf/*/trapd.conf
	
	     # **addgroup ovnnm**
	
	     # **chgrp ovnnm **
	     /etc/opt/OV/share/conf/*/trapd.conf
	
	 • *Solaris*
	
	     # **chmod 664 **
	     /etc/opt/OV/share/conf/*/trapd.conf
	
	     # **groupadd ovnnm**
	
	     # **chgrp ovnnm **
	     /etc/opt/OV/share/conf/*/trapd.conf
	
	 IMPORTANT: Other consumers (for example, your network administrator, HP integrations such as Network SPIs) need to be members of the group "ovnnm".

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

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

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.

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

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.

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

Solution	Change the default passwords of all default HPOM users to private passwords immediately after the HP Operations management server installation.
	You can change the default passwords in two ways:
	• **Individually by User**
	Log on to the Java GUI as each of the default HPOM users, and change their passwords manually.
	• **Using opccfguser**
	As an HPOM administrator, you can change the passwords of HPOM users using the following command:
	`#opccfguser -modify <user_name> -password <password>`
	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).
	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, `/etc/passwd`, OpenLDAP, ADS, Kerberos).

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.

Vulnerability	The default audit level is "Operator."
Impact	Configuration activities of HPOM administrators are not audited.
Relevance	High
Risk Level	Medium
Solution	After the installation, do one of the following: • If strict auditing of administrator activities is required, run opc_audit_secure. **CAUTION:** If you use opc_audit_secure, there is no way to reset the audit level. Also, opc_audit_secure 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 *opc_audit_secure(1m)* man page. • If strict auditing of administrator activities is *not* required, change the audit level to **Administrator**. After this change, the administrator can easily change the audit level.

Protecting Audit and History Download Files

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

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

Locking Administrator Audit Levels

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

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

Vulnerability	The audit event "Logon" does not include the machine name or the local system account name.
Impact	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.
Relevance	High
Risk Level	Medium
Solution	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

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

Solution	Use HPOM enhancements:
	• 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, *<$MSG_TEXT>* 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.
	• Remote action configuration file (remactconf.xml).
	In HPOM, the following is true by default:
	• Allows all remote actions from HTTPS nodes (certified nodes).
	• Always provides action string signature verification for remote actions for HTTPS agents.
	Example 5-1 shows the HPOM remote action configuration file:
	/etc/opt/OV/share/conf/OpC/mgmt_sv/ remactconf.xml
	NOTE: 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.
	CAUTION: Avoid variables in action strings. If you cannot avoid variables in action strings, use the "_NO_SHELL: " prefix before action strings.

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

Vulnerability	The private keys of the HP Operations management server and its corresponding certificate authority (CA) are the heart of the public key infrastructure. The key store is located in the following directory: `/var/opt/OV/shared/server/datafiles/sec` These keys could be lost or compromised.
Impact	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.
Relevance	High
Risk Level	High
Solution	Make sure that no unauthorized persons with root privileges have access to the management server. Make sure that no unauthorized persons have access to backup tapes from the management server. Make sure that the key store mentioned above can be restored easily in case of corruption of deletion. (Also, see the `/opt/OV/bin/OpC/opcsvcertbackup` utility, which can be used to generate a backup copy of the critical pieces.)

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 setting 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

Vulnerability	Unnecessary system services that are running on the HP Operations management server and HTTPS agent systems could be attacked remotely.
Impact	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.
Relevance	High
Risk Level	High

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

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 HP-UX	Service Sun Solaris	Required	Comment
514	shell(tcp) / syslog(udp)	syslog	No	Remote Command / Remote System Logging: Not required to run HPOM. **CAUTION:** 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. **NOTE:** 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: http://www.securityfocus.com/bid/2605 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 HP-UX, Linux Sun Solaris	Required by HPOM Server	Required by HPOM Agent	Comment
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 ovbbcb port number with ovconfchg. For details, refer to the *HPOM HTTPS Agent Concepts and Configuration Guide*.
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 HP-UX, Linux Sun Solaris	Required by HPOM Server	Required by HPOM Agent	Comment
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	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 `opcuihttps` process uses `inetd` to start the corresponding `opcuiwww` processes. The port needs to be available only locally on the management server. In `/var/adm/inetd.sec`, you can restrict it as follows: `ito-e-gui 2351/tcp \` `allow 127.0.0.1` You can configure an alternative port as follows: `ovconfchg -ovrg \` `server -ns \` `opc.opcuihttps -set \` `OPCUIWWW_PORT \ <port_value>`

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

Port	Services HP-UX, Linux Sun Solaris	Required by HPOM Server	HPOM Agent	Comment

5053	ovtrcd	(Yes)	(Yes)	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.
				
				 `# /sbin/init.d/OVTrcSrv \`
				 `stop`
				 Edit the `/sbin/init.d/OVTrcSrv` script to disable startup (for example, put **?exit 2?** before the ?start_service? entry).
				
				 Port 5053 can be opened for local loopback only by using the command `ovtrcadm -disableremotetracing`. You can set `disable_remote_tracing` at install time for agents by adding an according statement to the `bbc_inst_defaults` agent profile template (on the management server). If set, no XPL remote tracing is possible. On the management server, the `ovtrcadm -disableremotetracing` should be performed manually.

8081, 8444	ovtomcatB	Yes	No	OV Tomcat(B) Servlet Container

35211	opcuihttps	(Yes)	No	If you like to run the HPOM Java GUI in HTTPS mode, this service is required.
				
				 To changing the default port, enter the following command on the HPOM management server:
				
				 `# ovconfchg -ovrg \`
				 `server -ns \`
				 `opc.opcuihttps \`
				 `-set SERVER_PORT \`
				 `<port_value>`

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
ovbbccb	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

To check HPOM binary versions, build dates, and patch levels on HP-UX and Solaris:

Enter the following:

**what /opt/OV/bin/OpC/opc* | /usr/xpg4/bin/grep -e opc \
-e OpenView**

what /opt/OV/lib/libopc* | grep -e libopc -e OpenView

Check the Java Operator GUI Client

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

Check the Command-Line Interface

To check the version, the build date, and the source (patch level) of all installed HPOM management server binaries and libraries on HP-UX and Solaris, enter the following from the command line:

what /opt/OV/bin/OpC/utils/* | grep -e utils -e OpenView

```
HP OpenView EventAction Agent 08.54.001 (05/13/09)
HP OpenView EventAction Agent 08.54.001 (05/13/09)
HP OpenView EventAction Agent 08.54.001 (05/13/09)
HP OpenView EventAction Agent 08.54.001 (05/13/09)
```

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

HPOvDepl   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

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

Index

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
  command-line interface, 103
  Core Agent components, 104
  EventAction component, 106–107
  Java GUI, 102
  management server, 101
  non-HPOM components, 108
  OpenSSL, 105
CME, 104
COM+ Internet Service, 96
command, ovswitchuser, 59–60
command-line interface, checking version,
    103
Common Criteria, 12
Common Management Environment, 104
communication
  restricting Java GUI, 27
  single-port, 59
community string, changing SNMP, 54
components
  checking versions
    Core Agent, 104
    EventAction, 106–107
    non-HPOM, 108
  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, 104

D

daemon, SNMP trap, 52—53
database, securing, 45—50
default passwords, changing
  operator, 68—70
  Oracle Database, 45—46
Denial of Service
  protecting opcuiwww, 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, 106—107
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

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,
    108
Non-Stack Execution, 41–42
NSA, 12
ntp service, 95
NX, 41–42

O

opc_adm 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, 105
  implementing HTTPS protocol, 58
operating system
  checking version, 108
  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, 108
  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, 104
    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

Index

Index