HP OpenView Operations for UNIX

Security Advisory

Software Version: 8

Edition 1

Manufacturing Part Number: None

March 2006

Legal Notices

Warranty.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices.

Trademark Notices.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Linux® is a U.S. registered trademark of Linus Torvalds.

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

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

UNIX® is a registered trademark of the Open Group.

Contents

Support

Revisions

1. Introduction

2. OVO/UNIX Security Overview

3. Protecting OVO/UNIX Components

4. Protecting the IT Environment

6. Protecting OVO/UNIX Services

A. Checking OVO Versions

B. OvProtect

Support

Please visit the HP OpenView support web site at:

http://www.hp.com/managementsoftware/support

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

HP OpenView 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

Revisions

NOTE

The information in this document is based on the following software patch levels:

- OVO/UNIX management server: 8.14
- OVO/UNIX Java GUI: 8.14
- OVO HTTPS EventAction agent component: 8.11
- OVO HTTPS Core agent component: 8.11
- Network Node Manager: 7.5 with consolidated patch #1

If your HP OpenView Operations for UNIX (OVO/UNIX) product is installed with an earlier patch level, your application may be more vulnerable, and some of the described procedures to harden your OVO/UNIX environment may not be applicable.

To find out whether newer OVO/UNIX or Network Node Manager patches are available, check the following web site regularly:

http://www.hp.com/managementsoftware/support

To find the latest version of the Security Advisory:

1. Go to the following web site:

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

2. Under Support News, select **Now Available: OVO/UNIX 8 Advisory Guide (.PDF)***.

NOTE

If you are running your OVO/UNIX installation in a firewall environment, refer to the *Firewall Concepts and Configuration Guide*.

To get the Firewall Concepts and Configuration Guide:

1. Go to the following web site:

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

2. Select **Operations for UNIX** and version **8.x**.

CAUTION If you discover any other security issue that could potentially affect OVO/UNIX or any other HP software product, inform the HP support organization immediately.

1 Introduction

Document Overview

This document provides you with a summary of security information related to HP OpenView Operations for UNIX (OVO/UNIX).

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

The recommendations listed in this document are based on certifying OVO/UNIX 8.10 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 OVO/UNIX 8.10 Common Criteria EAL-2 certification, see the following web site:

http://niap.nist.gov/cc-scheme/st/ST_VID10011.html

NOTE

This is a living document. Check for updates regularly on the following web site:

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

Under Support News, select “Now Available: OVO/UNIX 8 Advisory Guide (.PDF)*.”

NOTE There is a new utility, called `ovprotect`, that helps you to address several of the outlined security risks automatically. For more information about `ovprotect`, see Appendix B, “OvProtect,” on page 121.

Document Audience

This document is intended primarily for the following audience:

- OVO/UNIX administrator
- Security expert in your company
- System and application administrators monitored by OVO/UNIX

2 OVO/UNIX Security Overview

Security Risks

HP OpenView Operations for UNIX (OVO/UNIX) 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 OVO/UNIX, 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 OVO/UNIX outlined below may or may not apply.

The OVO/UNIX 8 release contains many significant improvements to make the application as robust and secure as possible.

This document categorizes security risks to an OVO/UNIX implementation as follows:

- **OVO/UNIX Components**
    - OVO/UNIX Motif administrator GUI
    - OVO/UNIX Java GUI
    - OVO/UNIX Service Navigator
    - OVO/UNIX Motif operator GUI[1]
    - OVO/UNIX management server
    - OVO HTTPS agent
    - OVO DCE agent[2]

[1] The Motif operator GUI was *not* part of the Common Criteria certification for OVO/UNIX 8.10. As a result, additional security concerns may apply. Use the Java GUI, wherever possible.

[2] The OVO DCE agent was *not* part of the Common Criteria certification for OVO/UNIX 8.10. As a result, additional security concerns may apply. Use the OVO HTTPS agent, wherever possible.

For details, see Chapter 3, “Protecting OVO/UNIX Components,” on page 21.

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

  For details, see Chapter 6, “Protecting OVO/UNIX Services,” on page 83.

- **IT Environment**

  - Operating system
    (for example, HP-UX, Solaris, and so on)
  - Oracle Database
  - Network Node Manager (NNM)[1]
  - 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 35.

- **OVO/UNIX Configuration**

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

  For details, see Chapter 5, “Configuring OVO/UNIX 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.

[1] NNM is treated as an IT environment component because there is a dedicated Common Criteria certification for NNM 7.5 currently underway.

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 OVO/UNIX 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 OVO/UNIX" 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 OVO/UNIX.

Comment Description and recommendation.

3 Protecting OVO/UNIX Components

HP OpenView Operations for UNIX (OVO/UNIX) software components could be exposed to a wide variety of security risks.

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

Securing the OVO/UNIX Management Server

The standard installation of the OVO/UNIX 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.

X-Redirection

Vulnerability	OVO/UNIX operators use X-redirection to their display stations to run the Motif GUI, which cannot be run locally on the system console. This use of X-redirection makes OVO/UNIX vulnerable to security risks.
Impact	Information transferred through X-redirection can be “sniffed.”
Relevance	Low
Risk Level	Low
Solution	Do one of the following: • Use the Java GUI whenever possible. Stop using the OVO/UNIX Motif operator GUI. • Set up secure X-communication (for example, by using SSH with X11 forwarding). **CAUTION:** Applications that display an X window from a managed node will no longer work. For details, see the SSO document OV-EN016170: http://support.openview.hp.com/support.jsp In addition, you may want to remove the execution permission flag, or even delete the `/opt/OV/bin/OpC/opcuiop` binary, to prevent anyone from accidently starting the Motif operator GUI.

NOTE The Motif operator GUI was not part of the Common Criteria EAL-2 evaluation.

Motif Administrator GUI

To help secure the Motif administrator GUI, do one of the following:

- Work directly on the OVO/UNIX management server console.
- Set up secure X-communication, as described in “X-Redirection” on page 23.

HTTPS-based OVO Server-to-Server Communication

HP is working to provide HTTPS-based communication between OVO/UNIX 8 management servers. The solution is expected in early 2006.

Securing Files

This section describes vulnerabilities in the OVO/UNIX management server, NNM, and the OVO/UNIX Java GUI.

Securing OVO/UNIX and NNM Sockets

This section describes vulnerabilities in sockets used by the OVO/UNIX management server or NNM.

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 Appendix B, “OvProtect,” on page 121.

Securing the Java GUI

This section describes vulnerability risks in the OVO/UNIX 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 OVO/UNIX 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.

- IB*

  Embedded web browser cache directory.

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 OVO/UNIX 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. Starting with the Java GUI 8.14 patch level, the communication can be switched to HTTPS, which provides authentication and encryption.

Vulnerability	The `opcuiwww` socket on the OVO/UNIX 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 up to 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 OVO/UNIX management server. To find out how to configure the OVO/UNIX management server and the Java GUI, refer to the corresponding documentation. Detailed configuration and usage instructions are available in the *HTTPS-based Java GUI Support on the Management Server* white paper, available for download from the following web site: `http://ovweb.external.hp.com/lpe/doc_serv/` Select **`Operations for UNIX`** and version **`8.x`**. • Do not allow all systems in the network to access the OVO/UNIX 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 wanted 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 Appendix B, “OvProtect,” on page 121.

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

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

OVO/UNIX provides a rich set of APIs on the management server and the OVO agents. This section describes only the APIs that expose security-related risks.

Problem	The OVO/UNIX 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 OpenView Operations for UNIX (OVO/UNIX) 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.

OVO/UNIX 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 2.6 and higher (Sun SPARC)**

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

HP-UX 11.0, 11.11 (PA-RISC)

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

- **HP-UX 11.23 (PA-RISC, Itanium)**

  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 9**

  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 provides a kernel parameter that can be set through the SAM tool:

`executable_stack = 0`

HP-UX 11.23 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 kernel immediately terminates the program (sends a `SIGKILL` signal), and logs the apparent stack buffer overflow attack. The default kernel setting for HP-UX 11.23 PA-RISC and HP-UX 11.23 Itanium is the same for the `executable_stack` parameter.

`executable_stack = 1`

HP-UX 11.0/11.11 default. Causes all program stacks to be executable. This setting is *not* recommended. Change the setting in the SAM 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 2.6 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 2.6 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 OVO/UNIX during the ovoinstall phase. The SD user is added if you use the HP OpenView Service Desk (OVSD) or Service Navigator Value Pack (SNVP) 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 OVO/UNIX management server installation, the ovoinstall script requires that the Oracle user SYSTEM have its default password. Otherwise, the OVO/UNIX 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 OVO/UNIX internally in the file:

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

NOTE If the Oracle Database user and/or user password (used by SNVP) is changed, you need to change the SNVP database user account accordingly in the Accounts dialog of the “server settings editor” in SNVP.

For instructions, refer to the *Service Navigator Value Pack Installation Guide*, which is available for download on the following web site:

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

Select “Operations for UNIX” and version 8.x.

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 OpenView Reporter. It needs to be adapted in HP OpenView Reporter accordingly in the **File**→**Configure**→**Databases** menu.

Vulnerability	A local user who is not authorized to access the database may run OVO 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 OVO command-line tools.
Relevance	Medium
Risk Level	Medium
Solution	To change the permission of the OVO/UNIX password file, enter the following: `# chmod 0440 /etc/opt/OV/share/conf/OpC/mgmt_sv/.opcdbpwd.sec`

Running the Oracle Database on OVO/UNIX

If the OVO/UNIX 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 OVO/UNIX management server.

If you need to use a remote database for OVO, 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 OVO/UNIX management server, remote access to the database is not needed for normal operation of the OVO/UNIX 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 OVO/UNIX and Oracle processes.

   ```
   # ovstop
   # /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 OVO/UNIX processes:

   ```
   # /sbin/init.d/ovoracle start
   # ovstart
   ```

   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 OVO 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 OVO/UNIX 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 is an integral part of OVO/UNIX. However, not all NNM functionality is required to run OVO/UNIX.

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 OVO/UNIX Common Criteria evaluation perspective. NNM 7.5 itself is also currently being evaluated for Common Criteria EAL-2.

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, OV 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 OVO/UNIX, 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 OVO/UNIX.
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 the HP OpenView Web Server

NNM provides a web server, which listens on port 3443.

OVO/UNIX leverages this web server 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`

- **ovw**

  Use the Motif version of ovw.

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

To disable the HP OpenView web server:

Do one of the following:

- **Perform Manual Steps**

  Perform the following manual steps:

  ```
  # ovstop httpd
  ```

  ```
  # ovdelobj /etc/opt/OV/share/lrf/httpd.lrf
  ```

- **Run ovprotect**

  To automatically disable the HP OpenView 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 Appendix B, “OvProtect,” on page 121.

- **Block Firewall Port**

  Block port 3443 with your firewall.

To re-enable the HP OpenView web server:

Enter the following:

```
# ovaddobj /etc/opt/OV/share/lrf/httpd.lrf
# ovstart httpd
```

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

Securing SNMP and NNM

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

Changing the SNMP Community String

Typically, when NNM 7.5 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 opcinfo (for DCE agents) or 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 from the opcinfo file or 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 DCE RPC Communication

The OVO/UNIX 8 management server processes communicate locally using DCE RPC.

If you use only OVO HTTPS agents in your managed environment, and if you do not use message forwarding between OVO/UNIX management servers, you can safely disable the OVO DCE distribution manager and OVO DCE message receiver, which are no longer needed. This disabling removes the corresponding process entries from the mapping table of the DCE RPC `portmapper`, and closes unnecessary ports.

CAUTION You can perform the procedures below only if no OVO DCE agents are configured on the OVO/UNIX management server.

Verify That No OVO DCE Agents are Configured

To verify that no OVO DCE agents are configured in the OVO/UNIX management server, follow these steps:

1. Execute the following command:

   ```
   # /opt/OV/bin/OpC/utils/opcnode -list_nodes
   ```

2. Check the `Comm Type` values in the output of the command.

   Nodes with type `COMM_BBC` indicate OVO HTTPS agents.

Disable Distribution Manager and DCE Message Receiver

To disable the OVO distribution manager (`opcdistm`) and the DCE message receiver (`opcmsgrd`), follow these steps:

1. Stop the OVO/UNIX management server entirely:

   ```
   # ovstop ovoacomm
   ```

2. Set the following configuration variable:

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

3. Start the OVO/UNIX management server:

   ```
   # opcsv -start
   ```

   All server processes, except for `opcmsgrd` and `opcdistm`, should start normally.

4. Verify the status of all server processes:

   ```
   # opcsv -status
   ```

5. Verify that the OVO DCE distribution manager and OVO DCE message receiver are no longer registered at the `rpcd`:

   ```
   # rpccp show mapping
   ```

   The OVO DCE distribution manager and OVO DCE message receiver are no longer listed.

To automatically disable the DCE distribution manager and DCE message receiver, you can run the `ovprotect` utility. For details, see "Assessing Your System Vulnerability with ovprotect" on page 85. For more information about `ovprotect`, see Appendix B, "OvProtect," on page 121.

Activate OVO/UNIX in DCE RPC Daemon-less Mode

The OVO/UNIX management server can run without the DCE RPC daemon (rpcd/dced). In this case, all OVO/UNIX management server processes communicate directly without registration at the RPC portmapper.

You can run the `ovprotect` utility to automatically make the changes outlined below. For more information about `ovprotect`, see Appendix B, "OvProtect," on page 121.

To activate OVO/UNIX running in DCE RPC daemon-less mode:

1. Stop the OVO/UNIX management server entirely:

   ```
   # ovstop ovoacomm
   ```

2. Find an unused port number to which you want to bind the OVO display manager process:

   ```
   <my_portnumber>
   ```

   This port number needs to be set in the HP OpenView config settings file (step 3) and port files (step 4) consistently.

3. Set the following configuration variables:

   ```
   # ovconfchg -ovrg server -ns opc -set \
   OPC_COMM_LOOKUP_RPC_SRV FALSE
   ```

   ```
   # ovconfchg -ovrg server -ns opc -set \
   OPC_COMM_REGISTER_RPC_SRV FALSE
   ```

   ```
   # ovconfchg -ovrg server -ns opc -set \
   OPC_COMM_RPC_PORT_FILE \
   /etc/opt/OV/share/conf/OpC/mgmt_sv/ports
   ```

   ```
   # ovconfchg -ovrg server -ns opc.opcdispm -set \
   OPC_COMM_PORT_RANGE \
   <my_portnumber>
   ```

4. Create the file `/etc/opt/OV/share/conf/OpC/mgmt_sv/ports`:

   ```
   # ----------------

   NODE_NAME opcdispm <my_portnumber> <*>

   # ----------------
   ```

Example:

```
NODE_NAME opcdispm 11111 <*>
```

CAUTION

NODE_NAME is a keyword that may not be replaced by any other name. Also, the configured port may not be already used on the system.

5. Set the file permissions of /etc/opt/OV/share/conf/OpC/mgmt_sv/ports to 400:

```
# chmod 400 /etc/opt/OV/share/conf/OpC/mgmt_sv/ports
```

6. Start the OVO/UNIX management server:

```
# opcsv -start
```

7. Verify that the OVO display manager (opcdispm) is no longer registered at the rpcd:

```
# rpccp show mapping
```

The OVO display manager is no longer listed.

NOTE

If you still have OVO DCE agents running, you can also set up direct DCE RPC communication without having a DCE endpoint mapper running on the OVO DCE agents.

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

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

Select “Operations for UNIX” and version 8.x.

Securing the OVO Agent

You can secure the OVO agent by doing the following:

- "Installing the OVO Agent" on page 57
- "Switching to the OVO HTTPS Agent" on page 59
- "Running Non-Root OVO HTTPS Agents on UNIX Platforms" on page 60

Installing the OVO Agent

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

The communication between the OVO/UNIX management server and the OVO agent can be categorized as follows:

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

OVO/UNIX provides a comfortable mechanism for installing the OVO agent through the administrator GUI.

To install the OVO agent:

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

CAUTION It is *strongly recommended* that you use only a secure IT infrastructure for installing the OVO 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 OVO 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 OVO HTTPS Agent

OVO DCE agents are based on older technology. They use the DCE (or NCS) Remote Procedure Call mechanism to communicate with the OVO/UNIX management server.

If possible, switch the OVO DCE agent to the OVO HTTPS agent.

TIP

If you cannot switch to HTTPS, you might consider using the "DCE daemon-less" feature for OVO DCE agent.

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

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

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

As a general rule, communication between the OVO/UNIX 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 OVO heartbeat polling is based on HTTP and ICMP (normal ping). The ICMP part can be switched off by selecting the "RPC only" mode in the advanced node screen of the OVO administrator GUI. 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, a “single port” communication model is introduced with OVO/UNIX 8 for the HTTPS agents.

By default, all OVO-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 OVO/UNIX management server as well as the OVO 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://ovweb.external.hp.com/lpe/doc_serv/

Select “Operations for UNIX” and version 8.x.

HP also plans to introduce “outbound only” functionality in 2006, so that all communication from the OVO/UNIX management server and/or the OVO HTTPS agent will be opened from the more secure side only. This will allow you to completely close firewalls from the less secure side for OpenView product-related network traffic. For that purpose, a new concept — called “Reverse Channel Proxy” — will be introduced.

Running Non-Root OVO HTTPS Agents on UNIX Platforms

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

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

NOTE The OVO agent on the OVO/UNIX 8 management server must be an HTTPS agent.

The `ovswitchuser` command has the following limitations:

- **OVO Agent**

  The OVO agent must be always running as root on the OVO/UNIX management server.

- **SPIs**

  Some Smart Plug-ins (SPIs) require you to run the OVO 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 OVO/UNIX application bank require root privileges. Do not assign these applications to users who are responsible only for managed nodes, which run “non-root” OVO 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 OVO DCE/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 OVO/UNIX management server and the following:

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

In general, there are three major security risks for OVO/UNIX 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 OVO/UNIX in a Secure Way

HP OpenView Operations for UNIX (OVO/UNIX) 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 OVO/UNIX users, based on their skills and responsibilities.

Assigning Rights to Users

OVO/UNIX 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 OVO users, keep the following assumptions and guidelines in mind:

- **Guidelines**

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

- **Passwords**

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

- **Log-on Messages**

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

- **Root System Administrator**

  Make sure that the OVO administrator is a root system administrator on the operating system underlying the OVO/UNIX management server. Normally the OVO/UNIX management server is a dedicated management system used to manage your IT environment controlled by HP OpenView.

- **Super User**

  Make sure that the operating system super user on each OVO agent system is a trusted user who has the necessary administrative knowledge of local super users of OVO 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 OVO user logon for each employee.

If generic OVO 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 OVO 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 OVO 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 OVO operator may get more rights than necessary.

NOTE Applications requiring root/administrator privileges cannot be executed on OVO agents running as "non-root."

Assigning Broadcast and Virtual Terminal Applications

CAUTION 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

CAUTION Do not 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 OVO 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 OVO messages operators see and can work on.

Changing Default Operator Passwords

You can change default user passwords to prevent unauthorized persons from hijacking OVO/UNIX with default user passwords.

Vulnerability	The OVO/UNIX management server installation automatically creates several OVO 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 OVO 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 OVO users.
Relevance	High
Risk Level	High

Solution	Change the default passwords of all default OVO users to private passwords immediately after the OVO/UNIX management server installation. You can change the default passwords in two ways: • **Individually by User** Log on to the OVO Motif or Java GUI as each of the default OVO users, and change their passwords manually. • **Using the Motif Administrator GUI** Log on the OVO Motif GUI as `opc_adm`, and change the passwords of all default OVO users in the user bank. 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 OVO/UNIX, 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 integration configuration in the Motif administrator GUI.

To get details about the PAM integration configuration:

1. Start the Motif administrator GUI.
2. Select **Actions**→**Utilities**→**Change Password**.
3. In the **Change Password** window, click **Help**.
4. Click **Changing Your OVO Administrator's Password**.
5. Click **Set Up PAM User Authentication**.

NOTE OVO/UNIX 8.10 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 OVO/UNIX – PAM client interface was part of the Common Criteria evaluation. All other PAM components belong to the IT environment.

Auditing Users

You can configure OVO/UNIX to audit the activities of the OVO administrator, OVO template administrators, and OVO operators.

Auditing Administrator Activities

You can configure OVO/UNIX to audit administrator activities.

Vulnerability	The default audit level is “Operator.”
Impact	Configuration activities of OVO administrators or OVO template 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 OVO/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** in the Motif administrator GUI. 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 OVO/UNIX information.

Vulnerability	Audit and history download files may be readable by unauthorized persons.
Impact	An unauthorized person could get OVO/UNIX information.
Relevance	Medium
Risk Level	Medium
Solution	Change the download directories in the OVO/UNIX administrator GUI to a dedicated path. Protect this path by setting strict access permissions. Calling `opc_audit_secure` locks the path definitions in the OVO/UNIX administrator GUI. **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 OVO administrators and OVO template administrators are audited.

Vulnerability	The OVO administrator can change the audit level.
Impact	If the audit level is not “Administrator,” the activities of OVO administrators and OVO 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 OVO/UNIX. For details, see the *opc_audit_secure(1m)* man page.

Protecting Machine and Account Names

You must set up individual OVO 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	OVO/UNIX tracks the activities of OVO 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	OVO users may not share their OVO accounts. You must set up individual OVO users for each person. If you are running shift operations, or if you have special rotating OVO user duties, make sure each OVO user has a unique OVO account. This is especially important if multiple OVO users run Java GUI sessions with the same logon.

Securing Remote Actions

As part of the template and 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 OVO message has been intercepted. Carefully assign such policies to the OVO DCE and HTTPS agents. The OVO/UNIX 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 OVO certificate authority and management server are protected as well as possible.

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

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

Select “Operations for UNIX” and version 8.x.

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

Solution

Use OVO/UNIX 8 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 OVO/UNIX 8, the following is true by default:

- Allows all remote actions from HTTPS nodes (certified nodes). Denies all remote actions from DCE nodes.
- Always provides action string signature verification for remote actions for HTTPS agents.

Example 5-1 shows the OVO/UNIX 8 remote action configuration file, located in the following directory:

```
/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 OVO/UNIX. 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. Remote actions from DCE nodes are disabled.
****************************************************************************
-->
<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 (DCE nodes)</doc>
  <if>
     <source> <nodegroup>Group4</nodegroup> </source>
     <certified>false</certified>
   </if>
   <allow/>

</rule>
```

Securing the Certificate Server

Vulnerability	The private keys of the OVO management server and its corresponding certificate authority (CA) are the heart of the public key infrastructure, as introduced with OVO 8. 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 OVO 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 OVO message has been generated are not signature-checked on the OVO/UNIX 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 OVO 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 OVO/UNIX 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 OVO/UNIX 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 OVO/UNIX Services

HP OpenView Operations for UNIX (OVO/UNIX) and Network Node Manager (NNM) require 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

OVO/UNIX provides a new utility, called `ovprotect`, that helps you to determine and minimize the vulnerability risks of your systems from the HP OpenView perspective. It tests and disables unused services on the OVO/UNIX management server or on the OVO HTTPS agent platforms.

In addition, it checks local file permissions, and can perform some corrective actions on the local systems.

The `ovprotect` tool is modular. More extensions, as well as modules for other HP OpenView products, are expected to be released on a regular basis.

You can always download the latest version of the `ovprotect` tool from the OVO/UNIX web site:

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

For details and usage options, refer to the *ovprotect(1m)* man page. Also, see Appendix B, “OvProtect,” on page 121.

NOTE The tool `ovprotect` is a self-extracting archive. You can run it without installing OVO/UNIX.

You can apply `ovprotect` on the OVO/UNIX 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 OVO/UNIX 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. OVO/UNIX provides the tool `ovprotect`, which detects services that are unnecessary to OVO/UNIX. 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 OVO/UNIX

This section lists services that may run on a OVO/UNIX 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 OVO/UNIX

Table 6-1 lists the services and ports that are not provided and are *not* required by the OVO/UNIX management server, UNIX HTTPS agent, or Network Node Manager.

TIP To better understand this table, see "Key to Service Table Values" on page 19.

Table 6-1 Services and Ports Not Required by OVO/UNIX

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
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. OVO/UNIX can use telnet/ftp, remsh/rcp, or ssh/scp for OVO agent software deployment.
23	telnet	telnet	No	Telnet: It is strongly recommended that you disable telnet, and use ssh (22) instead. OVO/UNIX can use telnet/ftp, remsh/rcp, or ssh/scp for OVO 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 OVO.

Table 6-1 Services and Ports Not Required by OVO/UNIX (Continued)

Port	Service		Required	Comment
	HP-UX	Sun Solaris		
42	nameserver	nameserver	No	Host Name Server: Not required to have a name server running on the OVO/UNIX management server system. Nevertheless, many customers have a name server or caching name server on the OVO/UNIX management server. In fact, if name resolution is bad, it is recommended that you have a caching name server on the OVO/UNIX management server.
113	auth/ident	auth	No	Authentication Service: Not required to run OVO/UNIX. It should be disabled.
123	ntp	ntp	No	Network Time Protocol: Not required to run OVO/UNIX.
512	exec	biff	No	Remote Process Execution
514	shell(tcp) / syslog(udp)	syslog	No	Remote Command / Remote System Logging: Not required to run OVO/UNIX. **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.

Table 6-1 Services and Ports Not Required by OVO/UNIX (Continued)

Port	Service		Required	Comment
	HP-UX	Sun Solaris		
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 OVO/UNIX.
1508	diagmond		No	Diagnostic System Manager
1712	registrar		No	Resource Monitoring Service
2049	nfs		No	Network File System: Not required to run OVO/UNIX, but it might be required for the system. **NOTE:** NFS is temporarily needed to set up OVO 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 OVO/UNIX. 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.

Table 6-1 Services and Ports Not Required by OVO/UNIX (Continued)

Port	Service		Required	Comment
	HP-UX	Sun Solaris		
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 OVO/UNIX. 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 OVO/UNIX. It should be disabled, if possible.

Services Required by OVO/UNIX

Table 6-2 lists the services and ports that are provided or required by the OVO/UNIX management server, UNIX HTTPS agent, or Network Node Manager. 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 19.

Table 6-2 Services and Ports Required by OVO/UNIX

Port	Services		Required by			Comment
	HP-UX	Sun Solaris	OVO Server	OVO Agent	NNM	
22	ssh	ssh	(Yes)	No*	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.
111	sunrpc / portmap	sunrpc	(Yes)	No	No	Sun Remote Procedure Call / Portmapper. This service is required only on the OVO/UNIX management server in case you also manage Novell NetWare with the OVO agent. Its counterpart runs on the Novell NetWare managed node as well.

Table 6-2 Services and Ports Required by OVO/UNIX (Continued)

Port	Services		Required by			Comment
	HP-UX	Sun Solaris	OVO Server	OVO Agent	NNM	
135	epmap	epmap	(Yes)	No	No	DCE Endpoint Mapper. Required by default on the OVO server. It can be stopped in case the changes are made as outlined in “Securing DCE RPC Communication” on page 53.
161	snmp	snmp	(Yes)	(Yes)*	Yes	Simple Network Management Protocol Agent * Yes in case the OVO agent does SNMP trap interception or MIB monitoring.

162	snmptrap	snmptrap	(Yes)	(Yes)*	Yes	Simple Network Management Protocol Trap: Needed by NNM for remote trap interception.
						`# ovstop ovtrapd;`
						`# ovdelobj \`
						`/etc/opt/OV/share/lrf \`
						`/ovtrapd.lrf`
						* Yes in case the OVO agent does SNMP trap interception or MIB monitoring.

383	ovbbccb	ovbbccb	Yes	Yes	No	HP OpenView BlackBox Communication Broker: This is the HTTPS communication broker. It is required to run OVO/UNIX. You may not block it, but you may change the ovbbcb port number with `ovconfchg`. For details, refer to the *HTTPS Agent Concepts and Configuration Guide*.

Table 6-2 Services and Ports Required by OVO/UNIX (Continued)

Port	Services		Required by			Comment
	HP-UX	Sun Solaris	OVO Server	OVO Agent	NNM	
513	login(tcp)	login(tcp)	(Yes)	(Yes)	(Yes)	Remote Logon: It is strongly recommended that you disable this service, and use ssh (22) instead. OVO/UNIX uses the log-on service for opening a Virtual Terminal application (through opcrlogin). If you do not use the OVO Virtual Terminal application, you should disable this service
696	pmdmgr		Yes	N/A	Yes	HP OpenView Postmaster Manager: Required by NNM and by OVOU (indirectly).
1521	oracle / listener	oracle / listener	(Yes)	No	No	Oracle Listener: Required if the database is accessed remotely (for example, by OV Reporter). This is the default port for the listener, but you can configure Oracle to use a different port.
2389	ovsession mgr	ovsession mgr	(Yes)	N/A	Yes	HP OpenView Web Session Manager: Required by NNM for HomeBase application. # **ovstop ovsessionmgr** # **ovdelobj \** **/etc/opt/OV/share/ \** **lrf/ovsessionmgr.lrf**
2447	ovwdb	ovwdb	Yes	N/A	Yes	HP OpenView Object Database Daemon: Required by NNM.

Table 6-2 Services and Ports Required by OVO/UNIX (Continued)

Port	Services		Required by			Comment
	HP-UX	Sun Solaris	OVO Server	OVO Agent	NNM	

2531	ito-e-gui	ito-e-gui	Yes	N/A	No	HP OpenView Operations Java Console: Required for the communication of the Java GUI clients to the OVO/UNIX 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`
						Starting with the OVO/UNIX 8.14 server patch, you can configure an alternative port as follows:
						`ovconfchg -ovrg \`
						`server -ns \`
						`opc.opcuihttps -set \`
						`OPCUIWWW_PORT \`
						`<port_value>`

2532	ovtopmd	ovtopmd	Yes	N/A	Yes	HP OpenView IP Topology Daemon: Required by NNM and OVOU through the firewall.

Table 6-2 Services and Ports Required by OVO/UNIX (Continued)

Port	Services		Required by			Comment
	HP-UX	Sun Solaris	OVO Server	OVO Agent	NNM	
2690	ovembeddb	ovembeddb	(Yes)	N/A	Yes	HP OpenView Embedded DW Database: Required by NNM. Used locally only, but accessible remotely (for example, **telnet *<mgmt_sv>* 2690**). Block this port with a firewall.
2953	ovalarmsrv	ovalarmsrv	No	N/A	Yes	HP OpenView Alarm Server Listener Port: Required by NNM for xnmevents and so on. # **ovstop ovalarmsrv** # **ovdelobj \** **/etc/opt/OV/share/ \** **lrf/ovalarmsrv.lrf**
2954	ovalarmsrv_cmd	ovalarmsrv_cmd	No	N/A	Yes	HP OpenView Alarm Server Command Port: Required by NNM. Handled by ovalarmsrv (see above).
3443	ovhttp	ovhttp	(Yes)	N/A	Yes	HP OpenView Web Server: This web server is necessary only for the Service Navigator and the Java operator GUI online help. It can be disabled when these services are not needed. # **ovstop httpd** # **ovdelobj \** **/etc/opt/OV/share/lrf/httpd.lrf**

Table 6-2 Services and Ports Required by OVO/UNIX (Continued)

Port	Services		Required by			Comment
	HP-UX	Sun Solaris	OVO Server	OVO Agent	NNM	
5053	ovtrcd	ovtrvd	(Yes)	(Yes)	(Yes)	HP OpenView Trace Server: Required to get trace output. However, OVO/UNIX 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.
7501	OV Bus daemon	OV Bus daemon	No	No	Yes	HP OpenView Bus Daemon. This port is exposed only locally.

Table 6-2 Services and Ports Required by OVO/UNIX (Continued)

Port	Services		Required by			Comment
	HP-UX	Sun Solaris	OVO Server	OVO Agent	NNM	

7510	ovas	ovas	No	N/A	Yes	HP OpenView Application Server: Required by NNM.
						`# ovstop ovas`
						`# ovdelobj \`
						`++ \`
						`/etc/opt/OV/share \`
						`/lrf/ovas.lrf`

7777	ovuispmd	ovuispmd	Yes	N/A	Yes	HP OpenView UI Services Daemon: Required by NNM and OVO (indirectly).

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

Services for OVO 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 NT LM Security Support Provider.

Services Required by OVO HTTPS Windows Agents

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

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

Service	Port	tcp/udp	Required by OVO	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 OVO HTTPS Windows Agent

Service	Port	tcp/udp	Required by OVO	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.
DCE	1051	tcp	No	File Replication Service

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

Service	Port	tcp/udp	Required by OVO	Service Name
ansyslmd	1055	tcp, udp	Yes	ANSYS - License Manager
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 OpenView 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 OVO Versions

HP OpenView Operations for UNIX (OVO/UNIX) 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 OVO/UNIX Management Server

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

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

To check the OVO/UNIX management server version:

Enter the following:

```
# ovconfget -ovrg server opc | grep OPC_INSTALLED_VERSION

OPC_INSTALLED_VERSION=A.08.12

# 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 OVO/UNIX binary versions, build dates, and patch levels:

Enter the following:

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

/opt/OV/bin/OpC/opc:

        HP OpenView Operations for Sun Solaris A.08.12
ITOSOL_00403 (04/21/05)

/opt/OV/bin/OpC/opc.bin:

        HP OpenView Operations A.08.10.160 (10/22/04)

/opt/OV/bin/OpC/opc.ldap:

        HP OpenView Operations for Sun Solaris A.08.12
ITOSOL_00403 (04/21/05)

/opt/OV/bin/OpC/opc_audit_secure:

        HP OpenView Operations A.08.10.160 (10/22/04)

             :
```

```
# what /opt/OV/lib/libopc* | grep -e libopc -e OpenView
/opt/OV/lib/libopc_r.sl:
        HP OpenView Operations A.08.10.160 (10/12/04)
/opt/OV/lib/libopcassv.sl:
        HP OpenView Operations A.08.10.160 (10/20/04)
/opt/OV/lib/libopcassvn.sl:
        HP OpenView Operations A.08.10.160 (10/20/04)
/opt/OV/lib/libopcconf.sl:
        HP OpenView Operations A.08.10.160 (10/20/04)
/opt/OV/lib/libopccsa.sl:
        HP OpenView Operations A.08.10.160 (10/20/04)
/opt/OV/lib/libopcctrlovw.sl:
        HP OpenView Operations A.08.10.160 (10/20/04)
/opt/OV/lib/libopcdb.sl:
        HP OpenView Operations A.08.12 PHSS_32820 (04/21/05)
/opt/OV/lib/libopcdm.sl:
/opt/OV/lib/libopcecendec.sl:
    :
```

Check the Motif Administrator GUI

From the OVO/UNIX Motif administrator GUI, you can check the version of the OVO/UNIX management server, as well as the version of the NNM DevKit and ISA Dialog Manager that were used when building OVO/UNIX.

To check the NNM DevKit and ISA Dialog Manager versions:

In one of the OVO/UNIX Motif administrator GUI windows (for example, **OVO Node Bank**), select **Help**→**About OVO**.

To check the installed NNM version:

1. In the **Root** submap, select **Help**→**About HP OpenView**.
2. Click **More Info**.

Check the Motif Operator GUI

To check the version of the OVO/UNIX Motif operator GUI on HP-UX and Solaris, enter the following:

```
# what /opt/OV/bin/OpC/opcuiop | grep OpenView
```

```
HP OpenView Operations for Sun Solaris A.08.12 ITOSOL_00403
(04/21/05)
```

NOTE You may have renamed or removed the opcuiop binary according to the recommendation in “Securing the OVO/UNIX Management Server” on page 23.

Check the Java Operator GUI Client

To check the version of the OVO 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 OVO/UNIX management server binaries and libraries, enter the following from the command line:

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

```
/opt/OV/bin/OpC/utils/OpcNode.pm:

/opt/OV/bin/OpC/utils/OpcUtil.pm:

/opt/OV/bin/OpC/utils/disable_java_gui:

        HP OpenView Operations A.08.10.160 (10/20/04)

/opt/OV/bin/OpC/utils/ecsmgr:

/opt/OV/bin/OpC/utils/enable_java_gui:

        HP OpenView Operations A.08.10.160 (10/20/04)

/opt/OV/bin/OpC/utils/ha:

/opt/OV/bin/OpC/utils/inst_usr.sh:

        HP OpenView Operations A.08.10.160 (09/23/04)

/opt/OV/bin/OpC/utils/opc_chk_node_res.pl:

        HP OpenView Operations A.08.10.160 (10/20/04)

/opt/OV/bin/OpC/utils/opc_node_change.pl:

        HP OpenView Operations A.08.10.160 (10/20/04)

             :
```

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 OVO agent from the configuration and from the installer on HP-UX, Solaris, and Linux.

To check the OVO agent version deployable from the OVO/UNIX management server:

Enter the following:

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

To check the OVO agent version from the configuration:

Enter the following:

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

```
OPC_INSTALLED_VERSION=08.10.160
```

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

Enter the following:

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

```
HPOvEa.HPOVEAAGT      8.10.160       HP OpenView E/A Agent
```

To check the OVO agent version from the installer on Solaris:

Enter the following:

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

```
VERSION:  8.10.160
```

To check the OVO agent version from the installer on Linux:

Enter the following:

```
# rpm -q HPOvEaAgt
```

```
HPOvEaAgt-8.10.160-1
```

To check the OVO agent remotely from the management server:

Enter the following:

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

Check the DCE Agent

You can check the version of the OVO DCE agent in the `opcinfo` file.

To check the DCE agent version on AIX:

Enter the following:

```
# grep INSTALLED_VERSION /usr/lpp/OV/OpC/install/opcinfo
OPC_INSTALLED_VERSION A.07.28
PERF_INSTALLED_VERSION A.07.27
COMM_INSTALLED_VERSION 2.6.7.0
```

To check the DCE agent version on Tru64:

Enter the following:

```
# grep INSTALLED_VERSION /usr/opt/OV/bin/OpC/install/opcinfo
OPC_INSTALLED_VERSION A.07.28
PERF_INSTALLED_VERSION A.07.27
COMM_INSTALLED_VERSION 2.6.7.0
```

To check the DCE agent version on Windows:

View the following file:

`<InstallDir>\bin\OpC\install\opcinfo`

The default for `<InstallDir>` is `\usr\OV`.

To check the DCE agent version on all other UNIX platforms:

Enter the following:

```
# grep INSTALLED_VERSION /opt/OV/bin/OpC/install/opcinfo
OPC_INSTALLED_VERSION A.07.28
PERF_INSTALLED_VERSION A.07.27
COMM_INSTALLED_VERSION 2.6.7.0
```

Check Non-OVO/UNIX Components

You can check the versions of non-OVO/UNIX components, such as the operating system, Oracle Database, NNM, and DCE.

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

Enter the following:

```
# uname -r

B.11.11
```

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

Enter the following:

```
# su - oracle

$ sqlplus -v

SQL*Plus: Release 9.2.0.2.0 - Production

$ exit
```

To check the NNM binary versions, build dates, and patch levels:

Enter the following:

```
# what /opt/OV/bin/ov* | grep -e bin/ov -e OpenView

/opt/OV/bin/ov.envvars.csh:

        HP OpenView NNM Release B.07.01  Jan 12 2004

/opt/OV/bin/ov.envvars.pl:

        HP OpenView NNM Release B.07.01  Jan 12 2004

/opt/OV/bin/ov.envvars.sh:

        HP OpenView NNM Release B.07.01  Jan 12 2004

/opt/OV/bin/ovIfIndexRemap.ovpl:

        HP OpenView Release B.0X.XX (updated by copy_proot)

/opt/OV/bin/ovSetDBEnv:

/opt/OV/bin/ovactiond:
        HP OpenView Network Node Manager NNM Release B.07.01
/opt/OV/bin/ovaddobj:
        HP OpenView ICVT NNM Release B.07.01
/opt/OV/bin/ovaddr:
        HP OpenView Licensing NNM Release B.07.01
/opt/OV/bin/ovalarmadm:
        HP OpenView Network Node Manager NNM Release B.07.01
             :
# what /opt/OV/lib/libov* | grep -e lib/libov -e OpenView
/opt/OV/lib/libov.2:
        HP OpenView ov library NNM Release B.06.20
/opt/OV/lib/libov.3:
        HP OpenView ov library NNM Release B.07.01
/opt/OV/lib/libov.sl:
        HP OpenView ov library NNM Release B.07.01
             :
```

To check the DCE version on HP-UX:

Enter the following:

```
# what /opt/dce/bin/*

/opt/dce/bin/acl_edit:

        HP92453-02A.11.00 HP-UX SYMBOLIC DEBUGGER (END.O
ILP32) $Revision:

75.02 $

        HP DCE/9000 1.8 Module: acl_edit Date: Sep 23 2000
17:44:26

/opt/dce/bin/cdsadv:

        HP92453-02A.11.00 HP-UX SYMBOLIC DEBUGGER (END.O
ILP32) $Revision:

75.02 $

        dpeaclstore.c   7       (DECdns)        11/17/1991

        dpeaclaccess.c  4       (DECdns)        12/11/1991

       HP DCE/9000 1.8 PHSS_29964 Module: cdsadv Date: Nov
7 2003 16:25:41

            :
```

To check the DCE version on Solaris:

Enter the following:

```
# pkginfo -l HPlwdce | grep VERSION

VERSION:  1.1.4.22.1 (HP special version)
```

NOTE The DCE runtime on Solaris is delivered by the OVO/UNIX management server installation.

B OvProtect

Functionality

OvProtect is an elegant and easy-to-use tool for assessing and changing some of the security-exposed components of HP OpenView products described in this document. It enables you to check the current status of these components, and switch them on and off, as needed.

OvProtect is intended to protect the local host, as well as the HP OpenView applications running on that local host. It lists and categorizes the local services (required by HP OpenView applications) found by scanning the local system. The intuitive GUI enables in-depth analysis, and provides step-by-step guidance with platform-specific instructions. Some, but not all, of these instructions can also be performed automatically by OvProtect. In addition, a powerful command-line interface allows you to perform recurring checks with OvProtect (for example, check the system security aspects on a weekly basis on all deployed OVO HTTPS agents).

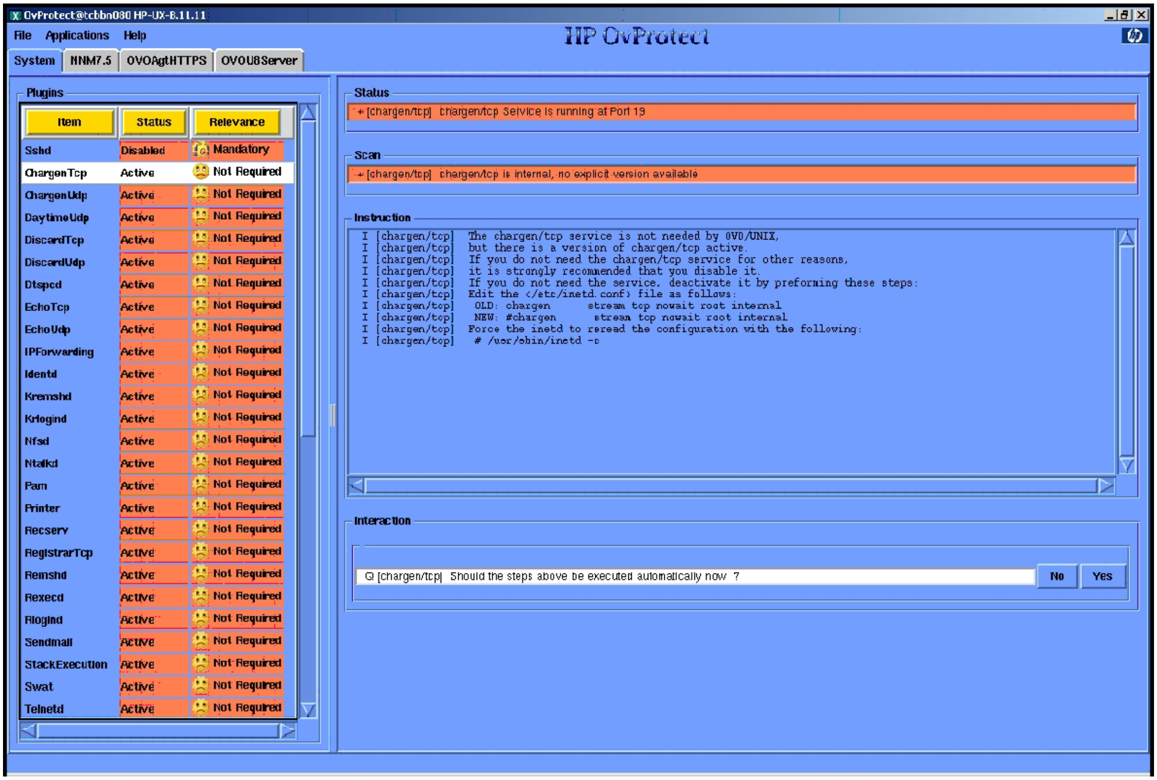
OvProtect is written entirely in Perl, but it is available as one self-contained, platform-specific executable to facilitate the download and installation process. It can be installed anywhere in your file system, and it does *not* require any HP OpenView application to already be installed.

The OvProtect package contains its own *Release Notes* document.

The scan and corrective task functionality for each security item is implemented as a plug-in. Plug-ins are updated or supplemented on a regular basis, and are available on the Internet as free downloads. OvProtect can perform the update and a rescan of the system in one step!

Figure B-1 illustrates how OvProtect lists the security items found by a scan as well as the instructions to solve the issues. The instructions can be executed manually by an administrator or by simply pushing the Yes button in the Interaction frame. The instructions assume that OvProtect was started with administrator privileges.

Figure B-1 Viewing Security Items Found by a Scan



Item	Status	Relevance
Sshd	Disabled	Mandatory
ChargenTcp	Active	Not Required
ChargenUdp	Active	Not Required
DaytimeUdp	Active	Not Required
DiscardTcp	Active	Not Required
DiscardUdp	Active	Not Required
Dtspcd	Active	Not Required
EchoTcp	Active	Not Required
EchoUdp	Active	Not Required
IPForwarding	Active	Not Required
Identd	Active	Not Required
Kremshd	Active	Not Required
Krlogind	Active	Not Required
Nfsd	Active	Not Required
Ntalkd	Active	Not Required
Pam	Active	Not Required
Printer	Active	Not Required
Recserv	Active	Not Required
RegistrarTcp	Active	Not Required
Remshd	Active	Not Required
Rexecd	Active	Not Required
Rlogind	Active	Not Required
Sendmail	Active	Not Required
StackExecution	Active	Not Required
Swat	Active	Not Required
Telnetd	Active	Not Required

```
+ [chargen/tcp]  chargen/tcp Service is running at Port 19
```

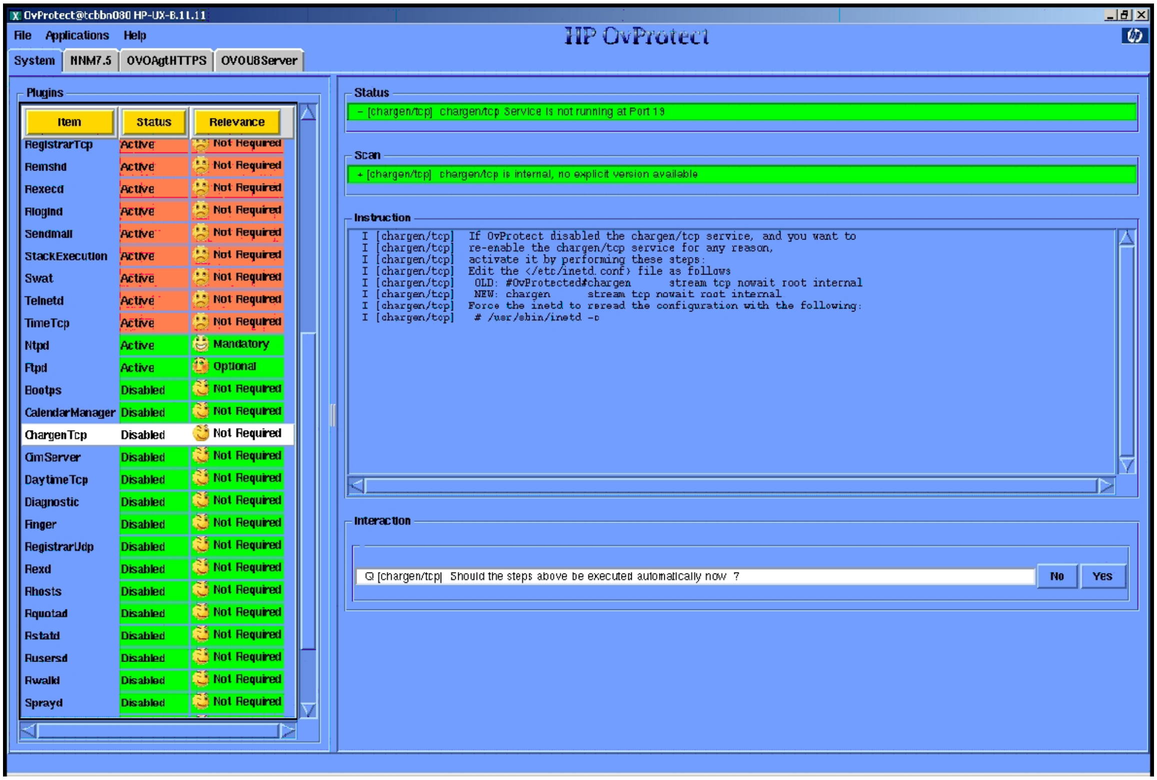
```
+ [chargen/tcp]  chargen/tcp is internal, no explicit version available
```

```
I [chargen/tcp]  The chargen/tcp service is not needed by OVO/UNIX,
I [chargen/tcp]  but there is a version of chargen/tcp active.
I [chargen/tcp]  If you do not need the chargen/tcp service for other reasons,
I [chargen/tcp]  it is strongly recommended that you disable it.
I [chargen/tcp]  If you do not need the service. deactivate it by preforming these steps:
I [chargen/tcp]  Edit the </etc/inetd.conf> file as follows:
I [chargen/tcp]   OLD: chargen      stream tcp nowait root internal
I [chargen/tcp]   NEW: #chargen      stream tcp nowait root internal
I [chargen/tcp]  Force the inetd to reread the configuration with the following:
I [chargen/tcp]   # /usr/sbin/inetd -c
```

```
Q [chargen/tcp]  Should the steps above be executed automatically now ?
```

Figure B-2 illustrates how a previously disabled item can be enabled again (for example, when another application needs this specific service). The administrator can manually perform the instruction steps listed in the Instruction frame, or let OvProtect perform the steps automatically by pushing the Yes button in the Interaction frame.

Figure B-2 Enabling Security Items Found by a Scan



Item	Status	Relevance
RegistrarTcp	Active	Not Required
Remshd	Active	Not Required
Rexecd	Active	Not Required
Rlogind	Active	Not Required
Sendmail	Active	Not Required
StackExecution	Active	Not Required
Swat	Active	Not Required
Telnetd	Active	Not Required
TimeTcp	Active	Not Required
Ntpd	Active	Mandatory
Ftpd	Active	Optional
Bootps	Disabled	Not Required
CalendarManager	Disabled	Not Required
ChargenTcp	Disabled	Not Required
CimServer	Disabled	Not Required
DaytimeTcp	Disabled	Not Required
Diagnostic	Disabled	Not Required
Finger	Disabled	Not Required
RegistrarUdp	Disabled	Not Required
Rexd	Disabled	Not Required
Rhosts	Disabled	Not Required
Rquotad	Disabled	Not Required
Rstatd	Disabled	Not Required
Rusersd	Disabled	Not Required
Rwalld	Disabled	Not Required
Sprayd	Disabled	Not Required

```
- [chargen/tcp]  chargen/tcp Service is not running at Port 19
```

```
+ [chargen/tcp]  chargen/tcp is internal, no explicit version available
```

```
I [chargen/tcp]  If OvProtect disabled the chargen/tcp service, and you want to
I [chargen/tcp]  re-enable the chargen/tcp service for any reason,
I [chargen/tcp]  activate it by performing these steps:
I [chargen/tcp]  Edit the </etc/inetd.conf> file as follows
I [chargen/tcp]   OLD: #OvProtected#chargen      stream tcp nowait root internal
I [chargen/tcp]   NEW: chargen      stream tcp nowait root internal
I [chargen/tcp]  Force the inetd to reread the configuration with the following:
I [chargen/tcp]   # /usr/sbin/inetd -c
```

```
Q [chargen/tcp]  Should the steps above be executed automatically now  ?
```

An audit trace and backup of system files modified by OvProtect are generated for each execution of OvProtect.

Disclaimer

The system administrator *must* back up the system before modifying it with OvProtect.

OvProtect is not a general system administration tool. It does *not* supersede any of the other well-known security assessment tools! The administrator must still to follow the operating system vendor's security advisories, as well as other well-known sources of security information.

NOTE OvProtect is not a replacement for the *HP OpenView Security Advisory* document, but a supplement. Not all relevant security aspects are covered by OvProtect.

Download

OvProtect and the plug-ins are available for download at the following location:

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

License

OvProtect is free of charge for customers who have a valid HP OpenView LTU. OvProtect is independent of any specific OV Application LTU and of any specific OV support contract.

The support is offered on a "best effort basis." In case of service or enhancement requests, use your typical HP support chain to log your request.

The underlying Perl and Perl modules follow the Perl "Artistic license."

Index

Index