

HP ProLiant Essentials Vulnerability and Patch Management Pack

Installation Poster



Legal notices

© Copyright 2004, 2006 Hewlett-Packard Development Company, L.P

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.

The information contained herein is subject to change without notice. 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.

Adobe and Acrobat are trademarks of Adobe Systems Incorporated. Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation. Windows Server 2003 is a U.S. trademark of Microsoft Corporation.

Part number: 367561-005

Fifth edition: September 2006



Overview

The HP ProLiant Essentials Vulnerability and Patch Management Pack extends the functionality of HP Systems Insight Manager (HP SIM) to provide vulnerability and patch management for target systems.

This document provides basic information about installing and using the Vulnerability and Patch Management Pack. The Vulnerability and Patch Management Pack and HP SIM can be installed together on a single server (referred to as a shared configuration), or each component can be installed on a separate server (referred to as a distributed configuration).

For detailed infrastructure, installation, configuration, and usage information, see the *HP ProLiant Essentials Vulnerability and Patch Management Pack User Guide*.

Prerequisites

The following prerequisites must be met to properly install the Vulnerability and Patch Management Pack.

VPM server requirements

The VPM server, the server on which the Vulnerability and Patch Management Pack software is installed, must meet the following hardware and software requirements. Requirements listed for the VPM server are independent of requirements for HP SIM and any other applications that coexist on the VPM server. For specific hardware and software requirements for the HP SIM server, see the *HP Systems Insight Manager Installation and User Guide*.

- A supported operating system:
 - Microsoft® Windows® 2000 Server SP4
 - Windows Server™ 2003 SP1
 - Windows XP Professional SP1
- Microsoft Internet Information Services (IIS) 5.0 or later, installed and running



IMPORTANT: HP strongly recommends enabling HTTPS if HP SIM and the Vulnerability and Patch Management Pack are installed on separate servers. To configure HTTPS service, see <http://support.microsoft.com/?kbid=324069>

- TCP/IP, with DNS properly configured so that system names can be resolved to IP addresses
- The following applications available either on the VPM server or on the network:
 - HP SIM 5.0 SP2 or later, installed on a Windows server with Windows Management Instrumentation (WMI) Mapper
 - Microsoft Internet Explorer 6.0 or later
 - Adobe® Acrobat® Reader 3.x or later (to view scan results)

- Any HP ProLiant server with:
 - At least 512 MB RAM
 - 1.5-GHz or higher processor
 - 1 GB available disk space for the Vulnerability and Patch Management Pack (150 MB in the TEMP directory for installation)
 - Additional disk space for scan reports and patches
 - New Technology File System (NTFS)
 - CD-ROM drive

HP Systems Insight Manager

HP SIM 5.0 SP2 or later must be installed and running in the server environment to properly install and use the Vulnerability and Patch Management Pack. HP SIM must be installed on a Windows server.

If you are not currently running HP SIM 5.0 SP2 or later, select one of the following migration paths depending on your server environment. For server environments currently using:

- **Systems Insight Manager 4.2**—Install HP SIM 5.0 SP2 or later.
- **Systems Insight Manager 4.1**—See the *HP Systems Insight Manager Installation and User Guide* for upgrade information.
- **Insight Manager 7**—See the *HP Systems Insight Manager Installation and User Guide* to upgrade to HP SIM 5.0 SP2 or later. Use the provided data migration tools to migrate key management data and configuration settings.
- **Neither Systems Insight Manager nor Insight Manager 7**—See the *HP Systems Insight Manager Installation and User Guide* to install HP SIM 5.0 SP2 or later.

For additional information about HP SIM, see <http://www.hp.com/go/hpsim>

Installing the Vulnerability and Patch Management Pack

Preinstallation steps

New versions of the Vulnerability and Patch Management Pack are automatically installed over a previous version. Any scheduled tasks, scan reports, and patch updates are retained.

1. Determine the appropriate Vulnerability and Patch Management Pack infrastructure for your server environment. The Vulnerability and Patch Management Pack and HP SIM can be installed together on a single server, or each component can be installed on a separate server.
2. Be sure to have the following items available before beginning the installation.
 - Location and credentials for HP SIM (user name, password, and domain)
 - Credentials for the VPM server, if installing on other than HP SIM server
 - Credentials for the Microsoft SQL Server database, if an existing SQL Server database will be used
3. Be sure HP SIM 5.0 SP2 or later and IIS are installed, properly configured, and running.

Installing from the Insight Control Data Center Edition DVD



IMPORTANT: HP SIM will be restarted after the Vulnerability and Patch Management Pack installation.



NOTE: The installation can take up to 20 minutes, depending on the speed of the server

1. Insert the Insight Control Data Center Edition DVD into the DVD-ROM drive of the intended VPM server. The ProLiant Essentials Software End User License Agreement appears. Click **Agree**.
2. At the Welcome screen, click **Run Installer...** to open the configuration wizard and initiate the installation process, or click on the **Products** tab to do a manual installation.
3. The prerequisites for installing the Vulnerability and Patch Management Pack are listed. Verify that all requirements are met before you perform the installation, and click **Next**.
4. Select a location for the installation files, and click **Next**.
5. At the Software Selection screen, select **HP ProLiant Essentials Vulnerability and Patch Management Pack**, and click **Next**.
6. Follow the onscreen instructions, entering your user-specific information when prompted.

Installing from the VPM download website

1. After downloading the Vulnerability and Patch Management Pack, double-click **setup.exe** to start the installation.
2. Follow the onscreen instructions, entering your user-specific information when prompted. Enter the same credentials used when installing HP SIM.
3. When the installation is complete, log in to HP SIM from an account with administrator privileges to access the Vulnerability and Patch Management Pack.

Installing the VPM Acquisition Utility (optional)

The VPM Acquisition Utility can be installed on a system with Internet access, allowing patch acquisitions and vulnerability updates without requiring the VPM server to be directly connected to the Internet.



IMPORTANT: In both a distributed and shared configuration, the VPM Acquisition Utility cannot be installed on the VPM server nor the HP SIM Central Management System (CMS).

For requirements for the system on which the VPM Acquisition Utility is installed, see the *HP ProLiant Essentials Vulnerability and Patch Management Pack Support Matrix*.

To install the VPM Acquisition Utility:

1. Insert the Insight Control Data Center Edition DVD into the DVD-ROM drive of the system on which patch and vulnerability updates will be obtained. The ProLiant Essentials Software End User License Agreement appears. Click **Agree**.

2. At the Welcome screen, click the **Products** tab and then select **Vulnerability and Patch Management Pack** from Foundation Management Products.
3. At the top of the screen, under HP ProLiant Essentials Vulnerability and Patch Management Pack, click **Install...**
4. At the Welcome screen, click **Install**.
5. At the Software Selection screen, select **VPM Acquisition Utility**, and click **Next**.
6. Follow the onscreen instructions to complete the installation.

Post-installation configuration steps

After the Vulnerability and Patch Management Pack is installed for the first time, perform the following steps to complete the configuration and install the latest vulnerability updates.



NOTE: An administrator can add new users and set up existing users to access the Vulnerability and Patch Management Pack. For instructions, see the *HP Systems Insight Manager Installation and User Guide*.

-
1. Log in to HP SIM from an account with administrator privileges.
 2. Configure global Web Based Enterprise Management (WBEM) credentials to enable access to target systems.
 - a. Select Options>Protocol Settings>Global Protocol Settings.
 - b. Configure settings for the \user account if the Vulnerability and Patch Management Pack is located on the HP SIM server or for the DOMAIN\user account if the Vulnerability and Patch Management Pack is on a separate server. Enter the Windows administrator account credentials in the Default 1 field and Red Hat administrator group credentials in the Default 2 field.
 - c. Click **OK**.



NOTE: If some target systems use individual administrator credentials, see the user guide for information about configuring System Protocol Settings.

-
3. Perform an automatic discovery to locate and identify target systems in the network that can be used with the Vulnerability and Patch Management Pack. For information, see the *HP Systems Insight Manager Installation and User Guide*.
 4. Modify the Vulnerability and Patch Management Pack settings:
 - a. Select Options>Vulnerability and Patch Management>Settings.
 - b. Select the source where patch and vulnerability updates will be obtained.
 - If the VPM server has direct Internet access, select **Acquire updates from Internet** to use the VPM server to obtain updates. If you use a proxy server, select the appropriate checkbox and enter your configuration information. If the proxy requires authentication, select the appropriate checkbox and enter your user credentials. Only basic (not encrypted) authentication is supported.

- If the VPM server does not have Internet access, select **Acquire updates from local repository** to use the VPM Acquisition Utility on another system with Internet access to acquire updates. The update files can either be manually relocated to the VPM server or accessed from the network. Designate the directory path where the update files will be located in the Source path field. If necessary, enter user credentials to access the designated directory. The VPM server must have read access to the designated directory.
 - c. Click **Apply**.
5. If Red Hat patch acquisitions will be run:
 - a. Verify the Red Hat library, `compat-libstdc++`, is installed on all Red Hat target systems.
 - b. Verify that each Red Hat target system to be patched has a valid subscription and license for the Red Hat Network, which are required for patch acquisitions. For information about subscribing to the Red Hat Network, see <http://www.redhat.com>
 - c. Log in to a Red Hat Enterprise Linux 2.1, 3, or 4 system as `root`.
 - d. Execute the following command:


```
rhn_register
```
 - e. Select **Existing**, and enter your user credentials.
 - f. Enter a unique profile name for this machine (such as the IP address or host name).
 - g. Exit the `rhn_register` application without applying any patches to the system.
 - h. Copy the file created by the `rhn_register` tool from `/etc/sysconfig/rhn/systemid` to `C:\Program Files\HP\VPM\radia\IntegrationServer\etc`.
 - i. Rename the `systemid` file to reflect the appropriate Red Hat distribution.
 - If the system that created the `systemid` file was running Red Hat Enterprise Linux 4, rename the file "redhat•4es.sid."
 - If the system that created the `systemid` file was running Red Hat Enterprise Linux 3, rename the file "redhat•3es.sid."
 - If the system that created the `systemid` file was running Red Hat Enterprise Linux 2.1, rename the file "redhat•2.1es.sid."
 6. Acquire the latest Vulnerability and Patch Management Pack updates, either from the VPM server or using the VPM Acquisition Utility installed on another system. The first update process after the initial software installation can take a long time, depending on the number of patch sources selected and the quantity of updates available from each source.



NOTE: HP updates and vulnerability scan definition files are always automatically downloaded.

- a. From the VPM server:
 - Select **Options>Vulnerability and Patch Management>Acquire Updates**.
 - Follow the onscreen instructions, selecting the appropriate update information for your server environment as prompted.

- Click **Schedule**, and select a suitable time to acquire daily Vulnerability and Patch Management Pack updates. Updates might not be available daily, but scheduling the event daily ensures that critical updates are obtained promptly.
 - Select the **Run now** checkbox to run the initial patch acquisition, and click **Done**. Progress can be monitored at C:\Program Files\HP\VPM\Radia\IntegrationServer\logs\patch-acquire.log.
- b.** Using the VPM Acquisition Utility:
- Access the VPM Acquisition Utility from the selected system.
 - Follow the onscreen instructions, selecting the appropriate update information for your server environment as prompted.
 - Click **Run Now** to run the patch acquisition. Patch acquisition progress can be monitored at C:\Program Files\HP\VPM Acquisition Utility\logs\patch-acquire.log.
 - Click **Done** when the acquisition process is complete.
 - On the VPM server, create a directory named “data” at C:\Program Files\HP\VPM\Radia\IntegrationServer. You can use a network share if the VPM server has read access to the share.
 - Copy downloaded files from the VPM Acquisition Utility server destination directory to the VPM server data directory.
 - From HP SIM, configure your import setting by selecting **Options>Vulnerability and Patch Management>Settings**.
 - Start the import process by selecting **Options>Vulnerability and Patch Management>Acquire Updates**.

The Vulnerability and Patch Management Pack interface

From the HP SIM toolbar menu, access the Vulnerability and Patch Management Pack installation.

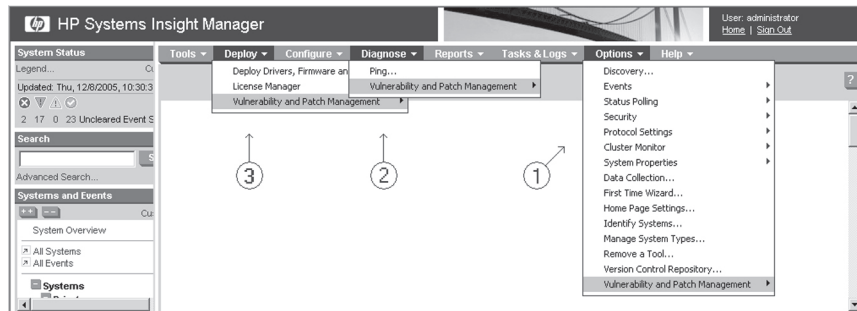


Table 1 lists the appropriate menu to select from the HP SIM toolbar, as illustrated in the previous figure, to initiate a Vulnerability and Patch Management Pack action.

Table 1 Vulnerability and Patch Management Pack interface

Menu	Action
1	Configure settings and acquire updates.
2	Perform or customize vulnerability scans, and view scan results, patch installation status, patches installed by VPM, patch reboot status, and the patch repository.
3	Deploy or remove patches and fixes, validate installed patches, and deploy the VPM Patch Agent.

Licensing systems

The Vulnerability and Patch Management Pack requires one license for each target system being managed.



IMPORTANT: After a license is applied to a specific system, the license cannot be removed or transferred to another system.



IMPORTANT: On a physical Vulnerability and Patch Management Pack kit, the license key is located on the back of the kit.

Five fully functional permanent licenses for use on servers or client systems are provided with the Vulnerability and Patch Management Pack for evaluation purposes. These licenses are available after the Vulnerability and Patch Management Pack is installed and can be applied to systems from the License Manager or as part of the sequence initiating a licensed function, such as scanning or patching.

To purchase additional licenses, see the Vulnerability and Patch Management Pack website at

<http://www.hp.com/go/vpm>

For additional information about licensing, see the user guide.

Scanning for vulnerabilities

1. Select **Diagnose>Vulnerability and Patch Management>Scan>Scan for Vulnerabilities**.
2. Select the target systems to scan by selecting a group from the dropdown list or by selecting the checkbox next to individual systems.
3. Click **Apply**.
4. Verify that the correct target systems appear in the lists, click **Add Targets** or **Remove Targets** if it is necessary to reselect target systems, and then click **Next**.
5. If any selected systems are unlicensed or licensed with a time-limited license, permanent licenses can be applied at this time. If licenses are available, select any unlicensed system in the list to license, and click **Apply License**. Server and client licenses are automatically applied to the appropriate systems, if available.
6. Click **Next**.

7. Enter a name for the vulnerability scan, select a scan definition, and click **Run Now** to run the scan immediately.
8. View scan results after the task completes by clicking the system status icon or viewing the VPM Events list.

For additional information about vulnerability scanning and creating customized scans, see the user guide.

Deploying patches and fixes

To deploy patches and configuration fixes after a vulnerability scan is complete:

1. Select **Deploy>Vulnerability and Patch Management>Patch-Fix Based on a Scan**.
2. Select the completed vulnerability scan, and click **Next**.
3. Select the vulnerabilities to patch or fix, and click **Next**.
4. Select the systems on which to apply patches or fixes, and click **Next**.
5. Designate when the patched systems should be rebooted, and click **Run Now** to deploy patches or fixes immediately.
6. View task results in the VPM Events list after the task completes.

For additional information about deploying patches, see the user guide.

Support and information

For HP support and software updates, see the Vulnerability and Patch Management Pack website at

<http://www.hp.com/go/vpm>

For the name of the nearest HP authorized reseller:

- In the United States, see http://www.hp.com/service_locator
- In other locations, see <http://www.hp.com>

For HP technical support:

- In North America:
 - Call 1-800-HP-INVENT (1-800-474-6836). This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored.
 - If you have purchased a Care Pack (service upgrade), call 1-800-633-3600. For more information about Care Packs, see the HP website <http://www.hp.com>
- Outside North America, call the nearest HP Technical Support Phone Center. For telephone numbers for worldwide Technical Support Centers, see the HP website <http://www.hp.com>