HP ProLiant Essentials Vulnerability and Patch Management Pack

Quick Setup Poster

Third Edition (July 2005)
Part Number 367561-003

Overview

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

This document provides basic information about installing and using Vulnerability and Patch Management Pack. Vulnerability and Patch Management Pack and HP SIM can be installed together on a single server, or each component can be installed on a dedicated server.

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

Prerequisites

The following prerequisites must be completed for Vulnerability and Patch Management Pack to function properly.

HP Systems Insight Manager

HP SIM 4.2 SP2 or HP SIM 5.0 must be installed and running in the server environment to properly install and use Vulnerability and Patch Management Pack. HP SIM must be installed on a Microsoft® Windows® server.

If you are not currently running HP SIM 4.2 SP2 or HP SIM 5.0, select one of the following migration paths depending on your server environment. For server environments currently using:

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

For additional information about HP SIM, refer to http://www.hp.com/go/hpsim.

VPM server software requirements

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

IMPORTANT: HP strongly recommends enabling HTTPS if HP SIM and Vulnerability and Patch Management Pack are installed on separate servers. For information about configuring HTTPS service, refer to 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 must be available either on the VPM server or on the network:
  - HP SIM 4.2 SP2 or HP SIM 5.0, 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)

VPM server hardware requirements

NOTE: Requirements listed for the VPM server are independent of requirements for HP SIM. For details about HP SIM requirements, refer to the *HP Systems Insight Manager Installation and User Guide.*

Vulnerability and Patch Management Pack can be installed on any ProLiant server meeting the following requirements:

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

1 Installing Vulnerability and Patch Management Pack

Preinstallation information

NOTE: If a previous version of Vulnerability and Patch Management Pack is already installed, this upgrade can be installed over the existing version, retaining any scheduled tasks, scan reports, and patch updates

1. Determine the appropriate Vulnerability and Patch Management Pack infrastructure for your server environment. Vulnerability and Patch Management Pack and HP SIM can be installed together on a single server, or each component can be installed on a dedicated server.
2. Be sure to have the following items available before beginning the Vulnerability and Patch Management Pack installation.
   - Location and credentials for HP SIM (username, password, and domain)
   - Credentials for the local server, if installing on other than HP SIM server
3. Be sure HP SIM 4.2 SP2 or HP SIM 5.0 and IIS are installed and running.

Installing from the Management CD

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

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

1. Insert the Management CD into the CD-ROM drive of the intended VPM server. An autorun menu appears.
2. Click **Install** under HP ProLiant Essentials Vulnerability and Patch Management Pack.
3. At the welcome screen, click **Install.**
4. At the Software Selection screen, select **Vulnerability and Patch Management Pack,** and click **Next.**
5. Follow the on-screen instructions, entering your user-specific information when prompted.

Installing from the VPM download website

1. After downloading Vulnerability and Patch Management Pack, double-click **setup.exe** to start the installation.
2. Follow the on-screen instructions, entering your user-specific information when prompted. Enter the same credentials used when installing HP SIM.

When the installation is complete, log in to HP SIM from an account with administrator privileges to access Vulnerability and Patch Management Pack.

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

Installing the VPM Acquisition Utility

The VPM Acquisition Utility can be installed on any system with Internet access to acquire patch information and patch files from selected vendor websites. This utility provides the ability to acquire patches and vulnerability updates without requiring the VPM server to be directly connected to the Internet, thereby reducing potential security risks. No other Vulnerability and Patch Management Pack components or database software are required to be installed on the system to download vulnerability and patch updates.

To install the VPM Acquisition Utility:

1. Insert the Management CD into the CD-ROM drive of the system where patch and vulnerability updates will be obtained. An autorun menu appears.
2. Click **Install** under HP ProLiant Essentials Vulnerability and Patch Management Pack.
3. At the welcome screen, click **Install.**
4. At the Software Selection screen, select **VPM Acquisition Utility,** and click **Next.**
5. Follow the on-screen instructions to complete the installation.

2 Post-installation configuration steps

After 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.

1. Configure global Web Based Enterprise Management (WBEM) credentials to enable access to target systems.

IMPORTANT: This configuration step must be completed for Vulnerability and Patch Management Pack to function properly.

   a. Select **Options>Protocol Settings> Global Protocol Settings.**
   b. Configure the WBEM credentials for the \user account if Vulnerability and Patch Management Pack is located on the HP SIM server or for the DOMAIN\user account if Vulnerability and Patch Management Pack is on a separate server.
   c. Enter the Windows administrator account credentials in the Default 1 field and Red Hat administrator group credentials in the Default 2 field.
   d. Click **OK.**

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

2. From within HP SIM, perform an Automatic Discovery to locate and identify target systems in the network that can be used with Vulnerability and Patch Management Pack. Refer to the *HP Systems Insight Manager Installation and User Guide* for information.
3. Configure your 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** if you want 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.** The VPM Acquisition Utility can be installed on another system with Internet access and used 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.
   c. Click **Apply.**
4. If Red Hat patch acquisitions will be run, verify the Red Hat library, compat-libstdc++, is installed on the Red Hat target systems.
5. If Red Hat patch acquisitions will be run, configure Red Hat Enterprise Linux acquisition settings:

IMPORTANT: Red Hat systems must have a valid subscription to the Red Hat Network for patch acquisitions. A valid Red Hat Network license is required for each system to be patched. For information about subscribing to the Red Hat Network, refer to http://www.redhat.com.

   a. Log in to a Red Hat Enterprise Linux 2.1, Red Hat Enterprise Linux 3, or Red Hat Enterprise Linux 4 system as `root`.
   b. Execute the following command:

```
rhn_register
```

   c. Select **Existing,** and enter your user credentials.
   d. Enter a unique profile name for this machine (such as the IP address or host name).
   e. Exit the rhn_register application without applying any patches to the system.
   f. Copy the file created by the rhn_register tool from /etc/sysconfig/rhn/systemid to C:\Program Files\ HP\VPM\radia\IntegrationServer\etc.
   g. Rename the systemid file to reflect the appropriate Red Hat distribution. For example:
   – 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 on-screen 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.
   – Select one or more sources from which to acquire patch updates, and click **Next.**
   – Select the appropriate operating system platforms and platform related applications, and click **Next.**
   – Select the appropriate languages for the required patches, and click **Schedule.**
   – Enter the appropriate destination path for downloaded files, either a local or accessible shared directory.
   – If you use a proxy, select the **I use a proxy** checkbox, and enter the appropriate configuration information.
   – If your proxy requires authentication, select the **My proxy requires authentication** checkbox, and enter the appropriate user credentials. Only basic (not encrypted) authentication is supported.
   – Click **Next.**
   – Click **Run Now** to run the patch acquisition. The vulnerability and patch acquisition begins. 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.**

3 Navigating the Vulnerability and Patch Management Pack interface

The HP SIM toolbar menu is expanded with the Vulnerability and Patch Management Pack installation, as shown in the following figure.

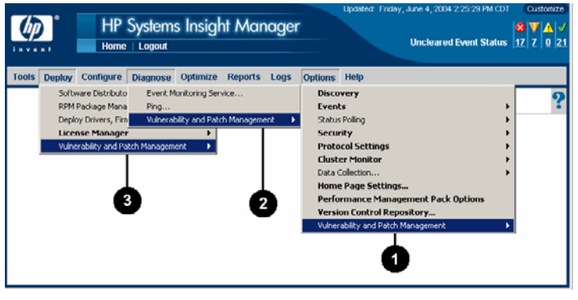

Table 1 lists the appropriate menu to select from the HP SIM toolbar, as illustrated in the previous figure, to initiate a Vulnerability and Patch Management Pack action.

Table 1: Vulnerability and Patch Management Pack interface

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

4 Licensing systems

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 non-expiring licenses for use on servers or desktops are provided with ProLiant Essentials Vulnerability and Patch Management Pack for evaluation purposes. These licenses are available after 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, refer to the Vulnerability and Patch Management Pack website at http://www.hp.com/servers/proliantessentials/vpm. For additional information about licensing, refer to the user guide.

5 Scanning for vulnerabilities

1. Select **Diagnose>Vulnerability and Patch Management> Scan>Scan for Vulnerabilities.**
2. Either select **All systems in the list,** selecting a parameter for selecting systems, or select **Individual systems in the list,** selecting the checkbox next to the systems to scan. Click **Apply Selections.**
3. Verify the selected target systems, click **Change Targets** if it is necessary to go back and reselect target systems, and then click **Next.**
4. If any selected systems are unlicensed, available licenses can be applied by selecting the systems and clicking **Apply License>Next.**
5. Enter a name for the scan, and select a scan definition.
6. To run the scan immediately, click **Run Now.**
7. View scan results after the task completes either by clicking the system status icon or viewing the VPM Events list.

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

6 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 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.
5. Designate when the patched systems should be rebooted.
6. To deploy patches immediately, click **Run Now.**
7. View task results in the VPM Events list after the task completes.

For additional information about deploying patches, refer to the user guide.

Support and information

For HP support and software updates, refer to the Vulnerability and Patch Management Pack website at http://www.hp.com/servers/proliantessentials/vpm.

HP Customer Support provides 90 days of phone-based support with Monday through Friday, 9-to-5 service coverage hours in your local time zone. For information:

- In North America, call 1-800-HP INVENT (1-800-474-6836). For continuous quality improvement, calls may be recorded or monitored.
- Outside North America, call the nearest HP Technical Support Phone Center. For telephone numbers for worldwide Technical Support Centers, refer to http://www.hp.com/support.