1 Release Notes

06 May 2005

This document provides an overview of the changes made to HP OpenView Patch Manager Using Radia Version 2 Service Pack 1. Application of the materials supplied in this Service Pack upgrade HP Openview Patch Manager using Radia from Version 2.0 to Version 2.0, Release 2.0.1.

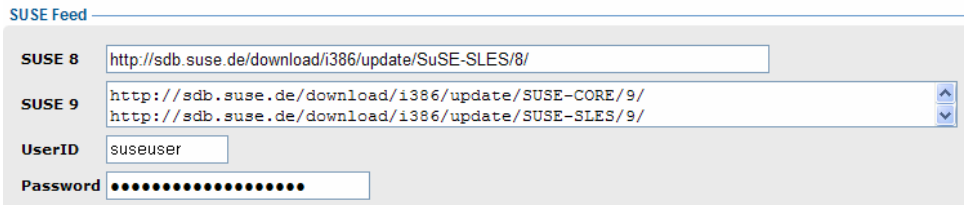
It contains important information not included in the manuals or in online help.

In This Version

- Patch acquisition and management capabilities have been added for SUSE Linux Enterprise Server Versions 8 and 9. For the purpose of SUSE security patch acquisition, you must establish a User ID and Password through your SUSE Linux vendor to access SUSE internet resources. These updates are reflected in:

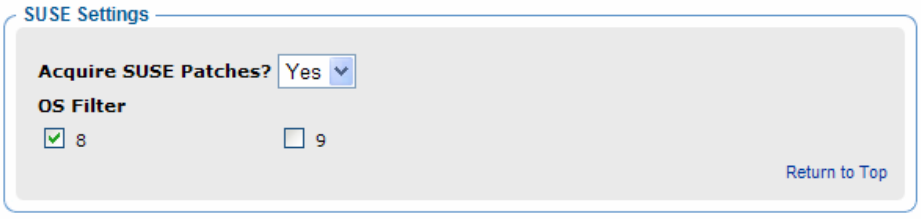
  — A new section in the Radia Administrator Configuration Settings Page for SUSE. The following settings are configured in the SUSE Feed section:

SUSE 8	Specify the url for acquiring updates for SUSE 8. This is set in the suse_urls parameter in patch.cfg. **Default:** http://sdb.suse.de/download/i386/update/SuSE-SLES/8/
SUSE 9	Specify the url for acquiring updates for SUSE 9. This is set in the suse_urls parameter in patch.cfg. **Defaults:** http://sdb.suse.de/download/i386/update/SUSE-CORE/9/ http://sdb.suse.de/download/i386/update/SUSE-SLES/9/
UserID	Specify your SUSE user ID. This is the same as the suse_user parameter in patch.cfg. Obtain a user id from the vendor.
Password	Specify the password for the SUSE UserID. This is the same as the suse_pass parameter in patch.cfg.



  — New values available for Acquisition parameters for SUSE.

Acquire SUSE Patches?	Select **Yes** if you want to acquire SUSE Patches. A list of operating system filters appears.
OS Filter	Select operating systems for the acquisition of SUSE Enterprise Server Linux security patches. This is the same as the vendor_os_filter parameter in patch.cfg.



  — The vendors parameter accepts a value of SUSE.

  — The vendor_os_filter parameter accepts the values of suse::8,suse::9.

  Note: All SUSE security advisories (bulletins) begin with the prefix of "SUSE". To acquire all SUSE bulletins, type SUSE* in the Bulletins field. In addition, some SUSE Security Advisories may take over 20 minutes to download. To account for this, consider increasing the HTTP Timeout parameter to value greater than 1200 seconds.

Support has been added for RedHat 4 security advisories for Advanced Server (AS) , 4 Enterprise Server (ES), and 4 Workstation (WS). This is reflected in the OS Filter options in the RedHat Settings for acquisition, and the vendor_os_filter option in patch.cfg. Acquisition of Red Hat Security Advisories requires a Red Hat Network account with at least one license for each of the Red Hat Enterprise Server OS versions for which you want to acquire and manage patches.

Note: Both Red Hat Security Advisory and SUSE Security Advisory removal is disabled deliberately in Radia Patch Manager. When a Linux vendor supplied patch is applied to a target system, the affected Linux software is updated to the current rpm package version and release that addresses the specific security vulnerability. Application of a Linux vendor supplied advisory (patch) does not maintain a backup of the original package, making automated rollback to a prior version impossible. An attempt to remove a Linux rpm package from a client computer would result in the removal of the patch as well as the rpm software package to which the patch applies. If a new vulnerability is found, Linux Security patch vendor's release a new patch. This is the nature of Red Hat and SUSE Security Advisories as provided by these patch vendors.

- This service pack was designed to alleviate performance issues found in the Radia Patch Manager and Radia Reporting Server patch reports. The scripts, zobjstat.sql and zobjstat.ora, contained in this service pack are intended to be used to split the nvd_zobjstat table entries into separate tables. Execution of the applicable script is a requirement for the reporting changes, The new tables created by running the scripts will cause Radia Patch Manager reports rendered through the Radia Integration Server to be disabled. Compliance, Research, and Acquisition reports will be available only through the Radia Reporting Server Version 4.1 with the object pack from this service pack applied.
- This service pack includes the following new features for Patch reporting through the Radia Reporting Server.
  - Compliance Exception Report
  - Research Exception Report
  - Filtering by Compliance Status for any compliance top level report
  - Drill down for graphical patch reports
  - Filter Lookup for Compliance Status

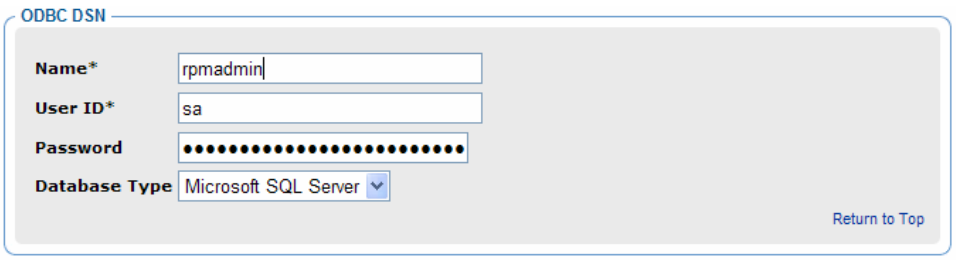
  The Compliance and Research Exception Reports were introduced to provide information about devices that do not meet the criteria for the standard research and compliance device reports. All of the devices in these exception reports are in some sort of exception state. The three main reasons for exception states are:
  - connection errors encountered during vulnerability and patch discovery
  - an acquisition was performed with force and replace options, that caused a disconnect between Security bulletin data and the client's status information
  - an inoperable Patch Client Agent

  To resolve the exception, HP recommends performing a new discovery on the device. The new discovery will either resolve the error, in the case of connectivity problems or resolve the disconnect between newly replaced bulletins and the agent status information. In addition, it will produce logs that can be used to troubleshoot the inoperable Patch Client Agent. The research exception report will likely show only a subset of the devices in the compliance exception report because the criteria for the research reports are less restrictive.

- A new parameter has been added to the Radia Patch Manager Administrator's DSN settings to specify the database type. This is the same as the db_type parameter in patch.cfg. The two possible values are mssql for Microsoft SQL Server and oracle for Oracle. Mssql is the default value.

  Note: If you are using Oracle, be sure to change this value to oracle before doing a patch acquisition or a database synchronization, failure to make this alteration would result in an error messages similar to:

  ```
  Error synchronising SQL Database S1000 1735 {[Oracle][ODBC][Ora]ORA-01735:
  invalid ALTER TABLE option Error synchronising SQL Database command "slave"
  already exists in namespace "::sync"
  ```



Installation Notes

Installation requirements, as well as instructions for installing HP OpenView Patch Manager Using Radia version 2, are documented in the *HP OpenView Patch Manager Using Radia Guide* provided on the technical support site. The minimum build of nvdkit is build 153 for Server components.

Note: Before installing this service pack, make sure that you are using the Version 4 Infrastructure Products including HP Openview Patch Manager Using Radia Version 2, and HP OpenView Reporting Server Using Radia Version 4.1.

Prerequisites

- Apply Radia Messaging Server 2.0 Service Pack 1. (Radia Messaging Server Service Pack 1, media is supplied separately)
- Confirm that your Radia Reporting Server is at version 4.1 before applying the service pack. Your Radia Reporting Server is at version 4.1 if you see a "?" icon on the top right section of the Radia Reporting Server Graphical Interface. Clicking this icon will bring up a small window with the current version and build numbers. If you do not see this icon, you are not at version 4.1 and need to upgrade your Radia Reporting Server before applying the service pack.
- Confirm that your Radia Integration Server patch environment is version 2.0 before applying the service pack. You can check your Radia Integration Server Patch environment two ways, either by placing your mouse over the Radia Patch Administrator Heading in the Radia Integration Server Patch graphical Interface (http://localhost:3466/patch/manage/admin.tsp) where it will display text regarding the version and build similar to "Patch Manager Version 2.0.0 Build 267" or by checking the contents of the log file httpd-port#.log for the following line.

  ```
  Info: patch: Radia Patch Manager Reporting - Version 2.0.0 - Build 267.
  ```

  If you see anything less than version 2.0.0 in either of these places, your Radia Integration Server Patch environment is not at version 2.0 and needs to be upgraded prior to applying the service pack.

To apply the service pack

1. Confirm that the Radia Messaging Server is stopped, and wait for any operations on the Radia Patch Manager database such as a database synchronization or patch acquisition to complete.

Note: The Radia Messaging Server Version 2.0 Service Pack 1 installation instructions state to leave the Radia Messaging Server stopped.

2. Stop the Radia Integration Server on the computer running the Radia Patch Manager module.
3. Back up the current `IntegrationServer\modules\patch.tkd`.
4. Copy the new `patch.tkd` supplied in the service pack media's `\Messaging Server` directory to the `IntegrationServer\modules` directory.
5. Edit your IntegrationServer\etc\patch.cfg configuration file and modify the PRODUCT attribute adding the text "SUSE::!sles*-yast2,SUSE::!sles*-yast2-*,SUSE::!sles*-liby2*" immediately before the closing brace of the PRODUCT attribute as shown below.

   Before:

PRODUCT {!Windows 95,!Windows 98*,!Windows Me}

After:

PRODUCT {!Windows 95,!Windows 98*,!Windows Me,SUSE::!sles*-yast2,SUSE::!sles*-yast2-*,SUSE::!sles*-liby2*}

Note: Failure to change the PRODUCT attribute value of the IntegrationServer\etc\patch.cfg configuration file could result in the application of SUSE Linux patches for the “yast” and “liby2” products. The application of patches for those products using the SUSE native program "online_update" may cause future patch applications to fail due to incompatible shared library dependencies.

6 Back up your ReportingServer directory.

7 Unzip the contents of the Radia Reporting Server Patch Object pack, `rrspatchobjects_sp1.zip`, located in the Service Pack’s `Reporting Server` directory, into to the …`ReportingServer\objects\english` directory.

8 Back up your `MessagingServer\etc\rms.cfg` file.

Note: Perform the following changes to the rms.cfg only on the Radia Messaging Server used to post to your Patch ODBC database. If you are using multiple Radia Messaging Servers in your environment, only the Radia Messaging Server posting to the Patch ODBC database needs to be upgraded as directed below.

9 Use a text editor to modify `MessagingServer\etc\rms.cfg`.

a *Replace* the text shown below in `rms.cfg` with the *entire* contents of `replacepatchroutersection.cfg` file located in the service pack’s `media\Messaging Server` directory. This text is in the msg::register_router section.

```
ROUTE       {
    TO      PATCH
    USE     patch
}
```

b *Replace* the word **patch** in the text shown below in `rms.cfg` with the word **patchodbc**.

```
msg::register patch {
  TYPE          ODBC
  DSN           "patch"
  USER          "rpmuser"
  PASS          "password"
}
```

When you have made the replacement, the result should look like:

```
msg::register patchodbc {
  TYPE          ODBC
  DSN           "patch"
  USER          "rpmuser"
  PASS          "password"
}
```

c *Copy* the entire contents of `appendtopatchodbc.cfg` located in the `media\Messaging Server` directory. Insert it before the closing brace in the patchodbc section shown in the previous step.

d *Append* the entire contents of the `newpatchfiltersection.cfg` file located in the `media\Messaging Server` directory to the end of the `rms.cfg` file.

e *Remove* the following lines if they are in your `rms.cfg`:

```
vfs::auto $Config(ROOT)/modules/patch.tkd -readonly
lappend auto_path $Config(ROOT)/modules/patch.tkd/lib
```

f Save and close `rms.cfg`.

10 Back up your Radia Patch Manager ODBC database. Locate the database scripts located in the Service Pack's `Integration Server` directory. If using Microsoft SQL server, run the `split_zobjstat.sql` on your Radia Patch Manager SQL Server Database to create new tables. If using Oracle, run the `split_zobjstat.ora` script to create the new tables.

Note: These scripts create new tables called nvd_device, nvd_de2pr, nvd_de2re. nvd_de2sp, nvd_de2pa, nvd_de2fc and nvd_de2rc based on the current contents of nvd_zobjstat table. The creation of the new tables is based on the value of the zobjclas attribute entries. The original nvd_zobjstat table is left untouched after the script is run. You may choose later to remove this table from your database. Note: After running these scripts, the nvd_zobjstat table will not be updated or used to render Radia Patch Manager Reports through the Radia Integration Server.

11 Restart the Radia Integration Server.

12 Restart the Radia Messaging Server.

Radia Patch Manager Version 2.0 has been updated to Release 2.0.1.

Windows and Linux Patch Manager agent updates

Application of Patch Manager agent updates using either of the procedures below would upgrade Patch Manager agents to Patch Manager Version 2.0, Release 2.0.1. These agent updates are backward compatible with Patch Manager Versions 1.2.X and 2.0

Notes specific to Windows patch Manager agent updates

If you intend to use Patch Manager to manage Microsoft Security Bulletins, this service pack supplies Radia Patch Manager Release 2.0.1 agent updates for Windows clients.

To apply these updates on agents installed using the Radia Management Portal, copy the files in the service pack's media\Patch Agent Maintenance\Win32\Maint to the "win32\maint" directory found under your installed Radia Management Portal's media directory.

To automatically publish and distribute Patch Manager agent updates, please refer to the Patch Manager Guide for additional information on agent update capabilities.

Note: The minimum version of the Radia Client is Version 3.1.2. Use of Radia Patch Manager agent on Windows platforms, at minimum, requires nvdkit build number 145.

Notes specific to Linux Patch Manager agent updates

If you intend to use Radia Patch Manager to manage security advisories on either Red Hat or SUSE Linux agents, the service pack's media`\Patch Agent Maintenance\Linux\Ram` contains a maint31.tar file which contains the Radia Patch Manager Release 2.0.1 agent updates for Red Hat or SUSE clients. To apply these updates on agents installed using the

Radia Management Portal copy the `maint31.tar` to your Radia Management Portal's `Integrationserver\media\client\default\linux\ram` directory (the same directory as the client31.tar file).

Once you have applied the patch.tkd supplied in this Service Pack to your Radia Integration Server and perform either a Red Hat or SUSE patch acquisition, the Radia Patch Manager agent updates supplied in this Service Pack will be REQUIRED to successfully patch a Linux system.

Failure to apply the supplied Linux agent updates to Patch Manager agents would result in failure to apply Linux Patches to the target systems. You can identify, this as the problem , if you observe a message similar to the following in the Patch Manager connect log file

```
20050408 16:20:55 Warning: Product probe error redhat-3es-tetex-fonts : invalid
command name "rpmpkg2::verify
```

To automatically publish and distribute Patch Manager agent updates for Linux, in, refer to the Patch Manager Guide for additional information on agent update capabilities.

The minimum version of the Radia Client is Version 3.1.2. Use of Radia Patch Manager on Linux platforms at minimum, requires nvdkit build number 145.

Post Installation Notes

- Check that your Radia Reporting Server has been upgraded during the service pack application. One indication that your Radia Reporting Server has been properly upgraded is that it now contains extra reporting views that it did not have before. Under the Reporting Views section of the Display Controls area on the left hand side of the Radia Reporting Server graphical interface you'll notice a Compliance Reports grouping. Clicking on the plus sign to open that grouping will result in an additional report named "Compliance Exceptions". If you do not see this new report, your Radia Reporting Server has not been properly upgraded.
- Check that your Radia Integration Server patch environment has been upgraded properly during the service pack application. You can check your new Radia Integration Server Patch environment two ways, by placing your mouse over the Radia Patch Administrator Heading in the Radia Integration Server Patch graphical Interface where it will display text regarding the version and build similar to "Patch Manager Version 2.0.1 Build 325" or by checking the log file httpd-port#.log for the following line.

  ```
  Info: patch: Radia Patch Manager Reporting - Version 2.0.1 - Build 325.
  ```

  If you see anything less than version 2.0.1 in either of these places, your Radia Integration Server Patch environment is not at version 2.0.1 and has not been properly upgraded.
- Check that the new tables generated by the split_zobjstat.sql or split_zobjstat.ora scripts were created and populated. Please note that any alterations to the original nvd_zobjstat table as supplied by HP, could cause the scripts to be unsuccessful since the nvd_zobjstat table is not intended to be altered outside of normal Radia Patch Manager processes.
- Access to the Radia Patch Manager update Web site (http://update.novadigm.com/patch/data) will be discontinued on or about May 1, 2005. A new location is accessible at: http://managementsoftware.hp.com/Radia/patch_management/data. In the Radia Patch Manager Administrator Configuration Settings page, make sure the address in the Patch Manager URL field is

http://managementsoftware.hp.com/Radia/patch_management/data. If it is not, correct it.

Enhancements and Fixes

The following items are fixed or enhanced in the current software release.

PROBLEM: Compliance by Device Report is taking too long to render results

FIX: Installation of this service pack will split device status information previously stored in the table nvd_zobjstat into several new tables. Reporting queries shall exploit these new tables to improve report rendering results.

PROBLEM: Certain Queries are taking a long time to complete.

FIX: Installation of this service pack will split device status information previously stored in the table nvd_zobjstat into additional SQL tables. Reports shall exploit these new tables to improve report rendering results.

PROBLEM: Clicking on Status Icon in Compliance By Devices View does not return details of the status selected. For example a ! indicates a warning, however the details of the warning are not displayed when the '!' is selected.

FIX: Corrected the SQL query within the reports.

PROBLEM: Newly acquired Bulletins and Patches could not be viewed in Acquisition Summary reports.

FIX: Server code was updated to appropriately set time stamps during acquisition.

PROBLEM: Patch acquisition command line parameters were not respected unless they appeared in lower case.

FIX: Command line parameters are now case insensitive.

PROBLEM: Use of an @ sign in a ODBC compliant database password caused database synchronization to fail.

FIX: Corrected DSN password parsing.

PROBLEM: If the Radia Configuration Server Administrative ID called RAD_MAST has been removed from the Radia Configuration Server database and an ODBC

database synchronization is attempted, the synchronization process would remove all data contained in the Radia Patch Manager ODBC database

FIX: Corrected authentication processing code.

PROBLEM: Alteration of the http timeout parameter through the Radia Patch Manager Administrator had no affect.

FIX: Administrator processing corrected.

PROBLEM: Patch Acquisition session information is displaying summary information with the numbers reversed, such that 412 of 63 is displayed instead of 63 of 412.

FIX: Corrected display of data counters.

PROBLEM: Using the Radia Patch Manager Administrator to create an acquisition file, on the product selection page, if the user then deselects 'Microsoft' which deselects all MS products, once the acquisition file is created it could not be used/altered.

FIX: Implemented a Product Selection list processing correction.

PROBLEM: Patch Acquisition with a bulletin selection list including Microsoft bulletins MS05-004 or MS05-005, MS05-006 shall prematurely abort acquisition with the following error displayed in the patch-acquire.log: 20050208 16:23:50 Error: can't unset "pr_array"•

FIX: Code modified to circumvent the premature ending of acquisition for bulletins with incomplete meta data.

PROBLEM: When displaying/filtering on a bulletin for a specific device a very large number of rows are displayed, including data referring to other bulletins.

FIX: Filters corrected.

PROBLEM: The number of Patch Manager managed devices appears to change unexpectedly on a daily basis.

FIX: Created new Compliance and Research exception reports to display the Patch Manager agent devices in error.

PROBLEM: Using a pristine Patch Manager ODBC database, without having run acquisition displays a bulletin count of 1, when no security bulletins have been acquired.

FIX: _BASE_INSTANCE_ removed from ODBC database synchronization

PROBLEM: The Compliance by Device Report by device, by bulletin returns excessive rows of data.

FIX: Filters corrected.

PROBLEM: Clicking on Status Icon in Compliance By Devices View does not return expected statuses.

FIX: New device status filters for top level compliance reports.

PROBLEM: Radia Report Server needs to return information faster.

FIX: Split nvd_zobjstat table to improve performance

PROBLEM: Synchronization task performed during acquisition resulted in the message, Error synchronising SQL Database S1000 1735 {[Oracle][ODBC][Ora]ORA-01735: invalid ALTER TABLE option Error synchronising SQL Database command "slave" already exists in namespace "::sync".

FIX: Resolved after the application of the Service pack providing you specify a Database Type of Oracle in the Radia Patch Manager Graphical User Interface's General Configuration page.

PROBLEM: In the Radia Patch Manager 2.0 Administrator, only two products listed in Step 3 of acquisition setup.

FIX: Problem resolved.

Support

Please visit the HP OpenView web site at: http://www.managementsoftware.hp.com/

This web site provides contact information and details about the products, services, and support that HP OpenView offers. You can also go directly to the support web site at:

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

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 being able to:

- Search for knowledge documents of interest
- 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

NOTE: Most of the support areas require that you register as an HP Passport user and log in. Many also require an active support contract. To find more information about support access levels, go to the following URL:

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

To register for an HP Passport ID, go to the following URL:

https://passport.hp.com/hpp2/newuser.do

To view release notes and other documentation:

1. Click using hp software--> product manuals.

   The **product manuals search** window opens. It is located at:

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

2. In the select product list, click [product name].
3. In the select version list, click [version number].
4. In the **OS** list, click **[OS type]**.
5. To start the search, click **Open** or **Download**.

NOTE: To view files in PDF format (*.pdf), Adobe Acrobat Reader must be installed on your system. To download Adobe Acrobat Reader, go to the following URL:

http://www.adobe.com

Legal Notices

©Copyright [2005] Hewlett-Packard Development Company, L.P.

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.