# Patch Management User Guide for HP-UX 11.x Systems

Part number: 5991-1163
published May 2005, Edition 4

## Legal Notices

## Acknowledgments

# About This Document

## Intended Audience

This guide presents introductory-level information about patches and patch management for HP-UX. Emphasis is on providing solutions that you can quickly understand and implement. At a novice level this guide is easy to use, but at an expert patching level you may find it less efficient.

Patching is a complex subject and as such should receive considerable attention from system administrators with patch-related responsibilities. HP understands, however, that this is not always possible, so this guide is targeted to less experienced system administrators who must acquire and use basic patch management skills in a short period of time.

This guide describes a simplified approach to patching and patch management of HP-UX systems that use the following release software:

- HP-UX 11.0 (B.11.00)
- HP-UX 11i v1 (B.11.11)
- HP-UX 11i v1.6 (B.11.22)
- HP-UX 11i v2 (B.11.23)

This guide does not apply to systems running HP-UX 11i v1.5 (B.11.20).

# Key Goals

The goals of this document are the following:

- Help less experienced system administrators acquire basic patch-related skills and knowledge in a short period of time. It allows them to perform basic HP-UX patch management tasks.
- Aid system administrators in developing a basic patch management strategy.
- Provide a Chapter  2: “Quick Start Guide for Patching HP-UX Systems” (page 17) for system administrators with immediate patching needs.

This document does not provide the following:

- Function as an all-encompassing source of information for patch management.
- Guide system administrators in determining the best or most efficient patch management strategy for their environment. Some recommendations in this guide may differ from recommendations in guides that are targeted at more experienced system administrators.

# Publishing History

This section provides the publishing history of the document.

| Manufacturing Part Number | Supported Operating Systems | Supported Versions | Edition Number | Publication Date |
|---|---|---|---|---|
| 5991-1163 | HP-UX | 11.0, 11i v1, 11i v2 | 4 | May 2005 |
| 5991-0686 | HP-UX | 11.0, 11i v1, 11i v2 | 3 | December 2004 |
| 5990-6753a | HP-UX | 11.0, 11i v1, 11i v2 | 2 | September 2004 |
| 5990-6753 | HP-UX | 11.0, 11i v1, 11i v2 | 1 | April 2004 |

# Document Organization

This guide includes the following topics:

- Chapter  1: “ HP-UX Patches and Patch Management ” (page 15)
- Chapter  2: “Quick Start Guide for Patching HP-UX Systems” (page 17)
- Chapter  3: “HP-UX Patch Overview” (page 27)
- Chapter  4: “Patch Management Overview” (page 57)
- Chapter  5: “What Are Standard HP-UX Patch Bundles?” (page 69)
- Chapter  6: “Using the IT Resource Center” (page 75)
- Chapter  7: “Using FTP as an Alternative Patch Source” (page 89)
- Chapter  8: “Using Software Depots for Patch Management” (page 99)
- Chapter  9: “Using Other Patch Tools” (page 127)
- Appendix  A: “Other Resources” (page 137)

# New and Changed Information in This Edition

This edition contains editorial and HP standards changes.

# Typographic Conventions

audit(5) HP-UX manpage. audit is the name and 5 is the section in the HP-UX Reference. On the web and on the Instant Information DVD, it may be a hot link to the manpage itself. From the HP-UX command line, you can enter “ `man audit` ” or “ `man 5 audit` ” to view the manpage. See man(1).

Book Title Title of a book. On the web and on the Instant Information DVD, it may be a hot link to the book itself.

| | |
|---|---|
| `Command` | Command name or qualified command phrase. |
| `ComputerOut` | Text displayed by the computer. |
| Emphasis | Text that is emphasized. |
| **Emphasis** | Text that is strongly emphasized. |
| **KeyCap** | Name of a keyboard key. Note that **Return** and **Enter** both refer to the same key. |
| Term | Defined use of an important word or phrase. |
| **`UserInput`** | Commands and other text that you type. |
| *`Variable`* | Name of a variable that you may replace in a command or function or information in a display that represents several possible values. |
| [ ] | Contents are optional in formats and command descriptions. If the contents are a list separated by \|, you must choose one of the items. |
| { } | Contents are required in formats and command descriptions. If the contents are a list separated by \|, you must choose one of the items. |
| ... | Preceding element may be repeated an arbitrary number of times. |
| \| | Separates items in a list of choices. |
| `<element>` | An element used in a markup language. |
| `attribute=` | An attribute used in a markup language. |

## Advanced Topics

This guide provides Advanced Topic sections that introduce you to more in-depth levels of discussion and procedures. We recommend that you read them as they may contain information that could be useful and relevant to your patching environment, but they are not necessary to using the main body of procedures in this guide.

## Related Documents

Your main resource to get patches is the IT Resource Center (ITRC) at **http://itrc.hp.com**.

For more information about the ITRC, go to Chapter 6: "Using the IT Resource Center" (page 75).

For additional sources of information, go to Appendix A: "Other Resources" (page 137).

## HP Encourages Your Comments

The HP technical documentation Web site team invites you to send us questions and comments about the documentation located on the docs.hp.com Web site. Please note that this site does not provide technical support for Hewlett-Packard products. If your inquiry concerns technical support for an HP product, regrettably we are not able to provide a response. Please consult the support Web site. For the United States, visit **http://welcome.hp.com/country/us/en/support.html**. For all other locations, consult the global directory at: **http://welcome.hp.com/country/us/en/othercountrieswel.html**, click on the link for your country or region and then click on the link for "Support and Drivers".

If your inquiry is related to the documentation located on the docs.hp.com site, you will receive a personalized reply within two business days. Occasionally the volume of e-mail we receive exceeds our ability to respond quickly.

To offer customer feedback, go to **http://docs.hp.com/en/feedback.html**.

# Table of Contents

## 4 Patch Management Overview

## 5 What Are Standard HP-UX Patch Bundles?

## 6 Using the IT Resource Center

## 7 Using FTP as an Alternative Patch Source

## 8 Using Software Depots for Patch Management

## 9 Using Other Patch Tools

# List of Tables

# List of Figures

# 1 HP-UX Patches and Patch Management

You may wonder why you should be concerned with patch management. HP recommends that you address patch management to reduce the risk of problems such as system hangs, panics, memory leaks, data corruption, application failures, and security breaches.

If your job involves any of the following concerns, then you need patch management:

- Having proper system functionality and performance
- Maintaining system security
- Maintaining system reliability and availability
- Obtaining the latest system enhancements and functionality
- Reading about problems and solutions before you encounter them
- Limiting the number of patches to install if you encounter a problem
- Limiting the amount of time required to troubleshoot problems

Patches are software that HP releases to deliver incremental updates to your system. Patches are best known for delivering defect fixes, but also deliver new functionality and features, enable new hardware, and update firmware. You can use HP-UX patches to update HP-UX software without having to completely reinstall your system application. For a description of patches, see Chapter 3: "HP-UX Patch Overview" (page 27).

Patch management involves any of the following tasks:

- Selecting or acquiring patches
- Applying patches
- Updating previously applied patches with more current patches
- Verifying patches
- Testing patches
- Listing patches already applied to existing software
- Copying patches
- Maintaining repositories, or depots, of patches for easy selection
- Committing applied patches
- Removing or rolling back applied patches

For a description of patch management, see Chapter 4: "Patch Management Overview" (page 57).

**NOTE:** You can approach patch management in many different ways with no one approach being the correct way. You must base decisions regarding patch management on the specifics of your individual situation. Even then, there may be more than one reasonable path.

## Patch Management Strategies

This guide addresses two basic patch management strategies. Most customers use a combination of both strategies:

- Proactive: Patching regularly to avoid problems
- Reactive: Patching after a problem occurs

No matter what strategy or combination of strategies you adopt, keep in mind that any change to a system, including change incurred during the process of patch management, risks the introduction of new problems to your system. This guide discusses some steps that you can take to mitigate the risk associated with patching your system.

## How Do I Get Patches?

HP provides numerous ways for you to acquire patches, ensuring that people with different goals and different levels of expertise can find a patch source to fit their needs. You can obtain patches individually or in groups of related patches known as patch bundles.

This guide discusses the following HP-UX patch sources:

- IT Resource Center (ITRC) Web site: **http://itrc.hp.com**
- Software Depot Web site: **http://software.hp.com**
- HP FTP Servers

  **ftp://ftp.itrc.hp.com**

  **ftp://singapore-ffs.external.hp.com**
- Patch Tools

  "Using the Patch Assessment Tool" (page 128)

  " Using the Security Patch Check Tool " (page 131)

## Where Do I Start?

If you have immediate patching needs, see Chapter 2: "Quick Start Guide for Patching HP-UX Systems" (page 17).

If you want to learn about your patching options, read all chapters in this guide, and then choose the resource that best meets your needs.

# 2 Quick Start Guide for Patching HP-UX Systems

This quick start guide is for system administrators who have immediate patching needs. It is a limited solution to general patching issues. If you need more in-depth information about patching, review the rest of this manual and the other patch-related resources in Appendix A: "Other Resources" (page 137).

**NOTE:** All software and tools discussed in this quick start guide are free of charge. You do require root user privileges to complete these procedures.

# Overview

This quick start guides you through basic patch management tasks and provides minimal detail.

- "Before You Begin" (page 19)

  Before you acquire and install the patch bundles or individual patches, you should consider some patch-related questions. See "Should I Use Standard HP-UX Patch Bundles?" (page 19) and "Should I Use Individual Patches?" (page 19).

- "Acquiring and Installing Standard HP-UX Patch Bundles" (page 20)

  When initially patching a system, it is important to establish a stable baseline of patches. This section shows you how to acquire and install the Quality Pack (QPK) patch bundle. This provides an easy and reliable way to update existing patches. The QPK patch bundle is designed for this purpose. The bundle has all stable defect-fix patches for core HP-UX, graphics, and networking drivers.

  The standard HP-UX patch bundles also include the Hardware Enablement (HWE) bundle, which is required for new systems and add-on hardware. For example, if you add hardware to your system or anticipate adding hardware, such as a new I/O card, you need to install the latest HWE bundle.

- "Acquiring and Installing Individual Patches" (page 23)

  In addition to the standard HP-UX patch bundles, you may occasionally need to install individual patches. For example, you may want more recent patches found on the HP IT Resource Center (ITRC) Web site than those contained in a standard HP-UX patch bundle on media. You may also want the latest security patches.

  For additional information, visit the ITRC Web site at **http://itrc.hp.com**.

# Before You Begin

The following sections contain questions that you should review before you begin the quick start procedures.

## Should I Use Standard HP-UX Patch Bundles?

Before you acquire and install standard HP-UX patch bundles, consider the following questions:

- Is this a new system?
- Do you want to establish a baseline of patches?
- Do you want to update the existing baseline of patches?
- Are you adding new hardware to the system?

If you answer yes to any of these questions, then you should continue with "Acquiring and Installing Standard HP-UX Patch Bundles" (page 20).

## Should I Use Individual Patches?

Before you acquire and install individual patches, consider the following question:

Do you need to add individual patches to the system?

If you answer yes to this question, then you should continue with "Acquiring and Installing Individual Patches" (page 23).

**NOTE:** In addition to the information in this guide, you should review the release notes for the product to install.

## Standard HP-UX Patch Bundles

Table 2-1 shows the bundle names for the HP-UX 11.0 and HP-UX 11i releases.

**Table 2-1** Standard HP-UX Patch Bundle Names

| **Bundle Name** | **HP-UX 11.0 (B.11.00)** | **HP-UX 11i v1 (B.11.11)** | **HP-UX 11i v1.6 (B.11.22)** | **HP-UX 11i v2 (B.11.23)** |
|---|---|---|---|---|
| Quality Pack | `QPK1100` | `GOLDAPPS11i`<br>`GOLDBASE11i` | N/A | `QPKAPPS`<br>`QPKBASE` |
| Hardware Enablement | `HWE1100` | `HWEnable11i` | N/A | `HWEnable11i` |
| Required Patch Bundle | N/A | `BUNDLE11i` | `BUNDLE11i` | `BUNDLE11i` |
| Feature Enablement Patch Bundle | N/A | N/A | N/A | `FEATURE11i` |
| Maintenance Pack | N/A | N/A | `MAINTPACK` | N/A |

**NOTE:** Standard HP-UX patch bundles are cumulative. The latest version of a bundle includes patches from all previous versions. Also, the QPK and HWE bundles may have overlapping content. This will not affect the patching process.

# Acquiring and Installing Standard HP-UX Patch Bundles

The standard HP-UX patch bundles provide recommended sets of HP-UX system patches, which you should use for proactive patching. This section details how to acquire and install the Quality Pack (QPK) patch bundle and the Hardware Enablement (HWE) bundle. You can, however, use the steps to install any of the standard HP-UX patch bundles.

If you have a new system and need to establish a patch baseline or want to update the existing patch base, then you would install the QPK patch bundle. If you are adding new hardware to your system, then you would install the HWE bundle. If you are unsure of which patch bundles or patches to install on your system, installing both the QPK and HWE bundles represents an excellent starting point for your patch management program.

## Acquiring the Bundles

To obtain the QPK and HWE bundles from the Web, perform the following steps:

1. Log in to the target system.
2. Determine the operating system release by entering this command: `uname -r`

   Record the information. You will use this information in step 8.

3. Be sure that you are logged in as a user with write permissions to the download directory that you plan to use.

   These instructions assume you are using the `/tmp` directory.

4. Log in to the ITRC at **http://itrc.hp.com**.

   Be sure to log in to the appropriate site (Americas/Asia-Pacific or European).

5. Select **maintenance and support (hp products)**.
6. Select **standard patch bundles - find patch bundles**.
7. Select **HP-UX patch bundles**.
8. Select the most recent **release name** for your operating system (by release date).
9. Select the **bundle** link.

   HP highly recommends that you download the following bundles. They are cumulative, choose the latest:

   - Hardware Enablement bundle

     For new hardware, install this bundle.

   - Quality Pack patch bundle

     For defect fixes, install this bundle.

   The bundle's main page displays:

   - Each patch contained in the bundle.

     If the bundle contains patches with warnings, which are notifications of known problems, they are listed near the top of the page.

   - All patch identifications (IDs) are linked to the patch database on the ITRC, and provide detailed patch information.
   - In the right-hand navigation menu under **documentation**, you can access the readme file for the bundle by using the **bundle readme** link. Review the readme for critical installation information.

10. Ensure all items are checked. Select **add to selected patch list**.

    If you see additional patches, the ITRC selected them to replace patches with warnings.

11. Review your choices to ensure all items are checked. Select **download selected**.

    The **download patches** page is displayed.

12. Under the heading **download items in one operation**, select a download server and a format option (HP recommends the gzip package). Choose a zip package only if you are certain that your HP-UX system can unpack a `.zip` file.

13. Select **download**. Make the appropriate selections (based on the browser you are using) to save the selected bundle to the `/tmp/`*`tmpdepot`* directory on the target system.
14. Record the name of the file being downloaded.

    The following section refers to the file as *`patches.xxx`* .

## Installing the Bundles

To install the downloaded bundle, repeat the following steps for each bundle.

1. Log in to the target system.
2. Unpack the downloaded file *`patches.xxx`* by using one of these commands:
    - If the downloaded file is *`patches`*`.tgz`:

      ```
      gunzip -c patches.tgz | tar xvf -
      ```

    - If the downloaded file is *`patches`*`.tar`: **`tar -xfv patches.tar`**
    - If the downloaded file is *`patches`*`.zip`: **`unzip patches.zip`**

      You must have an installed application that can unpack a `.zip` file. Not all HP-UX systems have such an application. If you do not have a system that can unpack a `.zip` file, then you would need to use a system that does, then transfer the unpacked files to the target system.
3. As root, run the `create_depot_hp-ux_11` script.
4. Verify the download by entering this command:

    ```
    swverify -d \* @ /tmp/tmpdepot/depot
    ```

    You will see the message `"* Verification succeeded."`
5. Find the bundle names: **`swlist -d @ /tmp/`*`tmpdepot`*`/depot`**
6. Record all bundle names.

    The bundle name is the first word of each line under the **Bundle(s)** heading.
7. This step is critical. When you install a QPK or HWE bundle, the system reboots automatically. Before you install a bundle (step 9), you need to follow your company's policy regarding a system reboot.
8. This step is critical. Before you install the bundle, back up your system.
9. Install the bundles:

    ```
        swinstall -s /tmp/tmpdepot/depot -x autoreboot=true \
             -x patch_match_target=true
    ```

    During the installation, the system prints progress details to the screen.
10. Monitor the screen for error messages.

    The system reboots automatically as part of the installation process.
11. Verify that the installation was successful:
    - Repeat the `swlist` command for each bundlename you recorded in step 6:

      ```
      swlist -l bundle bundle name
      ```

      Ensure that the bundle is shown in the output.
    - Repeat the `swverify` command for each bundle name you recorded in step 6:

      ```
      swverify bundle name
      ```

  - This command may not always complete in a short amount of time.
  - If the verification is successful, the last few lines of output contain the line `"* Verification succeeded."`
  - If the verification was not successful, view the log file `/var/adm/sw/swagent.log` for additional information related to the `swverify` failure. If this is not sufficient to resolve the problem, consult more advanced resources in Appendix A: "Other Resources" (page 137).

- View the `swagent` log file, located at `/var/adm/sw/swagent.log`. This log includes information related to the installation.
  - Find the section pertaining to the installation just performed (located near the end of the file if you check it immediately after the install). Review this section and make sure that there were no errors `("ERROR")`.
  - If you find errors, consult more advanced resources in Appendix A: "Other Resources" (page 137) to resolve the problem.

# Acquiring and Installing Individual Patches

At times, you may find it necessary to acquire and install one or more individual patches based on known patch IDs.

For example, you may read an HP-UX security bulletin in which HP recommends that you install specific patches. Another possibility is that you are installing software that requires specific patches for the software to function properly. Customers also frequently acquire and install individual patches for reactive patching. Whichever the case, you can use the Patch Database on the ITRC Web site to quickly and simply acquire specified patches as well as their dependencies. If you are unfamiliar with patches with dependencies, see Chapter 3: "HP-UX Patch Overview" (page 27).

**NOTE:** HP-UX patch IDs follow this format:

`PH`*`XX`*`_`*`#####`*

where `PH` is patch HP-UX, *`XX`* is replaced with one of the following values, and *`#####`* is replaced with a number.

`CO` = command, `KL` = kernel, `NE` = networking, `SS` = subsystem

## Acquiring the Patches

To acquire the patches from the Web, perform the following steps:

1. Log in to the target system.
2. Determine the operating system release, by entering this command: **`uname -r`**

   Record this information. You will use it in step 8.
3. Be sure that you are logged in as a user with write permissions to the download directory that you plan to use.

   These instructions assume you are using the `/tmp/`*`somePatchDir`* directory.
4. Log in to the ITRC at **http://itrc.hp.com**.

   Be sure to log in to the appropriate site (Americas/Asia-Pacific or European).
5. Select **maintenance and support (hp products)**.
6. Select **find individual patches and firmware**.
7. Select **HP-UX** to go to the **search for patches** page.
8. Enter the appropriate hardware and OS information.

   For the hardware, use **700** for workstations and **800** for servers. For the OS, use the information you recorded in step 2.
9. From the drop-down list, select **Search by Patch IDs**.
10. In the text box next to the drop-down list, enter the patch ID for the patch you want to download. Then select **search**.

    If it exists, the selected patch is displayed in the **search results** page. Patches (possibly differing from the patch you requested) display in one to three columns.
11. Review the patches in the table.

    - **specified:** Shows the patch ID you requested.
    - **recommended:** Shows the patch that HP recommends for download/install based on the patch you requested (it may be different than the patch you specified). If you see a patch in this column, it meets all requirements of the patch you requested. HP recommends that you download and install this patch.
    - **most recent:** Shows the most recent version of the requested patch.

    The following icons may be displayed along with the patch ID.

- This icon means that the patch has Special Installation Instructions. You should always read them.

  📋

- This symbol means that the patch has a warning associated with it. You should review the warning text to determine whether it applies to your system.

  ⚠

See Table 6-1: “Navigating the Search Results Table” (page 78) for a description of all table icons.

12. To review details about a patch, select the **patch ID** to open the **patch details** page.

    At a minimum, you should review the information provided in the following fields:

    - **Special Installation Instructions:** Read this section to determine if the chosen patch has additional steps that you must perform during installation.
    - **Warning:** This section will exist only if the patch has a warning associated with it. Carefully read the information to determine how or whether the patch's problems will impact your system. If the warning does impact your system, you must decide whether the problem appears severe enough to avoid installing the patch. If this is the case, choose an alternate patch if one is available.
    - **Patch Dependencies, Hardware Dependencies, Other Dependencies:** Note the patch IDs because you must later verify that the patches are included on the list of patches that you download.
13. When you finish viewing this page, select **search results** to return to the **search results** page.
14. On the **search results** page, check the box next to the patch ID of the patch to download.

**TIP:** If the **recommended** column appears, you should select the patch in that column unless you have a valid reason not to.

15. Add the checked patch to the list of patches to download by selecting **add to selected patch list**.
    - If the patch you chose has a warning associated with it, the **patch warning** page appears.
    - If this happens, verify which patch you are downloading and select **continue**.
    - The **selected patch list** page is displayed.
16. The Patch Database may automatically add some patches to the download list to satisfy dependencies. You should download these along with the patches you explicitly selected.
17. To add more patches to the patch list, select **search results** and repeat steps 8 through 16.
18. After acquiring all the patches you need, select **download selected** to open the **download patches** page.
19. Under the heading **download items in one operation**, select a download server and a format option (HP recommends gzip package). Select a zip package only if you are certain that your HP-UX system can unpack a `.zip` file.
20. Select **download**. Make the appropriate selections (based on the browser you are using) to save the selected bundle to the `/tmp/`*`somePatchDir`* directory on the target system.
21. Record the name of the file being downloaded.

    The following section refers to the file as *`patches.xxx`* .

## Installing the Patches

To install the downloaded patches, perform the following steps:

1. Log in to the target system.
2. Unpack the downloaded file, *patches.xxx* :
   - If the downloaded file is *patches*.tgz:

     **gunzip -c patches.tgz | tar xvf -**
   - If the downloaded file is *patches*.tar: **tar -xfv patches.tar**
   - If the downloaded file is *patches*.zip: **unzip patches.zip**

     You must have an installed application that can unpack a .zip file. Not all HP-UX systems have such an application.
3. As root, run the create_depot_hp-ux_11 script.

   The patches are now in a depot in the *somePatchDir* directory.
4. Verify the download:

   **swverify -d * @ /tmp/*somePatchDir*/depot**

   You will see the message "* Verification succeeded."
5. This step is critical. When you install the patches, the system may reboot automatically. Before you install patches (step 8), you need to follow your company's policy regarding a system reboot.
6. This step is critical. Before you install the patches, back up your system.
7. You can remove the following files to clean up your directory and save space:
   - patch files of the form PH*XX_#####*
   - .text files
   - .depot files
   - depot.psf file
   - downloaded .tgz, .tar, or .zip file
   - create_depot_hp-ux_11 file
   - readme file
8. Install the patches using the following command:

   ```
   swinstall -s /tmp/somePatchDir/depot -x autoreboot=true \
      -x patch_match_target=true
   ```

   During the installation, the system prints progress details to the screen.
9. Monitor the screen for error messages.

   The system reboots automatically if any of the patches you are installing requires it.

Be patient. The patch installation can be slow.

10. Verify that the installation was successful:

    - Enter the command **`swlist -l product`**

      Ensure that the installed patches are shown in the output.

    - Execute the `swverify` command on each of the new patches: **`swverify`** *`patch_id`*

      - This command may not always complete in a short period of time.
      - If the verification is successful, the last few lines of output contain the line `"* Verification succeeded."`
      - If the verification was not successful, view the log file `/var/adm/sw/swagent.log` for additional information related to the `swverify` failure. If this is not sufficient to resolve the problem, consult more advanced resources in Appendix A: "Other Resources" (page 137).

    - View the `swagent` log file, located at `/var/adm/sw/swagent.log`. This log includes information related to the installation.

      - Find the section pertaining to the installation just performed (located near the end of the file if you check it immediately after the install). Review this section, and ensure that there were no errors `("ERROR")`.
      - If you find errors, consult more advanced resources in Appendix A: "Other Resources" (page 137) to resolve the problem.

## Where to Go Next

To learn more about patching and patch management, go to Chapter 3: "HP-UX Patch Overview" (page 27) and Chapter 4: "Patch Management Overview" (page 57).

# 3 HP-UX Patch Overview

This chapter provides the following information about patching:

# Patch-Related Concepts

Although patches are best known for delivering defect fixes, they can also deliver new functionality and features, enable new hardware, and update firmware. You should review the following patch-related concepts:

- "Patch Identification" (page 28)
- "HP-UX Software Structure" (page 28)
- "Patch Bundles" (page 29)
- "Software Depots" (page 29)
- "Patch Status" (page 30)
- "Patch State" (page 30)
- "State" (page 31)
- "Category Tags" (page 31)

## Patch Identification

HP assigns each HP-UX patch a unique identification or patch ID. Each HP-UX patch ID has the form `PHXX_#####`, where:

- `PH` is an abbreviation for patch HP-UX
- *`XX`* is replaced with one of the following values for the HP-UX area being patched:
  - `CO` = command patches
  - `KL` = kernel patches
  - `NE` = network patches
  - `SS` = patches related to all other subsystems
- *`#####`* is replaced with a unique four- or five-digit number.

  In general, the numeric portion of the patch ID is higher for more recently released patches.

## HP-UX Software Structure

To understand some of the topics presented in this chapter, you should have a basic understanding of the structure of HP-UX software. Patches are part of this software structure. You will also need to use Software Distributor.

The following list provides an overview of the Software Distributor for HP-UX (SD-UX) software objects that compose HP-UX software.

- Fileset
  - A fileset is a grouping of one or more files contained in a product. A fileset groups a subset of a product's files into a manageable unit.
  - Filesets include the files and control scripts that make up a product. For more information about control scripts, see the Software Distributor Administration Guide on the HP Technical Documentation Web site at **http://docs.hp.com**.

    - Filesets must exist within a product.
    - Although a patch has a unique name, the names of the filesets contained in a patch match the corresponding base filesets that they patch.
- Product
    - A product is a software object that is packaged and distributed for users to acquire and install.
    - Products are composed of one of more filesets and may additionally contain one or more control scripts.
    - A product can exist either within a bundle or as its own entity.
- Bundle
    - A bundle is an encapsulation of products or filesets into a single software object.
    - Bundles are optional software objects.
    - Objects are included in a bundle by reference only.
    - If the products within the bundle are all patches, the bundle is known as a patch bundle.

For more information about these software objects, see the Software Distributor Administration Guide on the HP Technical Documentation Web site at **http://docs.hp.com**.

## Patch Bundles

Patch bundles play an important role in patch management. A patch bundle is a collection of patches that have been grouped into a single software object to meet a specific need. Many HP-UX users find that acquiring and installing these bundles, as opposed to acquiring and installing patches individually, simplifies the patch management process.

Your first encounter with patch bundles might be with the standard HP-UX patch bundles. These bundles contain patches that HP has assembled to meet a specific need. For example, the basic purpose of Quality Pack patch bundles is to deliver defect-fix patches for proactive maintenance. HP releases updated versions of the bundles on a regular schedule and tests them to ensure a high level of reliability. Using standard HP-UX patch bundles can be a less error-prone and more efficient way to patch a system than acquiring and installing individual patches. For more information, see Chapter 5: “What Are Standard HP-UX Patch Bundles?” (page 69).

Patch bundles also make it easier for you to determine the current level of patches on your system. For example, there could be hundreds of individual patches contained in an installed bundle, but the `swlist` command lists, by default, only the bundle name rather than each individual patch contained in the bundle. For example, if you installed the December 2003 Quality Pack patch bundles on an HP-UX 11i v1 (B.11.11) system, output for the bundles would be similar to the following:

```
GOLDAPPS11i  B.11.11.0312.4 Gold Applications Patches for
 HP-UX 11i v1, December 2003
GOLDBASE11i  B.11.11.0312.4 Gold Base Patches for HP-UX 11i v1,
 December 2003
```

For more information about listing the products on your system, see “Which Patches Are on My System?” (page 33).

You may also find yourself working with patch bundles if you use the IT Resource Center Patch Assessment Tool, which allows you to create your own custom patch bundles. For more information, see Chapter 9: “Using Other Patch Tools” (page 127).

## Software Depots

Software depots, or simply depots, are an integral part of patch management. A depot is a special type of file or directory that has been formatted for use by SD-UX as a software repository. In the general case, depots contain a diverse array of software products. However, this guide focuses on depots as repositories for patches and patch bundles. Such depots can be referred to as patch depots.

Patch depots are a very effective mechanism for managing patches. You can create your own custom patch depots to meet various patch management needs. You can also create special depots to be located on a patch server that acts as a source for patch or bundle installations on other systems.

HP uses patch depots to deliver patches and patch bundles. For more information about depots, see Chapter 8: "Using Software Depots for Patch Management" (page 99).

## Patch Status

Patches have an associated status. The initial value of a patch's status does not change, but over the life of the patch modifiers may be added (as described in this section). You can find the value for a patch's status in the **status** field. This field is in the patch's **patch details** page on the ITRC and in the patch text file. To obtain the most up-to-date values for patch status, use the **patch details** page. A patch status has the following values and modifiers to describe it.

Initial values for patch status include the following:

- `General Release (GR)`

  HP has approved `GR` patches for widespread use.

- `Special Release (SR)`

  HP intends an `SR` patch for limited distribution. It is available only through special channels.

Modifiers for patch status values include the following:

- `Superseded`

  Indicates that the patch has been replaced by a newer patch. For more information about supersession, see "Ancestors and Supersession" (page 37).

  Results in the additional patch status values `General Superseded` and `Special Superseded`.

- `With Warnings`

  Indicates that the patch has an associated warning. For more information about warnings, see "Patch Warnings" (page 53).

  Results in the additional patch status values `General Release With Warnings` and `Special Release With Warnings`.

Most patches have a status of `General Release` or `General Superseded`.

## Patch State

A patch that has been installed on a target system is assigned an attribute called `patch_state` that provides information about a patch. For example, the `patch_state` tells you whether the patch has been committed or superseded. For more information about attributes, see "Patch-Related Attributes" (page 41).

There are four values for `patch_state`:

- `applied`

  The patch is currently active on the system and is the most recent member of its supersession chain to have been loaded.

- `committed`

  The patch's rollback files have been deleted, or the patch was installed without saving rollback files. The patch cannot be directly removed from the system. For more information about patch rollback, see "Patch Rollback and Commitment" (page 45).

- `superseded`

  The patch has been superseded by another patch that has been installed on the system. For more information about supersession, see "Ancestors and Supersession" (page 37).

- `committed/superseded`

  The patch has been committed and superseded by another patch installed on the system.

**IMPORTANT:** For HP-UX 11.0 systems, you must install patch `PHCO_22526` or a superseding patch for proper functionality regarding the `committed/superseded patch_state`.

Use the following SD-UX commands to determine `patch_state` values:

- Show the `patch_state` value for patch *`patch_id`*:

  ```
  swlist -l fileset -a patch_state patch_id
  ```

- Show the `patch_state` values for all patches on the local system:

  ```
  swlist -l fileset -a patch_state *,c=patch
  ```

For more information regarding the `swlist` command, see "Which Patches Are on My System?" (page 33).

## State

Filesets (patch and nonpatch) have an attribute called `state` that indicates the current installation state of a fileset. During installation, software is transitioned through the following states: `transient`, `installed`, and `configured`. During removal, software is transitioned through these states: `configured`, `installed`, and `transient`.

An SD-UX operation leaves a fileset in one of the following states:

- `installed`

  Software has been successfully installed but not yet configured.

- `configured`

  Software has been successfully installed and configured. No further operations are required.

- `corrupt`

  SD-UX has encountered an unexpected condition during software installation checks.

- `transient`

  When SD-UX moves software from one location to another, the software is in a transient state. An interruption occurs during the transfer, the state remains `transient`.

For more information about these states, see the Software Distributor Administration Guide on the HP Technical Documentation Web site at **http://docs.hp.com**.

Use the following `swlist` command to view the state associated with patch *`patch_id`*:

```
swlist -l fileset -a state | grep patch_id
```

For more information about the `swlist` command, see "Which Patches Are on My System?" (page 33).

## Category Tags

Patches have categories, or category tags, associated with them to simplify the process of determining the general purpose of a specific patch. A patch may have multiple categories specified. This section provides a list of common patch categories. A patch always has the category tag `patch`.

Although you can use category tags in conjunction with several SD-UX commands, including `swinstall` and `swcopy`, you should use category tags only with the SD-UX command `swlist`.

Because of the cumulative nature of patches, many category tags for a patch are inherited from the patch's ancestors. Therefore, if patch A is created to deliver a critical fix, it will have a `critical` tag, and all patches superseding it will also have a `critical` tag.

You can determine patch categories for a given patch in the following ways:

- Viewing the **Category Tags** field on the **patch details** page or in the text file for the patch.
- Using the `swlist` command:

  ```
  swlist -l product -a category_tag patch_id
  ```

This command also shows any category tags that have been manually added to the patch by a user. For `swlist` examples that use category tags and for more information about the `swlist` command, see "Which Patches Are on My System?" (page 33).

The following list provides a subset of patch-related categories:

- `patch`

  This category tag is always present for patches because software objects with the `is_patch` attribute set to `true` have the built-in, reserved category of `patch`. For more information about attributes, see "Patch-Related Attributes" (page 41).

- `hardware_enablement`

  A patch that provides support for new hardware.

- `enhancement`

  A patch that provides an enhancement.

- `special_release`

  - A patch with restricted distribution, usually intended for installation by one specific customer or set of customers.
  - Information for `special_release` patches is not always available using the ITRC's Patch Database or other official HP information sources. However, you might encounter references to these patches when viewing information related to other patches.
  - A patch cannot inherit this tag.

- `critical`

  - A patch that repairs a critical problem. For more information, see "Critical and Noncritical Patches" (page 49).

    A patch that has a `critical` tag also has one or more of the following tags: `panic`, `halts_system`, `corruption`, `memory_leak`.

- `firmware`

  A patch that provides a firmware update.

- `manual_dependencies`

  - A patch that contains one or more dependencies that are not enforced by SD-UX tools. For more information, see "Patch Dependencies" (page 43).
  - A patch cannot inherit this tag.

# Which Patches Are on My System?

SD-UX is included with the HP-UX operating system and provides a powerful set of tools for centralized HP-UX software management. Many SD-UX commands start with `sw`; for example: `swlist`, `swinstall`, `swreg`, `swremove`, `swcopy`, and `swverify`. For more information about SD-UX, see the Software Distributor Administration Guide on the HP Technical Documentation Web site at **http://docs.hp.com**.

The `swlist` command can be invaluable in determining which patches and patch bundles are on your HP-UX system. You can use the `swlist` command to display information about software products that are installed on a local or remote host, or that are stored in a local or remote depot. You can use the various command arguments and options to customize the information returned. See swlist(1M).

This section presents some examples of `swlist` to display information about patches, bundles, and depots.

**NOTE:** For brevity and improved readability, some lines of SD-UX command output have been shortened or removed.

## Examples of swlist

If you use `swlist` with no arguments, you get a default listing of all top-level software installed on your local host. You will see output similar to the following:

```
> swlist
# Initializing...
# Contacting target "some_system"...
#
# Target:  some_system:/

# Bundle(s):
  BUNDLE11i B.11.11.0102.2 Required Patch Bundle for HP-UX 11i,
   February 2001
  GOLDAPPS11i B.11.11.0312.4 Gold Applications Patches for
   HP-UX 11i v1, Dec 2003
  GOLDBASE11i B.11.11.0312.4 Gold Base Patches for HP-UX 11i v1,
   December 2003
  HWEnable11i B.11.11.0309.4 Hardware Enablement Patches for
   HP-UX 11i, Sep 2003
  MOZILLA  1.4.0.00.00  Mozilla 1.4 for HP-UX
  T1471AA   A.03.50.000 HP-UX Secure Shell

# Product(s) not contained in a Bundle:
  PHCO_28848 1.0  Software Distributor Cumulative Patch
  PHCO_29010 1.0  shar(1) patch
  PHCO_29495 1.0  libc cumulative patch
  PHSS_28677 1.0  CDE Applications Periodic Patch
  vim   5.8  Vi IMproved
```

The `swlist` command has many arguments. This chapter considers only the following arguments and operands:

```
swlist [-d] [-l level] [-a attribute] [-s source] [software_selections]
[-x option=value] [@ target_selections]
```

- **-d**

  Directs swlist to operate on a software depot rather than on software currently installed on the system. When you use this argument, you must also use the **@** *target_selections* argument to specify the depot.

- **-l** *level*

  - Lists all software objects down to the specified level. The following is a partial list of supported *level* values:

    - depot: Lists products available from a depot.
    - bundle: Shows only bundles.
    - product: Shows only products.
    - patch: Shows all applied patches.
    - fileset: Shows products and filesets.
    - file: Shows products, filesets, files and numbers (used in software licensing).
    - category: Shows all categories of available patches for patches that have included category objects in their definition.

  - Specifies multiple values for *level*:

    **-l bundle -l product:** Shows bundles and the products they contain.

- **-a** *attribute*

  Specifies one or more attributes to display. For more information about attributes, see "Patch-Related Attributes" (page 41).

- **-s** *source*

  Specifies the software source to list. Use this argument as an alternative way to list a depot.

- *software_selections*

  - Specifies software objects to be listed.
  - Applies only if the *level* is bundle, product, fileset, file, or patch.
  - Use wildcards [ ], *, ? in the specification of the *software_selections* if you want to make multiple selections. For example:

    - A specification of bun[12] selects software bun1 and bun2.
    - A specification of * selects all software.

  - Views the manpages for sd(5) using the command: **man 5 sd**

- **-x** *option*=*value*
  - Sets the option to specified value.
  - The default behavior of `swlist` is to show only the latest patches installed on a system. It does not show patches that have been superseded. To list superseded patches, set the `show_superseded_patches` option to `true`:

    **swlist -x show_superseded_patches=true**
  - Specifies multiple `-x` options if needed.
- **@** *target_selections*
  - Specifies the target of the command. You can tell `swlist` to operate on a system other than the local host or on a depot. For example, to specify `swlist` operate on the system `host1`:

    **swlist @ host1**
  - Operates on the software depot `depot1` located in directory *some_dir* on the local host:

    **swlist @ /***some_dir***/depot1**
  - Operates on the depot `depot2` located in directory *some_dir* on the system `host1`:

    **swlist @ host1:/***some_dir***/depot2**

For a complete list of `swlist` arguments, consult the swlist(1M) manpage or the Software Distributor Administration Guide on the HP Technical Documentation Web site at **http://docs.hp.com**.

To filter the output to display only patches, you can use the `-l` argument in combination with a software selection using the category tag `patch`:

```
> swlist -l product *,c=patch
# Initializing...
# Contacting target "some_system"...
#
# Target:  some_system:/
PHCO_28848  1.0  Software Distributor Cumulative Patch
PHCO_29010 1.0  shar(1) patch
PHCO_29495 1.0  libc cumulative patch
PHSS_28677 1.0  CDE Applications Periodic Patch
...
```

The following command shows patches that have a `manual_dependencies` category tag:

```
> swlist -l product *,c=manual_dependencies
# Initializing...
# Contacting target "chb26006"...
#
# Target:  chb26006:/
PHCO_24198 1.0  ioscan(1M) patch
PHCO_25831 1.0  SCSI Ultra160 driver Online Addition script
PHCO_25841 1.0  Add Rock Ridge extension to mount_cdfs(1M)
PHCO_26252 1.0  mount_vxfs(1M) cumulative patch
...
```

The following command shows bundles on the system specified:

```
> swlist -l bundle @ some_system
# Initializing...
# Contacting target "some_system"...
#
```

```
# Target:  some_system:/
BUNDLE11i B.11.11.0102.2 Required Patch Bundle for HP-UX 11i, Feb 2001
GOLDAPPS11i B.11.11.0312.4 Gold Applications Patches for HP-UX 11i v1,
 Dec 2003
GOLDBASE11i B.11.11.0312.4 Gold Base Patches for HP-UX 11i v1,
 Dec 2003
HWEnable11i B.11.11.0309.4 Hardware Enablement Patches for HP-UX 11i,
 Sep 2003
MOZILLA  1.4.0.00.00    Mozilla 1.4 for HP-UX
T1471AA  A.03.50.000    HP-UX Secure Shell
```

Table 3-1: "Variations of the swlist Command" (page 36) lists numerous `swlist` command variations that you may find useful. These examples can also help you learn how to combine various `swlist` arguments.

**Table 3-1** Variations of the `swlist` Command

| `swlist` **Commands** | **Description** |
|---|---|
| `swlist -l depot` | Displays the registered depots located on your local system. |
| `swlist -l depot @` *`some_host`* | Displays the registered depots located on the system *`some_host`*. |
| `swlist -d -l product @ \`<br>*`some_host:/some_dir/some_depot`*<br>`swlist -l product -s \`<br>*`some_host:/some_dir/some_depot`* | Alternates commands that list the products stored in the software depot *`/some_dir/some_depot`* on the system *`some_host`*. |
| `swlist -d -l product *,c=patch @ \`<br>*`some_host:/some_dir/some_depot`* | Lists all patches in the depot *`/some_dir/some_depot`* on the system *`some_host`*. |
| `swlist -d -l category @ \`<br>*`some_host:/some_dir/some_depot`* | Lists all category tags associated with the contents of the depot *`/some_dir/some_depot`* on the system *`some_host`*. |
| `swlist -a readme -l product` *`patch_id`* | Displays the readme documentation for patch *`patch_id`*. |
| `swlist -a readme -l product *,c=critical` | Displays the readme documentation for all patches installed on the local system which contain critical functionality. |
| `swlist -l product` *`some_bundle`* | Lists the products contained in bundle *`some_bundle`*. |
| `swlist -l product -a category_tag` *`patch_id`* | Lists the category tags for patch *`patch_id`*. |
| `swlist -l product -a category_tag \*,c=patch` | Lists the patches installed on the local system and their corresponding category tags. |

# Ancestors and Supersession

The related concepts of ancestors and supersession are integral to patches and patch management. It is important that you gain a basic understanding of both. It may also be helpful for you to recall information presented in "HP-UX Software Structure" (page 28).

## Ancestors

The ancestor of a patch is the original software product that a patch modifies. Ancestry is defined only at the fileset level. Each patch fileset has only one ancestor fileset that composes the base software that a patch modifies. However, there may be one or more versions of this ancestor fileset. The patch fileset has the same name as its ancestor. For example, fileset `Xserver.AGRM` is the ancestor of patch fileset `PHSS_29183.AGRM`. You can see an additional example in "Advanced Topic: Determining a Patch's Ancestors" (page 37).

Ancestry impacts both patch installation and patch removal. A patch fileset cannot be installed on a system unless its ancestor fileset software either is already installed or is being installed during the same operation. Similarly, when an ancestor fileset is removed, all the patches that have been applied to it are also removed.

## Advanced Topic: Determining a Patch's Ancestors

You can determine a patch fileset's ancestor using the patch's `ancestor` attribute with the SD-UX command `swlist`. The following command lists the ancestor filesets for the filesets of patch *`patch_id`*:

```
swlist -l fileset -a ancestor patch_id
```

For example:

```
> swlist -l fileset -a ancestor PHSS_29183
# Initializing...
# Contacting target "chb26006"...
# Target:  chb26006:/

# PHSS_29183
PHSS_29183.AGRM    Xserver.AGRM,fr=B.11.11,v=HP
PHSS_29183.DDX-ADVANCED Xserver.DDX-ADVANCED,fr=B.11.11,v=HP
PHSS_29183.DDX-ENTRY  Xserver.DDX-ENTRY,fr=B.11.11,v=HP
PHSS_29183.DDX-LOAD  Xserver.DDX-LOAD,fr=B.11.11,v=HP
PHSS_29183.DDX-SAM   Xserver.DDX-SAM,fr=B.11.11,v=HP
PHSS_29183.DDX-SLS   Xserver.DDX-SLS,fr=B.11.11,v=HP
PHSS_29183.DDX-UTILS   Xserver.DDX-UTILS,fr=B.11.11,v=HP
PHSS_29183.X11-SERV   Xserver.X11-SERV,fr=B.11.11,v=HP
PHSS_29183.X11-SERV-MAN Xserver.X11-SERV-MAN,fr=B.11.11,v=HP
PHSS_29183.XEXT-DBE   Xserver.XEXT-DBE,fr=B.11.11,v=HP
PHSS_29183.XEXT-DBE-MAN Xserver.XEXT-DBE-MAN,fr=B.11.11,v=HP
PHSS_29183.XEXT-DPMS  Xserver.XEXT-DPMS,fr=B.11.11,v=HP
PHSS_29183.XEXT-DPMS-MAN Xserver.XEXT-DPMS-MAN,fr=B.11.11,v=HP
PHSS_29183.XEXT-HPCR  Xserver.XEXT-HPCR,fr=B.11.11,v=HP
PHSS_29183.XEXT-HPCR-MAN Xserver.XEXT-HPCR-MAN,fr=B.11.11,v=HP
PHSS_29183.XEXT-MBX   Xserver.XEXT-MBX,fr=B.11.11,v=HP
PHSS_29183.XEXT-RECORD  Xserver.XEXT-RECORD,fr=B.11.11,v=HP
```

Patch filesets that have been applied to an ancestor fileset are listed in the ancestor's `applied_patches` attribute.

For example:

```
> swlist -a applied_patches Xserver.AGRM
# Initializing...
# Contacting target "chb26006"...
# Target:  chb26006:/

   Xserver.Runtime.AGRM
```

```
    PHSS_21817.AGRM,fa=HP-UX_B.11.11_32/64
    PHSS_26619.AGRM,fa=HP-UX_B.11.11_32/64
    PHSS_26622.AGRM,fa=HP-UX_B.11.11_32/64
    PHSS_26638.AGRM,fa=HP-UX_B.11.11_32/64
    PHSS_29169.AGRM,fa=HP-UX_B.11.11_32/64
    PHSS_29183.AGRM,fa=HP-UX_B.11.11_32/64
```

For more information see the Software Distributor Administration Guide on the HP Technical Documentation Web site at **http://docs.hp.com**.

## Supersession

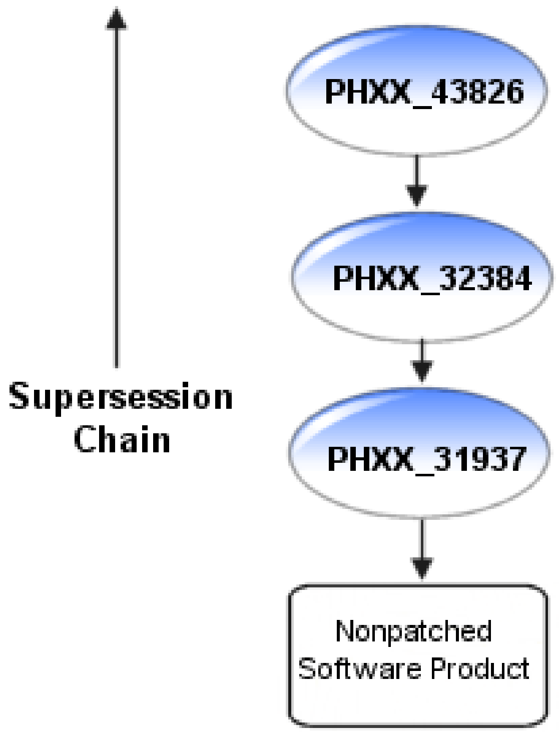
Supersession is the process of replacing an earlier patch with a new patch. A new patch supersedes all previous patches. Upon installation of the new (superseding) patch, its files replace files of the patches being superseded. Patches for HP-UX products are always cumulative. Each new patch contains all aspects of all its preceding patches.

A series of patches form a supersession chain. A supersession chain includes the following:

- The nonpatch software product being patched.
- Each patch that patches the nonpatch software product.
- Each patch that patches the patches.

Figure 3-1 shows a simple, hypothetical supersession chain in which a product has been superseded by PHXX_31937, which in turn has been superseded by PHXX_32384, which has been superseded by PHXX_43826. In general, patch numbers increase along a patch supersession chain.

**Figure 3-1** Patch Supersession Chain



The cumulative nature of a patch allows it to satisfy all dependencies on all patches it supersedes. The converse is not true, however. A superseded patch will not satisfy a dependency on a superseding patch. For more information about dependencies, see “Patch Dependencies” (page 43).

You can determine which patches a given patch supersedes by viewing either the patch's **patch details** page or the patch's patch text file. See the Supersedes field for more information.

## Advanced Topic: Displaying Supersession Information

By default, the SD-UX command swlist does not show superseded patches, but you can set it to show them:

**swlist -l patch -x show_superseded_patches=true**

You can also use the HP-UX Patch Tool show_patches (available via PHCO_18519 and its superseding patches) to show superseded patches. To show superseded patches, enter this command:

**show_patches –s**

You can list the filesets that have directly superseded the filesets of a given patch installed on your system. This is done by using the swlist command to show the superseded_by attribute of the patch. In the following example, patch PHSS_27875 is superseded by patch PHSS_28681:

```
  > swlist -l fileset -a superseded_by -x \
  show_superseded_patches=true PHSS_27875
  # Initializing...
  # Contacting target "some_system"...
  #
  # Target:  some_system:/
  #

  # PHSS_27875
  PHSS_27875.X11-JPN-S-MSG  PHSS_28681.X11-JPN-S-MSG,fa=HP-UX_B.11.11_32/64
  PHSS_27875.X11-RUN-CL        PHSS_28681.X11-RUN-CL,fa=HP-UX_B.11.11_32/64
  PHSS_27875.X11-TCH-B-MSG  PHSS_28681.X11-TCH-B-MSG,fa=HP-UX_B.11.11_32/64
```

You can also show the filesets that a given patch has superseded. These superseded filesets will be listed whether or not they are installed on your system. This is done by using the swlist command to list the supersedes attribute of the patch. Note that the first patch of any particular patch supersession chain does not have a supersedes attribute. In the following example, patch PHSS_28681 is shown to supersede patches PHSS_27875, PHSS_26498, and PHSS_25201. (The output has been reformatted to improve readability.)

```
     > swlist -l fileset -a supersedes PHSS_28681
     # Initializing...
     # Contacting target "some_system"...
     #
     # Target:  some_system:/
     #
     # PHSS_28681
       PHSS_28681.X11-JPN-S-MSG PHSS_27875.X11-JPN-S-MSG,fr=*
       PHSS_26498.X11-JPN-S-MSG,fr=*
       PHSS_28681.X11-RUN-CL
       PHSS_27875.X11-RUN-CL,fr=*
       PHSS_26498.X11-RUN-CL,fr=*
       PHSS_25201.X11-RUN-CL,fr=*
       PHSS_28681.X11-TCH-B-MSG
       PHSS_27875.X11-TCH-B-MSG,fr=*
       PHSS_26498.X11-TCH-B-MSG,fr=*
```

## Advanced Topic: Supersession and the patch_state Attribute

When a superseding patch is applied to a system, the superseded patch (if there was one) remains on the system but is not active. Only the top patch of the chain is in the active (applied) state. For more information about patch state, see “Patch State” (page 30).

You can use the following swlist command to show the patch_state attribute for patch *patch_id*:

**swlist -a patch_state -x show_superseded_patches=true** *patch_id*

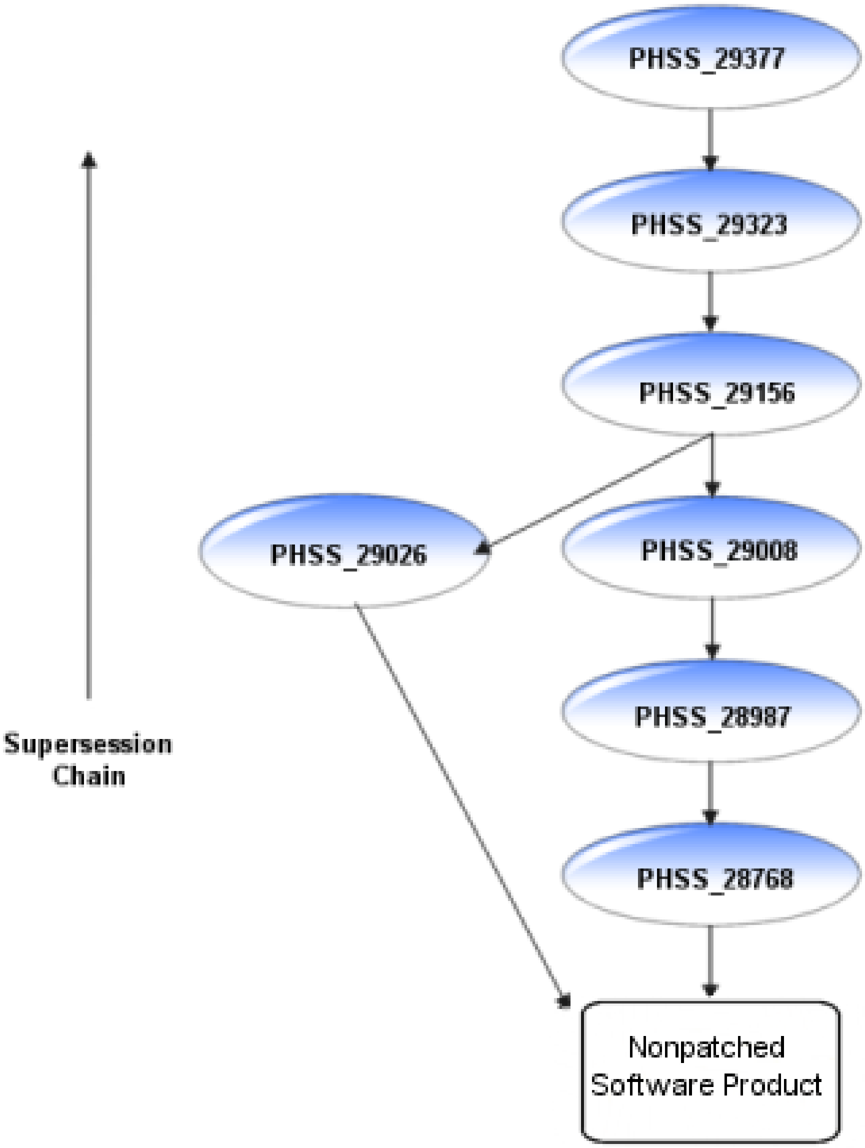
It is important to note that the availability of a newer, superseding patch does not preclude the use of the older patch. Depending on the circumstances, a superseded patch might be a better choice than the patch superseding it. Older patches have had more exposure to varied, real-world use. When they have been shown to induce no ill effects, they are generally safer than newer patches that supersede them. Thus, if two patches in a supersession chain solve the problem you are facing, you may find that the older patch is the better choice.

Because HP-UX patches are cumulative, a superseding patch negates the need for the previous patch. As an example, patch PHSS_29377 delivers all the features/fixes of all other patches shown in Figure 3-2: "HP-UX Patch Supersession Chain" (page 40). This patch will also satisfy any dependencies on all patches in the supersession chain.

SD-UX does not allow you to install a patch that has been superseded by another patch already installed on your system. Using Figure 3-2: "HP-UX Patch Supersession Chain" (page 40) as an example, if you have patch PHSS_29377 installed on your system SD-UX will not allow you to install patch PHSS_29323.

Patch supersession chains can be more complex than the one shown in Figure 3-2: "HP-UX Patch Supersession Chain" (page 40).

**Figure 3-2** HP-UX Patch Supersession Chain



The supersession chain in Figure 3-2: "HP-UX Patch Supersession Chain" (page 40) is composed of two separate supersession chains that were combined when patch PHSS_29156 superseded both PHSS_29026 and PHSS_29008. Again, because of the cumulative nature of HP-UX patches, patch PHSS_29377 delivers all the features and fixes delivered by the other six patches in this supersession chain.

## Patch-Related Attributes

Each of the SD-UX objects described in "HP-UX Software Structure" (page 28) has a set of properties known as attributes that provide information about the object's characteristics. For patches, these attributes control aspects of patch behavior and define patch properties and relationships. (See "State" (page 31) and "Patch State" (page 30).)

For information about how you can use attributes with the SD-UX `swlist` command, see "Which Patches Are on My System?" (page 33).

The following list describes a subset of available attributes:

- `ancestor`
  - Applies to filesets.
  - Identifies the fileset that must be on the system for the patch to be installable.
- `category_tag`
  - Applies to products or filesets.
  - Provides a label for a fileset or product. Several tags are defined during patch creation; users can create others with the `swmodify` command.
  - See "Category Tags" (page 31).
- `is_patch`
  - Applies to both patch products and filesets.
  - When set to `true`, `is_patch` enables patch behavior.
- `is_reboot`
  - Applies to filesets.
  - When set to `true`, `is_reboot` indicates that installation of the fileset will cause the system to reboot.
- `patch_state`
  - Applies to patch filesets.
  - Records the condition of patches.
  - See "Patch State" (page 30).
- `readme`
  - Applies to products.
  - Contains the patch's original text file.
- `software_spec`
  - Applies to bundles, products, or filesets.
  - Contains the fully qualified identifier for the bundle, product, or fileset. Uniquely identifies a specific instance of a software object.
- `state`
  - Applies to filesets.
  - Provides useful information about the installation state of software.
  - See "State" (page 31).

- `supersedes`
  - Applies to patch filesets.
  - Lists all prior filesets that a patch fileset supersedes.
  - See "Ancestors and Supersession" (page 37).
- `superseded_by`
  - Applies to patch filesets.
  - Records the software specification of the fileset that superseded the fileset on a given system. This attribute is set only for installed patch filesets, and never in software depots.
  - See "Ancestors and Supersession" (page 37).

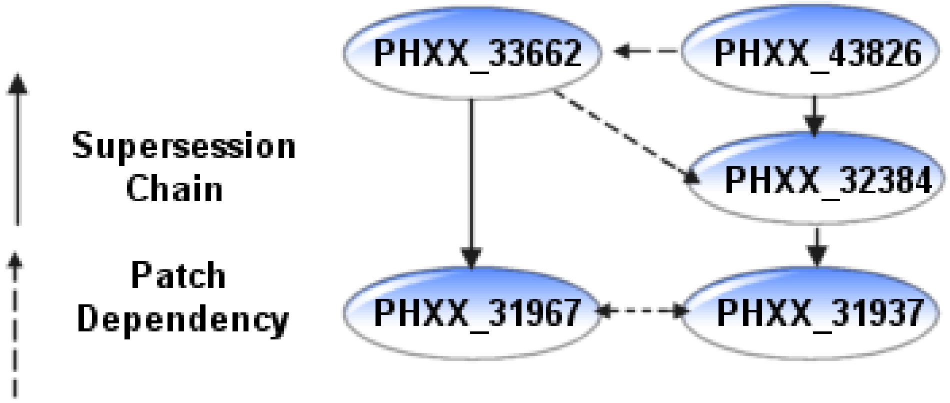
You can show these attributes with the `swlist` command using the `-a` *`attribute`* argument, replacing *`attribute`* with one of the previously listed attributes. For more information about `swlist`, see "Which Patches Are on My System?" (page 33).

# Patch Dependencies

A patch that depends on other software in order to install or run correctly is said to have a dependency on that other software. In order to become fully active, a patch may require changes to areas of the system other than those it modifies. Such a patch may have a documented dependency on one or more patches or nonpatch software products that are responsible for the changes in these other areas.

For example, in Figure 3-3: "Patch Supersession Chains and Patch Dependencies" (page 43), patch PHXX_33662 depends on patch PHXX_32384, and patch PHXX_43826 depends on PHXX_33662. Patches PHXX_31967 and PHXX_31937 depend on each other (mutual dependency).

**Figure 3-3** Patch Supersession Chains and Patch Dependencies



Because HP-UX patches are cumulative, a patch satisfies all the dependencies that all of its superseded patches satisfy. The opposite is not true, however. A superseded patch does not satisfy a dependency on a superseding patch. Figure 3-3: "Patch Supersession Chains and Patch Dependencies" (page 43) provides an example. Patch PHXX_33662 requires patch PHXX_32384, but PHXX_43826 can also satisfy this requirement because it supersedes PHXX_32384. However, patch PHXX_32384 does not satisfy PHXX_43826's dependency on PHXX_33662.

For more information about supersession, see "Ancestors and Supersession" (page 37).

## Types of Dependencies

HP provides patch dependency information for a patch in its patch text file and its **patch details** page. The dependency information is contained in the following fields:

- **Patch Dependencies**

  Patches that are required for proper operation.

- **Other Dependencies**

  Various dependencies that cannot be described as patch dependencies, such as those that are needed only under specific circumstances.

**NOTE:** While looking at a patch's patch text file or **patch details** page, you might notice an additional field that is dependency related. The **Hardware Dependencies** field represents a different type of dependency than those presented in this section. It does not show dependencies on other patches, but rather gives specific system models to which a patch is limited.

## Corequisites and Prerequisites

The following is a list of the most common dependency requisite types:

- A corequisite is a dependency in which one fileset requires that another fileset be installed or configured at the same time. For example, if fileset A requires that fileset B be installed at the same time, fileset B is a corequisite for fileset A.
- A prerequisite is a dependency in which one fileset requires another fileset to be installed or configured before the first fileset can be installed or configured. For example, fileset C may require that fileset D be installed before fileset C can be installed. Therefore, fileset D is a prerequisite for fileset C.

## Advanced Topic: Determining Corequisite/Prerequisite Filesets with swlist

You can use the following command to determine the dependent filesets. Replace *`dependency_type`* with either `corequisite` or `prerequisite`, as appropriate.

**`swlist -vl fileset -a`** ***`dependency_type fileset`***

For example:

```
 swlist -vl fileset -a corequisite PHSS_29964.DCEC-ENG-A-MAN
# Initializing...
# Contacting target "some_system"...
#  PHSS_29964.DCEC-ENG-A-MAN
fileset
corequisites   PHCO_24400.CORE-SHLIBS,fa=HP-UX_B.11.11_32/64
```

## Enforced and Unenforced (Manual) Dependencies

A patch's dependency upon another patch will either be enforced or unenforced by SD-UX. Starting with HP-UX 11i v1 (B.11.11), SD-UX install commands supported the use of requisites for enforcing dependencies. Prior to HP-UX 11i v1, users had to maintain dependencies manually.

- Enforced dependencies

  Dependencies that are registered using corequisite or prerequisite attributes and managed by SD-UX.

- Unenforced dependencies (also known as manual dependencies)

  Dependencies that SD-UX does not register as requisites and thus cannot enforce when performing patch installation. You can identify these types of dependencies by checking the `manual_dependency` category tag. The user must ensure that the required patches are installed to satisfy these manual dependencies.

## Impact of Dependencies on Acquiring Patches

HP strongly recommends that you use the ITRC as your primary source for acquiring patches. If you acquire individual patches using the ITRC's Patch Database, the patches required to meet the dependencies of these patches are automatically selected for download along with the patches you selected manually. The analysis performed by the Patch Database to select these patches takes into account supersession and patch warnings. Unless you have a specific reason to do otherwise, you should download these automatically selected patches along with the patches you explicitly selected. This automatic selection of patches represents one of the many time-saving features provided by the ITRC.

For a description of how to identify and acquire the additional patches that may be needed to satisfy dependencies, see "Advanced Topic: Checking for All Patch Dependencies" (page 81).

**NOTE:** If you download patches from sources other than the ITRC, such as an HP FTP server, you are completely responsible for identifying and downloading the patches required to satisfy all dependencies.

Standard HP-UX patch bundles, such as the Quality Pack, do not require users to perform any dependency analysis. All patches required to satisfy all dependencies are included in the bundles. Using standard HP-UX patch bundles increases confidence that you have obtained and installed all necessary patches to satisfy all dependencies.

# Patch Rollback and Commitment

This section describes patch rollback and commitment.

## Patch Rollback

You may occasionally want to remove a patch and restore the system to its prepatched state. This process is known as patch rollback. For example, if you installed a patch that resulted in unacceptable system behavior, you might choose to roll back this patch. However, rollback is possible only if certain files were saved as part of the patch installation process. During patch installation, the default behavior is to save copies of all files that are replaced by the new patch before the new versions of these files are loaded. These saved files are called rollback files and are the key to making patch rollback possible. When you roll back a patch, these rollback files are restored to the system. You should override the default behavior only if you have a complete understanding of the patch rollback process.

You cannot roll back a patch unless one of the following is true:

- Rollback files corresponding to the patch are available for reinstallation.
- Base software modified by the patch is removed at the same time (removing the base software also removes the patches associated with that software).
- For superseded patches, you must first roll back the superseding patch.

You can use the SD-UX command `swremove` to roll back a patch. Use the following command to roll back the patch *`patch_id`*:

```
swremove patch_id
```

As is true for many SD-UX commands, you can add the `-p` argument to execute the command in preview-only mode. This mode allows you to view output from the command without actual changes occurring. You initially should execute the command in preview mode:

```
swremove -p patch_id
```

## Advanced Topic: Patch Installation and Rollback Files

When installing patches, you can explicitly specify that rollback files not be saved. To do this, you add the `-x patch_save_files=false` option to the `swinstall` command:

```
>% swinstall -s /tmp/tmpdepot/depot -x autoreboot=true \
-x patch_match_target=true -x patch_save_files=false
```

Only use the false option if you will never remove a patch under any circumstances.

## Patch Commitment

Allowing for patch rollback does come at a cost, because the files required for patch rollback consume disk space. If disk space is an issue on your system, you can commit your patches; a process that deletes the associated rollback files, thereby freeing disk space. If disk space is not an issue on your system, you should avoid committing the patches, and leave rollback files in place. If any patch in a supersession chain is committed, all prior patches in the chain lose the ability to be restored, and the save area disk space for those patches will also be reclaimed.

Do not undertake patch commitment without serious consideration of the consequences. When you commit a patch, simple rollback of the patch is no longer possible. Because of this, you should carefully select which patches should be committed. Good candidates include patches that were thoroughly tested in your environment prior to installation, and patches that have been installed on the system for a significant period of time and have not resulted in unwarranted conditions. Other good candidates are patches that have been superseded multiple times. You should also consider a patch's warning status and its HP rating before committing the patch.

To commit an individual patch, execute the SD-UX command `swmodify` on the patch with the *`patch_commit`*`=true` option. To commit the patch *`patch_id`*, enter this command:

**swmodify -x patch_commit=true** *patch_id*

You can add the `-p` argument to this command so it will be executed in preview-only mode.

## Advanced Topic: Patch Cleanup Utility

The patch utility called `cleanup` allows you to commit all patches that have been superseded a specified number of times. You can execute this command in preview mode in order to see what effect the command will have without actually making any changes. You should always use the preview mode first. This is accomplished by including the `-p` argument. The command has the following format:

**cleanup [-p] -c** *number*

The cleanup utility is delivered by the following patches (and their superseding patches):·

- `PHCO_27779 (HP-UX 11.0, B.11.00)`
- `PHCO_27780 (HP-UX 11i v1, B.11.11)`

For example, the following command will execute in preview mode. When executed without the `-p` option, the command causes all patches superseded three or more times to be committed. The patches to be committed are shown in the output of the command.

```
> cleanup -p -c3
### Cleanup program started at 04/13/04  07:17:40
Preview mode enabled. No modifications will be made.
Commit patches superseded at least 3 time(s) on 'some_system'.
Obtaining superseded patch information...done.

The following patches superseded at least 3 time(s) can be committed:

Superseded  # Times Superseded  Disk Space in /var/adm/sw/save  Superseded By
==========  ==================  ==============================  =============
PHKL_23313           3                    66560 bytes             PHKL_26519
PHKL_26233           3                   180224 bytes             PHKL_28267
PHNE_23288           3                    59392 bytes             PHNE_23645
PHNE_26388           4                  6581248 bytes             PHNE_28103
PHNE_28103           3                  6694912 bytes             PHNE_28983
PHSS_21817           5                 12379136 bytes             PHSS_26619
PHSS_26492           3                  8761344 bytes             PHSS_27872
PHSS_26619           4                 14969856 bytes             PHSS_26622
PHSS_26622           3                 27064320 bytes             PHSS_26638

All information has been logged to /var/adm/cleanup.log.
### Cleanup program completed at 04/13/04  07:17:40
```

# HP-UX Patch Ratings

HP-UX patches have a corresponding quality rating called the HP rating. HP assigns a patch rating of 1 (numeral or star) to each HP-UX patch when it is released. Over time, HP may update the rating value to 2 or 3 (numeral or stars) to convey increased confidence in the patch. The higher the rating, the lower the risk of side effects and the more suitable the patch is for mission-critical environments.

You can use the ITRC's Patch Database to find the rating value for a specific patch. The ITRC graphically represents a patch's rating by displaying one to three stars beside the patch ID in the results of a patch search. "Obtaining Information Using the ITRC" (page 52) provides details on how to do this.

If HP learns of a problem caused by or exposed by an HP-UX patch, HP issues a patch warning describing the problem and ceases recommending the patch, but does not change the patch rating. If a patch has a warning associated with it, you will no longer be able to view the rating on the ITRC's patch database. For more information on patch warnings, see "Patch Warnings" (page 53).

The following rating related information pertains only to patches that have no associated warnings.

## HP Patch Rating of 1

Although these patches have passed rigorous prerelease testing, HP recommends that you use these patches only if all of the following conditions are true:

- If you are in a reactive patching situation.
- The highest-rated patch that addresses the problem is rated 1.
- You cannot wait for the patch to increase to a higher rating.

Whenever possible, you should wait until the patch gains more exposure and achieves a rating of 2 or 3. For more information on reactive and proactive patching, see Chapter 4: "Patch Management Overview" (page 57).

### Rating Details

The following list provides more details about patch ratings of 1:

- Upon release, patches are assigned a rating of 1.
- These patches have successfully completed internal testing by HP.
- Because they are new, these patches have an inherent level of risk associated with them that you may find unacceptable. However, they are made available in case you are willing to accept the increased risk because the patch resolves a specific issue on your system.
- If you choose to use one of these patches, you should evaluate and test it carefully prior to deployment on a system.

## HP Patch Rating of 2

HP recommends that you use patches rated 2 for both proactive and reactive patching and when a patch rated 3 is not available.

Patches rated 1 may be upgraded to a rating of 2 on any given day (based on the amount of customer exposure). Therefore, if you chose to defer patch installation to wait for a patch rating to be upgraded to a rating of 2, you can check for this upgrade on a daily basis.

### Rating Details

The following list provides more details on patch ratings of 2:

- These patches have met minimum criteria based on the number of days available to customers and the number of times downloaded with no problems reported.
- These patches may appear in the **recommended** column of the ITRC's Patch Database **patch search results** page (provided they have no associated patch warnings).

## HP Patch Rating of 3

Rating 3 is the highest rating HP assigns to a patch. These patches represent the lowest level of risk. HP recommends you use patches rated 3 whenever possible for both proactive and reactive patching.

If you are waiting for a specific patch to reach a rating of 3, check the patch quarterly to determine whether it has been promoted from a rating of 2 to a rating of 3.

### Rating Details

The following list provides more details on patch ratings of 3:

- These patches have passed more levels of testing than patches rated 1 or 2.
- These patches may appear in the **recommended** column of the ITRC's Patch Database **patch search results** page (provided they have no associated patch warnings).

## Critical and Noncritical Patches

HP-UX patches are considered to be either critical or noncritical. You can determine whether a patch is labeled as critical by looking at the **Critical** field on the **patch details** page or in the patch text file for the patch. This field identifies newly delivered critical content.

HP considers a patch to be critical if the patch provides a fix for a critical problem. Examples include patches that provide fixes for the following problems:

- System panic or hang
- Process abort, hang, or failure
- Data corruption
- Severe performance degradation
- Application-specific critical issues

HP considers a patch to be noncritical if the patch provides fixes for only noncritical problems. Examples of noncritical problems include the following:

- Extraneous debug, warning, or error messages
- Failure to address all documented issues
- Minor regressions in behavior

A patch is considered critical if it contains any critical fixes, even if they were introduced in earlier (superseded) patches. The **Critical** field for such a patch contains the following text:

`“No (superseded patches were critical)”`

In addition, the field gives the ID of the patch that introduced the critical fix. The **Critical** field for patch `PHSS_30011` is shown in Figure 3-4, “Critical Field for PHSS_30011”, and it shows that superseded patch `PHSS_29735` actually introduced the critical fix.

**Figure 3-4** Critical Field for PHSS_30011

```
Critical:No (superseded patches were critical)
PHSS_29735: CORRUPTION
```

Critical patches have a `critical` category tag. The category tags (and `swlist` command used to acquire the category tags) for this patch are shown in Figure 3-5: “Category Tags for PHSS_30011” (page 49). See “Category Tags” (page 31) for more information.

**Figure 3-5** Category Tags for PHSS_30011

```
> swlist -l product -a category_tag PHSS_30011
# Initializing...
# Contacting target "some_system"...
#
# Target:  some_system:/
#  PHSS_30011    patch defect_repair general_release critical enhancement
                            corruption manual_dependencies
```

## Finding Information for a Specific Patch

The best place to obtain information about a specific patch is the patch's **patch details** page on the ITRC.

## Patch Documentation

All patches have a **patch details** page, a patch text file, and readme information. The **patch details** page should be your first choice for obtaining information because it contains the most up-to-date information available. This is not always true for the patch text file or the patch readme.

You can find the documentation at the following resources:

- See Chapter 6: "Using the IT Resource Center" (page 75). For the **patch details** page, go to the ITRC Web site at **htttp://itrc.hp.com**.
- The patch text file will be in the downloaded file after you download a patch from the FTP servers or from the ITRC. See Chapter 6: "Using the IT Resource Center" (page 75), and Chapter 7: "Using FTP as an Alternative Patch Source" (page 89).
- The patch readme will be on your system after you install the patch.

The **patch details** page and the patch text file contain the same fields and provide detailed information about a patch. Table 3-2: "Subset of Fields in Patch Text File and Patch Details Page " (page 51) shows a subset of these fields.

**Table 3-2** Subset of Fields in Patch Text File and Patch Details Page

| Field | Description |
|---|---|
| **Patch Name** | The patch ID. See "Patch Identification" (page 28) for more information about the format of patch IDs. |
| **Patch Description** | A terse description of the patch. |
| **Creation Date** | The date the patch was created. |
| **Post Date** | The date the patch was released for general distribution. |
| **Warning** | If the patch has an associated warning, this field shows the date the warning was issued and provides information about the warning. This field is present only if the patch has an associated warning. For more information, see "Patch Warnings" (page 53). |
| **Hardware Platforms - OS Releases** | The hardware platforms and HP-UX OS releases where you can install the patch. |
| **Filesets** | A listing of the filesets that compose this patch. |
| **Automatic Reboot?** | This is set to **Y** if the installation of this patch requires a reboot. |
| **Status** | The support status of the patch. For more information, see "Patch Status" (page 30). |
| **Critical** | If this patch is considered critical, or if it supersedes a critical patch, additional information is provided. For more information, see "Critical and Noncritical Patches" (page 49). |
| **Category Tags** | A listing of the categories associated with this patch. For more information, see "Category Tags" (page 31). |
| **Path Name** | The location of this patch on the HP FTP servers. See Chapter 7: "Using FTP as an Alternative Patch Source" (page 89) for more information about the FTP servers. |
| **Symptoms** | The symptoms of the problem. |
| **Defect Description** | A detailed description of the defect. |
| **Enhancement** | This is set to **Y** if the patch is an enhancement. |
| **Patch Dependencies** | All patches that this patch depends upon for proper operation. You must install the listed patches if you are installing this patch. For more information, see "Patch Dependencies" (page 43). |
| **Hardware Dependencies** | The specific system models to which this patch is applicable. |
| **Other Dependencies** | The various dependencies that cannot be described in a simple manner. For example, dependencies that are needed only under specific circumstances will be listed here. For more information, see "Patch Dependencies" (page 43). |
| **Supersedes** | A list of all patches replaced, or superseded, by this patch. For more information, see "Ancestors and Supersession" (page 37). |
| **Installation Instructions** | The standard installation instructions common to all patches. |
| **Special Installation Instructions** | Any special instructions not included in those mentioned previously. This field occasionally includes dependency information. |

## Advanced Topic: The readme Attribute

Each patch has an SD-UX attribute called readme that you can view using the SD-UX command `swlist`. See "Patch-Related Attributes" (page 41) for more information about attributes. The readme attribute contains the patch's original text file. Be aware that, although the `readme` attribute allows you to quickly and conveniently access information about patches on your system, this information is static. Because of this, the readme will not contain more current information.

For example, even if a patch has an associated warning, the readme file won't contain a **Warning** field.Because the command returns a large amount of text, you may want to either redirect the output to a file or pipe the output to the `more` command, as follows:

```
swlist -l product -a readme patch_id | more
```

You can use other variations of the `swlist` command to obtain the `readme` information for multiple patches. For example, if you want to obtain the readme information for all patches on your local system that have manual dependencies, you can use the following command (output is redirected to the file `manual.txt`):

```
swlist -l product -a readme *,c=manual_dependencies > manual.txt
```

## Obtaining Information Using the ITRC

The ITRC's Patch Database is your best resource for acquiring information about a specific patch. Consult Chapter 6: "Using the IT Resource Center" (page 75) and Chapter 2: "Quick Start Guide for Patching HP-UX Systems" (page 17) for more information about using the Patch Database, including information about downloading patches and satisfying dependencies.

### Accessing Information on the ITRC

1. Log in to the ITRC at **http://itrc.hp.com**.

   Be sure to log in to the appropriate site (Americas/Asia-Pacific or European).

2. Select **maintenance and support (hp products)**.
3. Select **find individual patches and firmware**.

   You are now in the Patch Database.

4. Select **HP-UX** to go to the **search for patches** page.
5. To find instructions, select the **How would you like to search? and Search Criteria,** then read the **usage guide** links.
6. Enter the appropriate hardware and OS information.

   For the hardware, use **700** for workstations and **800** for servers.

7. From the drop-down list, select **Search by Patch IDs**.
8. In the text box next to the drop-down list, enter the patch ID for the patch you want to download. Then select **search**.

   If it exists, the selected patch displays in the **search results** page. Patches (possibly differing from the patch you requested) are displayed in one to three columns.

   - You can display the **patch details** page for a specific patch by selecting the patch ID.
   - Unless a patch has a warning, the HP rating is represented graphically by the number of asterisks (*, **, or *** ) displayed next to a patch's ID.
   - If a patch has a warning, the patch has a triangular yellow icon displayed beside it.
   - If the patch searched for has a warning, available replacement patches might be shown in the **recommended** and **most recent** columns. If you choose to use a replacement and there is a patch shown in the **recommended** column, this is the patch you should use.

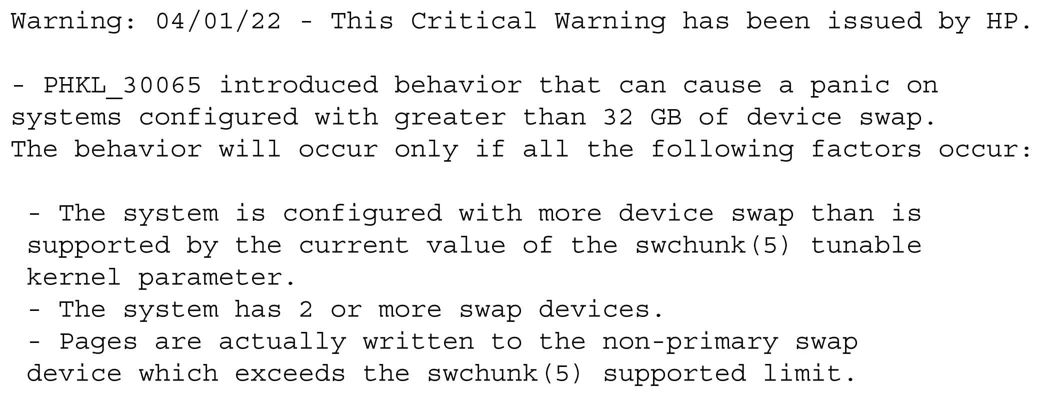
# Patch Warnings

Patch warnings are a notification that a patch causes or exposes adverse behavior. Patch warnings provide specific information about this incorrect behavior, as well as other important details and recommendations. This information helps you to make decisions, about the patch, such as whether to install or remove a patch with a warning from your system.

## The Warning Field

You can find patch warning information in the **Warning** field of a patch's **patch details** page or patch text file. This field exists only for patches that have a warning. The **Warning** field is your definitive source of information about a patch warning. Figure 3-6: "Warning text for PHKL_30065" (page 53) shows the **Warning** field for patch `PHKL_30065`.

**Figure 3-6** Warning text for PHKL_30065



```
Warning: 04/01/22 - This Critical Warning has been issued by HP.

- PHKL_30065 introduced behavior that can cause a panic on
systems configured with greater than 32 GB of device swap.
The behavior will occur only if all the following factors occur:

 - The system is configured with more device swap than is
 supported by the current value of the swchunk(5) tunable
 kernel parameter.
 - The system has 2 or more swap devices.
 - Pages are actually written to the non-primary swap
 device which exceeds the swchunk(5) supported limit.
```

The **Warning** field contains the following information:

- The issue date of any warnings (year/month/day format)
- Whether the patch warning is critical or noncritical (see "Critical and Noncritical Warnings" (page 53))
- A description of the problem
- A suggested course of action for the problem might be provided
- A reference to a replacement patch might be provided

See "Finding Information for a Specific Patch" (page 50) for a description of how you can access a **patch details** page and a patch text file.

## Critical and Noncritical Warnings

Patch warnings are either critical or noncritical. You can find this information in the first line of the **Warning** field in the patch's **patch details** page or in the patch text file.

HP considers a patch warning to be critical if the patch causes or exposes a critical problem. Examples of critical patches include the following:

- System panic or hang
- Process abort, hang, or failure
- Data corruption
- Severe performance degradation
- Application-specific critical issues

HP considers a patch warning to be noncritical if the patch causes or exposes a noncritical problem. Noncritical problems are those other than the ones described previously. Examples of noncritical problems include the following:

- Extraneous debug, warning, or error messages
- Failure to address all documented issues
- Minor regressions in behavior

## How to Handle Patch Warnings

Your initial response to a warning for a patch on your system should be to carefully read the associated warning text and research the issue to gain a complete understanding of how or if the warning will impact your system.

Because of the number and complexity of the factors involved, there is no single correct way of dealing with a patch with a warning. The following items show some possible courses of action:

- In some cases, such as if you encounter a critical problem on your system, immediate removal of the patch may be necessary.
- In many cases, removal and replacement can wait until the next scheduled maintenance window.
- In other cases, such as when the problem does not affect your hardware or software configuration, there is no need for you to take any action. In fact, HP discourages unnecessary change because it can cause down time and because there is always some risk when making a change to your system.

## Questions to Ask

If you must deal with a patch that has a warning, consider the following questions in deciding whether or not to use, or continue to use, the patch:

- Is your system environment susceptible to the problem?

  A patch with a warning may not cause problems for every customer. Exposure depends on your system-use models, and whether you have any of the affected configurations. Figure 3-6: “Warning text for PHKL_30065” (page 53) is a good example of this situation. Unless your system is configured with greater than 32 GB of device swap and meets all the other conditions listed, the patch warning given for patch `PHKL_30065` will have no impact on your system.

- Is a replacement patch available, and, if so, is its HP rating acceptable for your system?

  A replacement patch may be available. You can use the ITRC Patch Database to attempt to locate such a patch. Simply search using the explicit patch ID of the patch that has a warning. If there is a replacement patch, it will be displayed in the **search results** page. If a replacement patch exists, you must take into account its advantages and disadvantages. This includes consideration of the patch's HP rating. See “HP-UX Patch Ratings” (page 47).

After answering the previous two questions, you must consider the following questions in order to develop an appropriate course of action for your situation:

- What is the severity of the problem associated with the patch?
- If the patch is already on your system, has it caused any problems?
- What is your tolerance for down time if a reboot is necessary?
- What is the timing of the next maintenance window?
- What are your company's system administration policies?

As a final point, if you choose to remove a patch with a warning from your system, make sure that the patch is not contained in any of your depots used for patch installations. For more information about patch depots, see Chapter 8: “Using Software Depots for Patch Management” (page 99).

## Advanced Topic: Finding Patches with Warnings on Your System

HP provides the Security Patch Check Tool at no charge. The primary purpose of this tool is to allow you to generate a report of recommended security patches based an analysis of the filesets and patches installed on your system. However, the Security Patch Check Tool also reports any patches with warnings that are present on the system. See Chapter 9: “Using Other Patch Tools” (page 127).

You can download the HP Security Patch Check Tool from the Software Depot Home Web site at **http://software.hp.com**.

You can find more information about the Security Patch Check Tool by searching for the Security Patch Check FAQ on the HP Technical Documentation Web site at **http://docs.hp.com**.

## Backup and Recovery

Always perform a backup of your system before making patch-related system changes. You should have a backup in the event that unacceptable behavior occurs as a result of patching.

This section provides some resources that you can investigate for recovery strategies. It does not provide the details needed for recovering from patch-related problems.

- HP Ignite-UX (IUX)
    - IUX is a set of tools that you can use for system installation, recovery, and duplication.
    - The `make_net_recovery` and `make_tape_recovery` features of IUX can be good starting points for investigating IUX recovery tools.
    - See the following for more information about IUX:
        - **http://software.hp.com/products/IUX**
        - **http://docs.hp.com**

          Search for Ignite-UX.
- Data Protector is an HP product that you can use for data protection and disaster recovery.

  For more information, see the HP OpenView Storage Data Protector Web site at **http://h18006.www1.hp.com/products/storage/software/dataprotector/index.html**.

## Considerations

- You should have a detailed recovery plan formulated before you install any patches.
- You should know how long your system can be down for patch installation, and set aside a portion of that time for recovery in case it is required.
- When patching critical systems, some customers have a redundant environment in place to take over in the event that anything goes wrong with the production system.
- If you install patches with patch rollback files, then patch rollback will be an option if there are problems with the patch installation. See "Patch Rollback and Commitment" (page 45).

## Where to Go Next

Read more about patch management in Chapter 4: "Patch Management Overview" (page 57).

# 4 Patch Management Overview

Patch management is a process used to ensure that the appropriate patches are installed on a system. Patch management is becoming increasingly important for users of all types of systems, from desktop systems to mission-critical servers.

Industry experience has shown that failures in patch management can lead to financial loss, loss of data, exploitation of security vulnerabilities, and other negative consequences. Problems such as these can damage an organization's reputation, and can even result in legal consequences. Because of this, many organizations are finding that having a robust patch management process in place is no longer optional. Additionally, many of these organizations require their overall patching strategy to include a proactive patching component similar to the one presented in this chapter.

Although patch management should be a topic of concern to all users, a robust patch management strategy is especially important if your environment includes any of the following:

- Mission-critical systems

  Can lessen your exposure to a variety of risks.

- Large number of systems

  Can result in more efficient and effective patching.

The chapter presents some basic patch management strategies and concepts. Some of the concepts are general in nature, whereas others are specific to patching HP-UX systems.

## Patch Management Life Cycle

The following list presents the primary functions of a patch management life cycle:

1. Following a formal patch management strategy.

   You should develop and follow a formal patch management strategy, incorporating the appropriate concepts to meet your availability needs. Ideally, your strategy should include proactive patching, reactive patching, and a separate plan for security patches. These topics are described later in this chapter.

2. Identifying and acquiring patches.

   First, determine which patches you need in various circumstances:

   - If you encounter a problem, you must determine which patches you need to resolve it.
   - Monitor your systems regularly to determine whether there are security patches or critical patches available for your system, or whether warnings have been issued against installed patches.
     - The Security Patch Check Tool can help you identify security patches applicable to your systems, as well as patches installed on your system that have an associated warning. For more information, see Chapter 9: "Using Other Patch Tools" (page 127).
     - If you download patches using the HP IT Resource Center (ITRC), you will be sent an email notification if a warning is issued against any patch you downloaded. For more information, see Chapter 6: "Using the IT Resource Center" (page 75).
   - Determine whether the patches chosen for installation require additional patches or other software to satisfy dependencies. The ITRC Patch Database can help you with this task.

   Second, use standard HP-UX patch bundles as your starting point:

   - HP provides standard HP-UX patch bundles including the Quality Pack (QPK) and Hardware Enablement (HWE) patch bundles. The QPK consists of defect fixes and the HWE consists of patches that are required for new hardware products. These bundles generally consist of all recommended patches. This provides a convenient and timesaving starting point to acquire patches. Simply download the bundles from the ITRC or your latest HP media.
   - If you have constructed a list of patch needs, compare that with the patches in your selected bundles. If you are missing patches from your list, obtain them individually using the ITRC Patch Database.
   - For more information about standard HP-UX patch bundles, see Chapter 5: "What Are Standard HP-UX Patch Bundles?" (page 69).

3. Deploying patches.

   - Patch testing.

     You should install the patches on one or more levels of preproduction systems and perform testing. Testing is discussed in more detail later in this chapter.

   - Planning deployment.

     Determine the details regarding how the installation of the patches will occur on production systems. The frequency and timing of patch installation maintenance windows must be chosen to meet with your particular system down time limitations and your need to install the new patches. You might choose the timing of patching to coincide with your current maintenance windows. However, for reactive patching, you may be required to use unscheduled maintenance. For proactive patching, common intervals are quarterly, every other quarter, and yearly. You should also consider the availability of new patches and, if you are using standard HP-UX patch bundles, you will likely want to choose a schedule that in some way coincides with the release dates of new bundles.

     Some specific criteria to consider when plannning your change:

     - Backup of your system.
     - System down time.

    - When are your maintenance windows? What length of time are they?
    - In the event of patches causing negative side effects, what steps will you take to back out changes, and how long will it take to execute these steps?
  - Installing patches.
    - Review Special Installation Instructions.

      Prior to beginning the process of patch installation, review the patches to be installed to find any associated Special Installation Instructions.
    - Install patches on your systems.
    - Verify patches.

      Verify that the patches installed correctly and that the patch had the desired effect.
    - Recover disk space.

      If disk space is an issue, you may find that you need to commit patches. This process recovers disk space consumed by files that were saved to allow patch rollback. Your organization should develop a formal plan to determine when and how patches should be committed. See Chapter 3: "HP-UX Patch Overview" (page 27) for more information.

4. Tracking the patch levels of your systems. (Patch level refers to the set of active patches on the system.)

   You should know the patch levels of each of your systems.
   - Patch level is important when determining which patches are needed on each system.
   - You need to know the patch levels of your systems when interpreting patch testing results.
   - If you need to open a support call, you may be asked for the current patch level to aid in troubleshooting.

   You should keep all similarly configured production systems at the same patch level.
5. Managing patch-related changes to systems.
   - You may find it helpful to log all patch-related system changes.
   - You may find it helpful to document the results of patch testing and installation.
   - Many customers find it helpful to have a formal change-request process associated with their patch management process.

# HP Service Contracts

If you would like assistance with your patch management work, you can purchase a Mission Critical level HP service contract. This entitles you to a proactive service called patch analysis. In patch analysis, an HP support engineer furnishes you with a custom list of recommended patches. At the Mission Critical (highest) contract level, your assigned HP engineer even helps you define a patch management strategy based on the software change management principles defined in this chapter. For more information, visit the HP Software Support Services Web site at **http://www.hp.com/hps/software**.

# Advanced Topic: For More Information

If you want additional patch management information, see the following white papers:

- Patching Usage Models
- Patching Mission Critical Systems

Both are available on the HP Technical Documentation Web site at **http://docs.hp.com**.

# Patch Management and Software Change Management Strategies

Patch management is a complex topic. Because of the complexity, there is not one right way to perform patch management. If you ask 10 patching experts to describe their approach to patch management, you will likely get 10 different answers. You must determine which approach to patch management works best in your situation based on your particular environment and your constraints.

This section discusses software change management and recommendations, as well as the three basic patch management strategies among others:

- Proactive patch management strategy
- Reactive patch management strategy
- Security patch management strategy (Advanced Topic)

You may find that one of these strategies is a good fit for your organization. In most cases, a customized combination works well. For example, you could choose a reactive patching strategy for most patching, but proactively patch your most update-sensitive areas. Security patch strategies often do not fit within the proactive or reactive strategies. In these cases, you need to follow a different strategy. Again, there is more than one path to creating an acceptable patch management strategy.

## Establishing a Software Change Management Strategy

This section outlines a set of patch management strategies based on use and tolerance for down time. There is always a risk that software patches that have been successfully tested in a controlled environment will cause problems when applied to a new configuration. For this reason, it is important to limit the number of changes made to a target system.

The first step in defining your strategy is to determine what level of software change management you want to implement. HP has developed three strategies for dealing with software change management in mission critical environments. These strategies are based on operational requirements. The same concepts apply just as well to non-mission critical environments.

The following are three strategies for software change management. These strategies are described in Table 4-1: "Operational Factor/Patch Management Strategy Matrix" (page 63):

- Restrictive
- Conservative
- Innovative

The process of selecting an appropriate software change management strategy seeks to align behavior with the key business objectives of the systems involved. The goals of evaluating an operation and choosing an appropriate strategy include:

- Reduced risk
- Increased system and application availability
- Reduced maintenance time

There are four operational factors that should determine your appropriate strategy:

- New features

  Do you need to introduce new operating system or application features into the operating environment?

- Unplanned down time

  What is your tolerance for the operation being unavailable outside the scheduled maintenance windows?

- Impact on core business

  How are business functions affected by down time?

- Self-maintenance

  This is an indication of whether or not all system planning and maintenance activities are performed inhouse without vendor or third-party involvement.

**Table 4-1** Operational Factor/Patch Management Strategy Matrix

| Patch Management Strategy | New Features | Unplanned Down time | Impact on Core Business | Self-Maintenance |
|---|---|---|---|---|
| Restrictive | No | Unacceptable | High | No |
| Conservative | No | Unacceptable | Medium | No |
| Innovative | Yes | Acceptable | Low | Yes |

## Recommendations for Software Change Management

The following are recommendations for software change management that correspond to each software change strategy. They cover the following five areas:

- Operating System and Applications

  Includes versions of the operating system as well as the applications running in the environment.

- Proactive Patching

  Includes all patching activities for which no symptoms or problems are currently evident.

- Reactive Patching

  Performed in response to a visible system problem.

- Change Management

  Covers all processes and standards used to manage data center operations.

- Test Environment

  Includes systems, software, and equipment used to support the production operations. The test environment is used to evaluate changes before they are put into production.

Table 4-2: "Recommendations Based on Strategy" (page 63) offers recommendations to help you implement your chosen software change management strategy.

**Table 4-2** Recommendations Based on Strategy

| Strategy | OS & Applications | Proactive Patching | Reactive Patching | Change Management | Test Environment |
|---|---|---|---|---|---|
| Restrictive | Stable release, available for one year or more. | Use only thoroughly tested patches with the highest level of exposure. | Make fewest changes possible to restore function.<br>Perform full diagnostic analysis before attempting a solution. | Formal plan with explicit roles and responsibilities.<br>Prepared plan to back out changes, if necessary.<br>Documented disaster recovery plan that is updated and tested at least yearly. | Dedicated equipment that matches production environment, including simulated loads. |
| Conservative | Stable release, available for six months or more. | Use only thoroughly tested patches with substantial exposure. | Make fewest changes possible to restore function.<br>Perform full diagnostic analysis before attempting a solution. | Formal plan with explicit roles and responsibilities.<br>Prepared plan to back out changes, if necessary. | Dedicated equipment that matches production environment. |
| Innovative | Stable release, available for two months or more. | Carefully review patches for risks and benefits. | Focus on restoration of function.<br>Limit number of concurrent changes. | Established roles and responsibilities. | Test or development equipment or off hours on production environment. |

## Consideration of HP Patch Rating

Regardless of the type of patching strategy you choose to implement, you should include a policy detailing when it is appropriate to select patches for each HP patch rating. Based on rating alone, it is always appropriate to select a patch rating of 3, but under what circumstances will you allow patches rated 2 or 1 to be installed?

For more information about HP patch ratings, see "HP-UX Patch Ratings" (page 47).

## Patch Management and Software Depots

Users with multiple systems generally find that, regardless of the type of patching strategy they choose to implement, patch management is best accomplished by managing patches in centralized software depots. You should maintain one depot for each set of similarly configured systems. You then use these depots as your patch source for all patch installations. In this way, you can maintain the same patch level on all your systems with less overall effort. Using depots also minimizes reboots when you install new patches. You should be able to install the entire content of a single depot with only a single reboot.

For more information about these Software Distributor for HP-UX (SD-UX) software depots, see Chapter 8: "Using Software Depots for Patch Management" (page 99).

## Proactive Patching Strategy

The goal of a proactive patching strategy is problem prevention. Many patches that provide defect fixes are released long before you need them on your system. The crux of proactive patching is identifying these patches and applying them in a safe manner. By definition, your starting point for proactive patching should be a system you believe to be functioning normally. Most proactive patching can be scheduled and carefully controlled. This is one of the benefits of this approach.

As compared with the reactive patching strategy (see the following section), proactive patching generally creates more system change and requires regularly scheduled patch installation maintenance windows. Although the system down time associated with patch installation is a disadvantage of proactive patching, HP highly recommends a proactive patching as the strategy of choice.

The following benefits can be achieved by implementing a proactive patch management strategy:

- Problem avoidance
- Reduced risk
- Reduced unplanned down time
- Enhanced functionality and tools
- Increased time for testing

Because proactive patching involves installation of patches before a problem occurs, this strategy allows more time to complete sufficient testing than does reactive patching.

### Acquiring Patches for Proactive Patching

Although patching is not a one-size-fits-all process, the following generic recommended strategy embodies many of our customers' best practices:

1. Identify the patches to acquire. You can identify and track these on an ongoing basis, or you can engage in patch analysis that targets a specific proactive patching cycle.
2. Acquire the latest Quality Pack (QPK) patch bundle and, if you are planning any hardware changes, the latest Hardware Enablement (HWE) patch bundle.
3. Determine whether the patches included in the standard HP-UX patch bundles cover your entire list of identified patches. Use the ITRC Patch Database to acquire any missing patches.
4. Scan the patches for warnings, and run the Security Patch Check Tool.
5. Create one depot for the acquired patches and copy them into it. You can choose to copy the latest Operating Environment (OE) products to the depot.
6. Test the depot content.
7. Create a deployment plan and roll out the new depot within your maintenance window.

The following details apply to acquiring the latest QPK and HWE patch bundles:

- The QPK bundle is an excellent vehicle for proactive patching and was created for this purpose. The HWE bundle contains patches required by new hardware products that HP has released. To enable or preenable support for new hardware, you should select this bundle. New HP-UX core features are introduced as part of the Software Pack (SPK). If you want to install one of these new features, select the SPK.
- All the standard HP-UX patch bundles can be downloaded from the ITRC and are available on media from HP. For more information, see Chapter 5: "What Are Standard HP-UX Patch Bundles?" (page 69).
- If you have a support contract at the Mission Critical level, you are entitled to a regular customer patch analysis from HP. This analysis results in the creation of custom patch bundles for your distinct computing environments.

Use the ITRC Patch Database Tool to acquire any patches that you have not yet obtained. Compare the entire list of patches that you identified specifically for your environment with the content of your patch bundles.

- If you are missing just a few patches, use the ITRC Patch Database to acquire them. For more information about using the ITRC, see Chapter 6: "Using the IT Resource Center" (page 75).
- If you are missing numerous patches, you might prefer to use the ITRC Patch Assessment Tool to acquire them. See "Advanced Topic: The Patch Assessment Tool" (page 65).

The following details apply to patches with warnings, and security patches.

- Although HP attempts to include only the highest-quality patches in the standard HP-UX patch bundles, occasionally a warning is issued for a patch in one of those bundles. You can review individual patch bundles for warnings using the ITRC Patch Bundles page.
- You can acquire more up-to-date patches individually. Security patches are good examples of patches that you might obtain individually rather than as a part of a bundle. The Security Patch Check Tool can help you identify any security patches missing from your system. The ITRC should be your primary resource for downloading these individual patches.

### Advanced Topic: The Patch Assessment Tool

HP provides the Patch Assessment Tool, which you can access using the ITRC. Many HP-UX users find this tool to be especially well suited to acquiring patches for proactive patching.

With the Patch Assessment Tool, you can create a customized profile that selects patches that are of interest to you. For example, your choices include any or all of the following:

- All applicable patches
- Security patches
- Patches that provide critical fixes
- Updates for installed patches
- The latest Quality Pack patch bundle
- Replacement patches for patches with critical warnings
- Replacement patches for patches with any warnings
- Patches in a specific patch set. For example:
  - Omniback patch set
  - Oracle™ patch set
  - Java™ 1.4 patch set

For information about the Patch Assessment Tool, see Chapter 9: "Using Other Patch Tools" (page 127).

## Reactive Patching Strategy

Reactive patching involves installing patches to restore system functionality after a problem occurs. The goal of reactive patching is to fix the problem as quickly as possible and with as little user disruption as possible.

Because reactive patching is so disruptive, typically only the most critical problems: panics, failures, and corruption are reactively patched. Your action depends on the software change management strategy you use. The closer you are to a restrictive strategy ("Recommendations for Software Change Management " (page 63)), the fewer critical problems you need to reactively fix.

More granular changes are generally safer. While proactive patching usually involves the installation of many patches at one time, reactive patching involves installing only the patches believed to be necessary. Another difference between these two approaches is that reactive patching is likely to be performed under greater pressure and urgency than proactive patching. Even customers who typically use a proactive patch strategy may at times find it necessary to patch reactively.

The following are benefits of reactive patching:

- Timely problem resolution
- Controlled, minimal changes

## Acquiring Patches for Reactive Patching

The easiest way to identify your required patch is to call the HP Response Center. This works only if you have the appropriate support contract. Alternatively, you can carefully research the problem using resources such as the ITRC. The ITRC's self-solve tools links, such as the search technical knowledge base and the navigate knowledge trees can help with that query. For more information, see Chapter 6: "Using the IT Resource Center" (page 75).

Next, using the ITRC Patch Database, you must identify the patches needed to resolve the problem. For reactive patch management, patch acquisition and installation should be strictly limited to the smallest set of patches believed to provide a solution to a current system problem. Do not use the unplanned down time as an opportunity to make unrelated changes. This is especially true for mission-critical systems.

Once you know what patches are needed to solve the problem, you must determine when to patch your system. In making this decision, you should consider the following factors:

- Severity of the problem
- Frequency of occurrence
- Availability of system down time for patching

Reactive patching has some important disadvantages as compared with proactive patching. The process of identifying a problem fix can be made more difficult as your system falls further behind the most recent patch levels available. In addition, the required patch will likely contain much more new content than if you had performed frequent proactive updates. You might also find it difficult to perform adequate testing in reactive patching situations, and this could lead to the introduction of additional problems.

Follow these steps to patch your system reactively:

1. Isolate the problem and identify the patches with the highest HP rating that represent a potential fix.
2. Acquire the needed patches and any patches needed to satisfy dependencies.
3. If you have a patch depot, add these patches to it and use this as your test base.
4. Test the patch. In some cases the problem is so serious (such as a when a critical system is down), that you might need to omit the test step. This is especially true if it takes a long time to replicate the problem, or if the configuration is difficult to replicate. If you choose to omit testing, do so only with the knowledge of the risks you might incur.
5. Determine a suitable time to install the patches.
6. Install the patches.

If you have multiple, similarly configured systems and you need to patch one of them reactively, consider patching the remaining systems as soon as it is reasonably possible. This is because it is likely that your other systems will suffer the same problems at some future point. Additionally, there are benefits to maintain the same patch level on similar systems.

# Advanced Topic: Security Patching Strategy

Security patching requires both urgency and a need to be proactive. It does not fit neatly into the proactive or reactive patching strategies. At times, you might need to apply security patches proactively prior to the next scheduled patch installation maintenance window.

When you use the ITRC to acquire patches, it is safe practice to obtain patches listed as **recommended**. Because of the urgency associated with security fixes, there are many instances when a security patch is too new to have this rating. However, many customers give a new security fix priority over an older patch recommended by the ITRC. Because most patches that fix a security problem fix only a single problem, this practice is not as risky as it may seem.

## Advanced Topic: Scanning for Security Patches

You can use the Security Patch Check Tool to identify security patches for proactive installation. Many customers run this tool on a regular basis. This tool also identifies any patches on your system that have an associated warning. For more information about the Security Patch Check Tool, see Chapter 9: "Using Other Patch Tools" (page 127).

# Testing the Patches to Be Installed

The single most important action that can ensure the success of a software patch is to first test the changes in a nonproduction environment. Every environment is unique, and patch testing can uncover potential problems unique to the environment in which the patches will be installed. If you test thoroughly, you can reduce the chance of encountering problems with new patches.

The level of testing you can perform depends in part on the patch management strategy you choose. For example, because proactive patching involves installing patches before a problem occurs, it allows more time than reactive patching to complete a sufficient level of patch testing.

HP subjects all `General Release (GR)` and `Special Release (SR)` HP-UX patches to extensive testing. See Chapter 3: "HP-UX Patch Overview" (page 27) for more information about `GR` and `SR` patches. However, it is impossible to test all possible permutations of all patches on all possible hardware configurations. Therefore, prior to deploying the patches on production systems, you should test the set of patches you intend to install in a test environment that closely simulates your production configuration. Even if you are deploying a standard HP-UX patch bundle, you should still perform testing. Deploying any patch without first testing it in your environment increases your system's exposure to risk.

The following is an outline of a basic patch test scenario:

1. The patches to be installed are identified and acquired.
2. The acquired patches are installed on a test system and tested to a standard that your organization considers acceptable. Many organizations break this step into multiple levels of testing to accomplish distinct goals. If testing results in unsatisfactory results, you must perform an investigation to identify the root cause of the problem before proceeding.
3. The tested patches are installed on production systems.

The success of your testing approach relies heavily on how closely the configuration of your test environment matches the configuration of the production systems on which the tested patches will be installed. Within your hardware limits, it is a best practice to duplicate your production environment as closely as possible.

Ideally, you have a test system that is identical to the production system on which patches are to be installed, and you have sufficient time available to test all patches prior to deploying them. This situation allows you to perform very effective testing to verify that the patches to be installed will not result in unexpected or undesirable system behavior.

Many customers have a two- or three-tiered approach to testing. Patches are initially installed on a system that is often referred to as the development system. These types of systems are used for local development. In a three-tiered system, after certain organization-specific rules have been met, the patches are installed on another system that is often referred to as the test system. The patches must then meet another set of organization-specific rules. For example, many customers require that the patches be installed on the test system for some specified period of time with no problems. The amount of time varies widely and can be as short as a week. However, for many customers, one to three months is considered a reasonable timeframe for testing. Once these rules have been satisfied, the patches are installed on one or more production systems. Customers who initially install the patches on only a subset of their production systems typically monitor these systems for several weeks prior to installing the patches on the remaining production systems. For reactive patching, the longer testing time frames are usually not reasonable and a stripped-down approach to testing is usually required.

# Where to Go Next

Now that you have a strong understanding of patch management strategies, you should read Chapter 5: "What Are Standard HP-UX Patch Bundles?" (page 69).

# 5 What Are Standard HP-UX Patch Bundles?

Patches can be grouped into collections known as patch bundles, or simply bundles. HP provides a number of prepackaged, standard HP-UX patch bundles that you can install as a unit. This chapter shows you how to obtain standard HP-UX patch bundles. Table 5-1: “Standard HP-UX Patch Bundle Names” (page 71) shows the QPK and other standard patch bundles. HP tests these bundles rigorously to ensure a high level of reliability and updates many of them periodically. Using standard patch bundles can be a less risky and more efficient way to patch a system than installing patches individually.

HP recommends that you use standard HP-UX patch bundles for proactive patching, regardless of whether you have a support contract.

**NOTE:** Please note the following change:

For the HP-UX 11.0 (B.11.00) and HP-UX 11i v1 (B.11.11) releases, HP delivers standard HP-UX patch bundles and diagnostic tools on Support Plus media, ITRC, Software Depot, and FTP servers.

For the HP-UX 11i v2 (B.11.23) release, HP delivers standard HP-UX patch bundles on OE media, ITRC, Software Depot, and FTP servers. See Table 5-2: “Standard HP-UX Patch Bundle Use and Release Dates” (page 72).

## Key Features

Standard HP-UX patch bundles can be a very useful part of a proactive patch management strategy for the following reasons:

- The bundles save you time during patching and reduce the risk of errors.
- HP tests all patches in the bundle as a group.
- The bundles provide an easy way to standardize the level of patches on your systems.
- The bundles provide a solution commonly used by other customers.
- HP performs all dependency analysis to ensure standard HP-UX patch bundles contain all patches necessary to meet dependencies.
- Unlike installing multiple patches individually, which may require a reboot for each patch, installation of a bundle never requires more than one system reboot.
- You can use bundles to create standard patch depots for easy deployment to multiple systems.
- The bundles provide a convenient way to track patches on your system.
- ITRC provides support for standard HP-UX patch bundles.

## Standard HP-UX Patch Bundles

Table 5-1 (page 71) shows the individual bundle names for the HP-UX 11.0 and HP-UX 11i releases.

**Table 5-1** Standard HP-UX Patch Bundle Names

| Bundle Name | HP-UX 11.0 (B.11.00) | HP-UX 11i v1 (B.11.11) | HP-UX 11i v1.6 (B.11.22) | HP-UX 11i v2 (B.11.23) |
|---|---|---|---|---|
| Quality Pack | `QPK1100` | `GOLDAPPS11i`<br>`GOLDBASE11i` | N/A | `QPKAPPS`<br>`QPKBASE` |
| Hardware Enablement | `HWE1100` | `HWEnable11i` | N/A | `HWEnable11i` |
| Required Patch Bundle | N/A | `BUNDLE11i` | `BUNDLE11i` | N/A |
| Feature Enablement Patch Bundle | N/A | N/A | N/A | `FEATURE11i` |
| Maintenance Pack | N/A | N/A | `MAINTPACK` | N/A |

**NOTE:** Standard HP-UX patch bundles are cumulative, which means that you can install the latest version of the bundle to get all the previous changes.

The standard HP-UX patch bundles (QPK and HWE) may have overlapping content. This does not affect your patching.

For the HP-UX 11.0 and HP-UX 11i releases, Table 5-2 (page 72) shows when to use the bundles and also shows the release information.

**Table 5-2** Standard HP-UX Patch Bundle Use and Release Dates

| Patch Bundle | Description | When to Use | Update Schedule |
|---|---|---|---|
| Quality Pack (QPK) | For HP-UX 11.0 (B.11.00), the QPK was a single bundle that included all stable defect-fix patches for core HP-UX, graphics, and key networking drivers.<br>For HP-UX 11i v1 (B.11.11) and HP-UX 11i v2 (B.11.23), the QPK is delivered as two bundles:<br>• Base Quality Pack patch bundle has the same purpose as the single-bundle QPK.<br>• Applications Quality Pack patch bundle has all stable, defect-fix patches for the OE applications. | • To configure a new system.<br>• Use every 6 to 12 months for proactive patching.<br>• To obtain defect fixes. | HP-UX 11.0: Final release March 2004<br>HP-UX 11i v1: As needed<br>HP-UX 11i v2: As needed |
| Hardware Enablement (HWE) | HWE provides the minimal set of patches for supporting new and legacy hardware using HP-UX. | • To get a new system.<br>• To add new hardware to the system. | HP-UX 11.0: Final release March 2004<br>HP-UX 11i v1: As needed<br>HP-UX 11i v2: As needed |
| Required Patch Bundle (`BUNDLE11i`) | The HP-UX 11i v1 Required Patch Bundle consists of patches for HP-UX 11i v1, which are required to install and update the operating system. | Installed automatically with the appropriate core software. | HP-UX 11i v1: As needed |
| Feature Enablement Patch Bundle (`FEATURE11i`) | For HP-UX 11i v2, consists of patches required for HP-UX Virtual Partitions (vPars) functionality, USB-00, and future products with new features. | • To fix defects.<br>• To add new products to the system. | HP-UX 11i v2: As needed |
| Maintenance Pack (`MAINTPACK`) | The HP-UX 11i v1.6 (B.11.22) Maintenance Pack includes all stable defect-fix patches for this release of HP-UX. They have been bundled together and tested extensively. There was only one release of the HP-UX 11i v1.6 (B.11.22) Maintenance Pack in June 2003, and this is the only patch bundle that is available for HP-UX 11i v1.6 (B.11.22). | To fix defects. | HP-UX 11i v1.6: Single release, June 2003 |

## Obtaining Standard HP-UX Patch Bundles

The following options are available for obtaining patch bundles:

- Option 1: ITRC

  The ITRC is the preferred option for obtaining standard HP-UX patch bundles. Access requires you have an ITRC login, which is free. Follow the online instructions to register with the ITRC, or see Chapter 6: "Using the IT Resource Center" (page 75) for more information.

- Option 2: Software Depot

  You can access the HP Software Depot Web site directly at **http://software.hp.com**. See Chapter 8: "Using Software Depots for Patch Management" (page 99).

- Option 3: FTP Servers

  You can obtain standard HP-UX patch bundles from the HP FTP servers. See Chapter 7: "Using FTP as an Alternative Patch Source" (page 89) for more information.

**TIP:** Acquiring and installing standard HP-UX patch bundles is a two-step process. See Chapter 2: "Quick Start Guide for Patching HP-UX Systems" (page 17).

## Where to Go Next

Read Chapter 6: "Using the IT Resource Center" (page 75) and Chapter 7: "Using FTP as an Alternative Patch Source" (page 89) for instructions on how to acquire and install patches.

# 6 Using the IT Resource Center

The IT Resource Center (ITRC) is a Web site that you can personalize to provide a wide range of services and support, including support for HP-UX patch management. The ITRC Web site is your fastest connection to HP Support and is located at **http://itrc.hp.com**.

This chapter presents many of the ITRC HP-UX patch-related areas. You should explore the links on the ITRC main page and familiarize yourself with all that ITRC has to offer. From the ITRC home page, select **online help** or **introducing the ITRC** for more information.

Many ITRC services require that you obtain a free user account, and some ITRC services require additional authorization, such as a certain level of support agreement or an online purchase. All ITRC areas discussed in this chapter are available **free of charge**.

# Navigating Free Areas

Most ITRC areas require you have a user account. To obtain a free user account:

1. Go to the ITRC at http://itrc.hp.com.
2. Click **select language**.
3. Choose the appropriate site (Americas/Asia Pacific or European).
4. Select **register now!**

# Viewing the Maintenance and Support Web Page

This Web page is the starting point for all the topics presented in this chapter. The following topic headings and links are a subset of the list shown on the **maintenance and support (hp products)** page and are discussed here in order of importance. (Select the **maintenance and support (hp products)** link to see these topics.)

- **self-solve tools**
  - "Search Technical Knowledge Base" (page 88)
- **patching**
  - "Find Individual Patches and Firmware" (page 77)
  - "Standard Patch Bundles - Find Patch Bundles" (page 84)
  - "Custom Patch Bundles - Run a Patch Assessment" (page 85)
- **downloads/licensing**
  - "Find Individual Patches and Firmware" (page 77)
  - "Standard Patch Bundles - Find Patch Bundles" (page 84)
- **collaborate**
  - "Ask Your Peers in the Forums" (page 87)
- **assessment and warranty**
  - "Custom Patch Bundles - Run a Patch Assessment" (page 85)
- **notifications**
  - "Support Information Digests" (page 86)

# Find Individual Patches and Firmware

The ITRC Patch Database should be your primary means of searching for patches, getting information about patches, and acquiring patches. The Patch Database is an excellent tool for system administrators who employ a reactive patch management strategy. The Patch Database is also an excellent general-purpose tool to refresh specific patches with newer versions.

## Key Features

With the Patch Database, you can search for patches using a variety of criteria. Once the search returns the results, you can obtain information, including the following:

- The patch rating
- The patch that HP recommends, if any
- The most recent patch
- The patch warning, if any
- Supersession by another patch
- Supersession of other patches
- A **patch details** page containing comprehensive information about each patch returned

See Table 6-1: "Navigating the Search Results Table" (page 78) for descriptions of the search results.

## Accessing the Patch Database and Finding an Individual Patch

1. Log in to the ITRC at **http://itrc.hp.com**.

   You must log in to the appropriate site (Americas/Asia Pacific or European).

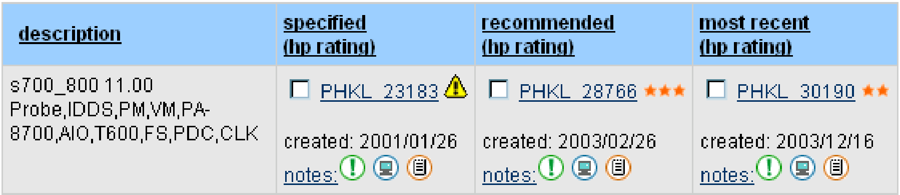
2. Select **maintenance and support (hp products)**, then select one of the **find individual patches and firmware** links.

   You are now in the Patch Database.

3. Select the **HP-UX** link.
4. To find instructions, select the **How would you like to search?**, **Search Criteria**, and **read our usage guide** links.
5. Enter your search parameters, then select **search**.

   Figure 6-1 (page 77) shows results from a Patch Database search for the patch `PHKL_23183`.

**Figure 6-1** Search Results Table



| description | specified<br>(hp rating) | recommended<br>(hp rating) | most recent<br>(hp rating) |
|---|---|---|---|
| s700_800 11.00 Probe,IDDS,PM,VM,PA-8700,AIO,T600,FS,PDC,CLK | □ PHKL_23183 ⚠<br>created: 2001/01/26<br>notes: ! 🖥 📄 | □ PHKL_28766 ★★★<br>created: 2003/02/26<br>notes: ! 🖥 📄 | □ PHKL_30190 ★★<br>created: 2003/12/16<br>notes: ! 🖥 📄 |

Patches returned by a search are shown in a **search results** table. Table 6-1 (page 78) shows how to interpret the information in the **search results** table.

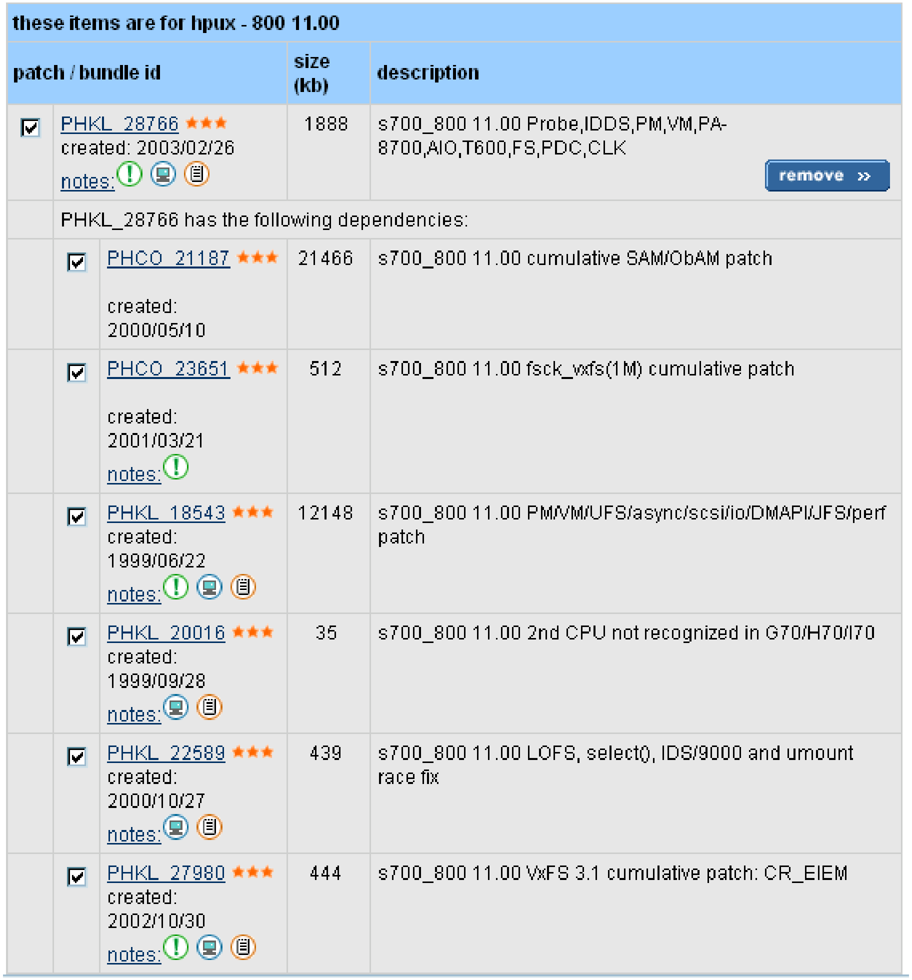
**Table 6-1** Navigating the Search Results Table

| **Term** | **Description** |
|---|---|
| Column Headings | Select a column heading to get a description of the heading. |
| **description** Column | Provides a terse patch description for the specified patch. |
| **specified** Column | If you search for a specific patch it displays in the **specified** column, which is only shown when a search is done for a specific patch ID. |
| **recommended** Column | If there is an HP recommended patch, it appears in the **recommended** column and may not be the patch you searched for. |
| **most recent** Column | Shows the latest patch without a warning in the supersession chain. |
| Patch Row | The patches shown in a row are the same or are related by supersession. |
| Patch ID Link | Access the **patch details** page associated with a patch by selecting the patch ID. This page contains extensive information about the patch. |
| **hp rating** | Indicates the quality rating assigned to a patch. Three stars is the highest rating assigned to any patch. The higher the rating, the lower the risk of side effects and the more suitable the patch is for mission-critical environments. |
| HP Patch Warning | If a patch has a warning associated with it, no stars are displayed. Instead, a yellow, triangular symbol appears:<br>⚠<br>Select the patch ID link to go to the **patch details** page. Read the **Warning** section. |
| **notes** Link | Provides additional information about icons and information returned with patches. |
| Table Icons | Icons are displayed along with the patches to provide additional information.<br>❗ critical fix<br>🖥 reboot required<br>🖥 possible reboot required<br>⊗ not available<br>⊕ enhancements only<br>📋 special instructions |

6. You can download one patch of your choice from each row of patches returned by the search.
   - Select the checkbox next to the patch ID link.
   - Select **add to selected patch list** button.
7. You should view the **special installation instructions** and check for **dependencies** for each patch you want to download.
   - See "Advanced Topic: Checking for Special Installation Instructions" (page 80).
   - See "Advanced Topic: Checking for All Patch Dependencies" (page 81).

   For example, in Figure 6-1: "Search Results Table" (page 77), if you selected `PHKL_28766` for download, you would then see the list shown in Figure 6-2 (page 79).

**Figure 6-2** Selected Patch List Table



| | | patch / bundle id | size (kb) | description |
|---|---|---|---|---|
| these items are for hpux - 800 11.00 | | | | |
| ☑ | | PHKL_28766 ★★★<br>created: 2003/02/26<br>notes: (!) 🖥 📄 | 1888 | s700_800 11.00 Probe,IDDS,PM,VM,PA-8700,AIO,T600,FS,PDC,CLK<br>remove » |
| | PHKL_28766 has the following dependencies: | | | |
| | ☑ | PHCO_21187 ★★★<br>created: 2000/05/10 | 21466 | s700_800 11.00 cumulative SAM/ObAM patch |
| | ☑ | PHCO_23651 ★★★<br>created: 2001/03/21<br>notes: (!) | 512 | s700_800 11.00 fsck_vxfs(1M) cumulative patch |
| | ☑ | PHKL_18543 ★★★<br>created: 1999/06/22<br>notes: (!) 🖥 📄 | 12148 | s700_800 11.00 PM/VM/UFS/async/scsi/io/DMAPI/JFS/perf patch |
| | ☑ | PHKL_20016 ★★★<br>created: 1999/09/28<br>notes: 🖥 📄 | 35 | s700_800 11.00 2nd CPU not recognized in G70/H70/I70 |
| | ☑ | PHKL_22589 ★★★<br>created: 2000/10/27<br>notes: 🖥 📄 | 439 | s700_800 11.00 LOFS, select(), IDS/9000 and umount race fix |
| | ☑ | PHKL_27980 ★★★<br>created: 2002/10/30<br>notes: (!) 🖥 📄 | 444 | s700_800 11.00 VxFS 3.1 cumulative patch: CR_EIEM |

## Advanced Topic: Checking for Special Installation Instructions

Some patches might have extra installation instructions, called **Special Installation Instructions**, that you should follow to install the patch successfully. The following steps show you how to access these instructions.

1. If there is a patch in the **selected patch list** that has the special instructions icon beside it, select the patch ID link to display the **patch details** page for the patch.
2. Read the **Special Installation Instructions** section. You should follow the instructions given here when you install the patch.
3. Select the **view selected patch list** link.
4. Repeat these steps for any remaining patches in the **selected patch list** that also have special instructions icons.

# Advanced Topic: Checking for All Patch Dependencies

The Patch Database automatically selects patches to meet certain dependencies for patches that have been selected for download. The Patch Database can detect and select patches that are required to meet enforced dependencies, and in most cases this is sufficient. However, if any of the patches selected for download have unenforced (manual) dependencies on other patches, the Patch Database does not identify these.

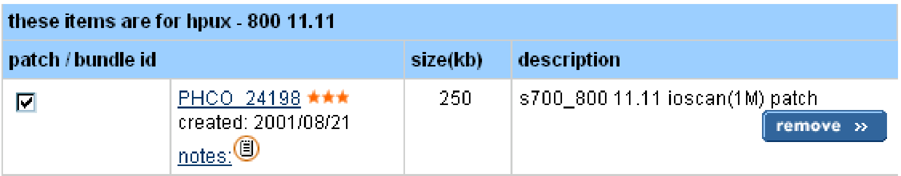
You are responsible for verifying that all patches necessary to satisfy dependencies have been selected for download. If you do not perform this verification, certain features related to your chosen patches might not attain full functionality upon installation. This section describes how to determine whether these patches are significant for your environment.

## Check for Patches with Dependencies

Perform the following steps after selecting patches to download (after step 6 in the "Accessing the Patch Database and Finding an Individual Patch" (page 77)). Repeat these steps for each patch on your **selected patch list**, including any new patches you add as a result of performing these steps.

1. Select a patch ID link in the **selected patch list** to display the **patch details** page for the patch. For example, in Figure 6-3: "Selected Patch List Example" (page 81), select `PHCO_24198`.

   **Figure 6-3** Selected Patch List Example



| these items are for hpux - 800 11.11 | | | |
|---|---|---|---|
| patch / bundle id | | size(kb) | description |
| ☑ | PHCO_24198 ★★★<br>created: 2001/08/21<br>notes: | 250 | s700_800 11.11 ioscan(1M) patch<br>remove » |

2. Read the **Other Dependencies** and **Special Installation Instructions** sections of the **patch details** page. The **Other Dependencies** section, and occasionally the **Special Installation Instructions** section, may list additional patches or products that are needed to obtain full functionality of the patch selected in step 1.

   If additional patches are listed, determine whether any are needed for your specific situation. If so, note the patch IDs for use in step 3.

   For example, Figure 6-4: " Other Dependencies Section of the PHCO_24198 Patch Details Page" (page 81) shows that `PHKL_24163` is needed only if you want a specific performance improvement. If not, you do not need to download the listed patch.

   **Figure 6-4** **Other Dependencies** Section of the `PHCO_24198` **Patch Details** Page

```
Other Dependencies
Kernel patch PHKL_24163 (or its superseding patch) must be
installed if "ioscan -k" performance improvement is desired.
```

3. Select the **view selected patch list** link. If any patches were noted in step 2 for download, verify that they are listed in the **selected patch list**. If not, you should manually add each one. To do this, select the **search results** link and then select and download the patches:

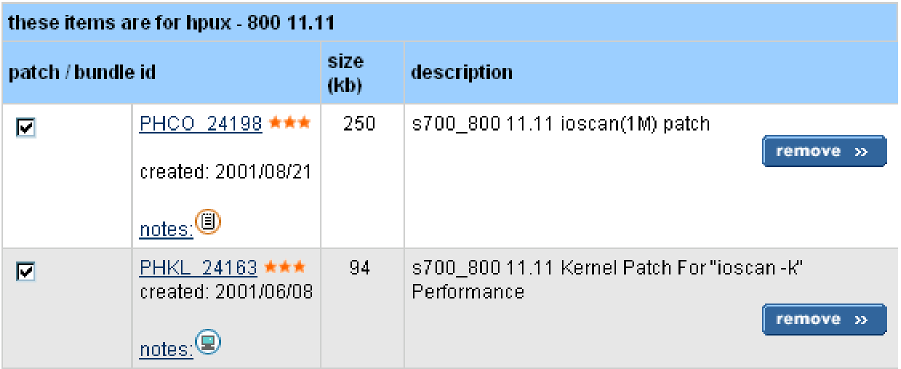
   - Enter your search criteria, including the patch ID, and then select **search**.

     Patches returned by a search are shown in a **search results** table.

   - You can choose to download one patch of your choice from each row of patches returned by the search. Keep in mind that you do not necessarily have to download the exact patch noted in step 2. There may be a better choice, such as a recommended patch that the search returned.
     1. Select the checkbox next to the patch ID link.
     2. Select **add to selected patch list** button.

     For example, if you choose to add patch `PHKL_24163` manually, the selected patch list is updated as shown in Figure 6-5 (page 82).

Figure 6-5 Selected Patch List Example



| these items are for hpux - 800 11.11 | | | |
|---|---|---|---|
| patch / bundle id | | size (kb) | description |
| ☑ | PHCO_24198 ★★★<br>created: 2001/08/21<br>notes: | 250 | s700_800 11.11 ioscan(1M) patch<br>remove » |
| ☑ | PHKL_24163 ★★★<br>created: 2001/06/08<br>notes: | 94 | s700_800 11.11 Kernel Patch For "ioscan -k" Performance<br>remove » |

# Advanced Topic: Searching for Patches for Your System Configuration

You can use the HP Patch Database to perform a patch search based on the configuration of a specific HP-UX system. Perform these steps to access this functionality:

1. Log in to the ITRC at **http://itrc.hp.com**.
2. Select **maintenance and support (hp products)**, and then select **patch/firmware database**.
3. Select **find patches for my HP-UX system**.
4. Select **upload new system information**.

   You will be required to run a data collection script on your system and upload the results to the ITRC to enable the search to be system specific. The **upload system information** page explains how to do this.

## Standard Patch Bundles - Find Patch Bundles

The **standard patch bundles - find patch bundles** link provides the **find bundles** page to help you acquire standard HP-UX patch bundles. See Chapter 5: “What Are Standard HP-UX Patch Bundles?” (page 69) for more information.

**TIP:** To download or obtain information about the Maintenance Pack for HP-UX 11i v1.6 (B.11.22), select **Obtain the HP-UX 11i version 1.6 Maintenance Pack patch bundle** to go to the Software Depot **HP-UX 11i v1.6 Maintenance Pack Patch Bundle** page.

To obtain information about Support Plus, select **HP-UX patch bundles**. Then select a specific Support Plus release to get additional information.

# Custom Patch Bundles - Run a Patch Assessment

The Patch Assessment Tool allows you to create custom patch bundles specific to your environment. This Web-based tool replaces the Custom Patch Manager Tool. The Patch Assessment Tool can be valuable for system administrators employing a proactive patch management strategy.

## Key Features

The following are key features of the Patch Assessment Tool.

- The patch assessment profile gives you control over which patches are recommended. You can specify various options, including the following:
  - Select or deselect patches that provide critical fixes.
  - Select or deselect patches that fix security vulnerabilities.
  - Include sets of patches that pertain to specific applications.
  - Select or deselect replacement (or superseding) patches for patches already on your system that have noncritical or critical warnings.
  - Require that a specific patch be included in the assessment.
- Conflict analysis is done automatically.
- Dependency analysis is done automatically for all patches. However, it finds only enforced dependencies; it does not find unenforced (manual) dependencies.
- Assessment results include information about why patches are recommended.
- You can download recommended patches in `tar`, `zip`, or `gzip` format, or you can download a script that will FTP the patches.

To access the Patch Assessment Tool:

1. Log in to the ITRC at **http://itrc.hp.com**.
2. Select **maintenance and support (hp products)**, and then select **custom patch bundles - run a patch assessment**.

**TIP:** On the **run a patch assessment** page, **useful links** has good information about the Patch Assessment Tool.

## Support Information Digests

The ITRC provides Subscriber's Choice, the home for digest subscriptions.

### Key Features

Digest subscriptions allow you to do the following:

- Stay up to date with the latest support information from HP via e-mail.
- Select your areas of interest and receive the appropriate digests from HP.

To access the **ITRC driver and support alerts/notifications sign-up** page:

1. Log in to the ITRC at **http://itrc.hp.com**.
2. Select **maintenance and support (hp products)**.
3. Under **notifications**, select **support information digests**.

# Ask Your Peers in the Forums

The ITRC forums are gathering places for IT professionals. You can use the forums to solve problems, exchange ideas, and learn from peers who also use the ITRC. HP engineers may participate in all of these forums to share their advice; however, these forums are intended primarily as a peer-to-peer resource.

To access patch-specific issues in the ITRC forums:

1. Log in to the ITRC at **http://itrc.hp.com**.
2. Select **maintenance and support (hp products)**.
3. Under **collaborate**, select **ask your peers in the forums**.
4. Select **HP-UX** and **patches**.
5. From the **patches** page, you can read previously posted questions and replies, or you can post a question or reply of your own.

# Search Technical Knowledge Base

This functionality allows you to search across the HP technical knowledge base for answers to your support-related questions and for technical support documents to solve problems. This interface makes it easy for you to narrow your searches to documents which pertain to a particular product area or platform by using predefined categories. Additionally, you can limit searches to particular document types. For information about this page, select the **help** link.

## Key Features

The Technical Knowledge Base helps you to do the following:

- Solve problems yourself with timely technical support information.
- Search the HP Technical Knowledge Base for technical documents, including patch information, security bulletins, and service requests related to HP-UX and a variety of other areas.
- Retrieve a specific document using its document identification (ID).

To access the **technical knowledge** page:

1. Log in to the ITRC at **http://itrc.hp.com**.
2. Select **maintenance and support (hp products)**.
3. Under **self-solve tools**, select **search technical knowledge base**.

## Where to Go Next

Read Chapter 7: "Using FTP as an Alternative Patch Source" (page 89) for instructions about how to acquire patches.

# 7 Using FTP as an Alternative Patch Source

This chapter, presents File Transfer Protocol (FTP) as an alternative means for you to acquire patch bundles and individual patches. For newer HP-UX system administrators, you will find using the ITRC a very complete and much simpler method. As you will see in this chapter, however, the FTP method does have some unique benefits.

There are two methods for obtaining patches by FTP:

1. **Using a Web browser** to access the FTP servers.

   This is the easiest and most user-friendly method to FTP files.

2. **Using a command line interface** to access the FTP servers.

   - This is a more powerful FTP method, but requires you to know the FTP commands.
   - FTP using a command line interface gives you more advanced features such as automated file download using scripts.

The instructions in this chapter assume you have access to FTP and a Web browser on the HP-UX system that is the final destination of the files to download. This is referred to as the target system. You will download the files using this system.

If this is not the case, simply download the files using a system other than the target system and then transfer the files to the target system. This intermediate system does not have to be an HP-UX system or even a UNIX™ system. For example, you could use a Web browser on a PC to download a patch to the PC using FTP and then transfer that patch to the target system using Secure Shell (SSH).

# Using HP FTP Servers

HP provides two servers for FTP access to standard HP-UX patch bundles and individual patches:

- ftp://ftp.itrc.hp.com

  Recommended for most users.

- ftp://singapore-ffs.external.hp.com

  Recommended for users in the Asia/Pacific region.

# What is the FTP Directory Structure?

The two FTP servers have the following HP-UX patch management related directories.

Some of the directories have a file named `catalog` that contains a listing and description of the patches or bundles in the directory.

1. `/patch_bundles/hp-ux/`
   - Contains standard HP-UX patch bundles.
   - The patch bundles are available for at least one year.
   - If you are new to patching, use the patch bundles.
   - Navigate to the directory containing the desired bundle type based on directory name:
     - The `GOLD` and `QPK` directories contain Quality Pack patch bundles.
     - The `HWE` directory contains Hardware Enablement bundles.
     - The `SPECIAL` directory contains special bundles, such as `BUNDLE11i` and `MAINTPACK`.
     - The `RELEASE` directory contains documentation associated with bundles, such as read before installing (RBI) booklets and user guides.

       See Figure 7-1: “FTP Listing of Root at ftp.itrc.hp.com” (page 92) and Figure 7-2: “FTP Listing of ftp.itrc.hp.com” (page 93) for more information.

2. `/hp-ux_patches/`
   - Begin your search here when looking for individual patches.
   - Contains current HP-UX patches. These patches do not have associated patch warnings, have not been superseded, and have not been archived.
   - To find a patch for your system, select the subdirectories that correspond to your hardware type and OS version.
   - If you are looking for a specific patch and cannot find it here, it may be located in one of the directories described in items 3, 4, or 5.
3. `/superseded_patches/hp-ux_patches/`
   - Contains HP-UX patches that have been superseded.
   - To find a patch for your system, select the subdirectories that correspond to your hardware type and OS version.
4. `/patches_with_warnings/hp-ux_patches/`
   - Contains HP-UX patches that have associated warnings.
   - To find a patch for your system, select the subdirectories that correspond to your hardware type and OS version.
   - The `recalled_patches` directory is linked to the `patches_with_warnings` directory.

5. /archived_patches/hp-ux_patches/
   - Contains HP-UX patches that have been archived (HP-UX versions 9.x and earlier).
   - To find a patch for your system, select the subdirectories that correspond to your hardware type and OS version.
   - The archived_patches directory is linked to the /data/archived_patches directory.
6. /export/patches/

   This directory contains useful information. Examples of directory content include the following:
   - The file hp-ux_patch_sums, which contains HP-UX Patch Checksum Information.
   - The file hp-ux_obs_patch_list, which contains the HP-UX Patch Replacement List that you can use to determine whether a patch has been replaced by another patch. However, you should use the ITRC to find replacement patches because it provides more complete information than is contained in this file.
   - Files used by the Security Patch Check Tool.

## Individual Patch Related Files

For the bundle directory described previously in item 1, there are two files for each bundle:

- The bundles are contained in tape depots having the filename format *bundle_name*.depot.
- Each bundle has a corresponding text file that has the filename format *bundle_name*.txt. These are also referred to as bundle readme files.

  The patch bundle readme files provide detailed information about the associated patch bundle. For some bundles, the bundle name, operating system version, and bundle release date are embedded in the file name. For example, the tape depot file GOLDQPK11i_B.11.11.0312.4.depot contains the December 2003 release of the Quality Pack bundles for HP-UX 11i v1 (B.11.11).

Each patch in the directories described in items 2 through 5 has two files:

- A patch text file

  The patch text file has the filename format *patch_id*.txt and contains detailed patch information similar to that found in the ITRC **patch details** pages (as discussed in "Find Individual Patches and Firmware" (page 77)). Remember to review the text file for essential information, such as special installation instructions and other dependencies. See Chapter 6: "Using the IT Resource Center" (page 75) for an example of a **Special Installation Instructions** section and an **Other Dependencies** section.

- A shell archive (shar) file

  The shar file has the same name as its corresponding patch and contains the actual patch software.

# Using a Web Browser with FTP

You can use a Web browser to download standard HP-UX patch bundles and individual patches using the FTP servers.

The following steps use the Mozilla Web browser, but you can use a different browser. Your screen displays should look similar to the following screens.

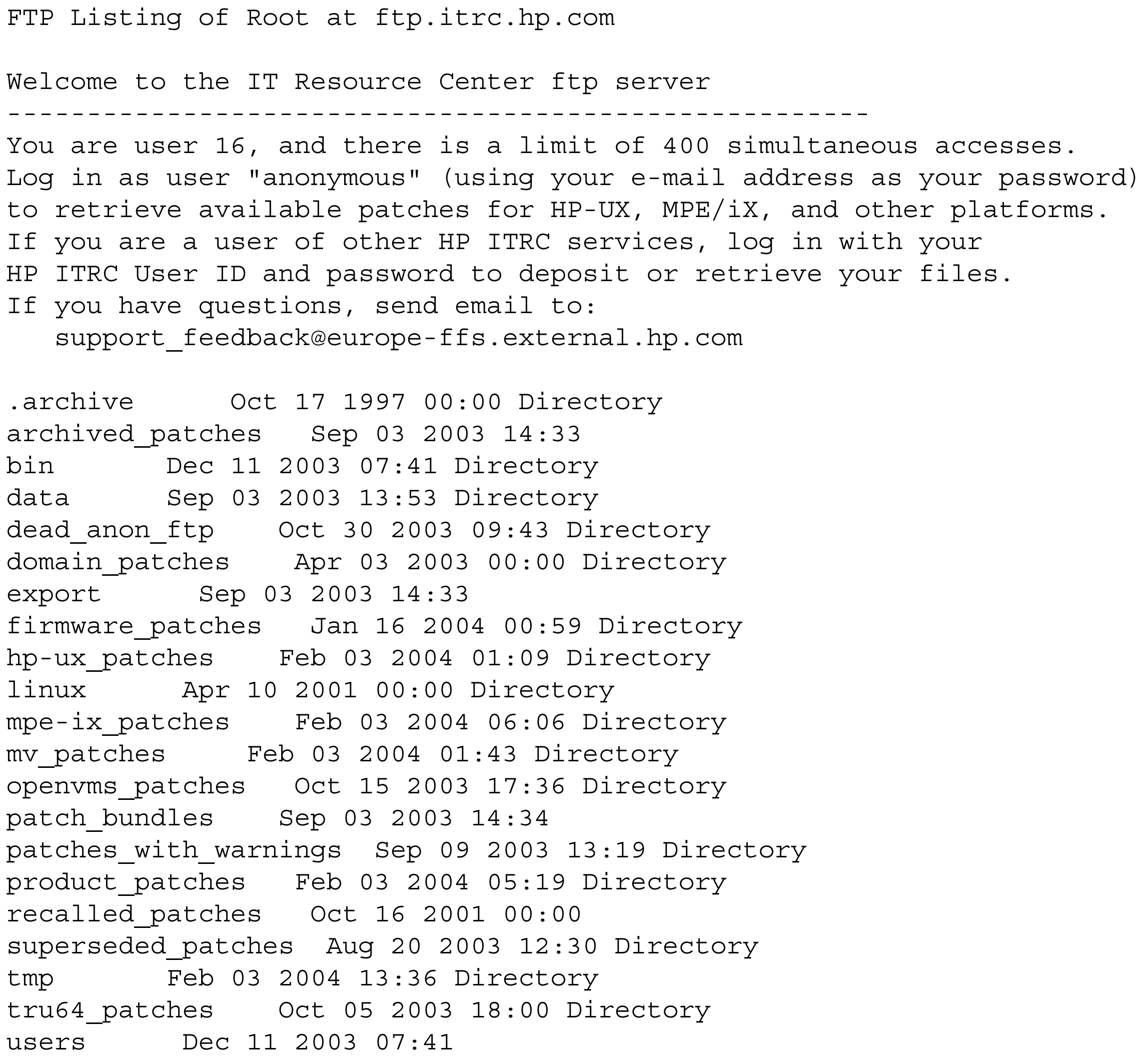
## Downloading Bundles and Patches Using a Web Browser

You can download a bundle or individual patch using a Web browser. Perform these steps to download an individual patch. You can also use these steps for downloading a bundle.

1. Log in to the target system.
2. Open a Web browser.
3. To establish a connection with the FTP server, enter one of the HP FTP server addresses:
   - ftp://ftp.itrc.hp.com (recommended for most users)
   - ftp://singapore-ffs.external.hp.com (for Asia-Pacific region)

   Figure 7-1 (page 92) shows the kind of screen that appears:

   **Figure 7-1** FTP Listing of Root at ftp.itrc.hp.com



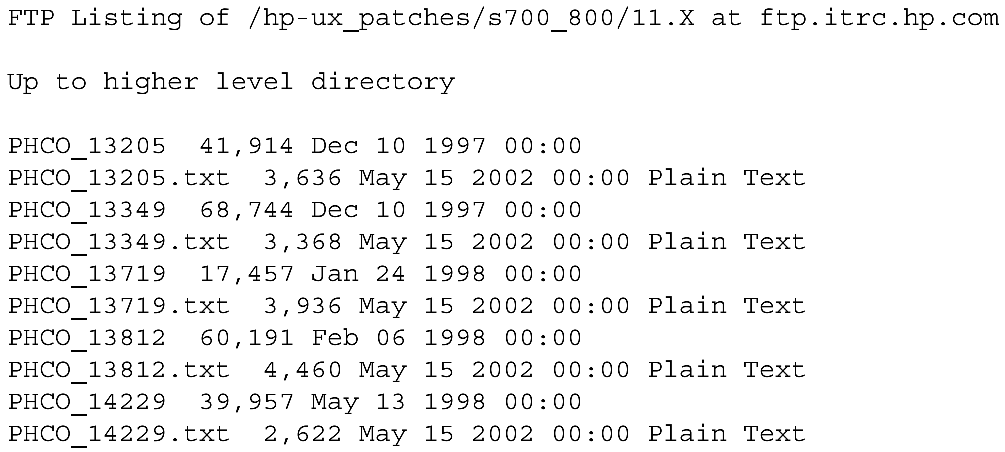
```
FTP Listing of Root at ftp.itrc.hp.com

Welcome to the IT Resource Center ftp server
------------------------------------------------------
You are user 16, and there is a limit of 400 simultaneous accesses.
Log in as user "anonymous" (using your e-mail address as your password)
to retrieve available patches for HP-UX, MPE/iX, and other platforms.
If you are a user of other HP ITRC services, log in with your
HP ITRC User ID and password to deposit or retrieve your files.
If you have questions, send email to:
   support_feedback@europe-ffs.external.hp.com

.archive      Oct 17 1997 00:00 Directory
archived_patches   Sep 03 2003 14:33
bin       Dec 11 2003 07:41 Directory
data      Sep 03 2003 13:53 Directory
dead_anon_ftp    Oct 30 2003 09:43 Directory
domain_patches    Apr 03 2003 00:00 Directory
export      Sep 03 2003 14:33
firmware_patches   Jan 16 2004 00:59 Directory
hp-ux_patches    Feb 03 2004 01:09 Directory
linux      Apr 10 2001 00:00 Directory
mpe-ix_patches    Feb 03 2004 06:06 Directory
mv_patches     Feb 03 2004 01:43 Directory
openvms_patches   Oct 15 2003 17:36 Directory
patch_bundles    Sep 03 2003 14:34
patches_with_warnings  Sep 09 2003 13:19 Directory
product_patches   Feb 03 2004 05:19 Directory
recalled_patches   Oct 16 2001 00:00
superseded_patches  Aug 20 2003 12:30 Directory
tmp       Feb 03 2004 13:36 Directory
tru64_patches    Oct 05 2003 18:00 Directory
users      Dec 11 2003 07:41
```

4. Navigate to the remote directory containing the bundle or patch you want to download. For example, go to `/hp-ux_patches/s700_800/11.X`. Figure 7-2 (page 93) shows a partial listing of the directory.

**Figure 7-2** FTP Listing of ftp.itrc.hp.com



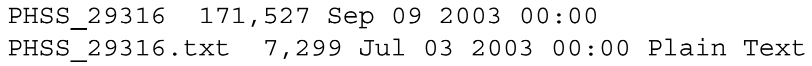
```
FTP Listing of /hp-ux_patches/s700_800/11.X at ftp.itrc.hp.com

Up to higher level directory

PHCO_13205  41,914 Dec 10 1997 00:00
PHCO_13205.txt  3,636 May 15 2002 00:00 Plain Text
PHCO_13349  68,744 Dec 10 1997 00:00
PHCO_13349.txt  3,368 May 15 2002 00:00 Plain Text
PHCO_13719  17,457 Jan 24 1998 00:00
PHCO_13719.txt  3,936 May 15 2002 00:00 Plain Text
PHCO_13812  60,191 Feb 06 1998 00:00
PHCO_13812.txt  4,460 May 15 2002 00:00 Plain Text
PHCO_14229  39,957 May 13 1998 00:00
PHCO_14229.txt  2,622 May 15 2002 00:00 Plain Text
```

5. If you scroll down through the listing, you will see the patch `PHSS_29316`. Figure 7-3 (page 93) shows a listing that contains the patch `shar` file (`PHSS_29316`) and the corresponding text file (`PHSS_29316.txt`).

**Figure 7-3** Partial Listing for PHSS_29316



```
PHSS_29316  171,527 Sep 09 2003 00:00
PHSS_29316.txt  7,299 Jul 03 2003 00:00 Plain Text
```

6. Right-click the bundle depot file or patch `shar` file to download, and make the appropriate selections to save the file to the target directory on your local machine.
7. If you want to download additional bundles and patches, repeat steps 4 through 6.
8. On your local system, open a terminal window.
9. Change to the target directory.
10. Enter the following command: **`ls -l | more`**
11. Unpack each `shar` file using the command: **`sh`** *`patch_id`* where *`patch_id`* is the filename.

    Repeat this step for each `shar` file.

    You can skip this step for bundles you have downloaded.

    After executing this command, you will have the original shell archive file ( *`patch_id`* ), a patch text file ( *`patch_id`*`.text`), and a tape depot ( *`patch_id`*`.depot`).
12. This step is critical. When you install the patches, the system may reboot automatically.

    At this point, you need to follow your company's policy regarding a system reboot.
13. This step is critical. Before you install the patches, back up your system.
14. To install the patches, enter the following `swinstall` command:

    ```
    swinstall -s /target_directory/depot -x autoreboot=true \
       -x patch_match_target=true
    ```

    where *`depot`* is the name of the *`.depot`* file.

    During the installation, the system prints progress details to the screen.

15. Monitor the screen for error messages.

    The system reboots automatically if any patches require it. Be patient. The patch installation may not proceed quickly.

16. To verify that the installation was successful, do the following:

    - Enter the following command:

      ```
      swlist -l product
      ```

      Ensure that the installed patches are shown in the output.

    - Execute the `swverify` command on each of the new patches:

      ```
      swverify patch_id
      ```

      This command may not always complete in a short period of time.

      If the verification is successful, the last few lines of output contain the following line:

      ```
      "* Verification succeeded."
      ```

      If the verification was not successful, view the log file `/var/adm/sw/swagent.log` for additional information. If this is not sufficient to resolve the problem, consult more advanced resources in Appendix A: "Other Resources" (page 137).

    - View the `swagent` log file, located at `/var/adm/sw/swagent.log`.

      This log includes information related to the installation.

      - Find the section pertaining to the installation just performed (located near the end of the file if you check it immediately after the install). Review this section and ensure that there were no errors `("ERROR")`.
      - If you find errors, consult more advanced resources in Appendix A: "Other Resources" (page 137) to resolve the problem.

# Using the Command Line Interface with FTP

You can also download standard HP-UX patch bundles and individual patches using FTP from a command line interface. You can use this method of FTP access both for manually downloading patches and bundles as well as for advanced purposes such as downloading patches and bundles automatically using scripts.

**IMPORTANT:** You might experience difficulty with FTP if you are behind a firewall, and you might need to access FTP through an FTP proxy server.

You should access the servers using anonymous FTP, which does not require a user account.

## Downloading Files Using the Command Line Interface

To download a bundle or patch using the command line interface, perform the following steps. Figure 7-4: "Anonymous FTP Using the Command Line Interface" (page 97) shows an FTP session that uses these commands.

1. Log in to the target system.
2. Change directories to the target directory where you want to download the bundle or patch.
3. Enter one of the following FTP commands:
   - **`ftp ftp.itrc.hp.com`** (recommended for most users)
   - **`ftp singapore-ffs.external.hp.com`** (for Asia/Pacific region)
4. When prompted by the FTP server for a username, enter **`anonymous`**.
5. When prompted by the FTP server for a password, enter *`your email address`* .

   You should now be logged in to the remote FTP server. The command prompt is now `ftp>`.
6. Set the transfer type to binary by entering **`binary`** or **`bin`**.
7. Change directories to the directory of the bundle or patch that you want to download.
8. Download the file to your local system by entering **`get`** *`filename`* .
9. To download additional bundles and patches, repeat steps 7 and 8.
10. To quit the FTP session, enter **`quit`**.

    The command prompt reverts back to the HP-UX command prompt for your local system. The downloaded bundles or patches will be located in the current directory.
11. Enter the following command:

    **`ls -l | more`**
12. Unpack each `shar` file by using the command **`sh`** *`patch_id`* , where *`patch_id`* is the filename.

    Repeat this step for each `shar` file.

    You can skip this step for bundles you have downloaded.

    After executing this command, you will have the original shell archive file ( *`patch_id`* ), a patch text file ( *`patch_id`*`.text`), and a tape depot ( *`patch_id`*`.depot`).
13. This step is critical. When you install the patches, the system may reboot automatically.

    At this point, you need to follow your company's policy regarding a system reboot.
14. This step is critical. Before you install the patches, back up your system.
15. To install the patches, use the following `swinstall` command:

    ```
    swinstall -s /target_directory/depot -x autoreboot=true \
       -x patch_match_target=true
    ```

    where *`depot`* is the name of the *`.depot`* file.

    During the installation, the system prints progress details to the screen.

16. Monitor the screen for error messages.

    The system reboots automatically if any patches require it. Be patient. The patch installation may not proceed quickly.

17. To verify that the installation was successful, do the following:

    - Enter the command **`swlist -l product`**

      Ensure that the installed patches are shown in the output.

    - Execute the `swverify` command on each of the new patches:

      **`swverify`** *`patch_id`*

      This command may not always complete in a short period of time.

      If the verification is successful, the last few lines of output contain the following line:

      ```
      "* Verification succeeded."
      ```

      If the verification was not successful, view the log file `/var/adm/sw/swagent.log` for additional information. If this is not sufficient to resolve the problem, consult more advanced resources in Appendix A: "Other Resources" (page 137).

    - View the `swagent` log file, located at `/var/adm/sw/swagent.log`.

      This log includes information related to the installation.

      - Find the section pertaining to the installation just performed (located near the end of the file if you check it immediately after the install). Review this section and ensure that there were no errors (`"ERROR"`).
      - If you find errors, consult more advanced resources in Appendix A: "Other Resources" (page 137) to resolve the problem.

Figure 7-4 (page 97) shows the output of an anonymous FTP session using the command line.

**Figure 7-4** Anonymous FTP Using the Command Line Interface

```
autgr_57> cd target_dir
autgr_57> ftp ftp.itrc.hp.com
Connected to ftp.itrc.hp.com (192.151.52.14).
220-
220-Welcome to the IT Resource Center ftp server
220-------------------------------------------------------
220-
220-You are user 13, and there is a limit of 400 simultaneous accesses.
220-
220-Log in as user "anonymous" (using your e-mail address as your password)
220-to retrieve available patches for HP-UX, MPE/iX, and other platforms.
220-
220-If you are a user of other HP ITRC services, log in with your
220-HP ITRC User ID and password to deposit or retrieve your files.
220-
220-If you have questions, send email to:
220-
220-   support_feedback@europe-ffs.external.hp.com
220-
220 i3107ffs FTP server (HP ASL ftpd, version(322)) ready.
Name (ftp.itrc.hp.com:richardm): anonymous
331 Guest login ok, send your complete e-mail address as password.
Password:
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> bin
200 Type set to I.
ftp> cd hp-ux_patches/s700_800/11.X
250 CWD command successful.
ftp> get PHSS_29316
local: PHSS_29316 remote: PHSS_29316
227 Entering Passive Mode (192,151,52,14,14,70)
150 Opening BINARY mode data connection for PHSS_29316 (171527 bytes).
226 Transfer complete.
171527 bytes received in 0.635 secs (2.6e+02 Kbytes/sec)
ftp> quit
221 Goodbye.
autgr_57> ls -l
total 336
-rw-r--r--   1 rar       users         171527 Sep  9  2003 PHSS_29316
autgr_57> sh PHSS_29316
x - PHSS_29316.text
x - PHSS_29316.depot [non-ascii]
autgr_57> ls
PHSS_29316        PHSS_29316.depot  PHSS_29316.text
```

## Where to Go Next

Read Chapter 8: “Using Software Depots for Patch Management” (page 99) for more instructions about how to use software depots.

# 8 Using Software Depots for Patch Management

A software depot, or simply depot, is a special type of file or directory formatted for use by Software Distributor for HP-UX (SD-UX). Depots can contain a variety of software products. This chapter focuses specifically on depots as repositories for patches and patch bundles. These depots are commonly referred to as patch depots.

Common uses for patch depots include the following:

- Patch depots are an extremely effective mechanism for managing patches. They can be especially beneficial in managing patches for groups of systems.
- Patch depots can be used as a single source of patches. This helps you to install all patches in a single installation session.
- Depots are used for software delivery. When you download patches or patch bundles from HP, you receive either a depot or a file that contains a depot.
- Patch depots can be transferred using email or file transfer protocol (FTP).

Patch depots are an extremely useful patch management tool for systems whose patching you manage as a group. For these groups, you can use patch depots to centrally manage tasks such as defining, testing, and updating patch configurations. First, you create a separate centralized depot for each group; then you manage the patches in each depot rather than on each individual system. These centralized depots, which can be accessed remotely, are used as the single patch source for patch installations on all systems in the corresponding group. This allows you to maintain the same patch level (set of active patches) on all your systems with less overall effort.

Another benefit of using depots is that they minimize the number of reboots required during patch installation. If you place all the patches to install into a single depot, you will be able to install the entire contents of the depot onto a system with a single reboot.

For information about depots beyond the scope of this guide, see the Software Distributor Administration Guide on the HP Technical Documentation Web site at **http://docs.hp.com**.

# Depot Types

There are two types of SD-UX software depots:

- Directory depots
- Tape depots

Both are commonly used and provide the same basic functionality. However, each has its own advantages for you to consider. This chapter focuses on using directory depots for patch management. Less emphasis is placed on the use of tape depots.

## Directory Depots

Directory depots, also known as network depots, are more practical than tape depots for patch management tasks. Directory depots exist as a directory structure, and the name of the depot's root directory is the name of the depot.

For patch management, directory depots offer the following advantages over tape depots:

- Can be made available to remote users. See “Registering and Unregistering Directory Depots” (page 108).
- Are optimized for random access by multiple simultaneous sessions.
- Allow for customized access controls. See “Advanced Topic: Access Control Lists” (page 109).
- Allow SD-UX verification. See “Verifying Directory Depots” (page 110).
- Allow modification.

Using these features, you can centrally define and support standardized sets of patches for members of your organization to use for patch installation.

There are other benefits to using directory depots. Installation from a directory depot on a local or remote disk is likely to be faster than installing from removable media. You can also install software onto a remote system without having to physically load the install media onto the system.

For example, consider a company with multiple locations over a large geographical region. This company creates and maintains a centralized directory depot for companywide use and locates it on a networked system at location A. Employees at location B can install software from this depot onto systems at location C without ever leaving their desks.

## Tape Depots

Tape depots, also known as serial access depots, are primarily used for software transfer. Tape depots are completely contained within a single file, which is formatted as a tape archive (`tar`), and are accessed in a serial manner. Within the archive, directory and file entries are organized using the same structure as that used for directory depots. Tape depots have the default file extension `.depot`. Although you are not required to use this extension, it can help you to easily distinguish tape depots from other files.

If you download patches or patch bundles from HP, you receive tape depots. These depots might be contained in another file, such as a `tar` file or a shell archive (`shar`) file. Although the tape depot format was designed to support software delivery on tape, tape depots are not limited to tape media. You can locate them anywhere a directory depot can be located.

# Using Depots

As you start identifying uses for depots in your patch management process, you should consider the intended purpose and use model for each potential depot. There are many appropriate patch management uses for depots, including the following:

- Periodic patch depot

  A periodic patch depot contains patches that define the current recommended patch level. These are patches that you have tested as a group on the target configuration. You would generate periodic patch depots on a regular basis. Here are some possible generation time frames:

  - Quarterly or every other quarter, to coincide with the release of specific-standard HP-UX patch bundles, such as Quality Pack (QPK) or Hardware Enablement (HWE).
  - Monthly, to allow more timely inclusion of critical fixes and security patches.
  - Regularly in advance of scheduled system down time to take advantage of the opportunity to install new patches.

    Many users find it unacceptable to modify the contents of a periodic patch depot after it has undergone analysis and testing. In this case, you can create a critical patch depot to supplement a periodic patch depot.

- Critical patch depot

  A critical patch depot contains critical fix or security-related patches that were not available when you created the latest periodic patch depot. Use this depot to update any systems that encounter known failures and to bring systems up to the latest level of security patches. You can use this depot as the starting point for the next version of the periodic patch depot.

- Application depot

  An application depot contains patches specific to a given application. This type of depot might actually be a specific version of a periodic patch depot.

After you have identified the need that a specific depot will address, you should determine whether a directory depot or a tape directory best suits your needs. Most often, directory depots will be more useful for patch management. You must also select a location for the depot.

# Choosing Depot Type and Depot Location

You should review the following considerations before creating and using depots:

- **Do you require the depot to be available remotely for use by SD-UX commands such as** `swinstall?`

  If you are creating a depot for remote access, you need a directory depot. You must place the depot on a networked system that is accessible by all of the intended users, and you must register the depot. See "Registering and Unregistering Directory Depots" (page 108).

- **Will you use the depot for remote downloads?**

  In this case, tape depots are the better option. You can locate tape depots on a server for remote downloads, as HP has done with its FTP servers. See Chapter 7: "Using FTP as an Alternative Patch Source" (page 89).

- **Will the depot be heavily used?**

  You should ensure that both the system and the network are capable of meeting performance needs based on the intended use. If multiple users will access the depot simultaneously, you need a directory depot.

- **What amount of disk space and what level of disk performance are required?**

  You should ensure that both the disk space and level of disk performance are capable of meeting these needs. Depots can be large, and depot operations can involve a significant amount of disk activity.

- **Is the availability of the depot critical?**

  If the answer to this question is yes, you should consider high-availability storage solutions such as disk arrays or mirroring.

- **Does your organization need a heightened level of security?**

  If the answer to this question is yes, you should give additional consideration to safeguarding the depot. Access Control Lists (ACLs) can play a role in depot security. See "Advanced Topic: Access Control Lists" (page 109). In many cases, users of depots install software from the depot as the root user. Therefore, any compromise of software in a depot could lead to a security breach.

Although overlooked at times, a well-conceived depot-naming scheme can be very helpful. This is especially true if you have multiple depots, and is even more important if multiple users will access the depots.

- You should combine all the patches needed for a given purpose into a single depot.
- Your depot should include all products (including patches) necessary to meet the dependencies of patches in your depot.
- You can help limit risk by making only the necessary changes to your depot.
- You can reduce the size of your depot by removing superseded patches. See "Advanced Topic: Removing Superseded Patches from a Depot" (page 114).

# Viewing Depots

Use the SD-UX `swlist` command to list the registered directory or tape depots on a local or remote system. You can also use `swlist` to view the contents of a directory or tape depot. This section provides examples of how to use `swlist` to view depots.

**Example 8-1** Viewing a list of registered depots on the local system

```
swlist -l depot
```

For example:

```
# swlist -l depot
# Initializing...
# Target "my_sys" has the following depot(s):
  /var/spool/sw
  /depot/patches/2003-07_periodic_depot
  /depot/patches/2004-01_periodic_depot
  /tmp_depot/PHSS_29735.depot
```

**Example 8-2** Viewing a list of registered depots on a remote system

```
swlist -l depot @ rem_sys
```

For example:

```
# swlist -l depot @ swdepot.xyz.com
# Initializing...
# Target "swdepot.xyz.com" has the following depot(s):
  /depot/patches/11.00
  /depot/patches/11.04
  /depot/patches/11.11
  /depot/patches/11.23
```

**Example 8-3** Listing the contents of a directory or tape depot

```
swlist -l level -d @ some_sys:/full_dir_path/some_depot
```

The following values for *`level`* are useful: `bundle`, `product`, and `fileset`. For more information about `level`, see Chapter 3: "HP-UX Patch Overview" (page 27).

For example:

```
# swlist -l product -d @ swdepot.xyz.com:/depot/patches/11.11
# Initializing...
# Contacting target "swdepot.xyz.com"...
#
# Target:  swdepot.xyz.com:/depot/patches/11.11
#
  PHCO_23263    B.11.11.15     HP AutoRAID Manager cumulative patch
  PHCO_23370    1.0            lint(1) library patch
  PHCO_23463    1.0            sysdef(1) patch
  PHCO_23492    1.0            Kernsymtab Patch
  PHCO_23702    1.0            cumulative header file patch for prot.h
  PHCO_23909    1.0            cu(1) patch
  ...
```

**Example 8-4** Viewing the contents of a specified directory depot at various levels

```
swlist -l level @ some_sys:/full_path/some_depot
```

The following values for *level* are useful: `bundle`, `product`, and `fileset`. This command does not work for a tape depot.

For example:

```
# swlist -l product @ swdepot.xyz.com:/depot/patches/1123.depot
# Initializing...
# Contacting target "swdepot.xyz.com"...
#
# Target:  swdepot.xyz.com:/depot/patches/1123.depot
#
  PHCO_29605    1.0            VxVM 3.5~IA.004 Command Patch 01
  PHCO_29793    1.0            audisp(1M) patch
  PHCO_29957    1.0            libc cumulative patch
  PHCO_30027    1.0            Release notes document
  ...
```

For more information about the `swlist` command, see the Software Distributor Administration Guide on the HP Technical Documentation Web site at http://docs.hp.com.

# Creating and Adding to a Directory Depot

You can use the SD-UX `swcopy` command to create a directory depot from an existing tape or directory depot. Software objects from the source depot are copied into the target directory. By default, the `swcopy` command automatically registers newly created directory depots for use by Software Distributor.

The `swcopy` command has many possible arguments. For information, consult the swinstall(1M) manpage or the Software Distributor Administration Guide on the HP Technical Documentation Web site at **http://docs.hp.com**.

In this chapter, consider only the following command arguments:

```
swcopy [-p] -s [source_system:]/some_directory/source_depot \
software_selections @ [target_system:]/some_directory/target_depot
```

The `swcopy` arguments are as follows:

- `-p`
  - Executes in preview mode when given the optional `-p` command line argument.
  - Does not perform the software copy. It shows what the output from executing the command will be.
  - Results in the creation of the root directory for the depot as well as a catalog directory and a `swagent.log` file. The log file contains useful information, including disk space analysis. The command output includes instructions for viewing the information in the log file. These instructions are similar to the following:

```
NOTE: More information may be found in the agent logfile using
  the command "swjob -a log target_system-1234 @
  target_system:/some_directory/target_depot".
```

- `-s [`*`source_system`*`:]/`*`some_directory`*`/`*`source_depot`*
  - Specifies the tape or directory depot from which patches will be copied.
  - Include the name of the *`source_system`* to specify a system other than the local one.
  - Use the appropriate path and depot name of the depot on the media to copy from a depot located on media, such as CD or DVD.
- *`software_selections`*
  - Specifies the software to be copied.
  - Replace *`software_selections`* with a wildcard to copy multiple products to the target depot with one command. For example:
    - `\*` selects everything from the source depot.
    - `\*,c=patch` selects all patches from the source depot.
    - `PHXX_12345` selects patch `PHXX_12345` from the source depot.
- `@ [`*`target_system`*`:]/`*`some_directory`*`/`*`target_depot`*
  - Specifies the depot directory into which the selected patches will be copied.
  - Include the name of the *`target_system`* to specify a system other than the local one.
  - If this target does not exist and you execute the `swcopy` command as a user with appropriate permissions, the target is created. If you do not have the required permissions, the command generates an error message that provides information about actions you can take to resolve the problem.

## Copying Patches to Depots

The following example shows how to copy patch `PHCO_27780` from a remote directory depot to a local directory depot. The process creates the local depot. The following information gives detail about the target and source for the copy operation.

- *source_system*: `rmt_sys`
- *source_depot*: `/depot/patches/11.11/`
- *target_system*: `my_sys`
- *target_depot*: `/my_depots/new_dir_depot/`

1. List the registered depots on the local system before copying the patch:

   ```
   # swlist -l depot
   # Initializing...
   # Target "my_sys" has the following depot(s):
     /var/spool/sw
   ```

   The *target_depot* `/my_depots/new_dir_depot/` does not yet exist.

2. List the registered depots on the remote system:

   ```
   # swlist -l depot @ rmt_sys
   # Initializing...
   # Target "rmt_sys" has the following depot(s):
     /depot/patches/11.00
     /depot/patches/11.04
    /depot/patches/11.11
     /depot/patches/11.23
   ```

   Note the *source_depot*.

3. Show the contents of the *source_depot* `/depot/patches/11.11/`:

   ```
          # swlist -l product @ rmt_sys:/depot/patches/11.11
   # Initializing...
   # Contacting target "rmt_sys"...
   #
   # Target:  rmt_sys:/depot/patches/11.11
   #
     ...
     PHCO_27752    1.0            audevent(1M) cumulative patch
     PHCO_27758    1.0            gsp parser & DIMM labels
      PHCO_27780    1.0            HP-UX Patch Tools
     PHCO_27781    1.0            su(1) cumulative patch
     PHCO_27828    1.0            ups_mond(1M) cumulative patch
     ...
   ```

   Note the patch to be copied into the *target_depot*.

4. Execute the `swcopy` command in preview mode by including the `-p` argument:

   ```
      # swcopy -p -s rmt_sys:/depot/patches/11.11 PHCO_27780 \
      @ /my_depots/new_dir_depot
   ```

   The `swcopy` command generates a log file. The `swcopy` output contains a `swjob` command.

5. Use the `swjob` command to read the log file. This command also verifies that there is sufficient disk space for the copy.

   ```
   # swjob -a log my_sys-0827 @ my_sys:/my_depots/new_dir_depot
   ```

6. Read the log file.
7. Execute the `swcopy` command without the preview argument:

   ```
    # swcopy -s rmt_sys:/depot/patches/11.11 PHCO_27780 \
      @ /my_depots/new_dir_depot
   ```

8. Show the registered depots on the local system again:

   ```
   # swlist -l depot
   # Initializing...
   # Target "my_sys" has the following depot(s):
     /var/spool/sw
     /my_depots/new_dir_depot
   ```

   The newly created depot is listed.

9. Show the contents of the new depot:

   ```
   # swlist -l product -d @ /my_depots/new_dir_depot
   # Initializing...
   # Contacting target "my_sys"...
   #
   # Target:  my_sys:/my_depots/new_dir_depot
   #
     PHCO_27780    1.0          HP-UX Patch Tools
   ```

   Note that `PHCO_27780` is present.

## Advanced Topic: Security Patch Check Tool

After you create or modify a depot, you can run the Security Patch Check Tool on the depot to analyze the patches in the depot. This tool is available for free download from the Software Depot Web site at **http://software.hp.com**.

The Security Patch Check Tool identifies two classes of patches that you should investigate before continuing with patch installation:

- Patches in the depot that have been the subject of patch warnings.
- Patches not in the depot that are recommended to improve system security.

For information, see Chapter 9: “Using Other Patch Tools” (page 127), security_patch_check(1m) manpage, and the Security Patch Check FAQ on the HP Technical Documentation Web site at **http://docs.hp.com**.

# Registering and Unregistering Directory Depots

You must register a directory depot if you want its contents to be available for remote access by SD-UX commands across a network. Conversely, you may have to restrict remote access to a specific directory depot.

For example, you may be in the process of creating a directory depot to use for patch installation on production systems. Prior to completing testing on the depot, you do not want users to perform any installations from this depot; therefore, you need to restrict access to the depot. In this case, you simply unregister the depot to prevent remote access. You can also register or unregister tape depots, but you cannot use a registered tape depot as a software source for remote systems.

**NOTE:**

- Registered depots on a network server are both visible and accessible to remote systems. These depots can be used as a software source for remote systems.
- Unregistered depots on a network server are neither visible nor accessible to remote systems. These depots cannot be used as a software source for remote systems.

Depots can be registered or unregistered in the following ways:

- The `swreg` command explicitly registers or unregisters depots.
- The `swcopy` command automatically registers newly created depots.
- The `swremove` command automatically unregisters a depot after removing all the software contained in the depot.

If you have a depot that you want other users to access, you must register it. You should do this only if you intend the depot to be used as a software source for remote systems.

Depot registration is not required for access from the local host. Registration also is not required for remote `swlist` of depot contents. For additional details about the `swreg` command, see the swreg(1M) manpage and the Software Distributor Administration Guide on the HP Technical Documentation Web site at http://docs.hp.com.

**Example 8-5** Registering a depot

```
swreg -l depot full_path_to_depot
```

For example:

```
$ swreg -l depot /depot/patches/2003-07_periodic_depot/
=======  05/05/04 09:55:53 MDT  BEGIN swreg SESSION (non-interactive)

       * Session started for user "some_user@my_sys".

       * Beginning Selection
       * Targets:                my_sys
       * Objects:                /depot/patches/2003-07_periodic_depot/
       * Selection succeeded.
=======  05/05/04 09:55:53 MDT  END swreg SESSION (non-interactive)
```

**Example 8-6** Unregistering a depot

**swreg -u -l depot** *full_path_to_depot*

For example:

```
$ swreg -u -l depot /depot/patches/2003-07_periodic_depot/
=======  05/05/04 09:40:17 MDT  BEGIN swreg SESSION (non-interactive)
       * Session started for user "some_user@my_sys".

       * Beginning Selection
       * Targets:                my_sys
       * Objects:                /depot/patches/2003-07_periodic_depot
       * Selection succeeded.
=======  05/05/04 09:40:17 MDT  END swreg SESSION (non-interactive)
```

## Advanced Topic: Access Control Lists

If you require finer control over directory depot access, you should familiarize yourself with Access Control Lists (ACLs) and the SD-UX command `swacl`. You can use ACLs to grant a variety of access rights to certain systems or users. For more information, see the Software Distributor Administration Guide on the HP Technical Documentation Web site at **http://docs.hp.com**.

# Verifying Directory Depots

You can use the SD-UX command `swverify` to verify the contents of a directory depot. Tape depots are not valid targets for the `swverify` command. Depot verification does the following:

- Verifies that all dependencies can be met. For more information about dependencies, see Chapter 3: "HP-UX Patch Overview" (page 27).
- Reports missing files.
- Checks file attributes, including permissions, file types, size, checksum, mtime, and major/minor attributes.

If a depot fails verification, it may still be usable for your needs. You must read the `swverify` output to determine the cause and the implications of the failure.

The `swverify` command has many arguments. For information, you should consult swverify(1M) and the Software Distributor Administration Guide on the HP Technical Documentation Web site at **http://docs.hp.com**.

In this chapter, consider the following command arguments:

```
swverify -d software_selection @ depot_location
```

A basic description of these `swverify` arguments follows:

- `-d`

  Directs `swverify` to operate on a directory depot rather than on software currently installed on the system.

  When you use this argument, you must also use the `@` *`depot_location`* argument to specify the depot.

- *`software_selection`*

  Use to specify the software to be verified.

  Verify multiple products by replacing *`software_selection`* with a wildcard. The following examples demonstrate basic use of wildcards:

  - `\*` will select everything from the source depot
  - `\*,c=patch` will select all patches from the source depot
  - `PHXX_12345` will select patch `PHXX_12345` from the source depot

- `@` *`depot_location`*

  Use to specify the directory depot containing the software to be verified.

# Verifying Depots

**Example 8-7** Verifying a directory depot

The following example verifies the directory depot /my_depots/new_dir_depot. You can see that the verification was successful as indicated by the output "Verification succeeded".

```
# swverify -d \* @ /my_depots/new_dir_depot
=======  05/03/04 12:28:51 MDT  BEGIN swverify SESSION
         (non-interactive) (jobid=my_sys-0831)

       * Session started for user "some_user@my_sys".

       * Beginning Selection
       * Target connection succeeded for
         "my_sys:/my_depots/new_dir_depot".
       * Software selections:
             PHCO_27780.CMDS-AUX,r=1.0,a=HP-UX_B.11.11_32/64,v=HP,fr=1.0,
             fa=HP-UX_B.11.11_32/64
       * Selection succeeded.

       * Beginning Analysis
       * Session selections have been saved in the file
         "/.sw/sessions/swverify.last".
       * The analysis phase succeeded for
         "my_sys:/my_depots/new_dir_depot".
      * Verification succeeded.

NOTE:    More information may be found in the agent logfile using the
         command "swjob -a log my_sys-0831 @
         my_sys:/my_depots/new_dir_depot".

=======  05/03/04 12:28:51 MDT  END swverify SESSION (non-interactive)
         (jobid=my_sys-0831)
```

**Example 8-8** Verifying a directory depot

The following example verifies the directory depot /my_depots/PHSS_30278_depot/. This depot contains one patch, PHSS_30278. This patch is dependent on patch PHSS_29657, which is not included in the depot. Because of this, the verification failed. The command output indicates how you can obtain more information about the failure. In this case, if patch PHSS_29657 is already installed on the target system, then you can use depot PHSS_30278_depot for installation of patch PHSS_30278 even though the depot failed verification.

```
# swverify -d \* @ /my_depots/PHSS_30278_depot
=======  05/03/04 13:04:00 MDT  BEGIN swverify SESSION
         (non-interactive) (jobid=my_sys-0841)

       * Session started for user "some_user@my_sys".

       * Beginning Selection
       * Target connection succeeded for
         "my_sys:/my_depots/PHSS_30278_depot".
NOTE:    The software "PHSS_30278" was successfully marked, but it
         depends on the following software items which could not be
         found in the source. However, these items may already be in
         the target. This will be checked during the Analysis Phase:
         PHSS_29657.LANG-AUX,fa=HP-UX_B.11.23_IA
       * Software selections:
             PHSS_30278.F90-JPN-E-MAN,r=1.0,a=HP-UX_B.11.23_IA/PA,
             v=HP,fr=1.0, fa=HP-UX_B.11.23_IA/PA
             PHSS_30278.F90-JPN-S-MAN,r=1.0,a=HP-UX_B.11.23_IA/PA,
             v=HP,fr=1.0, fa=HP-UX_B.11.23_IA/PA
             PHSS_30278.F90-RELNOTES,r=1.0,a=HP-UX_B.11.23_IA/PA,
             v=HP,fr=1.0, fa=HP-UX_B.11.23_IA
             PHSS_30278.FORT90-MAN,r=1.0,a=HP-UX_B.11.23_IA/PA,
             v=HP,fr=1.0, fa=HP-UX_B.11.23_IA/PA
             PHSS_30278.FORT90-PRG,r=1.0,a=HP-UX_B.11.23_IA/PA,
             v=HP,fr=1.0, fa=HP-UX_B.11.23_IA
       * Selection succeeded.

       * Beginning Analysis
       * Session selections have been saved in the file
         "/.sw/sessions/swverify.last".
ERROR:   "my_sys:/my_depots/PHSS_30278_depot":  The software
         dependencies for 1 products or filesets cannot be resolved.
       * The analysis phase failed for
         "my_sys:/my_depots/PHSS_30278_depot".
      * Verification had errors.

NOTE:    More information may be found in the agent logfile using the
         command "swjob -a log my_sys-0841 @
         my_sys:/my_depots/PHSS_30278_depot".

=======  05/03/04 13:04:01 MDT  END swverify SESSION (non-interactive)
         (jobid=my_sys-0841)
```

# Removing Software from a Directory Depot

If you find it necessary to remove patches from a directory depot, you can accomplish this task with the SD-UX command `swremove`.

`swremove [-p] -d` *`patch_to_remove`* `@ [`*`target_system`*`:]/`*`some_directory`*`/`*`target_depot`*

A basic description of these `swremove` arguments follows:

- `-p`

  Execute in preview mode by using the optional `-p` command line argument.

- `-d`

  Operate on a depot rather than installed software.

- *`patch_to_remove`*
  - Use to specify the patches to be removed.
  - Replace with a wildcard to remove multiple patches with one command. Basic examples follow:
  - - `\*` will select everything from the source depot
    - `\*,c=patch` will select all patches from the source depot
    - `PHXX_12345` will select patch `PHXX_12345` from the source depot

- `@ [`*`target_system`*`:]/`*`some_directory`*`/`*`target_depot`*
  - Include *`target_system`* if you want to specify a system other than the local one.
  - Use to specify the directory depot from which the selected patches will be removed.

The success or failure of the command execution is indicated in the output. The output text details how to get more information.

It is good practice to unregister a depot that has been made available for remote use prior to modifying the depot. When you have completed depot modifications, reregister the depot to make it available again.

**Example 8-9** Removing a patch from a directory depot

The following example shows how to remove patch `PHCO_27780` from directory depot `/my_depots/new_dir_depot` on system `my_sys`:

```
$ swremove -d PHCO_27780 @ my_sys:/my_depots/new_dir_depot
=======  05/03/04 13:25:01 MDT  BEGIN swremove SESSION
         (non-interactive) (jobid=my_sys-0843)

       * Session started for user "some_user@my_sys".

       * Beginning Selection
       * Target connection succeeded for
         "my_sys:/my_depots/new_dir_depot".
       * Software selections:
             PHCO_27780.CMDS-AUX,r=1.0,a=HP-UX_B.11.11_32/64,
             v=HP,fr=1.0, fa=HP-UX_B.11.11_32/64
       * Selection succeeded.

       * Beginning Analysis
       * Session selections have been saved in the file
         "/.sw/sessions/swremove.last".
       * The analysis phase succeeded for
         "my_sys:/my_depots/new_dir_depot".
       * Analysis succeeded.

       * Beginning Execution
       * The execution phase succeeded for
         "my_sys:/my_depots/new_dir_depot".
      * Execution succeeded.

NOTE:    More information may be found in the agent logfile using the
         command "swjob -a log my_sys-0843 @
         my_sys:/my_depots/new_dir_depot".
=======  05/03/04 13:25:02 MDT  END swremove SESSION (non-interactive)
         (jobid=my_sys-0843)
```

## Advanced Topic: Removing Superseded Patches from a Depot

If you have a depot that you are using for patch installation that contains both superseded patches and the corresponding superseding patch, the superseded patches will never be installed and are a waste of disk space. There is a patch utility called `cleanup` that you can use to remove all patches from a software depot if they have been superseded by patches that are also available in the depot. This command works only for directory depots, not tape depots.

The `cleanup` utility is delivered by the following patches (and their superseding patches):

- `PHCO_27779` (HP-UX 11.0, B.11.00)
- `PHCO_27780` (HP-UX 11i v1, B.11.11)

To execute `cleanup` on the depot *`some_depot`*, you can use the following command:

**`cleanup [-p] -d /`**_`some_directory`_**`/`**_`some_depot`_

If you use the `-p` option, the command executes in preview mode. You will be able to see what changes will be made without any changes actually occurring. HP recommends that you always execute the command in preview mode first.

For additional information and command options, see the cleanup(1M) manpage.

**Example 8-10** Using the `cleanup` command

The following example shows how to use the `cleanup` command to remove superseded patches from the depot `/my_depots/patch_depot`.

- Use `swlist` to show the contents of depot `/my_depots/patch_depot`. The depot contains two patches: `PHCO_24630` and `PHCO_27780`. The patch `PHCO_27780` supersedes `PHCO_24630`.

```
 # swlist -l product @ /my_depots/patch_depot
 # Initializing...
 # Contacting target "my_sys"...
 #
 # Target:  my_sys:/my_depots/patch_depot
#
    PHCO_24630    1.0            HP-UX Patch Tools
    PHCO_27780    1.0            HP-UX Patch Tools
```

- Execute the `cleanup` command in preview mode to see what changes will occur without actually making any changes. From the command output, you know that patch `PHCO_24630` will be removed because `cleanup` will remove superseded patches and the output states that `"PHCO_24630 superseded by PHCO_27780".`

```
$ /usr/sbin/cleanup -p -d /my_depots/patch_depot
### Cleanup program started at 05/04/04  07:48:27
Preview mode enabled. No modifications will be made.
Cleanup of depot '/my_depots/patch_depot'.
Obtaining the list of patches in the depot:
 /my_depots/patch_depot ...done.
Obtaining the list of superseded 11.X patches in the depot:
    /my_depots/patch_depot ...The following superseded patches
    exist in the depot:
====================================================
PHCO_24630 superseded by PHCO_27780
All information has been logged to /var/adm/cleanup.log.
### Cleanup program completed at 05/04/04  07:48:27
```

- Execute the `cleanup` command:

```
$ /usr/sbin/cleanup -d /my_depots/patch_depot
### Cleanup program started at 05/04/04  07:50:39
Cleanup of depot '/my_depots/patch_depot'.
Obtaining the list of patches in the depot:
   /my_depots/patch_depot ...done.
Obtaining the list of superseded 11.X patches in the depot:
     /my_depots/patch_depot ...The following superseded patches
     exist in the depot:
====================================================
PHCO_24630 superseded by PHCO_27780

Please be patient; this may take several minutes.

Removing superseded 11.X patches from depot:
   /my_depots/patch_depot ...done.
The superseded 11.X patches have been removed from the depot:
      /my_depots/patch_depot.
All information has been logged to /var/adm/cleanup.log.
### Cleanup program completed at 05/04/04  07:50:39
```

- Use `swlist` to show the contents of depot `/my_depots/patch_depot`. The depot now contains only one patch: `PHCO_27780`

```
# swlist -l product @ /my_depots/patch_depot
# Initializing...
# Contacting target "my_sys"...
#
# Target:  my_sys:/my_depots/patch_depot
#
   PHCO_27780    1.0            HP-UX Patch Tools
```

## Removing a Directory Depot

The method of depot removal described is a two-step process. You must first ensure that the depot is unregistered using the SD-UX command swreg. To complete the depot removal, you must manually remove the depot's root directory.

The following example shows how to remove directory depot /my_depots/PHCO_27780_depot on local system my_sys.

1. Execute the following swreg command to unregister the depot.

```
$ swreg -u -l depot /my_depots/PHCO_27780_depot
=======  08/06/04 14:10:35 MDT  BEGIN swreg SESSION
    (non-interactive)

       * Session started for user "root@my_sys".

       * Beginning Selection
       * Targets:                my_sys
       * Objects:                /my_depots/PHCO_27780_depot
       * Selection succeeded.
=======  08/06/04 14:10:36 MDT  END swreg SESSION
    (non-interactive)
```

2. Manually remove the depot's root directory and contents.

```
$ rm -r /my_depots/PHCO_27780_depot/
```

# Installing Patches from a Depot

To install patches from a directory or tape depot, use the SD-UX command `swinstall`.

- For more information about the `swinstall` command than is presented in this chapter, see the swinstall(1M) manpage and the Software Distributor Administration Guide on the HP Technical Documentation Web site at **http://docs.hp.com**.
- For more information about installing patches, see Chapter 2: "Quick Start Guide for Patching HP-UX Systems" (page 17).

When you execute the `swinstall` command, you can see the success or failure of the command in the output, and how to get additional information. Prior to actually installing patches with the `swinstall` command, you should execute the command in preview mode by including the `-p` argument in the command.

The `swinstall` command has many possible arguments; however, consider only the following:

```
swinstall [-p] -s source_system:/some_directory/source_depot \
-x autoreboot=true -x patch_match_target=true software_selections \
[@ target_selections]
```

A basic description of these `swinstall` arguments follows:

- `-p`

  Execute in preview mode by using the optional `-p` command line argument. When executed in preview mode, `swinstall` does not perform the software installation; rather, it shows what the output from executing the command would be.

  Creates a log file which contains information including disk space requirements and use. The command output includes instructions for viewing the log file. The instructions are similar to the following:

  ```
  NOTE:    More information may be found in the agent
  logfile using the command
  "swjob -a log some_sys-1251 @ some_sys:/".
  ```

- `-s` *`source_system`*`:/`*`some_directory`*`/`*`source_depot`*

  Use to specify the tape or directory depot from which patches will be installed. For a tape depot, this must refer to a local depot.

  To install from a depot located on media such as CD or DVD, use the appropriate path and depot name of the depot on the media.

- `-x autoreboot=true`

  Use to instruct `swinstall` to reboot the system when it is required.

- `-x patch_match_target=true`

  Use to select for installation only those patches which are applicable to the target system. This means that only those patches which correspond to products installed on the system will be selected.

- *`software_selections`*

  Use to specify the software to be installed. If you use the `-x patch_match_target=true` option, you do not need to specify a software selection.

  To install multiple products to the target depot with one command, replace *`software_selections`* with a wildcard. The following are basic examples:

  - `\*` will select everything from the source depot
  - `\*,c=patch` will select all patches from the source depot
  - `PHXX_12345` will select patch `PHXX_12345` from the source depot

- `@` *`target_selections`* Use to specify the system where the specified software will be installed. Use this optional argument if the target system is not the local system.

**IMPORTANT:** Before you install any patches, you should back up your system.

The previous `swinstall` command includes the `autoreboot=true` argument. In the **Automatic Reboot** field of a patch's **patch details** page or the patch text file, if the field is set to `true` then when you use `swinstall` and the `autoreboot=true` argument and install patches the target system will automatically reboot.

There will be a brief warning given prior to the system reboot, but the system will go down immediately after the warning is issued. Therefore, it is very important that prior to installing any patches that require a system reboot that you follow your company's policy regarding a system reboot.

For information, consult the Software Distributor Administration Guide and the `swinstall` manpage on the HP Technical Documentation Web site at **http://docs.hp.com**.

## Installing Patches from a Depot

**Example 8-11** Installing patches

To install all applicable patches in directory depot /my_depots/depot onto the local system.

For example:

```
$ swinstall -s /my_depots/depot \
  -x autoreboot=true -x patch_match_target=true

=======  05/03/04 14:07:16 MDT  BEGIN swinstall SESSION
            (non-interactive) (jobid=my_sys-0856)

       * Session started for user "some_user@my_sys".

       * Beginning Selection
       * Target connection succeeded for "my_sys:/".
       * Source connection succeeded for
         "my_sys:/my_depots/depot".
       * Source:                 /my_depots/depot
       * Targets:                my_sys:/
       * Software selections:
             PHSS_30501.AGRM,l=/,r=B.11.11.22,
               a=HP-UX_B.11.11_32/64,v=HP,fr=B.11.11.22,
               fa=HP-UX_B.11.11_32/64
  ...
             PHSS_30501.XEXT-RECORD,l=/,r=B.11.11.22,
             a=HP-UX_B.11.11_32/64,v=HP,
             fr=B.11.11.22,fa=HP-UX_B.11.11_32/64
       * Selection succeeded.

       * Beginning Analysis
       * Session selections have been saved in the file
         "/.sw/sessions/swinstall.last".
       * The analysis phase succeeded for "my_sys:/".
       * Analysis succeeded.
```

**NOTE: More information may be found in the agent logfile using the command "swjob -a log my_sys-0856 @ my_sys:/".**

```
=======  05/03/04 14:07:22 MDT  END swinstall SESSION
    (non-interactive)
         (jobid=my_sys-0856)
```

**Example 8-12** Using the swinstall command to select and install specific patches from a depot

swinstall -x autoreboot=true -s _depot software_selection_

Use the _software_selections_ argument to specify what software should be installed. Using wildcards, you can select multiple products for installation. The following are basic examples:

- * will select everything from the source depot
- *,_c=patch_ will select all patches from the source depot
- PHXX_12345 will select patch PHXX_12345 from the source depot

**Example 8-13** Installing a single patch

This example shows how to install a single patch, `PHCO_28175`, from directory depot `/my_depots/a_depot`.

For example:

```
$ swinstall -x autoreboot=true -s /my_depots/a_depot PHCO_28175
=======  05/03/04 14:22:52 MDT  BEGIN swinstall SESSION
         (non-interactive) (jobid=my_sys-0864)

       * Session started for user "some_user@my_sys".

       * Beginning Selection
       * Target connection succeeded for "my_sys:/".
       * Source connection succeeded for
         "my_sys:/my_depots/a_depot".
NOTE:    The patch match operation failed to find patches for target
         software on "my_sys" which passed the filter.
       * Source:                 /my_depots/a_depot
       * Targets:                my_sys:/
       * Software selections:
             PHCO_28175.CORE-ENG-A-MAN,r=1.0,a=HP-UX_B.11.11_32/64,v=HP,
             fr=1.0,fa=HP-UX_B.11.11_32/64
       * Selection succeeded.

       * Beginning Analysis and Execution
       * Session selections have been saved in the file
         "/.sw/sessions/swinstall.last".
       * The analysis phase succeeded for "my_sys:/".
       * The execution phase succeeded for "my_sys:/".
       * Analysis and Execution succeeded.

NOTE:    More information may be found in the agent logfile using the
    command "swjob -a log my_sys-0864 @ my_sys:/".

=======  05/03/04 14:23:38 MDT  END swinstall SESSION (non-interactive)
         (jobid= my_sys-0864)
```

## Custom Patch Bundles

Although bundles are not directly related to depots, this section discusses them as they can be helpful when you use them in combination with directory depots that you are using for patch management. Bundles allow you to group sets of related patches. A bundle can be more recognizable than a group of individual patches when located in a depot or installed on a system. For more information about bundles, see Chapter 3: "HP-UX Patch Overview" (page 27).

Creating your own custom bundles is not difficult; however, to use the method presented, you must have the HP Ignite-UX (IUX) installed on your system. IUX is an HP-UX administration toolset that helps with the following tasks:

- Installing HP-UX
- Creating custom install configurations or golden images
- Recovering HP-UX clients remotely
- Creating custom recovery media
- Managing and monitoring multiple client installation sessions

For more information about IUX, see the Ignite-UX Administration Guide available on the HP Technical Documentation Web site at **http://docs.hp.com**.

You can also visit the HP **Software Depot Ignite-UX Summary** Web page at **http://software.hp.com/products/IUX**.

You can use IUX to create custom bundles from patches that you have placed in a temporary depot. You can then move this bundle to a permanent depot, such as a periodic depot, for installation purposes. HP recommends custom bundle creation when you have a group of closely related patches that you want to place in a depot with other patches. This is advantageous for the following reasons:

- When you list the contents of the depot, you will see the bundle rather than the individual patches listed among the other patches contained in the depot.
- If you choose to install only this group of patches, you simply select the bundle for installation.
- After installing a bundle, when you use `swlist` to list the patches on a system you will see the bundle rather than the individual patches contained in the bundle.

Suppose you have a group of 10 patches related to software application XYZ for the first quarter of 2004. You can create a bundle of these patches and name it `2004_Q1_APP_XYZ`. You can then place this bundle in your periodic patch depot. When you `swlist` the depot, the bundle name will show up instead of the 10 individual patches. This can be very helpful when `swlist` returns a large list, because your bundle will be much more observable than the individual patches.

## Listing Patches and Bundles

The following is an example of `swlist` output in which the group of 10 related patches described previously were individually added to a depot and individually installed on a system. The `swlist` output for the depot and the system will appear similar to the following. Note that it is time consuming and tedious to determine if all the 10 patches are listed, as they are listed among all the other patches in the output.

**Example 8-14** Seeing the swlist output

```
#
# Bundle(s):
#
  SOME_BUNDLE_001               rev         bundle description
  SOME_BUNDLE_002               rev         bundle description

#
# Product(s) not contained in a Bundle:
#
  SOME_PATCH_001                rev         patch description
  INDIVIDUAL_XYZ_PATCH_001      rev      patch description
  SOME_PATCH_002                rev         patch description
  SOME_PATCH_003                rev         patch description
  SOME_PATCH_004                rev         patch description
  INDIVIDUAL_XYZ_PATCH_002      rev      patch description
  ...
  SOME_PATCH_067                rev         patch description
  SOME_PATCH_068                rev         patch description
  SOME_PATCH_069                rev         patch description
INDIVIDUAL_XYZ_PATCH_010      rev      patch description
  ...
  SOME_PATCH_134                rev         patch description
   INDIVIDUAL_XYZ_PATCH_015      rev      patch description
  SOME_PATCH_135                rev         patch description
  SOME_PATCH_136                rev         patch description
  ...
```

However, if you bundle the patches into a bundle called 2004_Q1_APP_XYZ_BUNDLE, it is much easier to determine if the patches are included in the swlist output.

```
#
# Bundle(s):
#
  SOME_BUNDLE_001               rev         bundle description
  SOME_BUNDLE_002               rev         bundle description
  2004_Q1_APP_X_BUNDLE          rev      bundle description

#
# Product(s) not contained in a Bundle:
#
  SOME_PATCH_001                rev         patch description
  SOME_PATCH_002                rev         patch description
  ...
```

## Creating a Custom Bundle

This example shows custom bundle creation. After performing an assessment, and based on the results, add the following patches to the periodic patch depot /my_depots/periodic_depot/:

- PHCO_24587
- PHCO_25130
- PHCO_28175
- PHCO_28830

Download the patches and create a temporary depot (/my_depots/tmp_depot/) containing the patches. The following steps show how to create a custom bundle containing these patches and copy the bundle to a periodic patch depot. The name of our new bundle is PATCH_ASSESSMENT_05042004. Note that 05042004 represents the date on which the patch assessment was performed.

1. List the patches in the temporary depot /my_depots/tmp_depot/, which contains the patches identified by the patch assessment.

```
# swlist -d @ /my_depots/tmp_depot/
# Initializing...
# Contacting target "my_sys"...
# Target:  my_sys:/my_depots/tmp_depot/

#
# No Bundle(s) on my_sys:/my_depots/tmp_depot/
# Product(s):
#
  PHCO_24587    1.0            psrset(1M) man page patch
  PHCO_25130    1.0            vPar manpage cumulative patch
  PHCO_28175    1.0            vPar commands man pages patch
  PHCO_28830    1.0            security(4) man page cumulative patch
```

2. Create a bundle containing these four patches. The following command will create a bundle named PATCH_ASSESSMENT_05042004 with a title of "May 04, 2004: HP-UX 11.11 Patch Assessment Patches" and a revision of 1.0 in the temporary depot.

```
$ make_bundles -B \
 -n PATCH_ASSESSMENT_05042004 \
 -t "May 04, 2004: HP-UX 11.11 Patch Assessment Patches" \
 -r 1.0 \
 /my_depots/tmp_depot/
```

3. List the contents of the temporary depot. Note the presence of the newly created bundle.

```
      # swlist -d @ /my_depots/tmp_depot/
      # Initializing...
      # Contacting target "my_sys"...
      # Target:  my_sys:/my_depots/tmp_depot/

      #
      # Bundle(s):
      #
        PATCH_ASSESSMENT_05042004   1.0   May 04, 2004:
        HP-UX 11.11 Patch Assessment Patches
```

4. Preview copying the bundle from the temporary depot to the periodic depot. Review the output generated by this command.

```
      $ swcopy -p -s my_sys:/my_depots/tmp_depot/ PATCH_ASSESSMENT_05042004 \
        @ my_sys:/my_depots/periodic_depot/

      =======  05/04/04 14:25:00 MDT  BEGIN swcopy SESSION (non-interactive)
               (jobid=my_sys-1132)

             * Session started for user "some_user@my_sys".

             * Beginning Selection
             * "my_sys:/my_depots/periodic_depot/":  This target does
               not exist and will be created.
             * Source connection succeeded for "my_sys:/my_depots/tmp_depot/".
             * Source:                 my_sys:/my_depots/tmp_depot/
             * Targets:                my_sys:/my_depots/periodic_depot/
             * Software selections:
                   PATCH_ASSESSMENT_05042004,r=1.0,a=HP-UX_B.11.11_32/64
                   PHCO_24587.ADMN-ENG-A-MAN,r=1.0,a=HP-UX_B.11.11_32/64,v=HP,
                     fr=1.0,fa=HP-UX_B.11.11_32/64
                   PHCO_25130.CORE-ENG-A-MAN,r=1.0,a=HP-UX_B.11.11_32/64,v=HP,
                     fr=1.0,fa=HP-UX_B.11.11_32/64
                   PHCO_28175.CORE-ENG-A-MAN,r=1.0,a=HP-UX_B.11.11_32/64,v=HP,
                     fr=1.0,fa=HP-UX_B.11.11_32/64
                   PHCO_28830.ADMN-ENG-A-MAN,r=1.0,a=HP-UX_B.11.11_32/64,v=HP,
                     fr=1.0,fa=HP-UX_B.11.11_32/64
                   PHCO_28830.CORE-ENG-A-MAN,r=1.0,a=HP-UX_B.11.11_32/64,v=HP,
                     fr=1.0,fa=HP-UX_B.11.11_32/64
                   PHCO_28830.PAUX-ENG-A-MAN,r=1.0,a=HP-UX_B.11.11_32/64,v=HP,
                     fr=1.0,fa=HP-UX_B.11.11_32/64
                   PHCO_28830.SEC-ENG-A-MAN,r=1.0,a=HP-UX_B.11.11_32/64,v=HP,
                     fr=1.0,fa=HP-UX_B.11.11_32/64
             * Selection succeeded.

             * Beginning Analysis
             * Session selections have been saved in the file
               "/.sw/sessions/swcopy.last".
             * The analysis phase succeeded for
               "my_sys:/my_depots/periodic_depot/".
            * Analysis succeeded.
```

**NOTE:** **More information may be found in the agent logfile using the command "swjob -a log my_sys-1132 @ my_sys:/my_depots/periodic_depot/".**

```
      =======  05/04/04 14:25:01 MDT  END swcopy SESSION (non-interactive)
               (jobid=my_sys-1132)
```

5. Copy the bundle from the temporary depot to the periodic depot.

```
$ swcopy -s my_sys:/my_depots/tmp_depot/ PATCH_ASSESSMENT_05042004 \
  @ my_sys:/my_depots/periodic_depot/

=======  05/04/04 14:25:20 MDT  BEGIN swcopy SESSION (non-interactive)
         (jobid=my_sys-1133)

       * Session started for user "some_user@my_sys".

       * Beginning Selection
       * "my_sys:/my_depots/periodic_depot/":  This target does
         not exist and will be created.
       * Source connection succeeded for "my_sys:/my_depots/tmp_depot/".
       * Source:                 my_sys:/my_depots/tmp_depot/
       * Targets:                my_sys:/my_depots/periodic_depot/
       * Software selections:
             PATCH_ASSESSMENT_05042004,r=1.0,a=HP-UX_B.11.11_32/64
             PHCO_24587.ADMN-ENG-A-MAN,r=1.0,a=HP-UX_B.11.11_32/64,v=HP,
               fr=1.0,fa=HP-UX_B.11.11_32/64
             PHCO_25130.CORE-ENG-A-MAN,r=1.0,a=HP-UX_B.11.11_32/64,v=HP,
               fr=1.0,fa=HP-UX_B.11.11_32/64
             PHCO_28175.CORE-ENG-A-MAN,r=1.0,a=HP-UX_B.11.11_32/64,v=HP,
               fr=1.0,fa=HP-UX_B.11.11_32/64
             PHCO_28830.ADMN-ENG-A-MAN,r=1.0,a=HP-UX_B.11.11_32/64,v=HP,
               fr=1.0,fa=HP-UX_B.11.11_32/64
             PHCO_28830.CORE-ENG-A-MAN,r=1.0,a=HP-UX_B.11.11_32/64,v=HP,
               fr=1.0,fa=HP-UX_B.11.11_32/64
             PHCO_28830.PAUX-ENG-A-MAN,r=1.0,a=HP-UX_B.11.11_32/64,v=HP,
               fr=1.0,fa=HP-UX_B.11.11_32/64
             PHCO_28830.SEC-ENG-A-MAN,r=1.0,a=HP-UX_B.11.11_32/64,v=HP,
               fr=1.0,fa=HP-UX_B.11.11_32/64
       * Selection succeeded.

       * Beginning Analysis and Execution
       * Session selections have been saved in the file
         "/.sw/sessions/swcopy.last".
       * The analysis phase succeeded for
         "my_sys:/my_depots/periodic_depot/".
       * The execution phase succeeded for
         "my_sys:/my_depots/periodic_depot/".
       * Analysis and Execution succeeded.
```

**NOTE: More information may be found in the agent logfile using the command "swjob -a log my_sys-1133 @ my_sys:/my_depots/periodic_depot/".**

```
=======  05/04/04 14:25:22 MDT  END swcopy SESSION (non-interactive)
         (jobid=my_sys-1133)
```

6. The periodic depot now contains the newly created bundle.

```
# swlist -d @ /my_depots/periodic_depot/
# Initializing...
# Contacting target "my_sys"...
# Target:  my_sys:/my_depots/periodic_depot/

#
# Bundle(s):
#
  PATCH_ASSESSMENT_05042004   1.0   May 04, 2004: HP-UX 11.11 Patch Assessment
  Patches
```

7. Lastly, remove the temporary depot.

```
$ swreg -u -l depot my_sys:/my_depots/tmp_depot/
$ rm -r /my_depots/tmp_depot/
```

## Where to Go Next

Go to Chapter 9: "Using Other Patch Tools" (page 127). It contains instructions on how to use the Patch Assessment Tool and Security Patch Check Tool. These tools can make patching and patch management easier in your environment.

# 9 Using Other Patch Tools

This chapter describes how to use the following tools:

- "Using the Patch Assessment Tool" (page 128)
- " Using the Security Patch Check Tool " (page 131)

# Using the Patch Assessment Tool

You can use the Patch Assessment Tool to create custom patch bundles for individual HP-UX systems and for multiple systems which you manage as a group. The Patch Assessment Tool simplifies the bundle creation process by guiding you through system-based patch analysis and selection. HP's Web-based Patch Assessment Tool is available at no charge on the IT Resource Center (ITRC): **http://itrc.hp.com**

The Patch Assessment Tool replaces the Custom Patch Manager (CPM) Tool.

In addition to custom bundle creation, you may also use the Patch Assessment Tool to do the following:

- Ensure that your system meets HP's currently recommended patch configuration.
- Ensure that all applicable security patches are installed on your system.
- Identify and acquire replacement patches for patches with warnings installed on your system.

If you are implementing a proactive patch management strategy, the Patch Assessment Tool can be useful as your primary method of patch selection. See Chapter 4: "Patch Management Overview" (page 57) for more information about proactive patching.

Benefits of using the Patch Assessment Tool to select and acquire patches include the following:

- The assessment returns a set of patches customized to your needs based on your input.
- The tool automatically checks your selected patches against each other as well as against patches currently installed on your system to detect conflicts and dependencies.
- The assessment results include information detailing why each patch was recommended.
- You can request application-specific patch sets.
- You can request the latest Quality Pack (QPK) bundle and any additional patches you may need.
- You can download recommended patches as a `tar`, `zip`, or `gzip` package.

To access the Patch Assessment Tool main Web page, use these steps:

1. Log in to the ITRC at **http://itrc.hp.com**.

   Please note that you need to log in to the appropriate site (Americas/Asia-Pacific or European).

2. Select **maintenance and support (hp products)**.
3. Select **custom patch bundles - run a patch assessment**.

   You are now on the **run a patch assessment** page.

4. You can access information regarding use of the Patch Assessment Tool, including how to complete the tasks in the previous list, by going to the **useful links** on the **run a patch assessment** page. Some links include the following topics:

   - **running a patch assessment**
   - **configuring an assessment profile**
   - **interpreting assessment results**

5. To run an assessment, you must complete the following tasks. This section provides an outline of the tasks, for procedures you can use th**useful links** in the previous step or "Using the Patch Assessment Tool" (page 129).

   - Download a collection script to the system to be analyzed.
   - Execute the collection script.

     The collection script creates a file called `hostname.fs`, where hostname is the result of `uname -n`. This file contains information such as what software, patches, and patch bundles are installed on the system.

   - Upload `hostname.fs` to the **Patch Assessment** site.
   - Choose an assessment profile.

     The assessment profile specifies what rules the tool will use when determining which patches and patch bundles to select for your system.

You may choose to use the default HP recommended assessment profile or configure a custom assessment profile.

- A custom profile allows you to choose a Patch Strategy.
- Creating a custom profile allows you to specify that the assessment select patches for any of the following:
  - Latest Quality Pack (QPK) patch bundle
  - Security patches
  - Replacements for installed patches with critical warnings
  - Replacements for installed patches with any warnings
  - Critical fixes
  - Updates for the patches already installed
  - Miscellaneous patches for the specific operating system of the system being assessed
  - Miscellaneous patches for the specific hardware model of the system being assessed
  - Application specific patch sets
  - All applicable patches

## Using the Patch Assessment Tool

The following example shows the steps that you would follow to create a custom patch assessment profile and run a patch assessment using this profile. You would be accessing the ITRC from the system to be analyzed. If this is not the case, you can still use the Patch Assessment Tool. However, you will have intermediate steps in which you transfer files from and to the system you are using to access the ITRC and the system to be analyzed.

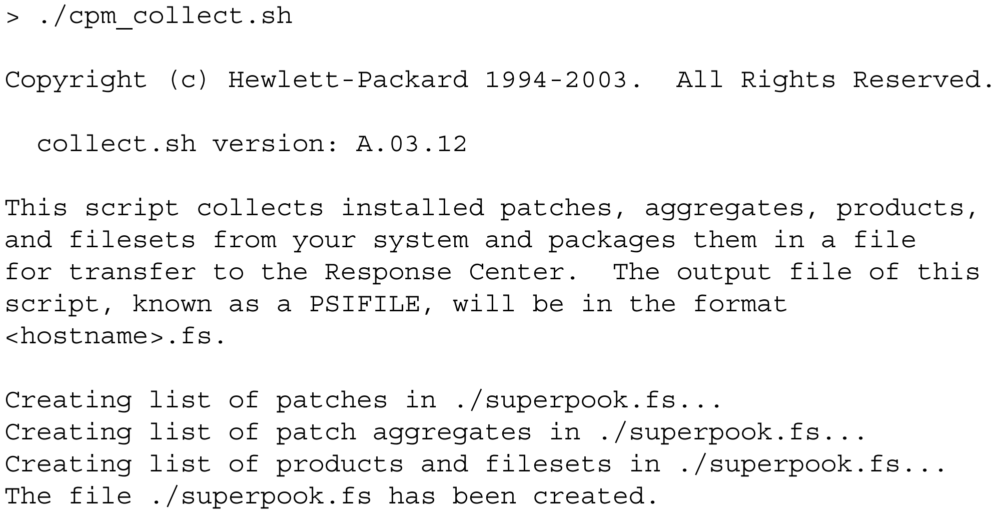
1. Open a browser on the target system.
2. Log in to the IT Resource Center at **http://itrc.hp.com**.
3. Select **maintenance and support (hp products)**.
4. Click **custom patch bundles - run a patch assessment**.

   You are now on the **run a patch assessment** page. This is the home page for the Patch Assessment Tool. You can see that no system information has been uploaded.
5. Select **upload new system information**.

   The **upload system information** page appears.
6. Select `cpm_collect.sh` and download the collection script to the target system.
7. Run the data collection script, `cpm_collect.sh`, on the target system.

   This creates an output file with a .fs extension. Figure 9-1: “Running cpm_collect.sh” (page 130) shows the script's output.

**Figure 9-1** Running cpm_collect.sh



```
> ./cpm_collect.sh

Copyright (c) Hewlett-Packard 1994-2003.  All Rights Reserved.

  collect.sh version: A.03.12

This script collects installed patches, aggregates, products,
and filesets from your system and packages them in a file
for transfer to the Response Center.  The output file of this
script, known as a PSIFILE, will be in the format
<hostname>.fs.

Creating list of patches in ./superpook.fs...
Creating list of patch aggregates in ./superpook.fs...
Creating list of products and filesets in ./superpook.fs...
The file ./superpook.fs has been created.
```

8. In the browser window that you opened in Step 1, click the **Browse** button and select the output file.
9. Select **submit** to upload the file.

   The new system appears.
10. Select the **create new assessment profile** link to open the **assessment profile** page.
11. Create and customize the assessment profile. After making your selections, select **save**.
12. Select the newly created profile and select the **display candidate patches** button.

    This produces the **patch assessment results**.
13. Review the patches in the **patch assessment results** and place a check by the patches you want to download.

    Each selected patch has text detailing the reason for patch selection.
14. Select **add to selected patch list**.

    The **selected patch list** appears.
15. Review the list.

    Additional patches needed to satisfy dependencies of your selected patches will appear in this list.
16. Select **download selected**.

    The **download patches** page appears.
17. Select the desired download format and select the **download** button to download the bundle to the target system.

    When the download is complete, the selected patches will be on your system and ready for the installation process.

# Using the Security Patch Check Tool

You can use the Security Patch Check Tool to analyze an HP-UX 11.x system and a software depot. The tool will determine which minimal security patches, updates, and manual actions have yet to be applied to the system, and generate a report listing the patches and actions recommended to become compliant with HP security bulletins. The tool also identifies patches with warnings present on the system or in the depot.

Using the Security Patch Check Tool can help you efficiently improve system security by determining if you have relevant security patches on your system. However, using this tool does not guarantee system security. HP's Security Patch Check Tool is available at no charge from the Software Depot Web site at **http://software.hp.com**.

---

**NOTE:** The Security Patch Check Tool works with the HP-UX 11.0 and HP-UX 11i operating systems. It does not analyze operating systems and products that are obsolete or unsupported.

In addition, some products require manual actions to resolve security issues. All HP-UX customers should subscribe to the HP-UX security bulletin mailing list on the ITRC to ensure they are notified of security patches, updates, or required manual actions.

---

Sources of additional tool information:

- Security Patch Check FAQ on the HP Technical Documentation Web site at **http://docs.hp.com**.
- security_patch_check(1M) manpage for information on updates, removals, and manual actions.

---

**NOTE:** HP recommends that you review the security_patch_check manpage for the latest functionality and options.

---

# Accessing a Security Catalog

When the Security Patch Check Tool analyzes your system (or depot), it compares the patches on your system (or in your depot) to a copy of the HP security catalog that is either on your system or downloaded from HP via the Internet. You can either direct the tool to perform the catalog update automatically when it runs or you can download it manually. HP updates this catalog nightly.

## Manual Download of Security Catalog

If you choose to manually download the security catalog, use these steps:

1. You can acquire the security catalog from the IT Resource Center (ITRC) using a Web browser or an FTP server:

   **ftp://ftp.itrc.hp.com/export/patches/security_catalog.gz**

2. After you have acquired the file, you must uncompress it:

   ```
   gunzip security_catalog.gz
   ```

3. Move the file to its final location on your system and note this location for use when running the tool.
4. To manually update the local copy of the security catalog and run the tool on the local system, use the following command:

   ```
   security_patch_check -c /path/to/catalog
   ```

   Where *`/path/to/catalog`* is the path to the security catalog.

   The following is an example of running the tool with the `–c` option.

   ```
   > security_patch_check -c /some_path/security_catalog

   *** BEGINNING OF SECURITY PATCH CHECK REPORT ***
   Report generated by: /opt/sec_mgmt/spc/bin/security_patch_check.pl, run as user

   Analyzed localhost (HP-UX 11.11) from nina
   Security catalog: ./security_catalog
   Security catalog created on: Sun Nov 28 23:30:13 2004
   ```

```
Time of analysis: Mon Nov 29 13:53:17 2004

List of recommended actions for most secure system:

#   Recommended  Bull  Cnt  Spec Reboot PDep Description
----------------------------------------------------------------------------------
1   MANUAL_ACTION    16      1st   man   ?       ?      Patch sums and the MD5 prog
2   MANUAL_ACTION    111     1st   man   ?       ?      Sec. Vulnerability with Ign
3   MANUAL_ACTION    150     1st   man   ?       ?      check swacl settings
4   CIFS-Server       157     1st   man   ?       ?      edit smb.conf to remove ma
5   CIFS-Server       164     1st   man   ?       ?      ensure "passwd program" op
/bin/passwd %u
6   MANUAL_ACTION    188r1   1st   man   ?       ?      Sec. Vulnerability in JAVA
7   MANUAL_ACTION    205r1   1st   man   ?       ?      RFC 1948 ISN randomization
8   MANUAL_ACTION    231     1st   man   ?       ?      Change insecure permissions
9   MANUAL_ACTION    239r1   1st   man   ?       ?      Affected versions and the c
 are listed elsewhere in this bulletin.
10  InternetSrvcs     246r5   1st   man   ?       ?      Modify /etc/mail/sendmail.
11  InternetSrvcs     253r8   1st   man   ?       ?      Modify /etc/mail/sendmail.
12  InternetSrvcs     266r4   1st   man   ?       ?      See MANUAL ACTIONS section
13  InternetSrvcs     281r8   1st   man   ?      ?      modify /etc/mail/sendmail.c
14  OS-Core           304     1st   man   ?       ?      unpack patches using the r
15  OBAM              1047    1st   man   ?       ?      disable the OBAM web admin
16  PHCO_28848       293r1   2nd   No    No      No    Software Distributor Cumulat
17  PHNE_27796        209r16  1st   Yes   No      Yes   libnss_dns DNS backend
18  PHSS_23067        137r3   1st   No    No     No    OnlineDiag/Support Tool Mana
19  PHSS_30478        1018    1st   No    No      No    X11 Font Library
20  PHSS_30789        1038    3rd   Yes   No      Yes   CDE Applications Periodic
21  PHSS_30871        1018    1st   No    Yes     No    Xserver cumulative
22  PHSS_31988        1088    3rd   No    No      No    X Font Server
23  PRM-Sw-Lib        1065    1st   upd   ?       ?      install revision C.02.02 c
24  CIFS-Server       1086   7th   upd   ?       ?      install revision A.01.11.03
----------------------------------------------------------------------------------
NOTE:    Security bulletins can be found ordered by Document ID at
  http://itrc.hp.com/cki/bin/doc.pl/screen=ckiSecurityBulletin
```

## Automatic Download of Security Catalog

If you choose to automatically download the security catalog, use these steps:

1. If both of the following are true, you will need to set the `ftp_proxy` environment variable or the `https_proxy` environment variable, depending on which one you are using, to indicate the proxy server for the local subnet:

   - You choose to have the tool automatically download the catalog when it runs.
   - Your system is behind a proxy-type firewall.

   The environment variable, either the `ftp_proxy` variable or the `https_proxy`, tells the Security Patch Check Tool how to perform file transfers from behind the firewall.

2. Use one of the following command formats to set the variable:

   **`export <ftp|http|https>_proxy=protocol://address:port`**

   where:

   - `protocol` is the method your proxy server uses: `https`, `http`, or `ftp`.
   - `address` is the address of your proxy server
   - `port` is the port used by your proxy server, usually `8088`

For example, **export https_proxy=https://myproxy.my:port**

3. To automatically update the local copy of the security catalog and run the tool on the local system, use the following command:

   **security_patch_check -r**

   The `-r` option specifies that the tool should automatically download and use the latest security catalog when analyzing your system.

   The following is an example of running the tool with the `-r` option.

```
> security_patch_check -r
NOTE:    Downloading from https://itrc.hp.com.

NOTE:    Downloading /export/patches/security_catalog.gz.
NOTE:    /export/patches/security_catalog.gz downloaded to ./security_catalog2.g
  successfully.

NOTE: HP has issued Non-Critical warnings for the active patch PHCO_19292 on
  the target system.  Its record, including the Warn field, is available from
  /home/myuser/security_catalog2, through the Patch Database area of the
  ITRC or by using the -m flag (security_patch_check -m ...).

NOTE:  HP has issued Non-Critical warnings for the active patch PHCO_20443 on th
  target system. Its record, including the Warn field, is available from
  /home/myuser/security_catalog2, through the Patch Database area of the ITRC or
  using the -m flag (security_patch_check -m ...).

WARNING:  HP has issued Critical warnings for the patch PHNE_17027 and it was
   found on the target. Unfortunately, security_patch_check was unable to detern
   if the patch is superseded or active on the target. You will need to determin
   yourself if you want to keep the patch, remove it from the system, or discove
   if it has been superseded by some other patch on the system. You can check
   its status with:
   swlist -a patch_state PHNE_17027
   or more accurately, with
   /usr/contrib/bin/check_patches
   (delivered in a patch for each OS, log onto http://itrc.hp.com to find it)

*** BEGINNING OF SECURITY PATCH CHECK REPORT ***
 Report generated by: ./security_patch_check.pl, run as myuserAnalyzed localhost
(HP-UX 11.00) from myhost
Security catalog: /home/myuser/security_catalog2
Security catalog created on: Fri Apr 9 11:55:08 2004
Time of analysis: Fri Apr 16 15:17:35 2004

List of recommended actions for most secure system:

#  Recommended    Bull   Cnt  Spec Reboot PDep Description
----------
1  MANUAL_ACTION  2r1     1st  man   ?    ?    Java(TM) Secure Socket Extension
2  MANUAL_ACTION  16      1st  man   ?    ?   Patch sums and the MD5 program
3  MANUAL_ACTION  26r1   1st  man   ?    ?    Preparing Your HP-UX System for SA
4  MANUAL_ACTION  65      1st  man   ?    ?    Security  Advisory in Netscape sh
...
15  InternetSrvcs    246r5    1st  man   ?    ?    Modify /etc/mail/sendmail.cf
16  InternetSrvcs    253r8    1st  man   ?    ?    Modify /etc/mail/sendmail.cf
17  PHSS_29201    263r1 1st  man   ?    ?    None
18  WUFTP-26     277r1 1st  man   ?    ?    WU-FTPD 2.6.1 from software.hp.com
```

```
...
77  PHSS_30010  309  12th  Yes  No  Yes  s700_800 11.00 CDE Runtime
```

## Running Security Patch Check on a Software Depot

You may want to run Security Patch Check on a depot. This can be especially helpful for depots that you are not familiar with.

To run the tool on a software depot, use one of the following commands:

- Use the `-r` option

```
swlist -l fileset -a supersedes -a revision -a software_spec -a state \
-d @ /path/to/depot | security_patch_check - -r -a -s 11.xx
```

- Use the `-c` option

```
swlist -l fileset -a supersedes -a revision -a software_spec -a state \
-d @ /path/to/depot | security_patch_check - -a -s 11.xx \
-c /path/to/catalog
```

where:

*/path/to/depot* is the path to the depot to be analyzed

*/path/to/catalog* is the path to the security catalog you downloaded

11.*xx* is the version of HP-UX which the system is running

The following is an example of running the tool on a software depot using the `-c` option.

```
> security_patch_check -c /some_path/security_catalog

NOTE: For information regarding secure catalog download, see the security_patch_check
  install instructions for details:
  http://software.hp.com/portal/swdepot/displayInstallInfo.do?productNumber=B6834AA

NOTE:    Downloading from
  http://itrc.hp.com/service/patch/securityPatchCatalog.do?item=security_catalog2.gz.

NOTE:    http://itrc.hp.com/service/patch/securityPatchCatalog.do?item=security_catalc
  downloaded to ./security_catalog.gz successfully.

NOTE: The security catalog was successfully downloaded to "./security_catalog".

*** BEGINNING OF SECURITY PATCH CHECK REPORT ***
Report generated by: /opt/sec_mgmt/spc/bin/security_patch_check.pl, run as user

Analyzed localhost (HP-UX 11.11) from nina
Security catalog: ./security_catalog
Security catalog created on: Sun Nov 28 23:30:13 2004
Time of analysis: Mon Nov 29 13:53:17 2004

List of recommended actions for most secure system:

#   Recommended  Bull  Cnt  Spec Reboot PDep Description
-------------------------------------------------------------------------------------
```

```
1   MANUAL_ACTION    16       1st   man   ?       ?      Patch sums and the MD5 prog
2   MANUAL_ACTION    111      1st   man   ?       ?      Sec. Vulnerability with Ign
3   MANUAL_ACTION    150      1st   man   ?       ?      check swacl settings
4   CIFS-Server       157     1st   man   ?       ?      edit smb.conf to remove ma
5   CIFS-Server       164     1st   man   ?       ?      ensure "passwd program" op
/bin/passwd %u
6   MANUAL_ACTION    188r1   1st   man   ?       ?      Sec. Vulnerability in JAVA
7   MANUAL_ACTION    205r1   1st   man   ?       ?      RFC 1948 ISN randomization
8   MANUAL_ACTION    231      1st   man   ?       ?      Change insecure permissions
9   MANUAL_ACTION    239r1   1st   man   ?       ?      Affected versions and the c
are listed elsewhere in this bulletin.
10  InternetSrvcs     246r5   1st   man   ?       ?      Modify /etc/mail/sendmail.
11  InternetSrvcs     253r8   1st   man   ?       ?      Modify /etc/mail/sendmail.
12  InternetSrvcs     266r4   1st   man   ?       ?      See MANUAL ACTIONS section
13  InternetSrvcs     281r8   1st   man   ?      ?      modify /etc/mail/sendmail.c
14  OS-Core           304     1st   man   ?       ?      unpack patches using the n
15  OBAM              1047    1st   man   ?       ?      disable the OBAM web admin
16  PHCO_28848       293r1   2nd   No    No      No    Software Distributor Cumulat
17  PHNE_27796        209r16  1st   Yes   No      Yes   libnss_dns DNS backend
18  PHSS_23067        137r3   1st   No    No     No    OnlineDiag/Support Tool Mana
19  PHSS_30478        1018    1st   No    No      No    X11 Font Library
20  PHSS_30789        1038    3rd   Yes   No      Yes   CDE Applications Periodic
21  PHSS_30871        1018    1st   No    Yes     No    Xserver cumulative
22  PHSS_31988        1088    3rd   No    No      No    X Font Server
23  PRM-Sw-Lib        1065    1st   upd   ?       ?      install revision C.02.02 c
24  CIFS-Server       1086   7th   upd   ?       ?      install revision A.01.11.03
-----------------------------------------------------------------------------------
NOTE:    Security bulletins can be found ordered by Document ID at
  http://itrc.hp.com/cki/bin/doc.pl/screen=ckiSecurityBulletin
```

**NOTE:** The Security Patch Check Tool offers you the option to flag bulletin revisions you have already reviewed as completed. This is the way to filter Security Patch Check output that pertains to manual actions you've already completed. See the ignore file in the security_patch_check(1M) manpage.

## Where to Go Next

Now that you have a stronger understanding of patching and patch management, HP recommends you use the ITRC frequently to monitor your patch environment.

# Appendix A Other Resources

This appendix lists patch-related resources. HP encourages you to explore the following FTP servers and web sites.

**Table A-1** HP FTP Servers

| HP FTP Servers | Location |
|---|---|
| Recommended for most users | ftp://ftp.itrc.hp.com |
| Recommended for Asia-Pacific users | ftp://singapore-ffs.external.hp.com |

**Table A-2** HP Web Sites

| HP Web Sites | Location |
|---|---|
| Home Page | http://www.hp.com |
| Software Depot | http://software.hp.com |
| Technical Documentation<br>HP recommends the following documents::<br>• Patch Management User Guide for HP-UX 11.x Systems<br>• Ignite-UX Administration Guide<br>• Security Patch Check FAQ<br>• Software Distributor Administration Guide<br>• Support Plus User Guide<br>• Read Before Installing Support Plus<br>• Using HP-UX | http://docs.hp.com |
| HP-UX 11i features and news | http://unix.hp.com/operating |
| Ignite-UX | http://software.hp.com/products/IUX |
| IT Resource Center (ITRC) | http://itrc.hp.com |
| Software Distributor | http://software.hp.com/SD_AT_HP |
| Support Plus | http://software.hp.com/SUPPORT_PLUS |
| System diagnostic and monitoring tools | http://docs.hp.com/hpux/diag |
| Updates for some HP software and products | http://software.hp.com<br>Check the HP product Web site. |

**Table A-3** Non-HP Web Sites

| Non-HP Web Sites | Location |
|---|---|
| hpux-admin mailing list:<br>Provides discussion for HP-UX system administration. | http://www.dutchworks.nl/htbin/hpsysadmin |
| The International Association of Hewlett-Packard Computing Professionals (Interex) | http://www.interex.org/home.html |
| Interex HP-UX Portal | http://www.interex.org/tech/9000/portal.html |
| Interex listing of user groups | http://www.interex.org/users/usergrps.html |
| Interex Patch Special Interest Group Page | http://www.interex.org/advocacy/mcgs/patch/index.html |
| The HP-UX Porting and Archive Centre:<br>Makes public domain, freeware, and Open Source software more readily available to users of HP-UX systems. | http://hpux.cs.utah.edu<br>http://hpux.its.tudelft.nl<br>http://hpux.connect.org.uk |

# Glossary

This glossary provides patch-related terms. HP recommends the Software Distributor Administration Guide at **http://docs.hp.com** for additional terms.

**Ancestor** An ancestor of a patch is the preexisting software that is being modified or replaced by the patch.

**Applied** The state in which a patch is installed. When a patch is installed, by default it has the patch_state of applied. Other patch states include committed, superseded, and committed/superseded.

**Architecture** A keyword that represents the operating system platform on which the product runs.

**Attributes** Information describing a software object's characteristics.

**Base Software** The software that will be modified by a patch.

**Bundle** A bundle is an encapsulation of products, subproducts and filesets into a single software object. It is a convenient way to group software objects together for easy selection. When a bundle is specified in a Software Distributor operation, all products or filesets contained in that bundle are included in the operation. If the filesets within the bundle are patches, this is known as a patch bundle.

**Catalog/Catalog Directory** An area within a depot that contains all the information needed by SD-UX to define the organization and contents of the products stored in the depot. It includes a global INDEX file and a directory of information for each product version in the depot. It is sometimes referred to as the catalog directory.

**checksum** Cyclic Redundancy Check (CRC), a computed value that is compared with stored data to tell if a file has been corrupted during transfer.

**CLI** Command Line Interface. See Command Line User Interface.

**Command Line User Interface (CLI/CLUI)** Text-formatted commands and options entered at an HP-UX command line prompt or executed by a script.

**Committed** The patch state in which the patch is applied and rollback files have been deleted.

**Committed/Superseded** A patch state in which the patch is both committed and superseded. See also Superseded.

**Control Script** An optional script that is run during software installation, software removal, or software configuration.

**Corequisite** A dependency in which a fileset requires that another fileset be installed or configured at the same time. For example, if fileset A requires that fileset B is installed at the same time, fileset B is a corequisite. See Dependency and Prerequisite.

**Cumulative Patch** See Superseding Patch.

**Dependency** A relationship between fileset in which one requires another in a specific manner. For example, before fileset A can be installed, it may require fileset B to be installed. SD-UX supports corequisite, exrequisite, and prerequisite dependencies. See Dependent.

**Dependent** A fileset that has a dependency on another fileset. For example, if fileset A depends on fileset B, then B is a dependent or has a dependency on A.

**Depot** A repository of software products and a catalog, organized so SD-UX commands use it as a software source. The contents of a depot reside in a directory structure with a single, common root. A depot can exist as a directory tree on a SD-UX file system or on CD or DVD media, and it can exist as a tar archive on a serial media (tape). All depots share a single logical format, independent of the type of media on which the depot resides. Depots can reside on a local or remote system. You can package software directly into a depot or copy packaged software into the depot from elsewhere.

**Depot Source** See Depot.

**Directory Depot** The directory on a target host where a depot is located. The default is /var/spool/sw.

**Fileset** A grouping of one or more files contained in a product or subproduct. It groups a subset of a product's files into a manageable unit. Most Software Distributor operations are performed on filesets.

**Ignite-UX** Toolset used on HP-UX for doing cold-installs and system recovery. Makes use of SD for doing package based installs, and can also use golden-images for supplying software. Ignite-UX is an application that facilitates installing and configuring HP-UX systems.

**Installed Product** A product that has been installed on a host so that its files can be used by end-users, as opposed to a product residing in a depot on a host's file system. Sometimes referred to as an available product.

**Installed Products Database (IPD)** Describes the products that are installed on any given host (or within an alternate root). Installed product information is created by swinstall, and managed by swmodify. The contents of an IPD reside in a directory structure with a single common root.

**IPD** See Installed Products Database.

**IUX** See Ignite-UX.

**Media** Physical data storage media on which software is stored, such as tape, CD-ROM, or DVD.

**Object** The pieces of software that SD-UX packages, distributes, installs, and manages. There are three classes of objects: software (installed on target roots or available in depots), containers (depot, roots, alternate roots), and jobs.

**OS** Operating System.

**Patch** Software designed to update specific bundles, products, subproducts, filesets, or files on your system. By definition, patch software is packaged with the is_patch attribute set to true.

**Patch Bundle** See Bundle.

**Patch Rollback** The process of removing a patch from the system and restoring the system to the pre-patched state.

**Path** An attribute that specifies the full pathname for a file.

**Prerequisite** A dependency in which one fileset requires another fileset to be installed or configured before the first fileset can be installed or configured. For example, fileset A may require that fileset B is installed before fileset A can be installed. Therefore, fileset B is a prerequisite for fileset A. See Dependency, and Corequisite.

**Product** A software object which vendors package and distribute, and which users acquire and install. A product contains one or more filesets and zero or more subproducts.

**Product Directory** The root directory of a product object, in which most of its files are contained. You can change (relocate) the default product directory when you installing a locatable product.

**SD** See Software Distributor.

**Serial Depot** See Tape Depot.

**Software Depot** A SD format structure that contains one or more software products that can be installed on other systems or copied to other depots.

**Software Distributor** The native toolset used on HP-UX for managing software packages.

**Software Object** The objects packaged, distributed, installed, or managed by SD. A software object may be a file, fileset, bundle, or product. Most operations are performed on filesets.

**Subproduct** A subset or partitioning of a software product. It is an optional component of a product. and contains one or more filesets.

**Superseded** The state in which a patch was applied but was then replaced by a superseding patch. Other patch states include applied and committed.

**Superseding Patch** A patch that supersedes all previous patches to a given fileset.

**swinstall** An SD command that installs software. swinstall may also perform software configuration.

**swlist** An SD command that lists software elements, their attributes, and their organization. It lists both installed software and software contained within a depot.

**swmodify** An SD command that lets you change information in the installed products database or depot catalog files.

**swreg** An SD command used to register or unregister depots.

**swremove** An SD command that removes previously installed software or removes packaged software from a depot.

**swverify** An SD command that verifies installed software or depot software for correctness and completeness.

**Systems** Computers that are either stand-alone or networked to other computers.

**Tape Depot** A software depot stored in a tar (tape archive) format. Within the archive, directory and file entries are organized using the same structure as any other SD-UX format depot.

# Index