Paper 4165

Developing a Patching Strategy for HP-UX 10.x

Scott W. Sarisky

Hewlett Packard Company
20 Perimeter Summit Blvd., M/S 1003
Atlanta, Georgia 30319

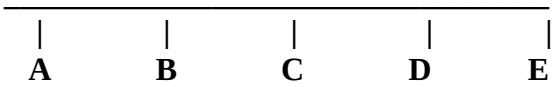
sws@atl.hp.com

It seems like we are always living in a reactive world. Something happens and we react to it. These scenarios can tend to lead to stressful situations and there

is no shortage of stress these days. If these situations lead to stress, it stands to reason that the opposite would lead away from stress. Therefore, the opposite of reactive is proactive. Proactive, by definition means to be in favor of or supportive of being active. In other words, take action/control of a situation before it takes control of you.

One of the proactive things you can do regarding HP-UX, is to have a plan or strategy for patching your computers. If you have already made a decision to proactively patch your system(s), you have made a step in a good direction. The next step is to determine the how,
what, when and where. In other words, you need to develop your patching strategy.

Before getting into what strategy makes sense for you, let us first consider what approaches can be taken towards patching. Operating system patching is much more than a simple yes or no. Yes we patch or no we do not patch. Consider the following diagram, at any given point in time, you are at some point on this line. You may be directly on one of the letters or you may fall between two letters. However, just because you are at a certain point today, does not mean you will always be at that same point. Just like many other things, circumstances can have a great influence on how we look at situations.



A - apply no patches

B - apply a patch for a specific problem (reactive)

C - conservatively apply patches (proactive)

D - aggressively apply patches (proactive)

E - apply every patch

A and E would probably be considered highly unique and special cases. B's are either truly of the mindset, "if it is not broke, do not fix it" or they are former A's in a jam. This leaves us with C and D. As you can see, they are both in the category of proactive. Now almost everyone, either consciously or not, is at some point on this line. Furthermore, the point at which you are today, may not be the point where you were a year or two ago. We tend to change in relation to

circumstances. However, for the purpose of this paper and the idea of maximizing system up time, the proactive patching, i.e. conservative or aggressive is what needs to be determined. Proactive patching in a broad sense means that nothing you are aware of is specifically or significantly wrong or broken. So, if we look at the two types, conservative proactive and aggressive proactive, here are some of the things we'll see.

Aggressive Proactive Patching

When things are in a dynamic state on your system, i.e. new or modified application systems are being introduced often or on a regular basis, the chance of running into a problem is greater. Also, when new code is introduced, it may mean configuration changes and/or increase in system load. All of these changes have the potential of creating new scenarios, i.e. new roads traveled, which can lead to system related problems. With HP's large installed base of systems, the new problem that you have just encountered, may have already been experienced at another site and a fix or workaround may already be available. Given these reasons, an aggressive proactive patching plan should be considered. This means new patches should be installed on a regular basis. Ideally, the aggressive approach should have a good test environment that closely resembles the production environment for testing purposes.

Conservative Proactive Patching

When things are in a fairly static state on your system, i.e. few changes are being introduced, the chances of encountering new problems is far less as compared to the dynamic environment. Patches should still be applied, but on a less frequent basis. Possibly, only critical patches should be applied. You may cycle through periods where aggressive makes sense and then go into a more static phase where you can take a more conservative approach.

When developing your patching strategy for a single system, it is obviously much easier when compared to an entire enterprise. A single system can be categorized for what it does. An enterprise is made up of many systems, and is therefore more difficult to exclusively be conservative or aggressive. Therefore, it may be very possible that you have a mixture in your overall enterprise patching strategy. Next, there are many different ways to obtain patches. Following are a number of ways for you to obtain HP-UX patches. Listed with each method are a few of the benefits and trade offs.

1. HP Electronic Support Center.

Anyone who has access to the web can browse and download HP-UX patches from the following url:

http://us-support.external.hp.com

Current HP-UX patches that are in a GR (general release) state are available to be downloaded from this web site. You should read the patch text via the browse option to determine if this is the patch you want and that all dependencies have been met. Also, you will find installation instructions in the patch text file.

Benefits:	**You can download patches when you want/need them.** **You have the option to download many patches and** **This method can be much quicker as compared to waiting**
Trade	**You must check all dependencies (found in the patch text** **Some patches can be very large in size and will take** **Some people only have web access through their PC, not**

Off

2. Extension Software CD-ROM.

Every two months, customers with a support contract with HP, will receive the Extension Software CD-ROM. The CD-ROM will contain patch bundles for current HP-UX operating system levels. The 10.x patch bundles can be installed on your system using swinstall with the match_target=true option. Typically, there will be three new patch bundles per release of the bi-monthly CDROM. In other words, if the CDROM contains 9.04, 9.05, 10.01, 10.10 and 10.20, three of them would be new bundles. The ones that are not new will be the same bundle as the previous copy of the CDROM.

Benefits:	**Patches are tested as a "bundle" of patches. They are** **Interdependency logic is built into the bundle. In other** **The CDROM is automatically sent every other month to** **Patches on the CDROM are seasoned patches.** **This is by far the "ease of use" method for putting** **These patch bundles typically contain many patches.** **You do not have to spend time doing a patch analysis.**
Trade	**If your needs cause you to be on the leading edge of** **You have little control over what patches go on your box.** **Since there are typically many patches in the bundle, it** **Not all patches critical to your operations are included,**

Off

3. Custom Patch Manager.

Custom Patch Manager is or will be available for those customers that have a support contract with HP. This method of obtaining patches requires that you, as a customer, are familiar with doing custom patch analysis. You can access Custom Patch Manager from the web at the following url:

http://us-support.external.hp.com

You must register, via the web, prior to using this tool. This method of obtaining patches allows you to determine what patches will be selected for your system.

Benefits: **You will get the latest patches from HP.**
Allows the customer to configure and download custom
CPM provides automated analysis; it reports dependent patches and patch conflicts to you.
You are in control of what patches go on your system,

Trade **You will need to supply a knowledgeable person or** **Off**
Patches are not tested as a unit.
Basically, this method is a time vs. money decision.

4. Reactive Patching from the HP Response Center.

For the customers who have a support contract with HP, they can call the HP Response Center (800) 633-3600 when a problem occurs. If the problem is a known problem and there is a patch available, you can request that the Response Center Engineer send that patch to you.

Benefits: **No up front work on your part until there is a problem.**
It is your risk, but you only spend time dealing with patches when a problem occurs.

Trade **Sooner or later a problem will occur. You will be** **Off**
Minimum turn around time for receiving at tape from
By not planning your own proactive strategy, you may

5. Proactive Patch Analysis from HP as part of an on going support contract.

For the customers that have a support contract at the PSS (Personalized System Support) level or higher, they can have HP send them a custom patch bundle.

Benefits: **All of the patch analysis labor is HP's, you do not need**
You will receive custom patch bundles on a regular basis as per your support contract.
HP people doing your patch analysis typically know you and are familiar with your approach to patching.
The custom patch bundle will contain the latest patches from HP.

Trade Off: **The higher level support contracts cost more.**

6. Proactive Patch Analysis from HP on a time and material basis.

For the customers that do not have a support contract at the PSS (Personalized System Support) level or higher, they can have HP send them a custom patch bundle. This is part of HP's consulting business and the work is performed typically on a time and material basis.

Benefits: **All of the patch analysis labor is HP's, you do not need**
You only purchase this service when you need it.
The custom patch bundle will contain the latest patches

Trade Off: **The cost of a time and material patch analysis is more then what a patch analysis would cost as part of an on going PSS or higher support contract.**
Turn around time is determined by resources available at the time.

7. Do nothing.

This option is basically the same as patching on a reactive basis. Your plan may be to do nothing, and that works until something does go wrong.

Okay, now you are aware of conservative and aggressive approaches, benefits vs. trade offs on various methods of obtaining patches. This information will help you decide what strategy best fits your environment. It is very possible that your strategy could be a composite of quite a few of these pieces. For instance, you may have some systems where it makes sense to use the Software Extension CDROM solution and yet have other more critical systems, where CPM or custom patch bundles from HP make sense. Another aspect of your strategy that you must consider, is frequency. A decision will need to be made on how often patches should be applied. Again, this too could vary from system to system.

One of the new concepts of HP-UX 10.x is using a depot to store your patches. A depot is basically a directory that holds software products and all of the information required for swinstall to install from. In this case, the software products are the patches. You could create a depot for each version of HP-UX that you utilize. Patches can be added or removed from this depot. The command to add patches to your depot is swcopy and the command to remove patches from your depot is swremove, with the -d option. Therefore, you can manage your patch depot for the entire environment instead of looking at each machine individually. The depot can be set up on any 10.x system, and providing that it is on the network, patches can be installed across the network. Currently, to do this you would execute swinstall on the system that you are applying patches to and point back to the depot over the network to the system where the depot resides. One caveat to be aware of is when you add a patch to the depot, you must remove any patches, already in your depot, that the new patch supersedes. The manual way to do this is to check the patch text file of the new patch and compare the patches that it supersedes with the patches currently in your depot. The automated way to do this is with the patch_depot_ck script. This script can be executed for your depot after you have added new patches to it. The distribution method of this script has not been determined at the time of the writing of this paper. More specific information will be given at the actual paper presentation. The current thinking on this is to put this script in a patch that will supersede PHCO_5400. Again, more specific information will he given at HPWorld in Chicago.

Review of Software Distributor

The following pages are a review of SD (Software Distributor). First, there is a new way to handle or manage not only patches, but all software and sub systems as well. The new utility is called SD-UX, which is an acronym for Software Distributor for HP-UX. There are a number of new commands in SD. Following are some of the new SD commands that are relevant to patching.

Command Purpose

swinstall.....install software products and patches

swlist.....display information about installed products and patches

swcopy.....copy software products or patches into a depot

swremove.....remove software products or patches

Another term that is new with 10.x is depot. A depot is a directory location which contains software for installation. When you get a patch from the web and unshar it, you will have a .text and a .depot file. The .depot file is where the binaries are for that particular patch.

It is highly recommended that you become familiar with the operation of the product installation tool, SD, before attempting patch installation. The document for becoming familiar with SD is: "Managing HP-UX Software with SD-UX", part number B2355-90054. Also, the best way to learn after becoming familiar with SD is to practice. This can be accomplished either on a crash and burn system if you have that option or install an "easy" patch and follow it through the process.

SWINSTALL

The SD command to install patches is the swinstall command. There are many options to this command. By definition, this command is for installing and configuring software products at 10.x. For the purpose of SD-UX, patches are considered software products at 10.x. This command can be run in three different "styles". It can be run as a stand alone command from the command line, or it can be run as a GUI, (graphical user interface) or TUI (terminal user interface). The GUI and
TUI are interactive. Swinstall runs other scripts as part of the process to install a patch. The scripts that run are:

Script Purpose

checkinstall.....Tests for hardware and software configurations that might prevent install.

preinstall.....Cleans up from predecessor fileset; it removes obsolete files, kills daemons owned by fileset.

postinstall.....Enhances kernel functionality; adds drivers,

modifies kernel parameters.

configure.....Creates any special files, performs conditional moves of delivered files, modifies system configuration files, and warns/informs administrator as necessary

So, as you can see, swinstall does a number of things in the process of installing patches. As an example, if you pulled a patch from the web, the command to install on a 10.x system would look like:

```
swinstall  -x  autoreboot=true    -x  match_target=true
           -s  /tmp/PHKL_6686.depot
```

In the example above, this would be typed in at the prompt. The"-x" is for option parameters, and in this case we have told SD that autoreboot is true which means the system will automatically be rebooted . Next we told SD, match_target=true, this tells SD to only install software (patch in this case) where the file set(s) required are already on the system. Last, the "-s" option tells SD where to find the software (patches) to be installed.

As it is with all of the SD commands, they are extremely verbose in their logging of any actions performed. All output from SD commands is logged in the appropriate file in the /var/adm/sw directory. In this case the log file would be /var/adm/sw/swinstall.log.

SWLIST

The swlist command displays information about software products that are currently on your system. Patches are considered software products at 10.x, at least for the purposes of SD-UX. Again, there are many aspects and options to this command. For the purpose of patching, following is the swlist command that you will primarily use in determining what patches are on your system.

```
swlist -l product PH\*
```

SWCOPY

The swcopy command will copy software products to a directory depot. In other words, if you want to move a patch and create a depot for it, you would use this command. If, for instance, you were pulling several patches from the web and you wanted to install all of then at the same time, you could put them all in one

depot with the swcopy command. If you have three patches in /tmp and you want to put them in one depot, you could do the following:

```
swcopy -s /tmp/PHCO_1234.depot PHCO_1234 @ /tmp/abc.depot
swcopy -s /tmp/PHKL_5678.depot PHKL_5678 @ /tmp/abc.depot
swcopy -s /tmp/PHSS_9911.depot PHSS_9911 @ /tmp/abc.depot
```

You would now have all three patches in one depot. Swcopy can also be executed as a gui/tui.

SWREMOVE

The swremove command does just the opposite of swinstall, it removes software products. This command can be run in three different "styles". It can be run as a stand alone command from the command line, or it can be run as a GUI, (graphical user interface) or TUI (terminal user interface). The GUI and TUI are interactive. Swremove runs other scripts as part of the process to remove a patch. The scripts that run are:

Script	Purpose
checkremove.....	Checks for existence or absence of files, hardware/system/kernel configuration.
unconfigure.....	Undoes what the configure script (swinstall) does, kills processes from previous fileset, removes client-specific files, such as log files.
preremove.....	Move or remove files and directories under shared directories; sever symbolic links from a shared directory to another shared dir.
postremove.....	Remove newly emptied directories which are exclusive property of fileset and reside in a shared directory; remove fileset's log files.

For example, if PHCO_1234 needs to be removed from the system, the following command would do it:

```
swremove  PHCO_1234
```

As long as the NOSAVE option was not used when PHCO_1234 was installed, the system would be put back to the state it was in prior to installing

PHCO_1234. If the NOSAVE option was used, the attempt to remove it would fail.

If you are at HP-UX 10.10 or below, swremove will not regen the kernel or reboot the box automatically if you are removing a patch that required a reboot when it was first installed. If you are at HP-UX 10.20, the default when removing a patch that required a reboot when installed, is to automatically regen the kernel and reboot the system.