HP Server Automation

Version: 9.13 or later

Whitepaper: SA Solaris 11 Patching Support

Document Release Date: May 17, 2012

Software Release Date: May 2012

Contents

SA Solaris 11 Patching Support

Oracle Solaris 11 uses IPS packages to deliver software and software updates. IPS (Image Packaging System) is a network-based package management system that is used for the entire software lifecycle, including package installation, upgrade and removal.

Server Automation's Solaris 11 platform support for server patching allows you to update your managed servers to the latest versions of existing software without installing new software. This is a powerful way to keep your system up to date in an environment that no longer supports explicit patch units.

Solaris 11 patching support leverages the existing Solaris patching functionality, with a few differences to adapt to the new Solaris IPS package delivery structure. Additionally, there are setup requirements for setting up the initial IPS Package database. This whitepaper describes the Solaris 11 Patching setup steps and the differences in SA patching with Solaris 11.

Getting Started with Solaris 11 Patching

The advantage of the IPS package structure is that it contains the metadata and the binaries, combined. IPS packages are used for everything from the initial software installation to the updates. Because IPS packages are so complete, they have internal integrity, which means they require the complete package and are not divided into patch units.

Because of these structural differences, there are some typical patching functions that are not relevant for Solaris 11.

The process for creating a vendor recommended patch policy is different. For example, Solaris 10 looks at installed packages and computes what needs to be updated based on the existing installations. With Solaris 11, Server Automation uses the IPS tools to find the recommended patches and their dependencies.

SA 9.13 comes with a predefined software policy, Solaris 11 IPS Package Acquisition Tool, which enables you to set up the initial IPS Package database.

STEPS Summary

Complete the following steps to set up your initial IPS Package database and enable Solaris 11 patching with SA. The initial IPS Package acquisition only needs to be done using one Solaris 11 managed server. After the initial acquisition, additional updates will need to be done periodically to maintain compliance. These instructions are just for the initial acquisition.

RECOMMENDATION: The entire IPS Package repository could be as large as 40 GB. To make sure there is ample room on your server, choose a Solaris 11 managed server with 100GB or more.

This summary has two parts:

A. Set up your Solaris 11 IPS Package Database
B. Create a recommended patch policy and remediate your Solaris 11 managed servers

NOTE: Detailed instructions for each of these steps are provided under STEP Instructions.

A. Set up your Solaris 11 IPS Package Database

1) Remediate the chosen Solaris 11 managed server with the SA-provided software policy, **Solaris 11 IPS Package Acquisition Tools**.

   This installs SA UAPI access and IPS import tools on the server, which will be used to acquire IPS packages from the vendor.

2) Complete the import prerequisite steps before importing IPS packages:

a. Setup Managed Server Customers to have visibility to all relevant IPS packages in the SA Library.

b. If your environment requires HTTP proxies to access the desired repository, set up the proxies on your managed server before attempting to import the IPS packages.

c. Configure `sol_ips_import.conf`

3) Import all IPS packages onto the core by running the IPS import script (`sol_ips_import`) from the chosen Solaris 11 managed server.

4) If software registration has not yet occurred, run the Software Registration script (`bs_software`).

This completes the IPS Package Database set-up steps. Next, create the patch policy and remediate your Solaris 11 servers.

B. Create a recommended patch policy and remediate your Solaris 11 managed servers

1) Create the recommended patch policy for the managed server by running the patch policy script (`solpatch_import`) on the core.

2) From the SA Client, attach the recommended patch policy to the server and remediate.

STEP Instructions

STEP 1: Remediate the managed server with the Solaris 11 IPS Package Acquisition software policy

1) From the SA Client, navigate to **SA Library > By Type** and select **Solaris 11 IPS Package Acquisition Tools**.

2) From the Actions menu, select **Attach Server…**.

3) Select **Remediate Servers Immediately**. (This option enables the remediation process to run immediately after attaching the servers.)

4) Select the desired servers to remediate and click **Attach**.

5) In the Remediate window, accept all remaining defaults and click **Start Job** to remediate the selected servers.

STEP 2: Complete the Import Prerequisites

Grant a managed server's customer visibility to all relevant IPS Packages in the SA Library

Granting customer visibility is a prerequisite to running the `sol_ips_import` script to import the IPS packages.

The IPS packages are delivered to a directory in the SA Library on the core, but the import script is run from the managed server. There is one customer per managed server and the customer governs the managed server's visibility into the SA Library. When the `sol_ips_import` script runs, it bases the analysis of what to import on the set of IPS packages the managed server's customer can see. For this reason, the customer associated with the managed server where the import is being run must have visibility to all IPS packages.

To achieve that, grant the customer folder permission for the parent folder of the destination directory for the IPS packages.

1) Identify the managed server's customer from the managed server properties view.

a. From the SA Client, navigate to **Devices** and select the managed server you wish to update.

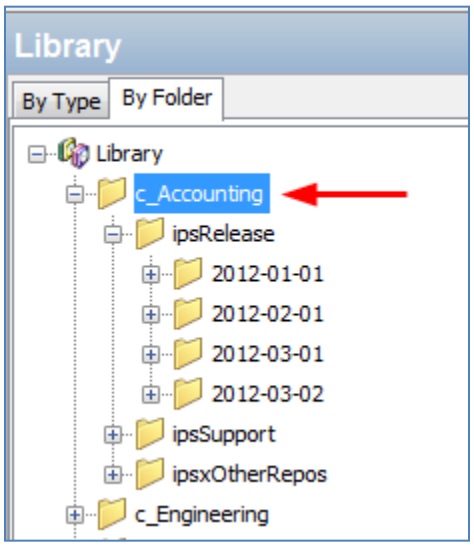
b. Select **View > Properties** to display the server properties in the details pane.

c. The customer is displayed under the Management Information section.

2) Grant IPS package folder permission to the customer:

a. From the SA Client, navigate to **SA Library > By Folder** and select the parent folder for the customer's Solaris 11 IPS packages.

For example, for "Accounting" customer:



Example File Structure for "Accounting" Customer

In this example, the library has folders organized by customers; Accounting and Engineering. All the IPS packages associated with each customer are under the customer folders. In this case, you would select the "c_Accounting" parent directory because you want to give the customer permission to the upper-most directory for that customer to make sure it has visibility to ALL the IPS packages.

b. Select **Actions > Folder Properties > Customer** tab

c. Click **Add** and select the customer for the managed server with the IPS import tools.

d. Click **Add** and then **OK**.

WARNING: Running the `sol_ips_import` script without giving the managed server's customer visibility to this folder could have adverse effects. The customer's folder permissions affect what patches are recommended for the server. Without correct customer folder permissions, the script might unnecessarily re-upload thousands of patches to the core.

Set the HTTP proxies

If your environment requires HTTP proxies (e.g., http_proxy, https_proxy) to access your desired repository, make sure they are set correctly on your managed server before importing the IPS packages.

Configure the IPS package import configuration file (sol_ips_import.conf)

Setting up the `sol_ips_import.conf` configuration file before running the `sol_ips_import` import script is recommended to save time and improve reliability.

1) From a remote server window, log in to the Solaris 11 managed server.
2) Navigate to `/opt/opsware/solimport#`
3) Open the configuration file: `sol_ips_import.conf`
4) Edit the configuration file to define your preferences for the IPS package download process:

Configuration File Option	Explanation and Example
User name and password	Specify your SA login credentials
Local download directory	Specify the staging directory on your managed server where the packages are initially downloaded from the vendor. For example: `download_dir=/var/<UserFolderName>/IPSPkg_Stage` **RECOMMENDATION**: The entire IPS Package repository could be as large as 40 GB. To make sure there is ample room on your server, choose a Solaris 11 managed server with 100GB or more.
SA Folder Upload directory	Specify the final destination directory on the SA Core where the IPS packages will be stored. For example: `core_destination_folder=/Home/<AllSolaris11CustomersFolderName>/`
URL of the IPS repository	Specify the URL of the vendor's IPS repository from which the packages will be acquired. For example: `repo_url=https://pkg.oracle.com/solaris/support` or: `repo_url=https://pkg.oracle.com/solaris/release` **Note**: This is an example of Oracle's repositories for demonstration purposes only. In this example, the `…/release` URL contains updates for each new release of Oracle Solaris, and `…/support` contains bug fixes and updates, but is restricted to those with support contract. Many vendors supply IPS packages and may deliver packages to different directories for various purposes. Specify the one for your purpose.
Get only the latest packages	Set to `True` to acquire all packages; `False` to only get the latest versions. For example: `all_versions=False`

Certificate and Key files	If the vendor's repository requires a certificate and key authentication, you can set them up here.
	For example:
	`cert=/var/pkg/ssl/Oracle_Solaris_11_Support.certificate.pen`
	`key=/var/pkg/ssl/Oracle_Solaris_11_Support.key.pen`

Note: all examples are for demonstration purposes only.

STEP 3: Import all IPS packages onto the core by running the IPS import script (sol_ips_import)

Unless otherwise specified in the command line, the `sol_ips_import` command will run according to the details specified in the `sol_ips_import.conf` configuration file in the previous step.

1) Log in to the Solaris 11 server where you installed the IPS Acquisition tools.

2) Test the connection to the remote repository before running the import, run the `sol_ips_import` command with a string filter first. For example, to display all packages containing 'telnet', run:

```
./sol_ips_import -f 'telnet' -n
```

where `-n` indicates preview instead of download, and `-f` specifies a filter.

3) Run the IPS Package import, run the command:

```
./sol_ips_import
```

The IPS packages will download from the vendor's repository to the local staging directory on the managed server and then upload to the final destination directory on the core as specified in the `.conf` file.

TIP: When the IPS Package import process is complete, the `fmrifail_<DATE>` file tracks any files that failed to upload to the core. This file can be manually run with the `--fmri_file` option:

```
./sol_ips_import --fmri_file fmrifail_<DATE>
```

where `<DATE>` is the date and time that the upload started, as included in the filename.

If any files have failed to upload, the import script will automatically attempt to re-download and upload them. If the automatic upload does not work, you can also use the `--force_process` flag to manually force a re-download and upload.

```
./sol_ips_import -f '<package name>' --force_process
```

Note: Run `./sol_ips_import -h` for information about additional command options.

Command Options for sol_ips_import

Command Option	Description
`--all_versions`	Get ALL available package versions from the remote repository. Defaults to latest. Results in ~30% more packages
`-c REPO_CERT, or --cert=REPO_CERT`	Certificate file for IPS repository such as `Oracle_Solaris_11_Support.certificate.pem`
`--config=CONFIG_PATH`	Read command line options from this file. Defaults to `sol_ips_import.conf`
`-d DOWNLOAD_DIR, or --download_dir=DOWNLOAD_DIR`	Directory on local system to store packages
`--download_only`	Download packages only
`-f PKG_FILTER, or --filter=PKG_FILTER`	Uses a Python regular expression string to filter available packages. In upload-only mode, this filters the file name
`--fmri_file=FMRI_FILE`	File containing one FMRI per line that will be used to filter the repository's available packages. In upload-only mode, this will filter against the FMRI associated with a file

`--force_process`	Force acquisition and upload of packages that have been previously uploaded to the core.
`-h, or --help`	Show this help message and exit
`-k REPO_KEY, or --key=REPO_KEY`	Key file for IPS repository such as `Oracle_Solaris_11_Support.key.pem`
`-m, or --manual`	Show manual page and exit
`-n, or --preview`	Show what would be downloaded from the remote repository (dry-run)
`-p HPSA_PASS, or --hpsa_pass=HPSA_PASS`	SA password that will be used to upload packages
`-s REPO_URL, or --sourcerepourl=REPO_URL`	URL of a IPS repository
`-u HPSA_USER, or --hpsa_user=HPSA_USER`	SA user that will be used to upload packages
`--upload_only`	Uploaded packages from local directory specified by `--download_dir`
`--version`	Show program's version number and exit
`-w OPSWARE_FOLDER, or --core_destination_folder=OPSWARE_FOLDER`	Destination folder in the SA folder system

STEP 4: Register the software

Software Registration occurs automatically during SA Agent deployment or within 24 hours of deployment, depending on the options set during deployment.

If software registration has not yet occurred, you can run the Software Registration script manually:

1) Log in to the managed server.
2) Run the Software Registration script:

```
/opt/opsware/agent/pylibs/cog/bs_software –full
```

STEP 5: Create the recommended patch policy (run solpatch_import)

1) Log in to the SA core server as `root`.
2) Create recommended patch policy for the managed server by running the `solpatch_import` script.

   For example:

```
/opt/opsware/solpatch_import/bin/solpatch_import -a policy --
policy_path='svrname-policy-all-new' --filter="rec,server=svrname"
```

where `path` = the name of the policy, `filter` = the name of the server, and `rec` = recommended patches.

Note: Both of the path and filter options are required to create a recommended patch policy for a particular server.

TIP: To perform a preview before creating the policy use the `-a show` option.

For example, to preview the policy with recommended patches for the 'kalai' server, run:

```
/opt/opsware/solpatch_import/bin/solpatch_import -a show --
filter="rec,server=kelai"
```

Then, to create a patch policy named 'kalai-policy-all-new' on the 'kelai' server, run:

```
/opt/opsware/solpatch_import/bin/solpatch_import -a policy --
policy_path='kelai-policy-all-new' --filter="server=kelai"
```

Note: Run `/opt/opsware/solpatch_import/bin/solpatch_import -h` for information about additional command options. Additional details about the `solpatch_import` command options are provided in the Solaris chapter in the *SA 9.10 User Guide: Server Patching*.

STEP 6: Attach the recommended patch policy to a server and remediate

To attach a Solaris patch policy to a server:

1) In the navigation pane, select **Devices > Servers > All Managed Servers** or **Devices > Device Groups**.
2) In the content pane, select the desired Solaris 11 servers or device group.
3) From the **Actions** menu, select **Attach > Patch Policy** to open the Attach Solaris Patch Policy window.
4) From either the **Browse Solaris Patch Policies** or **Browse Folders** tab, find and select the recommended patch policy that you just created.
5) Select **Remediate Servers Immediately**. (This option enables the remediation process to run immediately after attaching the servers.)
6) Click **Attach**.
7) In the Remediate window, accept all remaining defaults and click **Start Job** to remediate the selected server.

RECOMMENDATION: You may remediate multiple servers at once, but since the IPS Packages in the policy are based on a specific server, the servers that you remediate must be at the same level of maintenance in order for the policy to be a perfect fit. The recommended best practice is to use one policy per server, or to manage servers via a device group to keep their maintenance levels in sync.

SA Patching in Solaris 11

Solaris 11 patching support leverages the existing Solaris patching functionality, with a few differences to adapt to the new Solaris IPS package delivery structure.

IPS Packages and Server Types in Solaris 11 Recommended Patch Policies

The recommended Solaris 11 patch policy that is created via the `solpatch_import` command applies to both types of Solaris 11 servers: SunOS 5.11 (SPARC) or SunOS 5.11 x86 (x86). Individual IPS Packages can apply to Solaris 11 servers with SPARC architecture, x86 architecture, or both. The SA remediation process prevents irrelevant or *wrong* packages from installing.

Differences in Solaris 11 Patch Policies

- All patch units are IPS Packages, so when adding items to Solaris 11 patch policies, there are only two item types: IPS packages and scripts.
- The Resolve Dependency action is not needed because the dependency check is done during remediation for Solaris 11. For previous versions of Solaris, the Resolve Dependency action was a separate step that needed to be done within the policy before remediation.
- A Solaris 11 patch policy only performs applicable updates on IPS packages that are already installed on a managed server.

  For instance:

  If a managed server has the following files:

  - X version 1 and
  - Y version 2

  and you try to install these files:

  - X version 2,
  - Y version 2, and
  - Z version 2

  only *X version 2* will be installed because it is an update to *X version 1*, which is already installed on the server.

  Package Y will be omitted from the install because it is already up to date; Z will be omitted because it was not updating a package that already existed on the server.

Differences in Solaris 11 Remediation

- **Applicability analysis**: SA verifies that the IPS package is relevant to the server by determining if a previous version of the package has already been installed on the server. If a previous version does not exist or if a superseding package does, then the IPS package is considered not applicable.
- **Remediation process**: Remediating IPS packages essentially installs the new IPS package version on top of the previous version.

  After running the remediation job, a new boot environment (BE) may be created. In this case, the server will not be compliant until after the server reboots and the new packages are available. If a new BE is required, then the system will need to reboot. The reboot options defined for the remediation job will be obeyed.

  WARNING: It is strongly recommended that you do not change the reboot setting for Solaris 11 patch policies. When remediating a Solaris 11 patch policy, the reboot option for remediation is automatically set to 'Hold all server reboots until all actions are completed'. Changing this default reboot setting may result in patches not being installed during a patch policy remediation.

  Note: See Solaris documentation for information on Solaris 11 boot environments and zones.

Solaris 11 Patch Policy Rules

Solaris 11 Patch Policy Supersedence Rules

1. If IPS package Z version 1 and version 2 are included in a policy, Z version 1 will be marked as superseded by Z version 2 and will not be installed.

2. If IPS package Z version 1 is in the policy, and Z version 2 is NOT in the policy, but has been loaded into SA, then Z version 2 will be added to the policy. Z version 1 will be marked as superseded by Z version 2 and will not be installed. The policy will attempt to install Z version 2.

Solaris 11 Patch Policy Applicability Rules

1. If IPS package Z version 2 is in the policy, and no previous version of Z is installed on the managed server, Z version 2 will not be installed.
2. If IPS package Z version 1 is in the policy, and Z version 2 is installed on the managed server, Z version 1 will be marked as superseded by an installed package and will not install.
3. If IPS package Z version 1 is in the policy, and Z version 1 is installed on the managed server, Z version 1 will be marked as already installed and will not install.

Reasons an IPS Package Might Not Install

Patch Policy rules are applied first:

1. **Base Package Does Not Exist:** IPS Package A version 1 cannot install because there is no previous version of package A installed on the managed server
2. **Newer Version Is Already Installed**:
    a. Package A version 1 cannot install because a newer version, package A version 2, was found in the SA repository and installed instead
    b. Package A version 1 cannot install because a newer version, package A version 2, was also included in the policy and was installed instead.
    c. Package A version 1 cannot install because package A version 2 (newer package) is already installed on the managed server

Generic rules for all policies (software or patch) are applied second:

1. **Dependency**: Package B version 1 cannot install because it requires package A version 3, which is not in the SA repository.
2. **Blocker**: Package A version 1 cannot be installed because package X, which is installed on the managed server, prevents it.
3. **Duplicate**: Package A version 1 cannot install because it is already installed
4. **Other**: Additional reasons may apply per Solaris IPS analysis. SA passes the Solaris error messages through to the SA remediation job.

Other Differences

The `patchadd` utility is not applicable to Solaris 11 because there is no concept of a patch unit like there is in previous versions (version) of Solaris. All units are IPS packages, which use the 'pkg' command instead.

Additional Information

In this section:

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: http://support.openview.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: http://h20229.www2.hp.com/passport-registration.html, or click the **New users – please register** link on the HP Passport login page.

You can also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at: http://support.openview.hp.com/

This web site provides contact information and details about the products, services, and support that HP Software offers. HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business.

As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

- To register for an HP Passport ID, go to: http://h20229.www2.hp.com/passport-registration.html
- To find more information about access levels, go to: http://support.openview.hp.com/access_level.jsp

Support Matrices

For complete support and compatibility information, see the support matrix for the relevant product release. All support matrices and product manuals are available here on the HP Software Support Online website:

http://support.openview.hp.com/sc/support_matrices.jsp

You can also download the HP Server Automation Support and Compatibility Matrix for this release from the HP Software Support Online Product Manuals website:

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