Department of Labor
Employment and Training Administration

ETA

Solaris Patch Installation SOP for OUI (DRAFT)
October 16, 2012

Submitted to:

Shane Amerman
OIS)

Submitted by:

SoftTechConsulting

Table of Contents

1 Background

1.1 Description

This Standard Operating Procedure defines how OIST installs patches on UI servers that use the Solaris 10 operating system. It provides high-level guidance on installing patches for the Operating System (OS) in three different scenarios:

- Installing a specific patch on a target UI system immediately (i.e. in an emergency).
- Installing a specific patch on a target UI system as previously scheduled.
- Installing a Recommended Patch Set on all UI systems as previously scheduled.
- Installing a specific patch on all UI systems as previously scheduled.

1.2 Trigger Events

This SOP will be triggered when the following events occur:

- The UI Operations/OS (OPS/OS) Team determines that a specific patch must be applied to a server to solve a problem identified during an incident.
- The Security Team identifies a patch as needing to be installed on all or specific servers as a response to a security audit finding or CERT.
- The predetermined patching schedule date occurs.
- The UI OPS/OS Team applies previously determined patches to all servers during the monthly maintenance window.

1.3 Responsibility

The personnel who are responsible for performing the tasks in this SOP are described in the following table:

Role	Responsibilities
COTR	Provides oversight over the personnel involved with the patching process via the Operations Technical Team Leader.
Federal Manager	Provides oversight over the personnel and timing of the patching.
UI Operations Technical Team Leader (OPS TTL)	Determines when a specific patch will proceed. Also initiates the patching process by assigning the patch installation task(s) to a Network Security Administrator via the Service Desk system.
UI System Administrators (SA)	Responsible for performing the following tasks: • Installing one or more patches on a specific server. • Installing one or more patches on all the servers (usually during the maintenance window).
UI OPS/OS Team (OPS/OS)	Responsible for carrying out UI OPS-related tasks assigned to them by the Federal Manager.

1.4 Authority

The COTR provides the Operations Technical Team Leader with the authority to initiate patches through previously established SOPs, guidelines, and directives.

2 Install Single Patch on Single System (Emergency)

2.1 Provide Authorization and Patch Information

If the Operations Technical Team Lead (Ops TTL) determines that a patch must be installed onto a specific server or an instance of a server immediately, he or she initiates the process by directing the System Administrator (SA) to open a ticket and apply a specific patch to a specific server using this Emergency Patch Installation procedure.

The Ops TTL shall provide the following information as necessary:

- Name of target server
- Name of pretesting server
- Information about the patch that is to be installed
  - Name of patch (filenames, etc.)
  - Location of patch
  - Location of patch documentation
  - Location of any additional OIST-specific information needed for installation
- Duration of freeze period for patching (if necessary). Arrangements for a server freeze should be provided under the Server Freeze SOP.

2.2 Installing the Patch on the Target System (Emergency)

The Emergency Patch Installation procedure requires the SA to install the patch directly into the production environment without creating a test copy of the target server. This procedure is faster than a scheduled single-patch installation but is less robust.

1. Acquire the patch from Oracle/Solaris support site and expand the patch from Oracle/Solaris in the designated local software/patch repository (currently for OUI in 2012 on NAS storage, normally NFS mounted on `/software` and under `/software/patches)`.
2. Open the `README` document for the patch and review it for installation instructions and any potential issues.
3. The SA reviews the installation procedures from the `README` document and installs the patch onto the appropriate target. During installation, the SA should monitor the process for problems, resolving problems until a successful patch installation is obtained. If a problem cannot be resolved, the SA should consult with the Technical Team Lead to determine the appropriate course of action.
4. Once the patch is installed, the SA examines the newly patched system and determines if the patch has resolved the problem. Also for any potential problems that might hinder server functionality, including: sendmail operations, unimplemented security changes, insufficient filesystem space, and so on.
5. Return the system to normal operation.

3 Install Single Patch on Single System (Scheduled)

3.1 Provide Authorization and Patch Information

If the Operations Technical Team Lead (Ops TTL) determines that a patch must be installed onto a specific server or an instance of a server and can schedule the installation of that patch, he or she initiates the process by directing the SA to open a ticket and apply a specific patch to a specific server at a previously determined time.

The Ops TTL shall provide the following information as necessary:

- Name of target server
- Name of pretesting server
- Information about the patch that is to be installed
  - Name of patch (filenames, etc.)
  - Location of patch
  - Location of patch documentation
  - Location of any additional OIST-specific information needed for installation
- Duration of freeze period for patching (if necessary). Arrangements for a server freeze should be provided under the Server Freeze SOP.

3.2 Prepare Patch for Network Installation (Pretest Phase)

During the initial phase, the SA will create an image of a target system from the Development environment, install the patch on that system, and resolve any issues that occur on the target image after installation.

1. Acquire the patch from Oracle/Solaris support site and expand the patch from Oracle/Solaris in the designated local software/patch repository (currently for OUI in 2012 on NAS storage normally NFS mounted on `/software` and under `/software/patches`.)
2. Open the `README` document for the patch set and review it for installation instructions and any potential issues.
3. Make a bootable disk copy (pretest image) of the server to be patched. Edit the appropriate files on the pretest image to do the following:
   a. Eliminate possible conflicts (network addresses and such) with other servers in the Production environment.
   b. Eliminate all metadisk (Solaris Volume Manager – SVM) entries that would prevent the pretest image from being bootable.
4. Determine the current metadevice configuration for use in the recreation of the metadevices on the pretest image.
5. Unmount the prepared disk.
6. Remove the disk and put it in Slot 0 of the pretesting system.
7. Boot the pretesting system.

Once the pretest image has been booted, the Administrator should do the following:

1. Create the metadevices using the information gathered during Step 4 in Section 3.2 (see above).
   a. Create the metadb SVM device (`metadb –afc 3 c0t0d0s7`).
   b. Use the metastat-p-sorted file created earlier in conjunction with the `/etc/lvm/md.tab` file to create all hard and soft metadevices.

  c. Run metaroot to set the root device (`metaroot d10`).
  d. Copy the edited `vfstab.meta` and `system.meta` files to `/etc/vfstab` and `/etc/system` respectively.

2. Reboot the system with SVM devices (`shutdown –g0 –i6 –y`).
3. After the reboot, check that the metadevices for the non-global zones are mounted as expected.
4. If any non-global zones are still running, shut them down.
5. Check that the pretest image is able to mount (via NFS) the software filesystem where the patches are located.
6. Reboot the pretest image to single user mode, then mount the rest of the filesystems. The pretest image is now ready to be patched.

After the pretest image is ready to be patched, the Administrator should follow the installation procedures from the `README` document. During installation, the Administrator should monitor the process for problems, resolving problems until a successful patch set installation is obtained. If a problem cannot be resolved, the Administrator should consult with the Technical Team Lead to determine the appropriate course of action.

Once the patch set is successfully installed, the System Administrator examines the system for any potential problems that might hinder server functionality, including: sendmail operations, unimplemented security changes, insufficient filesystem space, and so on. If the Administrator cannot resolve those issues, he or she must consult with the Technical Team Lead to determine the appropriate course of action.

4 Installing a Specific Patch on All Servers (Global Emergency Procedure)

This specific procedure does not normally occur unless an emergency security situation occurs. Since it is an emergency situation an immediate content freeze would be done, most likely accompanied by isolating the systems to their own subnets. There is no set procedure for performing this task and both the Ops TTL and the SA will need to plan, coordinate, and perform the needed activities for this situation.

5 Installing a Recommended Patch Set

The Operations Technical Team Lead initiates the process by directing the SA to apply a recommended patch set to all servers. Normally, this process is finished during the monthly maintenance window (see the Scheduled Maintenance Window and System Freeze SOPs).

This process has four phases:

- Prepare RPS for Network environment (Pretest)
- Install RPS in Development
- Test RPS in Development
- Install RPS in Test(QA) and Production

5.1 Provide Authorization and Patch Information

The Ops TTL shall provide the following information as necessary:

- Name of target servers
- Name of pretesting server
- Information about the patch set that is to be installed
  - Name of patch set (filenames, etc.)
  - Location of patch set
  - Location of patch set documentation
  - Location of any additional OIST-specific information needed for installation
- Duration of freeze period for patching (if necessary). Arrangements for a server freeze should be provided under the Server Freeze SOP.

5.2 Prepare Patch for Network Installation (Pretest Phase)

During the initial phase, the SA will create an image of a target system from the Development environment, install the RPS on that system, and resolve any issues that occur on the target image after installation.

1. Acquire the patch from Oracle/Solaris support site and expand the patch from Oracle/Solaris in the designated local software/patch repository (currently for OUI in 2012 on NAS storage normally NFS mounted on `/software` and under `/software/patches`.
2. Open the `README` document for the patch set and review it for installation instructions and any potential issues.
3. Make a bootable disk copy (pretest image) of the server to be patched. Edit the appropriate files on the pretest image to do the following:
   a. Eliminate possible conflicts (network addresses and such) with other servers in the Production environment.
   b. Eliminate all metadisk (Solaris Volume Manager – SVM) entries that would inhibit the pretest image from being bootable.
4. Determine the current metadevice configuration for use in the recreation of the metadevices on the pretest image.
5. Unmount the prepared disk.
6. Remove the disk and put it in Slot 0 of the pretesting system.
7. Boot the pretesting system.

Once the pretest image has been booted, the Administrator should do the following:

1. Create the metadevices using the information gathered during Step 4 in Section 5.2.
    a. Create the metadb SVM device. (`metadb –afc 3 c0t0d0s7`)
    b. Use the metastat-p-sorted file created earlier in conjunction with the `/etc/lvm/md.tab` file to create all hard and soft metadevices.
    c. Run metaroot to set the root device (`metaroot d10`).
    d. Copy the edited `vfstab.meta` and `system.meta` files to `/etc/vfstab` and `/etc/system` respectively.
2. Reboot the system with SVM devices (`shutdown –g0 –i6 –y`).
3. After the reboot, check that the metadevices for the non-global zones are mounted as expected.
4. If any non-global zones are still running, shut them down.
5. Check that the pretest image is able to mount (via NFS) the software filesystem where the patches are located.
6. Reboot the pretest image to single user mode, then mount the rest of the filesystems. The pretest image is now ready to be patched.

After the pretest image is ready to be patched, the Administrator should follow the installation procedures from the `README` document. During installation, the Administrator should monitor the process for problems, resolving problems until a successful patch set installation is obtained. If a problem cannot be resolved, the Administrator should consult with the Technical Team Lead to determine the appropriate course of action.

Once the patch set is successfully installed, the System Administrator examines the system for any potential problems that might hinder server functionality, including: sendmail operations, unimplemented security changes, insufficient filesystem space, and so on. If the Administrator cannot resolve those issues, he or she must consult with the Technical Team Lead to determine the appropriate course of action.

5.3 Apply and Test Patch Set in the Development Environment

Once the SA and the OPS TTL determine that the patch set is ready, the SA will apply the RPS to the Development environment for further testing by the OUI user community.

For every target system in the Development environment, do the following:

1. Locate the downloaded copy of the target RPS and ensure that it is the correct RPS for this installation task.
2. Open the `README` document for the patch set and review it for installation instructions and any potential issues.
3. Create a bootable copy of the target system on a disk. Edit the appropriate files on the bootable copy to achieve the following goals:
    a. Eliminate possible conflicts (network addresses and such) with other servers in the Production environment.

   b. Eliminate all metadisk (Solaris Volume Manager – SVM) entries that would prevent the bootable copy from booting properly.

4. Retrieve the current metadevice configuration—it will be used after the target system has been rebooted from the bootable copy.
5. Unmount the prepared disk.
6. Remove the bootable copy and put it in Slot 0 of the target system.
7. Reboot the target system.

Once the Development target system has been successfully rebooted from the copy, the SA should do the following:

1. Create the metadevices using the information gathered during Step 4 in Section 5.3.
   a. Create the metadb SVM device (`metadb –afc 3 c0t0d0s7`).
   b. Use the metastat-p-sorted file created earlier in conjunction with the `/etc/lvm/md.tab` file to create all hard and soft metadevices.
   c. Run metaroot to set the root device (`metaroot d10`).
   d. Copy the edited `vfstab.meta` and `system.meta` files to `/etc/vfstab` and `/etc/system` respectively.
2. Reboot the system with SVM devices (`shutdown –g0 –i6 –y`).
3. After the reboot, check that the metadevices for the non-global zones are mounted as expected.
4. If any non-global zones are still running, shut them down.
5. Check that the pretest image is able to mount (via NFS) the software filesystem where the patches are located.
6. Reboot the copy to single user mode and mount the rest of the filesystems.

After the bootable copy of the target system is ready to be patched, the Administrator should follow the installation procedures from the `README` document. During installation, the Administrator should monitor the process for problems, resolving problems until a successful patch set installation is obtained. If a problem cannot be resolved, the Administrator should consult with the Technical Team Lead to determine the appropriate course of action.

Once the patch set is successfully installed, the System Administrator examines the system for any potential problems that might hinder server functionality, including: sendmail operations, unimplemented security changes, insufficient filesystem space, and so on. If the Administrator cannot resolve those issues, he or she must consult with the Technical Team Lead to determine the appropriate course of action.

This process is repeated until all the target systems have been patched.

5.4 Install Patch in Test and Production Environments (All Locations)

After the SA and OPS TTL are satisfied that the patched Development systems are performing properly, the Test and Production environments are patched per the procedure in Section 4.3.

5.5 Return to Normal Operation

After the Development, Test, and Production environments have been successfully patched, all system freezes end (per the System Freeze SOP), the appropriate ticket is closed, and normal operation resumes.

6 Installing a Specific Patch Across All Servers

6.1 Provide Authorization and Patch Information

The OPS TTL initiates the process by directing the Network Security Administrator to apply a specific patch to all servers. Typically, this occurs during the monthly maintenance window.

Once the Network Security Administrator is directed to patch a specific server, he or she opens a ticket and enters the following information:

- Names of all target servers
- Name of swap server
- Information about the target patch
  - Name of patch (filenames, etc.)
  - Location of patch
  - Location of patch documentation
  - Location of any additional OIST-specific information needed for installation
- Scheduled freeze period for patch.

6.2 Prepare and Test Patch Image

Before a patch can be implemented on an operational server, the Network Security Administrator must prepare a pretest image of that server, install the patch on the pretest image, and test the pre-image for possible issues. If the Administrator is patching a specific server, normally any issues will be resolved in this phase.

1. Acquire and expand the target patch from Oracle/Solaris in the NAS under `/software/patches`.
2. Open the `README` document for the RPS and review it for any potential issues.
3. Once the copy is done, mount the root filesystem of the newly copied disk to `/mnt`.
4. Edit the appropriate files on the pretest image to do the following:
   a. Eliminate possible conflicts with other Production systems.
   b. Eliminate all metadisk (Solaris Volume Manager – SVM) entries.
5. Determine the current metadevice configuration.
6. Unmount the prepared disk (`umount/mnt`).
7. Remove the disk and put it in slot 0 of the target system.
8. Boot the system.

Once the pretest image has been booted, the Administrator should do the following:

1. Create the metadb (`metadb –afc 3 c0t0d0s7`) SVM device.
2. Use the `metastat-p-sorted` file created earlier in conjunction with the `/etc/lvm/md.tab` file to create all hard and soft metadevices.
3. Run metaroot to set the root device (`metaroot d10`).
4. Copy the edited `vfstab.meta` and `system.meta` files to `/etc/vfstab` and `/etc/system` respectively.
5. Reboot the system with SVM devices (`shutdown –g0 –i6 –y`).
6. After the reboot, check that the metadevices for the non-global zones are mounted as expected.

7. If any non-global zones are still running, shut them down.
8. Check that the pretest image is able to mount (via NFS) the software filesystem where the patches are located.
9. Reboot the pretest image to single user mode and then mount the rest of the filesystems. The pretest image is now ready to be patched.

After the pretest image is ready to be patched, the Administrator should follow the installation procedures from the target patch’s `README` document. During installation, the Administrator should monitor the process for potential problems and ensure that any problems are resolved before the patch process continues. If a problem cannot be resolved, the Administrator should consult with the Technical Team Lead to resolve them or determine that the patching process cannot proceed.

If the patch is successfully installed, the Administrator should reboot the pretest image and examine the system for any potential problems that might hinder server functionality, including: send mail operating, unimplemented security changes, insufficient filesystem space, and so on. If the Administrator cannot resolve those issues, he or she must consult with the Technical Team Lead to determine whether the patch should be installed or the installation process should not proceed.

6.3 Apply and Test Patch in the Development Environment

Once the SA and the OPS TTL determine that the patch is ready, the SA will apply the RPS to the Development environment for further testing by the OUI user community.

For every target system in the Development environment, do the following:

1. Locate the downloaded copy of the target patch and ensure that it is the correct RPS for this installation task.
2. Open the `README` document for the patch and review it for installation instructions and any potential issues.
3. Create a bootable copy of the target system on a disk. Edit the appropriate files on the bootable copy to achieve the following goals:
    a. Eliminate possible conflicts (network addresses and such) with other servers in the Production environment.
    b. Eliminate all metadisk (Solaris Volume Manager – SVM) entries that would prevent the bootable copy from booting properly.
4. Retrieve the current metadevice configuration—it will be used after the target system has been rebooted from the bootable copy.
5. Unmount the prepared disk.
6. Remove the bootable copy and put it in Slot 0 of the target system.
7. Reboot the target system.

Once the Development target system has been successfully rebooted from the copy, the SA should do the following:

1. Create the metadevices using the information gathered during Step 4 in Section 6.3 above.
    a. Create the metadb SVM device. (`metadb –afc 3 c0t0d0s7`)
    b. Use the metastat-p-sorted file created earlier in conjunction with the `/etc/lvm/md.tab` file to create all hard and soft metadevices.

    c. Run metaroot to set the root device (`metaroot d10`).
    d. Copy the edited `vfstab.meta` and `system.meta` files to `/etc/vfstab` and `/etc/system` respectively.
2. Reboot the system with SVM devices (`shutdown –g0 –i6 –y`).
3. After the reboot, check that the metadevices for the non-global zones are mounted as expected.
4. If any non-global zones are still running, shut them down.
5. Check that the bootable copy is able to mount (via NFS) the software filesystem where the patches are located.
6. Reboot the copy to single user mode and mount the rest of the filesystems.

After the bootable copy of the target system is ready to be patched, the Administrator should follow the installation procedures from the `README` document. During installation, the Administrator should monitor the process for problems, resolving problems until a successful patch set installation is obtained. If a problem cannot be resolved, the Administrator should consult with the Technical Team Lead to determine the appropriate course of action.

Once the patch set is successfully installed, the System Administrator examines the system for any potential problems that might hinder server functionality, including: sendmail operations, unimplemented security changes, insufficient filesystem space, and so on. If the Administrator cannot resolve those issues, he or she must consult with the Technical Team Lead to determine the appropriate course of action.

This process is repeated until all the target systems are patched.

6.4 Install Patch into Network Environment (All Locations)

After the SA and OPS TTL are satisfied that the patched Development systems are performing properly, the Test and Production environments are patched per the procedure in Section 4.3.

7 Certify Patch/Patch Set Installation

When the Network Security Administrator closes the patch installation ticket, the Administrator is certifying that he or she followed this SOP as appropriate. Any variances from the SOP must be added to the ticket, along with a justification for each variance. The Administrator is responsible for properly installing the patch/patch set and he or she must inform the Operations Technical Team Leader of any problems which arose from a successful installation process yet could not be resolved before the freeze period ended.