ORACLE
SOLARIS

An Oracle Technical Paper
January 2011

Oracle Solaris10 Recommended Patching Strategy

ORACLE

Introduction

This document provides an overview of the recommended patching strategy for the Oracle Solaris 10 operating system (OS).

An alternative maintenance regime that takes precedence over this strategy may be prescribed for specific systems.

Recommended Patching Strategy for Oracle Solaris 10

The following is the recommended patching strategy for Oracle Solaris 10:

- Schedule periodic major maintenance windows. Their cadence will typically be dictated by your business constraints. Major maintenance windows are often associated with hardware roll-outs. It is recommended that you schedule major maintenance windows for every 18 to 24 months.
- Minor patching maintenance windows should be scheduled for every 3 months. They should be aligned with the Oracle Critical Patch Update (CPU) schedule so that the rest of your Oracle stack can be patched at the same time. CPUs are released on the Tuesday closest to the 17th of January, April, July, and October. See http://www.oracle.com/technetwork/topics/security/alerts-086861.html.
- Reactive patching may occasionally be required at short notice to address break-and-fix issues.
- Always install the latest patch and package utility patches prior to installing anything else, including patches for Oracle Solaris Live Upgrade and any other patch automation tool you use. The Oracle Solaris 10 patch utility patches are `119254-%` (SPARC) and `119255-%` (x86/x64).
- Use Oracle Solaris Live Upgrade. Alternatively, for Oracle Solaris Cluster systems, a rolling upgrade of the cluster nodes may be performed.
- Install or upgrade to the latest Oracle Solaris 10 Update release during your next major maintenance window. You should be running a Solaris 10 Update released within the last 2 years. The latest Solaris 10 Update release is available from the Oracle e-Delivery portal at http://edelivery.oracle.com. Simply search for "Oracle Solaris." A valid alternative is to install the Oracle Solaris Update Patch Bundle corresponding to the Update release that is available from My Oracle Support (details below).
- Install the Oracle Solaris OS Recommended Patch Cluster in all scheduled maintenance windows. You should be running a Recommended Patch Cluster released within the last 6 months. These are available from the Patches&Updates tab on My Oracle Support (MOS) at https://support.oracle.com. Simply select Product is Solaris Operating System, Release is Solaris 10 Operating System, and Type is Patchset. Valid alternatives are to install the quarterly Oracle Solaris OS Critical Patch Update, which is an archived copy of the Recommended Patch Cluster available from the same location, or the Enterprise Installation Services (EIS) patch set, which is a superset of the Recommended Patch Cluster.
- Install firmware updates to servers, storage, and so on in all maintenance windows. You should be running on firmware released within the last 6 months. These updates are available from My Oracle Support.
- Install any additional patches that prevent or fix issues specific to your environment.

- Apply updates for third-party and homegrown software and hardware. Note that bug fixes for some third-party or community-based software delivered as part of Oracle Solaris may be provided through package upgrades rather than patches. This is done to synchronize with the delivery mechanisms of the third-party or community-based software.
- Conduct pre-deployment testing on a system that mimics the production environment as closely as possible, including functional and peak load testing.

Oracle Solaris 10 Recommended Patching Strategy Summary

TABLE 1: SUMMARY OF ORACLE SOLARIS 10 RECOMMENDED PATCHING STRATEGY

	MAJOR MAINTENANCE WINDOWS	MINOR MAINTENANCE WINDOWS	REACTIVE PATCHING
Frequency	Every 18 to 24 months	Every 3 months, aligned to CPU schedule	As necessary
Install the latest patch utility patches first?	Yes	Yes	Yes
Use Oracle Solaris Live Upgrade or rolling cluster node upgrade?	Yes	Yes	Yes
Apply the latest Oracle Solaris Update or Oracle Solaris Update Patch Bundle?	Yes		
Apply Oracle Solaris Recommended Patch Cluster, CPU, or EIS patch baseline?	Yes	Yes	
Update firmware on servers, storage, and so on?	Yes	Yes	If applicable
Apply any other patches required?	Yes	Yes	Yes
Apply updates for third-party and homegrown software and hardware?	Yes	Yes	If applicable
Conduct pre-deployment testing?	Yes	Yes	As much as possible

Overview of Patching Components

- **Oracle Solaris Update Releases** are full release images containing all available Oracle Solaris OS bug fixes, as well as new features and support for new hardware. Patches are pre-applied into the release image. Oracle Solaris Update Releases provide functionally rich, stable, and well-tested baselines on which to standardize deployments.
- **Oracle Solaris Recommended Patch Clusters** provide critical Oracle Solaris fixes for security, data corruption, and system availability issues. Installing these critical recommended Oracle Solaris OS patches regularly keeps systems as secure, integral, and highly available as possible.
- **Firmware updates** have become increasingly important over the last few years on SPARC, especially T-series hardware, as well as x86 systems. For example, on early Oracle Sun SPARC Enterprise T2000 servers, system performance can be doubled by updating the firmware version installed. Firmware updates may provide functional enhancements, for example, to Oracle VM for SPARC. Many serious issues, such as panics, race conditions, and so on, are fixed in firmware updates. These are often misdiagnosed as hardware failures. Storage devices, switches, and so on may also need firmware updates. Therefore, be sure to keep firmware up to date as part of your patching strategy.
- **Patch and Package Utility patches** ensure the tools used to apply other updates are up to date. Before installing any other patch, always verify that the latest patch utilities patch has been installed on the live boot environment. These patches are available from My Oracle Support. This practice minimizes the chance of encountering patching related issues. The latest patch utility patches are always included in the Oracle Solaris Recommended Patch Clusters, and are positioned as far up the installation order as possible. Ensure the latest patches for Oracle Solaris Live Upgrade and any patch automation tool you use are applied prior to using them.
- **Additional patches or updates** should be installed to prevent or fix issues specific to your environment. These may be Oracle Solaris OS patches or patches or updates for other products in your environment that are not covered by the items mentioned in this document.
- **Oracle Solaris Live Upgrade (LU)** reduces the downtime, risk, and complexity involved in upgrading or patching a system.

  Oracle Solaris Live Upgrade reduces maintenance downtime by enabling production to continue on the live boot environment while Oracle Solaris Live Upgrade modifies a separate, inactive boot environment. Once the modifications to the inactive boot environment have been completed and checked, just a single reboot is needed to activate it. If for any reason the new boot environment doesn't perform as expected, you can revert to the old boot environment by simply rebooting back into it.

Special Install Instructions in some patch README files can include manual steps to correctly install some patches. Some of these manual steps are needed only when applying patches to the live boot environment, so using Oracle Solaris Live Upgrade to apply patches to an inactive boot environment eliminates some of complexity associated with patching.

In Oracle Solaris Cluster environments, a rolling upgrade of the cluster nodes may be a preferred method of achieving the same effect as using Oracle Solaris Live Upgrade.

- Conducting pre-deployment testing on a test environment that mimics the production environment as closely as possible is an excellent way to further mitigate risk. Oracle Solaris 10 Updates and patches are intensely tested as part of Oracle Integrated Stack Testing. Issues are rare.

  However, your systems may include third-party hardware or software or homegrown applications. Therefore, pre-deployment testing in your specific environment is an excellent method to further mitigate risk. Try to mimic the production environment as closely as possible in terms of hardware configuration, software configuration, and the test load driven through the system. Ideally, the test load should mimic peak loads (for example, end-of-quarter and end-of-year loads) and should be as functionally similar to the production load as possible.

Resources

Downloads and Information

My Oracle Support (MOS) is the one-stop shop for all your support needs, including patches, patch bundles and clusters, and information. You need an Oracle support contract to access MOS.

The full functionality flash version is at https://support.oracle.com.

A limited functionality HTML version is available at https://supporthtml.oracle.com.

Patches, patch clusters, and bundles can be downloaded from the Patches&Updates tab.

For example, to download any of the Oracle Solaris 10 patch clusters or patch bundles, from the Patches&Updates tab on MOS at https://support.oracle.com, simply select Product is Solaris Operating System, Release is Solaris 10 Operating System, and Type is Patchset.

Downloads from MOS can be automated using the `wget` utility. See https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1199543.1.

The latest Oracle Solaris Update Release is available from http://edelivery.oracle.com. Simply search for "Oracle Solaris."

Oracle Proactive Services and Tools

Oracle provides proactive services and tools to save you time and money in maintaining systems.

An overview of the Oracle Sun Management and Diagnostics Tools is available at https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=411786.1.

These services and tool include the following:

- Oracle Sun System Analysis, which is used to analyze specific systems to produce tailored reports identifying known issues, including security, data corruption, and availability issues as well as configuration issues. This process takes the generic recommended patching strategy documented here a step further by providing system-specific recommendations. See https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1194234.1.
- Oracle Auto Service Request (ASR) for Sun Systems, which auto-generates service requests. ASR leverages the Oracle Solaris Fault Management Architecture and built-in hardware diagnostics to automatically identify and report issues. See https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1185493.1.
- Oracle Services Tools Bundle (STB), which contains a set of useful tools including Explorer, which you can use to harvest configuration information for analysis by Oracle Sun System Analysis and debugging of issues by Oracle support personnel. See https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1153444.1.
- Oracle Shared Shell, which you can use to allow Oracle support personnel to debug system issues. See https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1194226.1.

Oracle also provides a range of Advanced Customer Services (ACS) to provide tailored proactive services for your environment. See http://www.oracle.com/us/support/software/advanced-customer-services/index.html or contact acsdirect_us@oracle.com.

Oracle Enterprise Manager Ops Center 11*g*

Oracle Enterprise Manager Ops Center is an enterprise-class system provisioning and management tool, including the application of patches and firmware updates. See http://www.oracle.com/technetwork/oem/ops-center/index.html.

Oracle Enterprise Manager Ops Center does the following:

- Automatically downloads all firmware and patches to your site
- Covers T-series, M-series, and X-series hardware, as well as disk and RAID Controller firmware updates

- Offers enterprise-class deployment features, such as rollback and support for Oracle Solaris Live Upgrade along with audit and policy control
- Leverages enhanced package and patch dependency and Special Instructions metadata
- Integrates telemetry and knowledge from the independent, government-approved common vulnerability repository at http://cve.mitre.org/
- Offers built-in profiles to check OS patch levels
- Integrates OS patch-level compliance reports with Oracle Enterprise Manager Grid Control Applications Violations for a single Oracle stack compliance report
- Facilitates the usage of single software compliance statements that span multiple operating systems
- Facilitates the creation of Service Requests (SRs)

Patching Strategy Considerations

The typical objective of a patching strategy is to maximize production system availability, performance, and security by optimizing proactive maintenance to prevent issues from occurring.

Although common wisdom says that change implies risk, minimizing risk on a production system is not as simple as minimizing change. For example, some systems might be exposed to newly discovered security vulnerabilities that need to be addressed. Other systems might perform sub-optimally or performance might deteriorate as the operational load changes over time. Functional issues might occur that demand resolution.

A key rationale for a patching strategy is that planned proactive maintenance downtime is usually far less costly than unplanned, reactive break-and-fix downtime. That is, prevention is better than cure.

Bringing all systems up to the same software level provides a more homogeneous environment, which helps to reduce complexity and, hence, to reduce system administration overhead and TCO.

The patch strategy recommendations described in this document also provide a "safety in numbers" effect, because if, on the rare occasion, an issue occurs, it is likely to be caught early and resolved quickly before the majority of customers encounter it. The fact that many customers are using the same patching strategy and, hence, may be exposed to the same issue is likely to increase the priority of producing a fix for such an issue.

Contrast this to "dim sum" patching, whereby customers select unique patch combinations such as a `libc.so` patch that is 4 weeks old in combination with a kernel patch that is 18 months old and a `zoneadmd` utility that hasn't been patched in 3 years. Although it is extremely rare for such unique software combinations to result in issues, thanks to the rigorous development and QA processes employed for Oracle Solaris, on the rare occasion when issues do result, they are likely to be unique, which may make them more difficult to diagnose and, hence, may potentially delay the release of a fix.

Some customers like to wait for a set period of time after a patch is released before applying it on the assumption that if a patch has a serious issue, it will be discovered and reported within that time period. Analysis of the time between patch release and patch withdrawal shows no statistically significant time period, although serious pervasive issues are usually found within 10 days of release.

A patch is withdrawn from release if it does more harm than good for the majority of customers.

For less serious or configuration-specific issues, a Note is typically added to the Special Install Instructions section of the patch README warning users of the issue and specifying any workaround or resolution.

Security issues are announced in Critical Patch Updates and at http://www.oracle.com/technetwork/topics/security/alerts-086861.html or via the Security blog (http://blogs.sun.com/security) for third-party components. An alert will be issued for data corruption and system availability issues; see "Alerts" under the Knowledge tab on My Oracle Support at https://support.oracle.com.

Oracle Solaris patch quality is extremely good. For example, over 4,300 patches were released in the last 12 months (to January 6, 2011) but only 17 have been withdrawn from release during that period due to serious issues.

When deciding on the change risk/reward "sweet spot," consider which are the best-tested and best-quality baselines upon which to standardize deployments and the best method to mitigate risk when applying updates.

- Oracle Solaris 10 Update releases are intensely tested by many teams across Oracle, including hardware QA teams, system test teams, functional regression test teams, performance regression teams, Oracle Solaris Cluster teams, and many more, each providing a slightly different perspective to provide overlapping and reinforcing test coverage.
- The Oracle Solaris OS Recommended Patch Cluster is updated whenever a patch meeting the inclusion criteria is released. Each patch is tested and verified individually and the patch cluster is also tested as a unit prior to release. The Oracle Solaris OS Recommended Patch Cluster provides the minimum amount of change required to get all critical Oracle Solaris bug fixes.
- Oracle Solaris Live Upgrade reduces maintenance downtime by enabling production to continue on the live boot environment while Oracle Solaris Live Upgrade modifies a separate, inactive boot environment.

Variations on the Recommended Patching Strategy

This section describes some alternative options for the recommended patching strategy described earlier.

Oracle Solaris Update Patch Bundles as an Alternative to Oracle Solaris Update Releases

Oracle Solaris Update Patch Bundles provide the equivalent set of patches corresponding to each Oracle Solaris Update Release. These patch bundles bring all **pre-existing** packages up to the same software level as the corresponding Oracle Solaris Update Release.

Oracle Solaris Update Patch Bundles provide all the functional enhancements for pre-existing packages, including all Oracle Solaris bug fixes available at the time the corresponding Oracle Solaris Update Release was being built. Oracle Solaris Update Patch Bundles leverage the intense testing of each Oracle Solaris Update Release and, hence, are an acceptable alternative to upgrading to, or installing, the Oracle Solaris Update Release. Application of an Oracle Solaris Update Patch Bundle appends a line to `/etc/release`. Thus, you can see both the original Oracle Solaris 10 release installed and the Oracle Solaris Update Patch Bundle applied.

Oracle Solaris Update Patch Bundles were requested by customers whose internal change control procedures prevent them from upgrading to the latest Oracle Solaris Update Release but allows them to patch. Each Oracle Solaris 10 Update release since Oracle Solaris 10 5/08 (Update 5) has had a corresponding Oracle Solaris Update Patch Bundle.

These bundles are available from the Patches&Updates tab on My Oracle Support (MOS) at https://support.oracle.com. Simply select Product is Solaris Operating System, Release is Solaris 10 Operating System, and Type is Patchset.

Because the Oracle Solaris Update Patch Bundles don't contain new packages introduced in an Oracle Solaris Update Release, new functionality that depends upon such new packages is not available in the Oracle Solaris Update Patch Bundles.

New hardware might run only on the latest Oracle Solaris Update Release, so applying the corresponding Oracle Solaris Update Patch Bundle to pre-existing systems enables you to bring pre-existing packages on those systems up to the same software level as a system running the latest Oracle Solaris Update Release.

Bringing all systems up to a similar software level provides a more homogeneous environment, which helps to reduce complexity and, hence, to reduce system administration overhead and TCO.

The recommended best practice is still to install/upgrade to the latest Oracle Solaris Update Release where change control policies allow. This practice provides the full functionality, including new packages, available in the Oracle Solaris Update Release image.

Enterprise Installation Standards (EIS) Patch Sets as an Alternative to Oracle Solaris Recommended Patch Clusters

The monthly Enterprise Installation Standards (EIS) release includes a patch set that is a superset of the Oracle Solaris Recommended Patch Cluster and, hence, can be used as a substitute for it. The EIS patch set includes patches for additional products, such as Oracle Solaris Cluster, Sun SAM-FS, Sun QFS, and SunVTS.

The EIS methodology is used by Oracle personnel to provide best-practice installation services for customers. It is also used to construct factory pre-install images for Oracle Sun hardware.

The full EIS methodology is not directly available to end customers, but the monthly EIS patch set is available to customers as "Patch Baselines" in the Oracle Enterprise Manager Ops Center product. The Oracle Solaris Recommended Patch Clusters are also available from Oracle Enterprise Manager Ops Center.

Oracle Solaris Critical Patch Updates (CPUs) as an Alternative to Oracle Solaris Recommended Patch Clusters

Oracle standard practice is for each product to release a quarterly Critical Patch Update (CPU) patch set on the same date containing the latest security fixes. This policy enables customers to plan maintenance windows to coincide with the scheduled quarterly CPU releases. The release of some security fixes may be timed to coincide with the CPU schedule.

CPUs are released on the Tuesday closest to the 17th of January, April, July, and October. See http://www.oracle.com/technetwork/topics/security/alerts-086861.html.

Oracle Solaris now complies with this practice, issuing CPUs that are renamed, archived copies of the Oracle Solaris Recommended Patch Clusters.

An Oracle Solaris Recommended Patch Cluster is updated whenever a patch meeting its inclusion criteria is released, for example, an Oracle Solaris patch that fixes a security, data corruption, or system availability issue.

An Oracle Solaris Recommended Patch Cluster will always contain the very latest critical fixes, while the CPU will be updated only quarterly.

These CPUs are available from the Patches&Updates tab on My Oracle Support (MOS) at https://support.oracle.com. Simply select Product is Solaris Operating System, Release is Solaris 10 Operating System, and Type is Patchset.

Rolling Upgrade of Oracle Solaris Cluster Nodes as an Alternative to Oracle Solaris Live Upgrade

Oracle Solaris Cluster customers might prefer to use a rolling upgrade of the cluster nodes as an alternative to using Oracle Solaris Live Upgrade.

Upgrading cluster nodes one at a time produces a similar effect to using Oracle Solaris Live Upgrade, because each node can be upgraded and patched offline. If a problem occurs when the system is switched over to the updated node(s), the system can be reverted back to the node(s) running the original configuration.

Applying All Available Oracle Solaris 10 Patches

Applying all available Oracle Solaris patches is a perfectly reasonable strategy. However, a total of 4,675 patch revisions have been released (as of January 6, 2011) for Oracle Solaris 10 on SPARC alone, including 742 in the previous 12 months. Trying to keep up to date with all of them would be an onerous task.

The Oracle Solaris Sustaining Director for EMEA, Jim "Jimmo" Moore, has noted that the vast majority of bugs reported more than 18 months after an operating system version is released are for corner cases in highly specific configurations that don't affect the vast majority of customers.

Because change implies risk, taking all fixes for other customers' corner-case issues in between major maintenance windows is debatable as an optimal patching strategy.

While the new features included in each Oracle Solaris 10 Update Release reset this 18-month clock to some extent, this resetting effect is becoming less significant as the scope of new features in Oracle Solaris 10 declines and the preparation for the release of Oracle Solaris 11 intensifies.

All available Oracle Solaris bug fixes will be included in each Oracle Solaris Update Release and corresponding Oracle Solaris Update Patch Bundle.

In between applying these, the recommendation patching strategy is to stay up to date with the most critical fixes by applying the Oracle Solaris Recommended Patch Cluster in all scheduled maintenance windows and to apply additional patches only if they prevent or fix issues specific to your environment.

Patching the Live Boot Environment as an Alternative to Oracle Solaris Live Upgrade

While using Oracle Solaris Live Upgrade is strongly recommended to reduce the downtime, risk, and complexity associated with patching Oracle Solaris, enhancements have been made to make patching the live boot environment safe and improve patching performance.

Deferred Activation Patching

The Deferred Activation Patching (DAP) enhancement enables arbitrary changes to be applied to the live boot environment. DAP addresses the issue of newly patched objects that are potentially incompatible with old processes running in memory being invoked during the patch application process.

For example, `zoneadmd`(1M) took 5 arguments in the original Oracle Solaris 10 3/05 release, but enhancements resulted in this being extended to 8 and then 11 arguments in subsequent releases. If a new version of `zoneadmd` is patched onto the system, and `patchadd`(1M) then calls it as part of the procedure to patch non-global zones, the new version of `zoneadmd` might be interacting with old processes loaded in memory that are expecting 5 or 8 arguments to be passed instead of 11. Unexpected behavior might occur as a result.

A small number of patches that deliver major feature changes are susceptible to this issue. These patches have `SUNW_PATCH_SAFE_MODE=true` in their `pkginfo`(1) files. These patches are typically the kernel patches associated with each Oracle Solaris 10 Update release, starting with Kernel patch 120011-14 (SPARC) and 120012-14 (x86) in Oracle Solaris 10 8/07 (Update 4).

`patchadd` automatically invokes DAP mode when installing such patches on a live boot environment. DAP overlays each patched object with the original unpatched object using loopback file system (LOFS) mounts. This practice ensures that if such objects are invoked during the remainder of the patching process, they will be consistent with whatever is running in memory.

`patchadd` will automatically implicitly invoke DAP for any other patches subsequently applied before the system is rebooted that specify a requirement on any other patch applied using DAP mode. This practice ensures complete consistency throughout the patching process.

The result may be a large number of temporary loopback file system mounts. Once the system is rebooted, these loopback file system mounts are torn down, revealing the patched objects.

Patch dependencies, specified by the `SUNW_REQUIRES` field in the `pkginfo` files of patches ensure consistency between patches.

DAP ensures consistency *during* the patching process on a live boot environment.

Zones Parallel Patching

The Zones Parallel Patching enhancement enables you to configure multiple non-global zones to be patched in parallel to improve patching performance. Zones Parallel Patching is an enhancement to the standard Oracle Solaris 10 patch utilities and is delivered in the patch utilities patch from revisions 119254-66 (SPARC) and 119255-66 (x86) onwards.

Once this patch is applied to the system, the maximum number of non-global zones to be patched in parallel can be set in the configuration file `/etc/patch/pdo.conf`. This configuration file contains instructions describing how to optimize the number of non-global zones to be patched in parallel.

This enhancement works for all Oracle Solaris 10 systems. It also works well with higher-level patch automation tools, such as Oracle Enterprise Manager Ops Center.

The global zone is still patched first, but the Zones Parallel Patching enhancement can dramatically improve overall zones patching performance by patching non-global zones in parallel.

While the performance gain is dependent on a number of factors, including the number of non-global zones, the number of online CPUs, the speed of the system, the I/O configuration of the system, and the like, a performance gain of approximately 300% can typically be expected for patching non-global zones, for example, on an Oracle Sun SPARC Enterprise T2000 server with five sparse root non-global zones.

Because this enhancement is a pure parallelization enhancement to `patchadd`, it provides normal `patchadd` functionality, for example, you can subsequently remove patches using `patchrm`.

The only change is that patching non-global zones with Zones Parallel Patching invoked is now much faster.

Special Install Instructions

Patches may contain Special Install Instructions in the patch README files. Some of these instructions are necessary only when installing patches on a live boot environment. For example, a Special Install Instruction might say to stop a daemon, apply the patch, and restart the daemon.

The advantage of applying patches to an alternate boot environment (for example, using Oracle Solaris Live Upgrade) is that such Special Install Instructions are not applicable and can be safely ignored.

In the above example, the daemon is obviously not active on the inactive boot environment. Therefore, you would not need to stop it prior to patching it or restart it afterward when patching the inactive boot environment.

This example illustrates that applying patches to an inactive boot environment using Oracle Solaris Live Upgrade can reduce the complexity of patching compared to applying patches to the live boot environment.

Background Information

This section provides more detailed information about Oracle Solaris Update Releases, Oracle Solaris Update Release Bundles, and Interim Diagnostics and Relief.

Oracle Solaris Update Releases

Oracle Solaris Update Releases are complete releases of the Oracle Solaris operating system. Each is cumulative of preceding releases. Oracle Solaris Update Release names end in the date of publication. For example, "Solaris 10 9/10" was the Oracle Solaris 10 Update released in September 2010. Because it was the ninth such update of Oracle Solaris 10, it's also unofficially commonly known as "Solaris 10 Update 9."

Each Oracle Solaris 10 Update Release introduces new functionality and enhancements to existing functionality, which can include new software enhancements and new hardware support. Each Oracle Solaris 10 Update Release also includes all Oracle Solaris bug fixes that were available at the time it was built.

There is effectively just one customer-visible code branch for the whole of Oracle Solaris 10. All code changes are made to the tip of that code branch. All changes to pre-existing packages are delivered as patches. Therefore, patches might contain new features and enhancements to existing features as well as bug fixes. New software features and feature enhancements are typically turned off by default to prevent surprising customers with unexpected changes when applying patches.

Oracle Solaris Update Releases are built from the available patches. The patches are pre-applied to the packages in the release. They can be listed using `patchadd -p`, but because they are pre-applied into the release image, they cannot be backed out using the `patchrm` utility. Oracle Solaris Update Releases might also introduce new packages, typically to support major new feature enhancements

Oracle Solaris Update Patch Bundles

Oracle Solaris Update Patch Bundles contain the equivalent set of patches to the corresponding Oracle Solaris Update Release. However, they don't contain new packages delivered in Oracle Solaris Update Releases. Therefore, an Oracle Solaris Update Patch Bundle will bring all pre-existing packages up to the same software level as its corresponding Oracle Solaris Update Release.

All functionality provided by these pre-existing packages, including feature enhancements, are available once the Oracle Solaris Update Patch Bundle is applied. For example, all Oracle Solaris Container (Zones) and ZFS functionality, including feature enhancements, are available via patches and, hence, can be added to any Oracle Solaris 10 system.

Additional fixes for security, data corruption, and system availability issues may be released after the contents of an Oracle Solaris Update Release and corresponding Oracle Solaris Update Patch Bundle are finalized, so be sure to install the latest available Oracle Solaris Recommended Patch Cluster in addition to bring your systems fully up to date with bug fixes.

Note: A small number of special and script patches are included in each Oracle Solaris Update Release whose sole purpose is to facilitate the correct pre-application of patches into the Oracle Solaris Update Release image. Because these patches have no purpose outside of this pre-application process, they are not included in the corresponding Oracle Solaris Update Patch Bundle, nor are they released as downloadable patches.

Oracle Solaris Recommended Patch Cluster

The Oracle Solaris Recommended Patch Cluster contains critical Oracle Solaris fixes for security, data corruption, and system availability issues. It also contains the latest patch utility patches to ensure correct application of patches and any other patches required to complete the installation of the patch set.

The Oracle Solaris Recommended Patch Cluster is updated whenever a patch is released that matches the above inclusion criteria, which can potentially happen several times each month. The README file in the Oracle Solaris Recommended Patch Cluster specifies the last update date.

The Oracle Solaris Recommended Patch Cluster includes a sophisticated install script and a comprehensive README file describing the installation procedure and contents.

The Oracle Solaris Recommended Patch Cluster should be applied in all maintenance windows.

Note that many of the patches contained in the Oracle Solaris Recommended Patch Cluster might already have been applied to the target system. The `patchadd` utility that applies patches is efficient at determining which patches have already been applied, so running the Oracle Solaris Recommended Patch Cluster installation script will apply any missing patches in an efficient manner.

Interim Diagnostics and Relief (IDR)

When a customer reports an issue, the responsible Sustaining Engineer may issue an Interim Diagnostics and Relief (IDR) either to enable diagnosis of the issue if no reproducible test case has been defined or to provide initial relief from the issue if the root cause is known or suspected.

IDRs are not patches, but they do leverage the patch architecture. IDRs are produced at an early stage of the bug fix process and do not undergo the rigorous design review, code review, and testing that released patches go through. They are designed for preliminary diagnosis and test purposes to verify that the proposed fix resolves the issue. It is not recommended that you install them on production systems unless there is no alternative.

IDRs have a naming format similar to IDR123456-01. Installed IDRs have an IDR prefix and can be listed using the `patchadd -p` command. They are built from temporary code branches.

When applied to a system, IDRs lock down the packages they modify to prevent them from being accidentally overwritten by a patch or another IDR. Therefore, if a system with IDRs installed is to be patched, make sure that the IDRs installed do not modify the same packages as the patches to be applied. If they do, then you need to remove the IDRs before the patches can be applied to those packages.

Make sure you check whether the patches fix the issue that the IDR addresses. If they don't, then a new IDR built on top of the source base of the patches may be required.

Always check with the person who provided the IDR in such circumstances.

Because of the issues above, applying IDRs to production systems can increase the complexity of subsequent patching processes and, hence, should be avoided where possible.

For More Information

Here are additional resources.

- The Patch Corner Blog at http://blogs.sun.com/patch provides a wealth of information about items discussed in this document.
- The Oracle Technology Patching Center at http://www.oracle.com/technetwork/systems/patches/overview/index.html provides a wealth of patching information about Oracle Solaris, firmware, and other patches, including online training courses on Oracle Solaris patching best practices, such as the use of Oracle Solaris Live Upgrade.
- The Oracle Solaris Installation, Booting, and Patching Forum at https://communities.oracle.com/portal/server.pt/community/oracle_solaris_installation,_booting_and_patching/397 provides a community forum in which customers can discuss issues, ask for advice, and connect with other customers as well as Oracle technical experts.

- Changes in security policies for the Sun product lines are described at http://www.oracle.com/technetwork/topics/security/changesforsunsecuritypolicies-162219.html.
- Critical Patch Updates (CPUs) and Security Alerts are detailed at http://www.oracle.com/technetwork/topics/security/alerts-086861.html.
- The Security Blog at http://blogs.sun.com/security provides information on security vulnerabilities for third-party code provided by Oracle, and includes CVE and CVSS mappings for Oracle Solaris patches.
- For information on Oracle Solaris data corruption and system availablly issues, see "Alerts" under the MOS Knowledge tab.

Oracle is committed to developing practices and products that help protect the environment

Oracle Solaris10 Recommended Patching Strategy
January 2011
Author: Gerry Haskins

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Hardware and Software
Engineered to Work Together