

Wie lebe ich Solaris 11 Updates im Rechenzentrum

Thomas Wagner
Oracle Deutschland B.V. & Co KG
Stuttgart

Schlüsselworte

Solaris 11, Update, IPS, SRU, Change Management, signierte Pakete

Version 01

Einleitung

Mit Oracle Solaris 11 wurde die neue Paketverwaltung „IPS“ eingeführt. Mit IPS werden alle Pakete und Metadaten in einem Paket-Repository abgelegt. Die in früheren Solaris Versionen genutzte SVR4 Paketverwaltung wird in Oracle Solaris 11 von IPS (Image Packaging System) abgelöst. Die Aktualisierung auf einen neueren Solaris Versionsstand kann nun mit IPS in sehr vielen Fällen durch ein sehr einfaches „pkg update“ erledigt werden. Aktualisierungen sind nur noch als neue Paketversionen ausgeführt, die altbekannten „Patches“ gibt es nicht mehr. Jedoch ist es im manchem Rechenzentrumsbetrieb mit einem einfachen "pkg update" spätestens dann vorbei, wenn die Beauftragen für IT-Security und Change-Management gleichzeitig vor ihnen stehen und man es keinem der Beiden recht machen kann: Der eine verlangt die sofortige Installation der Sicherheitsupdates, der andere will nur nach Test und Abnahme der neuen Paketversionen den Produktiveinsatz erlauben.

Im Vortrag wird eingegangen auf einen exemplarischen Aufbau von mehreren Repositories für Test / Abnahme / Produktion, notfalls lockern der festen "Versionsvorgaben" für Pakete innerhalb eines Solaris-Release am Beispiel eines einzelnen Security-Updates (package facet.version-lock.*), im Support-Fall die Funktion von Interim Diagnostic Relief (IDR) Paketen in IPS, Updates nur für "Indivisible Core" (Solaris Basisfunktionen) und Incorporations (z.B. Desktop) oder nur für Einzelpakete. Für Updates der Non-Global-Zones wird der „Zonesproxy“ für IPS gezeigt und eine kurze Betrachtung von signierten Paketen vorgenommen.

Latest&Greatest, der einfachste Fall für ein Solaris 11 Update

Was ist der einfachste Update-Fall? Eine existierendes Solaris 11 Installation erhält eine Aktualisierung auf die jüngste von Oracle bereitgestellte Solaris 11 Version.

Der Probelauf (dryrun) mit Anzeige der zu aktualisierenden Pakete zu ihrer Information:

```
pkg update -nv
```

Für den Update selbst werden die Pakete über Internet (oder eine lokale Kopie) des Solaris 11 IPS Repository von <http://pkg.oracle.com> aktualisiert:

```
pkg update -v
```

Die Installation der Pakete erfolgt in der Regel in eine automatisch angelegte Kopie der laufenden Installation (ZFS snapshot / clone), danach wird vom Administrator verlangt das System für die Aktivierung der neuen Version zu rebooten. Für einen raschen Rollback steht die Originalumgebung weiterhin zur Verfügung.

Im Detail: Das Kommando `pkg update` lädt die Metadaten der Pakete, ermittelt welche Pakete

aktualisiert werden müssen und legt gegebenenfalls ein neues Bootenvironment an (BE, das ist ein ZFS snapshot und clone des „/“ und „/var“ und die Vergabe eines BE-Namens). In das neue BE werden die Pakete vom offiziellen IPS Paketserver geladen und installiert (pkg.oracle.com, alternativ eine lokale Kopie). Das BE wird für den nächsten Reboot als Zielumgebung voreingestellt. In einem kurzen Wartungsfenster erfolgt dann kontrolliert der Reboot.

Vorteile: Alle Paketversionen entsprechen denjenigen die von Oracle für die Freigabe des Updates als Ganzes getestet wurden.

Für Kunden mit passendem Support-Vertrag stehen Solaris Releases vor allem die zugehörige Solaris Service Update Releases (SRU) zur Verfügung. Sofern nicht anders angegeben wird immer auf die jüngste erschienene Version aktualisiert. Die kann z.B. der jüngste SRU sein. Hierfür wird das Solaris Support Repository als IPS publisher eingetragen).

Der komplexe Update Fall

Es sollen bestimmte Solaris Pakete isoliert vom restlichen System aktualisiert werden oder im Gegenteil sollen bestimmte Solaris Pakete vom Update ausgenommen werden. Gründe hierfür können in der Praxis unter anderem sein:

- security Anforderungen erfordern die rasche installation eines einzelnen Paketupdates bei minimaler Betriebsunterbrechung und minimalen Änderungen am restlichen System (z.B. wegen großem Zeitbedarf für die Requalifizierung der Applikationen)
- eine Anwendung ist nur mit einer bestimmten Version eines Solaris Pakets kompatibel

Die Abweichung von den vorgegebenen Versionen sollte immer eine Ausnahme sein. Es kann beispielsweise dazu führen, dass weitere (erwünschte!) Pakete nicht aktualisiert werden können, da für diese die Voraussetzungen für die Installation nicht mehr erfüllt werden. Sollte es jedoch dringend nötig sein einzelne Pakete vom Update auszuschliessen oder abweichende Paketversionen zu installieren, dann kann dies im Rahmen der in den Paketen selbst angegebenen Paketabhängigkeiten erreicht werden. Die Kommandos `pkg freeze paketname` und `pkg unfreeze paketname` stehen zum einfrieren der Version einzelner Pakete zur Verfügung.

Für die Installation eines einzelnen Paketes in einer neueren Version wird zusätzlich zum Paketnamen auch die Versionsangabe angegeben: `pkg install pkg://web/server/apache-22@2.2.20-0.175.0.0.0.2.537`. Diese Installation kann unter Umständen verweigert werden, weil andere Pakete nicht in der benötigten Version vorliegen.

Solaris 11 Releases und Solaris 11 Service Update Releases (SRU)

Als Installationskandidaten stehen die von Oracle regelmäßig veröffentlichten Solaris Releases (z.B. Solaris 11 11/11 (11.0), Solaris 11 nn/nn (11.x)) zur Verfügung. Zwischen diesen Releases werden darauf aufbauende Service Update Releases veröffentlicht. Die von den Vorgängerversionen (z.B. Solaris 10) bekannten vorgefertigten Patchcluster werden durch die SRU ersetzt. Wichtig ist hierbei, daß nun immer alle installierten Pakete auf den neuen Versionstand aktualisiert werden. Einen teilweisen Update wie man es durch weglassen oder ändern von Patchversionen in gewissen Grenzen bei den Vorgängerversionen von Solaris erreichen konnte ist nicht mehr der Standardfall. Nachinstallierte Pakete werden mit IPS ebenfalls gleich in der passenden aktualisierten Version installiert.

Wie bisher auch wird empfohlen, zeitnah die Systeme auf die jeweils aktuellen Versionen zu aktualisieren.

Vorteil: Viele vergleichbare (weil identische) Systeme im Rechenzentrum und auch bei anderen Anwendern

Nachteil: Die Paketversionen sind eine fixe Zusammenstellung (aber: siehe Vorteil)

Testen der Updates vor dem Ausrollen

In manchen besonders kritischen Anwendungsbereichen ist es wichtig, daß Änderungen an den System vor der Produktionsfreigabe ausführlich getestet werden können. Nachfolgend wird skizziert wie dies mit IPS ausgeführt werden kann:

Im Beispiel sollen die Abschnitte Test&Entwicklung, Integration&Abnahme und Produktion dargestellt werden.

Test&Entwicklung:

- lokale Kopie des IPS Paket-Repository ("Test")
- füllen des IPS Paket-Repository via DVD oder mit direktem Zugriff auf <http://pkg.oracle.com>
- Vorrätige Solaris Releases und SRUs:
11.0, 11.0 SRU1, 11.0 SRU2, 11.0 SRU3 ... 11.0 SRU8
11.1, 11.1 SRU9, 11.1 SRU10
- Automated Installer (AI) greift auf das IPS Repository "Test" zu um die Testsysteme zu installieren oder aktualisieren
- Solaris Updates für existierende Testsysteme werden von "Test" geladen
- Die Nachinstallation von Paketen erfolgt aus "Test"

Integration&Abnahme:

- lokale Kopie des IPS Paket-Repository ("Entwicklung")
- füllen des IPS Paket-Repositories wie bei "Test" via DVD oder <http://pkg.oracle.com> (alternativ: Kopie des "Test" IPS Paket-Repository)
- Vorrätige Solaris Releases und SRUs:
11.0, 11.0 SRU1, 11.0 SRU2, 11.0 SRU3, 11.0 SRU4
11.1, 11.1 SRU9, 11.1 SRU10
- Automated Installer (AI) greift auf das IPS Repository zu um die Entwicklungssysteme zu installieren oder aktualisieren
- Solaris Updates für existierende Entwicklungssysteme werden von "Entwicklung" geladen
- Die Nachinstallation von Paketen erfolgt aus "Entwicklung"

Produktion

- lokale Kopie des IPS Paket-Repository ("Produktion")
- Laden der IPS Paket-Repositories wie bei Test / Entwicklung via DVD oder <http://pkg.oracle.com> (alternativ könnten nur ausgewählte für die Produktion freigegebene Versionsstände auf dieses Repository gelegt werden)
- Automated Installer (AI) greift auf das IPS Repository zu um die Produktionssysteme zu installieren oder aktualisieren
- Solaris Updates für existierende Entwicklungssysteme werden von "Produktion" geladen
- Die Nachinstallation von Paketen erfolgt aus "Produktion"

Im Support-Fall könnte ein IDR „Interim Diagnostic Relief“ nötig sein

Für kurzfristige Abhilfe im Support-Fall oder zur Verifizierung einer Korrektur im Rahmen eines Service Request (SR) können für die individuellen Fälle „IDR“ Pakete bereitgestellt werden. Die Freigabe erfolgt durch den Oracle Support und für jedes System einzeln im Rahmen von Support Requests (SR). Diese IDR werden als spezielle aktualisierte Pakete installiert und sobald die endgültige Lösung in einem offiziellen Solaris 11 Release Update oder SRU enthalten ist, wird das IDR Paket auch wieder automatisch ohne weiteres zutun entfernt.

Non-Global-Zones und IPS

Für einen stabilen Betrieb ist es nötig, die Inhalte der Non-Global-Zones synchron mit den Inhalten aus der Global-Zone zu halten. Mindestens die Kernkomponenten aller Non-Global-Zones müssen daher fest an die Versionsstände der Global-Zone gekoppelt sein. Das IPS Paketsystem trägt dafür Sorge, dass bei einem „zoneadm attach“ die Versionsstände überprüft und gegebenenfalls aktualisiert werden. Die Kommunikation zwischen der Non-Global-Zone und der Global-Zone erfolgt hierbei über einen „zonesproxy“ welcher für die IPS Paketverwaltung den Zugriff auf die Solaris IPS Pakete auf der Global-Zone ermöglicht. Somit benötigt eine Non-Global-Zone keinen eigenen Netzwerkzugriff auf die IPS Paketreservoirs.

Bei einem System-Update wird zunächst die Global-Zone aktualisiert und nach dem Reboot wird vor dem Start der Zonen deren Versionsstand geprüft und ebenfalls aktualisiert.

Signierte Pakete

Alle für Oracle Solaris 11 herausgegebenen Pakete sind signiert. Somit erfolgt eine Installation nur dann, wenn die Signatur auf den Inhalt jedes Paketes als gültig geprüft werden konnte. Dies verhindert unbemerkte Änderungen an den von Oracle über DVD oder Internet <http://pkg.oracle.com> gelieferten Paketen.

Für selbst erstellte IPS Pakete kann eine eigene Signatur vorgenommen werden. Auf dem Zielsystem wird das eigene Zertifikat (public) hinterlegt um so die Gültigkeit der selbst erstellten Pakete bei der Installation zu prüfen.

Verweise, Links, Dokumentation

Für eine aktualisierte Liste der Verweise ist noch ein Update dieses Manuskriptes zur Zeit der DOAG-Konferenz geplant. Bitte besuchen sie dann noch einmal die DOAG Website für den Download der Präsentation und des Manuskriptes. Die können mir auch gerne eine Email schreiben und ich sende ihnen gerne die Präsentation und das Manuskript zu.

How to Update Oracle Solaris 11 Systems From Oracle Support Repositories

<http://www.oracle.com/technetwork/articles/servers-storage-admin/o11-018-howto-update-s11-1572261.html>

*** More Tips for Updating Your Oracle Solaris 11 System from the Oracle Support Repository

<http://www.oracle.com/technetwork/articles/servers-storage-admin/tips-maintain-s11-sru-1627108.html>

Hinweis: Für teilweise Systemupdates oder z.B. einfrieren von Einzelpaketversionen lesen sie bitte speziell die weiterführenden Links im Abschnitt „Updating Your System“

How to Create Multiple Internal Repositories for Oracle Solaris 11

<http://www.oracle.com/technetwork/articles/servers-storage-admin/int-s11-repositories-1632678.html>

Kontaktadresse:

ORACLE Deutschland B.V. & Co. KG

Thomas Wagner

Liebkechtstraße 35

D-70565 Stuttgart

Telefon: +49 (0) 711-72840-375

E-Mail Thomas.X.Wagner@oracle.com

Internet: www.oracle.com

Disclaimer

The preceding is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions.

The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Version 01