Unix Patchday – der Patchkalender
oder
Wie patcht man regelmäßig mehrere tausend Systeme

Sylke Fleischer, Marcel Pinnow
DB-Systel
Erfurt

Schlüsselworte

Oracle Solaris, Linux, Patchmanagement, Patchday, Patchtool, LiveUpgrade, Softwareupdate, Firmwareupdate, Konfigurationsanpassung, Release, Wartungsfenster

Einleitung

Die DB Systel ist einer der größten IT Dienstleister des DB Konzern. Im UNIX Umfeld werden mehrere tausend Linux und Solaris Server betreut. Diese Server werden wiederum von hunderten internen und externen Kunden des DB Konzern nach unterschiedlichen Servicelevel Vereinbarungen genutzt. Ein regelmäßiges Patchen aller Systeme war noch vor 3 Jahren nur mit enormem manuellem Aufwand verbunden. Jedes Wartungsfenster musste einzeln mit den Kunden vereinbart und manuell durchgeführt werden Die vorhandene Vielzahl unterschiedlicher Sparc- und x86 - Hardware sowie verschiedene OS - Stände machte die Aufgabe nicht leichter.

Es stellte sich die Frage: „Wie halten wir unsere Systeme aktuell?“

In einem Umfeld dieser Größenordnung muss ein Patchen der Systeme weitgehend automatisiert erfolgen. Der Unix Patchday wurde entwickelt, um ein regelmäßiges und den IT Prozessen konformes Patchen von Systeme zu gewährleisten. Er bietet, im Rahmen eines Patchkalenders, den Benutzern der Systeme eine Planungssicherheit und einen Status ihres Systems im Rahmen des Patchprozesses.

Folgende Punkte standen bei der Umsetzung des Unix Patchday im Vordergrund:

- aktuelle und stabile Plattform
- minimaler Abstimmungsbedarf
- automatisiertes Ausrollen der Patches
- Einbettung in ITIL-Prozesse mit vertretbarem Aufwand
- Einhaltung der Servicelevel

Dieser Vortrag ist ein Praxisbeitrag über die Einführung und Implementierung eines funktionierenden Patchmanagements und die erfolgreiche Organisation regelmäßiger Wartungsfenster. Wir gehen auf die Anbindung des Unix Patchkalenders an eine interne CMDB und das selbst entwickelte Patchtool ein. Es wird beschrieben, wie entsprechende ITIL –Prozesse umgesetzt wurden.

Verwendete Technologien:

OS:	Solaris 10, SLES 10, SLES 11, RHEL6
Solaris Patchen :	LiveUpgrade, CPU / RPC Patchcluster, Patchtool, Patchday
Linux Patchen:	Support Repository, Patchtool, Patchday

Begriffsklärung

Unix – Patchday / Patchkalender

Mit Hilfe des Unix Patchkalenders wird für jedes Solaris- bzw. Linux System ein Zeitfenster pro Quartal festgelegt. Danach wird ein Server zum Beispiel immer am 8.Mittwoch im Quartal um 21:00 Uhr gewartet. Das eigentliche Wartungsfenster orientiert sich an der jeweiligen ServiceLevel Vereinbarung mit dem Kunden. Einmal vereinbarte Termine stehen fest und werden jedes Quartal erneut genutzt. Mit Hilfe eines einzigen Planungschanges je Patchzyklus (Quartal) wird der Abstimmungsbedarf mit den Kunden minimiert und der Patchinhalt dokumentiert. Terminänderungen für konsolidierte Systeme sind lediglich per Changeprozess möglich.

Schaubild

Unix Patchday / Patchkalender

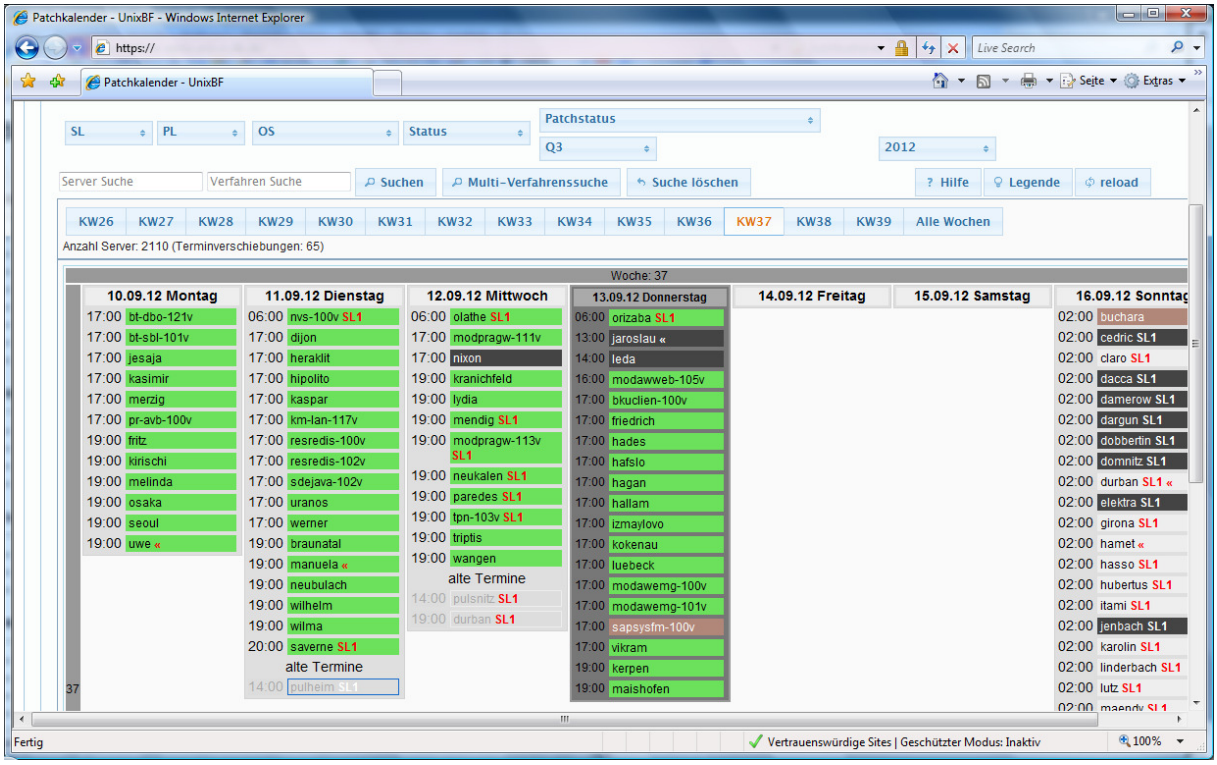

Abbildung 1 : Einblick Unix Patchkalender

Der Kunde hat über den Unix Patchday die Möglichkeit den Status seines Systems im Rahmen des Wartungsfensters zu verfolgen. Zur Erklärung die Legende des Patchkalender im Schaubild 2.

Schaubild

Legende Unix Patchkalender

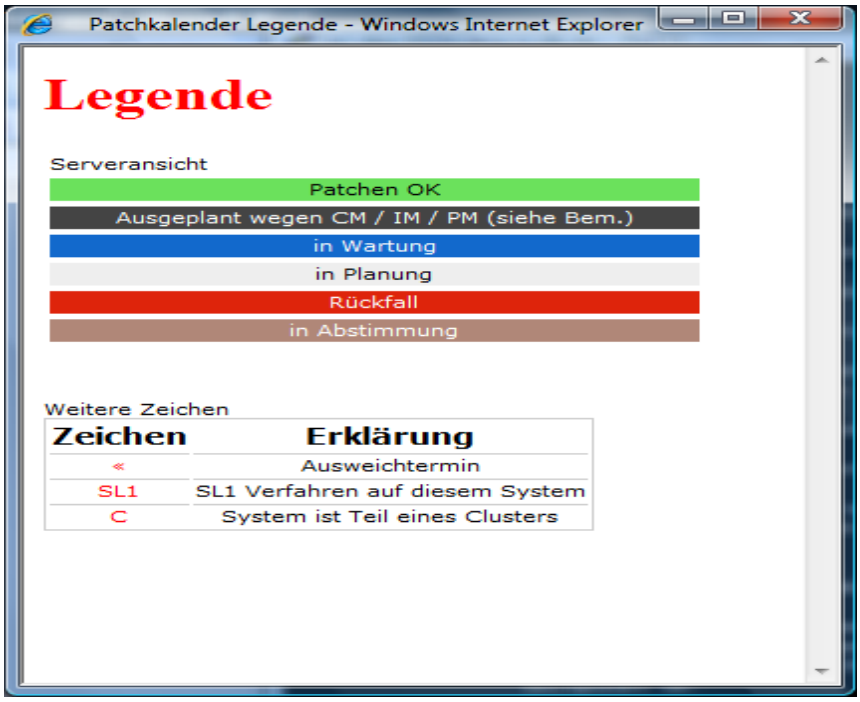

Abbildung 2 : Legende Unix Patchkalender

Der Unix Patchkalender wiederum steuert das Patchtool und richtet sich dabei nach den Patchterminen der Systeme.

Patchtool

Ursprünglich wurde dieses Tool ausschließlich zum Patchen und Upgraden bzw. Updaten für Linux-Server entwickelt. Durch dessen Weiterentwicklung können heute die verschiedensten Aufgaben, wie z. B. das Anpassen von Konfigurationsdateien, Installation von Software, ein-/ausschalten von Services u. v. m. erledigt werden. Selbstverständlich werden auch OS-Updates bzw. OS-Upgrades durchgeführt. Heute steht das Tool für Linux und Solaris zur Verfügung. Es wird im Normalfall einmal pro Quartal ausgeführt.

Schaubild

Ablauf Patchtool für Solaris 10

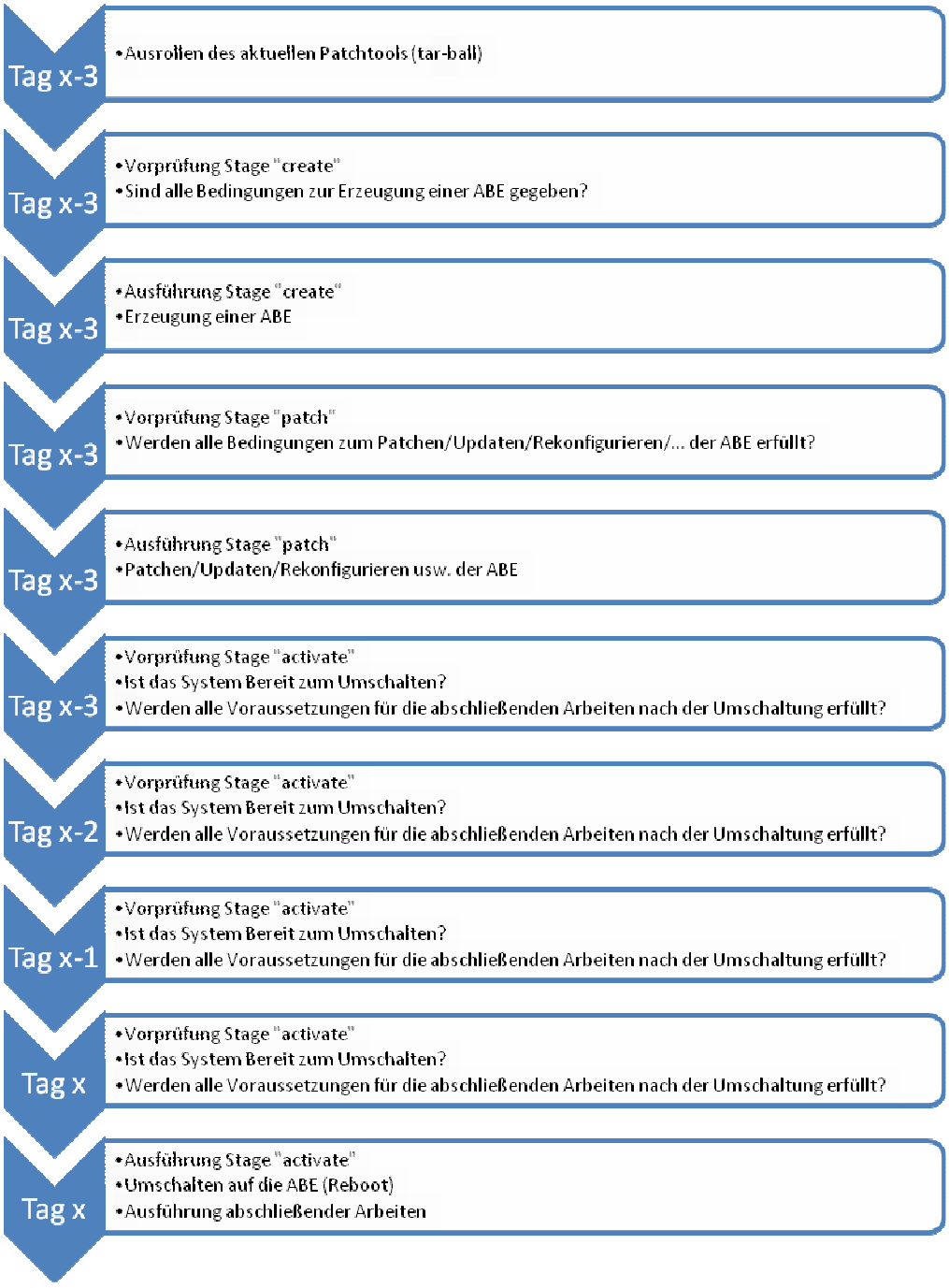

Abbildung3 :Ablauf Patchtool für Solaris 10

Ein Ausschnitt der Patchtool – Kommandos:

patchtool -h
<KOMMANDO> ist eines der folgenden:

check:	fuehrt nacheinander checkrepo, checkpkg, checkconf und checkscript aus.
checkbaseconf:	Prueft ob eine Updatebasiskonfiguration auf dem Installserver existiert.
checkrepo:	Prueft, ob ein Patchrepostory existiert und lokal eingebunden ist.
checkpkg:	Prueft, ob aktualisierbare Pakete in den konfigurierten Repositories existieren.
getscript:	Laedt explizit ein vorhandenes Patchskript herunter.
makepatchrepo:	Legt das laut upstat vorhandene Patchrepository an.
upstat:	Zeigt alle vorhandenen upstat-Informationen an.
parse-upstat:	Zeigt gefiltertet upstat-Informationen fuer diese Maschine an.
simulate:	ruft da aktuelle Patchskript mit Option simulate auf
checkprereqs:	ruft das aktuelle Patchskript mit der Option checkprereqs auf.
startupdate:	ruft das aktuelle Patchskript mit der Option start auf.
abort:	bricht einen laufenden Patchprozess zum naechstmoeglichen Zeitpunkt ab.
reset:	Setzt interne Statusinformationen zurueck. Schaltet fuer den naechsten Reboot wieder auf Runlevel 3 um. Ein laufendes Patchskript muss vorher explizit mit 'patchtool abort' abgebrochen werden.
patchlog:	zeigt das Logfile des aktuellen Patchskriptes an.
currentstate:	zeigt die letzte Zeile des aktuellen Patchskriptes an.
patchhistory:	zeigt an, welche Patchskripte auf dieser Maschine erfolgreich abgelaufen sind.
runtarget:	fuehre angegebenes Patchtarget aus.
listtargets:	zeige alle ausfuerbaren Patchtargets an.

Das nächste zu erwartende Patchrelease wird in „dbs-patchinfo“ eingetragen.

$ cat dbs-patchinfo
PATCHRELEASE=2012Q3

Eine Zusammenfassung der durch das Solaris Patchtool abgelaufenen Schritte ist in nachfolgendem Logfile zu finden:

$ cat patch_history
#
##
Timestamp(uptime): 1337075581
Systemname: werner

Datum: 06.09.12
Zeit: 13:51:54
OBE-Name: d10_be
OBE-Kernel: 147440-09
OBE-Patchrelease: 2012Q1

#
*** Umschaltung ***
#
Datum: 11.09.12
Zeit: 17:17:29
ABE-Name: d40_be
ABE-Kernel: 147440-09
ABE-Patchrelease: 2012Q3
#
Ergebnis der Umschaltung von OBE auf ABE: O.K.
##

Mit Hilfe des Unix Patchday in Verbindung mit dem Patchtool für Linux und Solaris ist es uns möglich, unsere Systeme aktuell sowie stabil zu halten und gleichzeitig die Sicherheitsvorgaben der Plattform bei der DB Systel GmbH umzusetzen. Durch die wiederkehrenden Patchtermine je Quartal, wird dem Kunden einen Planungssicherheit gegeben und der Abstimmungsaufwand minimiert.

Kontaktadresse:

Sylke Fleischer
DB Systel GmbH
Schlachthofstrasse, 80
D-99085 Erfurt

Telefon: +49 (0) 361 300 5706
Fax: +49 (0) 361 300 5981
E-Mail sylke.fleischer@deutschebahn.com
Internet: http://www.dbsystel.de