Zero Downtime Patching von Oracle Linux und OracleVM

Friedrich-Wolfgang Weinhappl
Oracle Austria
Wien

Schlüsselworte

Ksplice, ULN, Oracle Linux, OL, Oracle VM, OVM, Zero Downtime

Einleitung

In der heutigen Zeit ist es immer wichtiger, Server und vor allem Services mit so wenig Downtime wie möglich online zu halten. Einen Einfluss auf sogenannte „ungeplante Downtimes“ hat man so gut wie nie, jedoch die „geplanten Downtimes“, wie das Patchen von Servern können sehr wohl koordiniert werden. Dies bedingt aber in den meisten Fällen einen oder mehrere reboots der Server, um alle notwendigen Patches einzuspielen und zu aktivieren.
Hier verfolgt nun Oracle mit dem Thema Ksplice den Ansatz, wichtige Kernelpatches bzw. Security-patches ohne Unterbrechung der Applikation bzw. des Betriebssystems in den Kernel bzw. den Userspace zu bringen.

Ksplice – Wo fängt man an?

Mit einem kurzen Überblick zu Oracle Linux (OL) und Oracle VM (OVM):

Oracle Linux als auch Oracle VM sind Open Source Distributionen. Beide Produkte sind kostenfrei herunterladbar, nutzbar und stehen zur Weitergabe zur Verfügung.
Es werden seitens Oracle Supportverträge für Oracle Linux und Oracle VM angeboten, welche für Enterprise Umgebungen mit darauf laufenden Enterprise Applikationen dringend empfohlen werden.

Oracle Linux ist ein 100% binärkompatibler Klon von RedHat Linux. Oracle nutzt dieselben Source Pakete, dieselben Compiler inklusive deren Einstellungen, um Oracle Linux zu erzeugen. Alle Pakete sind mit einer Oracle Signatur versehen.

Oracle Linux wird mit zwei Kernel Optionen ausgeliefert:
- UEK – Unbreakable Enterprise Kernel = Default Kernel (aktuell UEK4 - Kernel 4.1.12)
- RHCK – RedHat Compatible Kernel = Kernel für einfachen Migrationsweg von RHEL zu OL

Mittels des RHCK haben RedHat Enterprise Linux Kunden die Möglichkeit, ohne Änderung in deren Betriebssystemen bzw. den installierten Applikationen - das heißt ohne Neuinstallation bzw. ohne Reboot! – einen Switch von RHEL nach OL durchzuführen. Nach diesem Switch wird das ehemalige RHEL System mit Patches seitens Oracle versorgt. Selbiges gilt auch für CentOS.

Oracle Linux ist das Betriebssystem für Cloud Umgebungen:
- Entwickelt für geschäftskritische Anwendungen.
- Benutzt aktuellste Technologien (LXC, Docker, OpenStack, …).
- Nutzt die Beiträge von Oracle zum Mainline Kernel.
- Wird auch in Oracle’s Engineered Systems und der Oracle Cloud eingesetzt.

Ebenso wie Oracle Linux ist auch Oracle VM in bzw. mit den oben genannten Optionen und Funktionen ausgestattet. Oracle VM basiert auf Oracle Linux, die Entwicklungsteams von Oracle Linux, Oracle VM und den Engineered Systems arbeiten sehr eng zusammen, um die bestmögliche Leistung in allen genannten Produkten zu Gewährleisten.

Vermeidung von teuren Unterbrechungen:

Durch den Reboot einen Produktionssystems sind in der Regel auch weitere Systeme bzw. Prozesse, die damit in Zusammenhang stehen, betroffen. Meist müssen geschäftskritische Applikationen 7x24 verfügbar sein, daher sind die „geplanten Downtimes“ ebenfalls relativ schwer zu planen und durchzuführen.

Hier kommt in der heutigen Zeit ein weiterer Aspekt zum Tragen – das Thema Security.
Oft passiert es, dass Tage nach einer geplanten Downtime sicherheitsrelevante Patches zur Verfügung stehen, diese aber erst bei der nächsten geplanten Patch Session installiert und vor allem aktiviert werden können.

Hier kommt Oracle mit Oracle Linux und dem Produkt **Ksplice** ins Spiel.

Ksplice – Kernel Security und Bug Fixes:

Das Thema Patchen ohne Reboot des Betriebssystems und ohne Unterbrechung der Applikationen ist nicht neu. Seit 2008 ist Ksplice im Markt, gegründet von Absolventen des MIT, seit 2011 Teil von Oracle und damit Bestandteil von Oracle Linux. Bisher sind mehr als 250000 Systeme mit Ksplice geschützt, über 4 Millionen Reboots dadurch verhindert und über 10 Millionen Patches eingespielt.

Mittels Ksplice haben Kunden mit Oracle Premier Support die Möglichkeit, sowohl den Kernel, als auch einige Libraries im Userspace (glibc und OpenSSL) mit sicherheitsrelevanten Patches als auch mit Bug Fixes ohne Reboot schnell und sicher auf den aktuellen Stand zu bringen.

Durch die Veröffentlichung eines Patches seitens Oracle zur Behebung einer Sicherheitslücke wird durch das Ksplice Team dieser Patch nahezu zeitgleich als Ksplice Patch unseren Kunden mit Premier Support zur Verfügung gestellt. Diese haben dann die Möglichkeit, entweder automatisiert oder manuell diesen Patch einzuspielen. Schneller kann eine Sicherheitslücke nicht beseitigt werden.

Mittels Ksplice können auch für Diagnosezwecke sogenannte Debug Kernels zur Verfügung gestellt werden, welche nach erfolgter Tätigkeit ebenfalls ohne Reboot wieder aus dem System genommen werden können. Diese Technik kann auch zum Rollback von Patches bzw. Bug Fixes angewandt werden, falls diese irgendwelche Probleme bereiten und entfernt werden müssen.

Wichtig ist die Tatsache, dass Ksplice sowohl für den UEK als auch für den RHCK zur Verfügung steht. Sowohl Oracle Linux 5*, 6 als auch 7 ist mit Ksplice patchbar.

Userspace Pakete (glibc und OpenSSL) sind für Oracle Linux 6 und 7 verfügbar.

* Oracle Linux 5 ab Kernel 2.6.18-164.el5

Ksplice – Technologie:

Patchen mittels Ksplice Technologie passiert generell nur im Hauptspeicher.
Ein zum Patchen vorgesehener Inhalt im Speicher (Library, Treiber, etc.) bleibt bestehen, damit der Rollback funktionieren kann. Beim Installieren bzw. Aktivieren des Patch wird an der Einsprungadresse ein Pointer zum Beginn des Patch gesetzt, selbiges passiert beim Aussprung aus dem Patch – dort wird an das Ende des zu patchenden Speicherinhalts zurückgesprungen (siehe Abb. 1). Diese Technologie wird für alle Ksplice Patches angewandt, sowohl Kernel (auch Ksplice Uptrack bezeichnet) als auch Userspace (auch Ksplice Enhanced Client bezeichnet).

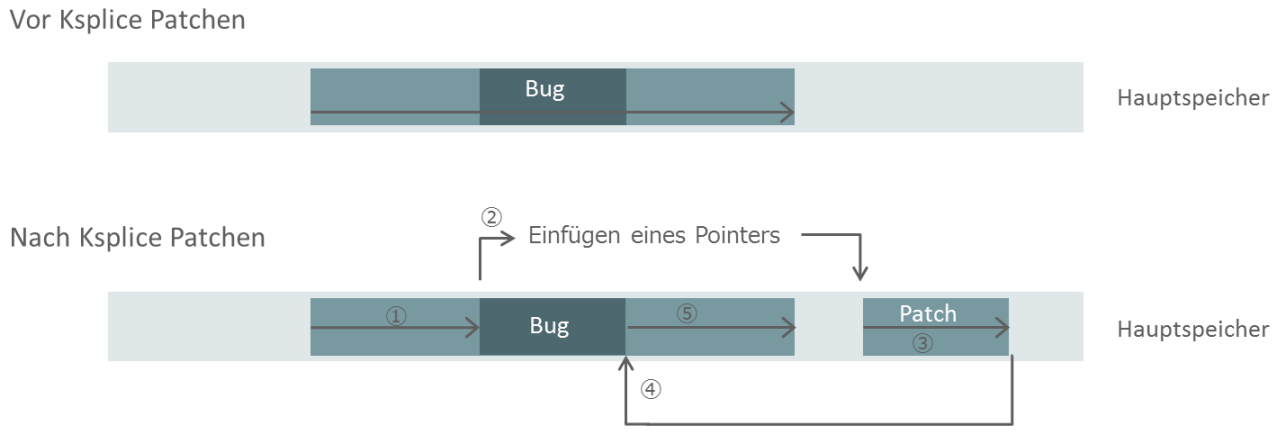

Abb. 1: Ksplice Technologie

Das mit Ksplice gepatchte System speichert sowohl die Ksplice Patches lokal ab, als auch den Status des Kernel bzw. Userspace.
Da alle Änderungen im Speicher passieren, wird im Falle eines Reboot beim nächsten Start des Systems der in der `/etc/grub.conf` eingetragene (alte) Kernel gebootet, während der Startsequenz wird auf den gespeicherten Status vor dem Reboot wieder mittels Ksplice gepatcht. Dies passiert solange, bis das Betriebssystem, somit auch der Kernel, mittels `# yum update` gepatcht wird. Zu diesem Zeitpunkt werden die Dateien des Kernels auf Platte geschrieben und auch die Startreihenfolge in `/etc/grub.conf` auf den neuen Kernel geändert.
Nach dem geplanten Reboot startet das System mit dem aktualisierten Kernel, Ksplice Patches werden dann passend zu diesem Kernel installiert, das heißt, der neue gebootete Kernel bildet die Baseline für die Patches.
Applikationen bekommen von all dem nichts mit, sie profitieren aber von gepatchten Sicherheitslücken bzw. Bux Fixes.

Oracle VM und Ksplice:

Für OVM 3.3 und OVM 3.4 ist seit April 2016 die Möglichkeit des patchen mittels Ksplice gegeben. Siehe: https://blogs.oracle.com/virtualization/entry/oracle_vm_3_4_dom0
Damit können Kunden mit aktivem Support Vertrag für OVM die Vorteile von Ksplice in der Dom0 von OVM genauso nutzen, wie Oracle Linux Kunden. Für OVM 3.3.x kommen die Patches für den UEK3 (Kernel 3.8.13) zum Einsatz, bei OVM 3.4.x die Patches für den UEK4 (Kernel 4.1.12).

Kommandos zur Administration:

Da viele Applikationen die Standard Unix Kommandos nutzen, um Kernelversion, etc. abzufragen, gibt es mit der Installation von Ksplice Uptrack ein Set zusätzlicher Kommandos (`uptrack-upgrade, uptrack-install, uptrack-show, uptrack-remove, uptrack-uname`).
Diese dienen zur Administration von Ksplice Kernel Updates. Ein Beispiel ist das Kommando `uptrack-uname -r`, welches den aktuell laufenden Kernel anzeigt, wohingegen ein gleichzeitig abgesetztes `uname -r` den gebooteten Kernel anzeigt.
Mit der Installation des Ksplice Enhanced Clients (Userspace Ksplice) kommt noch ein weiters Kommando dazu: `ksplice`. Damit wird der Enhanced Client gesteuert, es besteht aber mittels Parametern auch die Möglichkeit, `ksplice` auch zur Administration des Kernels zu verwenden.

Zur Einbindung von Linux und Ksplice in 3rd Party Produkte steht ein RESTful Web API zur Verfügung (http://ksplice.oracle.com/uptrack/api).

Dokumentation:

Oracle Linux 6 Documentation Library: http://docs.oracle.com/cd/E37670_01/index.html
Oracle Linux 7 Documentation Library: http://docs.oracle.com/cd/E52668_01/index.html

Ksplice Documentation: http://docs.oracle.com/cd/E52668_01/E39380/html/index.html

OVM 3.3 Documentation Library: http://docs.oracle.com/cd/E50245_01/index.html
OVM 3.4 Documentation Library: http://docs.oracle.com/cd/E64076_01/index.html

Fazit:

Mittels Ksplice geschützte Oracle Linux Installationen mit Premier Support Vertrag sind wesentlich besser gegenüber Sicherheitslücken und Bugs geschützt, als solche Systeme, die nur zu bestimmten Zeitpunkten (Patchfenstern) mit verfügbaren Patches versorgt werden.

Kein anderer Hersteller außer Oracle kann derzeit ein wirklich produktiv einsetzbares Tool für das unterbrechungsfreie Patchen des Kernel **und** des Userspace anbieten.
Für alle unter Support stehenden Linuxversionen (Oracle Linux 5, 6 und 7) und vor allem für alle auf diesen Versionen verfügbaren Kernel Stände ist Ksplice verfügbar und komfortabel einsetzbar.

Kontaktadresse:
Friedrich-Wolfgang (Fritz) Weinhappl
Oracle Austria
Wagramerstraße 19
1223 Wien
Österreich

Telefon: +43 664 8103 163
Fax: +43 1 33777 333
E-Mail friedrich-wolfgang.weinhappl@oracle.com

Internet: oracle.com/linux
oracle.com/virtualization
ksplice.com

Blog: blogs.oracle.com/linux
blogs.oracle.com/virtualization