
ORACLE®

Zero Downtime Patching von Oracle Linux und Oracle VM

Fritz Weinhappl
Presales Consultant Oracle Linux und Virtualisation
DACH-Region

ORACLE

Safe Harbor Statement

The following 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.

Agenda

- Oracle Linux / Oracle VM
- Ksplice
- Demo

Überblick Oracle Linux

- Oracle Linux ist 100% binärkompatibel mit Red Hat Enterprise Linux
- Wird mit zwei Kernel Optionen ausgeliefert:
  - **Unbreakable Enterprise Kernel** (UEK = Default-Kernel)
  - Red Hat Compatible Kernel (RHCK) – Bietet einen einfachen Migrationsweg für bestehende Red Hat Kunden
    - Kunden, die RHEL benutzen, müssen das OS **nicht** neu installieren.
    - Applikationen, welche auf RHEL supportet sind, laufen 1:1 auch auf Oracle Linux.
- Bewährter, globaler 7x24 Support mit den Oracle Linux Basic bzw. Premier Wartungsverträgen.
- Unbreakable Linux Network (ULN)
  - Bug fixes, Security Updates, CVE Informationen

ORACLE

Oracle Linux Angebot

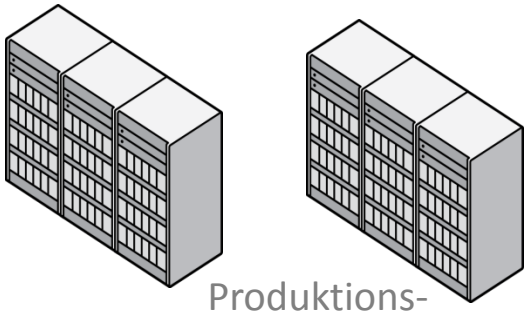
Unser Angebot, kein “Lock-In”

- Frei downloadbar
- Frei zu verteilen
- Frei nutzbar
- Sie wählen den Support Level individuell pro Server
- Das selbe OS und die selben Updates / Errata auf allen Systemen (Produktion, QA, Entwicklung)
- Offene Linuxentwickung – alle Änderungen sind in der Public Git Repository hinterlegt

ORACLE

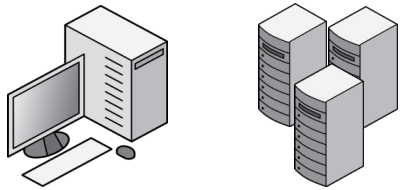
Vereinfachen Sie ihre Entwicklungs- und Produktionsumgebung

RHEL



Produktions-Systeme

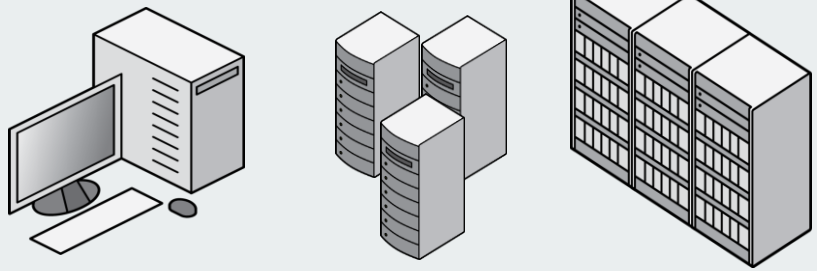
CentOS



Entwickler Workstations

Test Umgebung

Oracle Linux



Entwickler Workstations

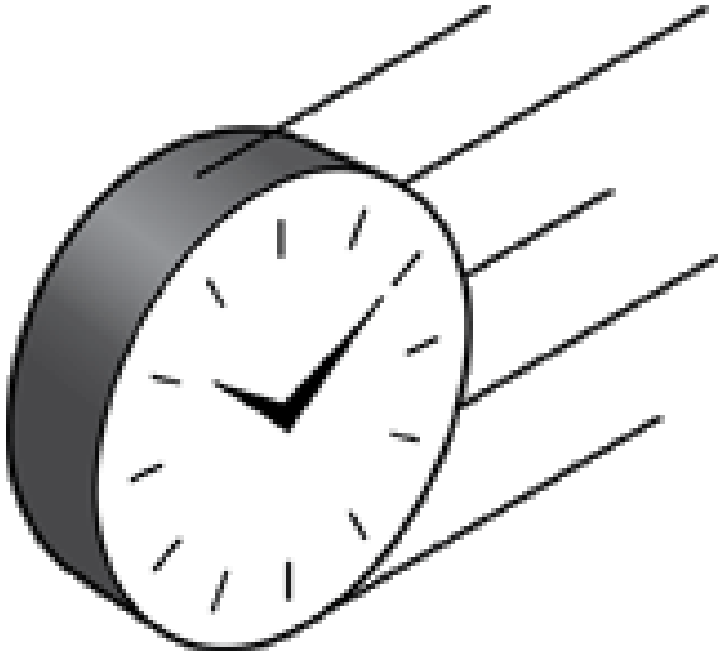
Test Umgebung

Produktions-Systeme

Vermeidung von teuren Unterbrechungen

Ein Reboot hat viele Auswirkungen

- Jeder Reboot eines Produktivsystems beeinflußt auch Systeme, die mit diesem verbunden bzw. von diesem abhängig sind:
  - Middleware Systeme
  - Datenbank Systeme
  - Storage Systeme
  - Applikations Systeme
- Gastsysteme müssen migriert werden – d. h. ausreichend Resourcen verfügbar sein!
- Auswirkungen auf andere Abteilungen in einer Organisation.



Oracle VM

- Für Oracle-Software und Drittanbieter-Anwendungen
- KnowHow & Support für:
  - Datenbank & Betriebssystem
  - Applikations-Server & Middleware
  - Business Applikationen
- Integriert in Oracle's Engineered Systems
- Die **einzige vollständig** zertifizierte Virtualisierungslösung für Oracle Produkte

- **Keine Lizenzkosten**
- **Hohe Performance**
- **24x7 Enterprise Support**
- **Schnellere Applikationsverteilung**
- **Zentrales Management – EM13c**

(von der Hardware bis zur Applikation)

ORACLE VM

ORACLE

Oracle VM und Oracle Linux

- Entwickelt in enger Zusammenarbeit von OL und OVM Teams
- Oracle VM Server nützt den Unbreakable Enterprise Kernel von Oracle Linux (UEK4)
- Gemeinsame Entwicklung, um hohe I/O-Leistung für virtualisierte Anwendungen bieten zu können
- OpenSource Produkte, Patches über Yum Server, geringe Kosten für Support
- Einfache, schnelle und sichere Installation von Oracle Anwendungen mittels Oracle Templates

Oracle Linux, Oracle VM und Ksplice

Zero-Downtime Kernel Diagnose und Patchen

- Kernelprobleme in Produktionsumgebungen ohne Ausfallzeiten (downtime, reboot) diagnostizieren
- Übernehmen von Kernel-Updates (Bugs und Sicherheitspatches) ohne Neustart des Systems
- Erhöhen des Sicherheitsstandards von kritischen Systemen durch einspielen der neuesten Patches / Errata ohne Auswirkungen auf die Applikationen
- Flexible Einsatzmöglichkeiten um bestehende operativen Prozesse zu ergänzen

ORACLE

Agenda

- Oracle Linux / Oracle VM
- Ksplice
- Demo

Ksplice - Kernel Security und Bug Fixes

Zero downtime Patching

Patchen ohne Reboot des Betriebssystems bzw. ohne Unterbrechung von Applikationen bzw. Gastsystemen.
Nicht nur der Kernel, sondern auch **Userspace** Applikationen können gepatcht werden:

glibc und **openssl**

Rollback

Falls etwas mit dem eingespielten Patch nicht passt, kann dieser wieder ohne Downtime entfernt werden.

Diese Funktion wird auch für Diagnosezwecke durch unseren Support benutzt (Debug Kernel)

Schnelle Errata Veröffentlichung

Oracle liefert nach der Veröffentlichung der Patch Daten den Patch zur Nutzung mit Ksplice nach ausführlichen Tests so schnell wie möglich.

Bewährte Technologie

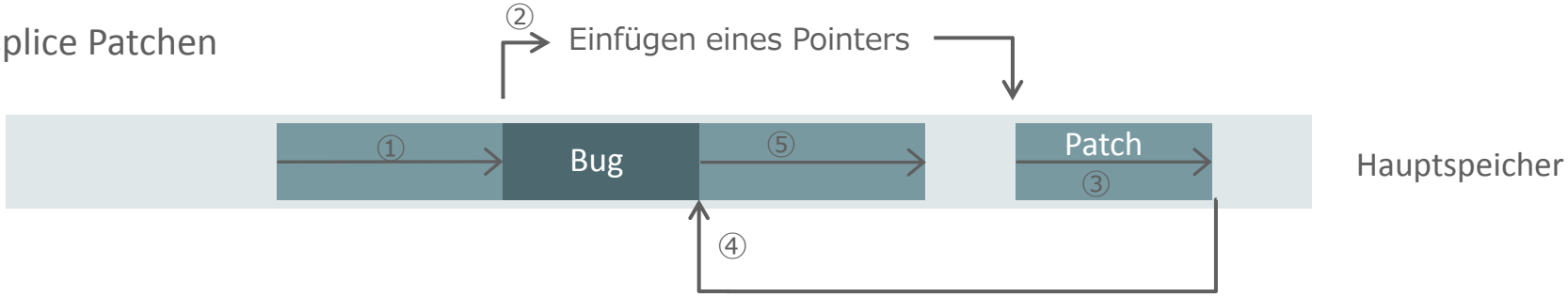
Gegründet 2008 (MIT)
Teil von Oracle seit 2011
Über 250000 Systeme mittels Ksplice geschützt

Ksplice Technologie

Ksplice

Vor Ksplice Patchen

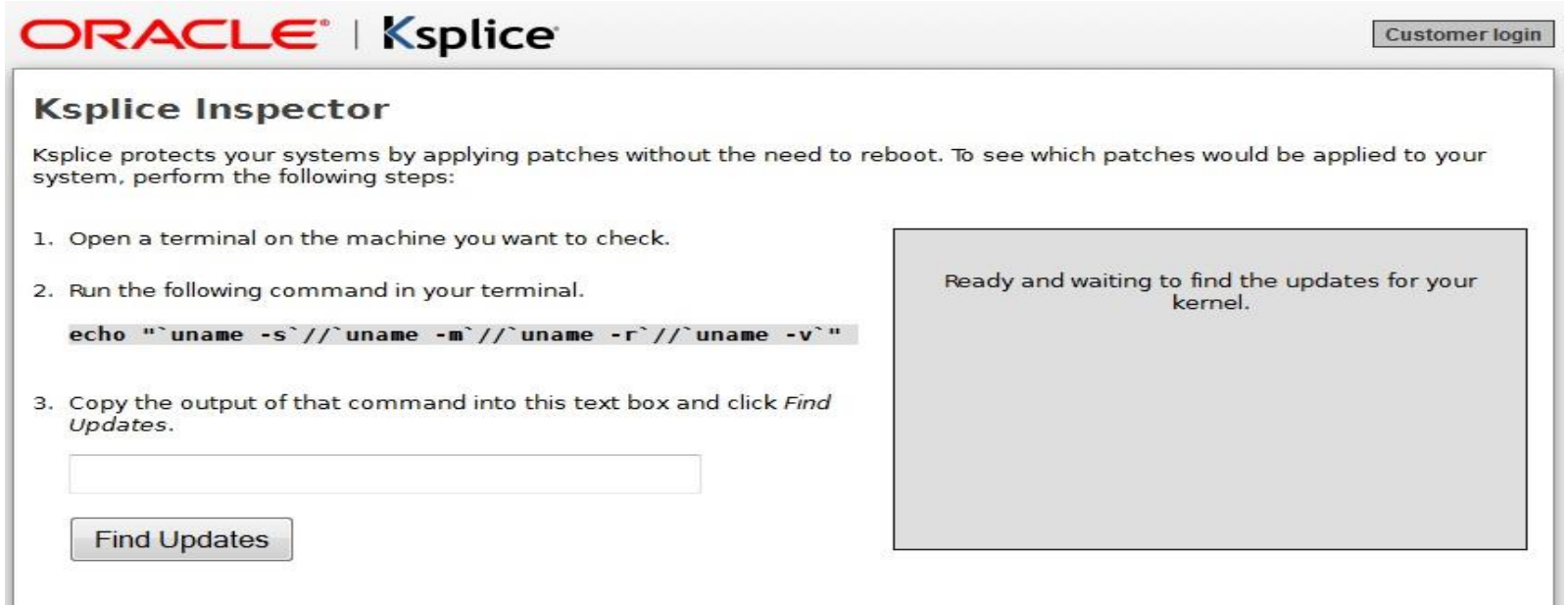
Nach Ksplice Patchen



ORACLE

Ksplice Inspector

- https://ksplice.oracle.com/inspector
- Überprüfung des Patch Level Ihres Kernels und Ausgabe der benötigten Patches

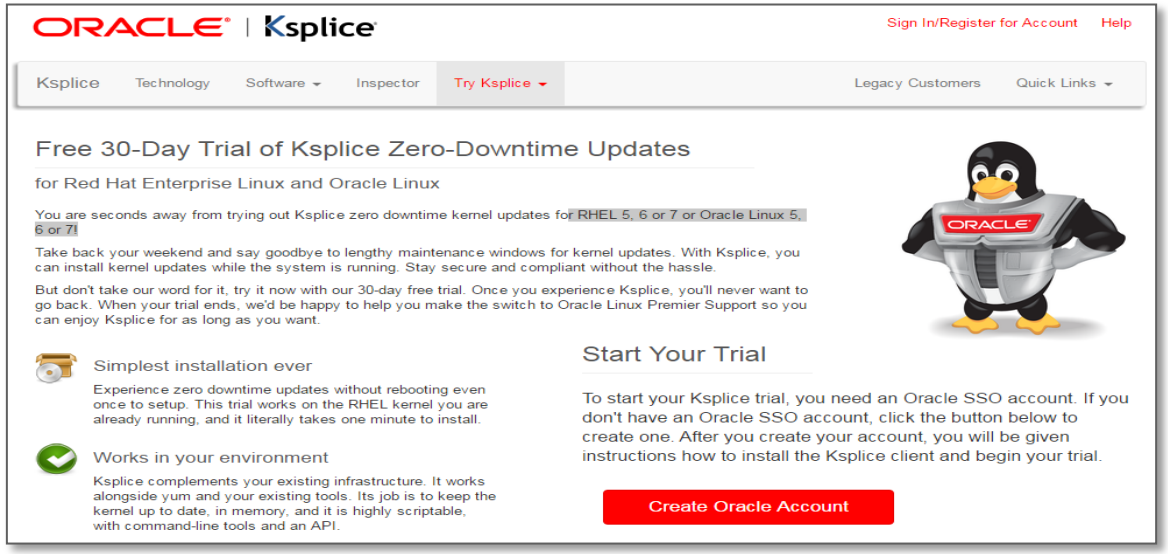


Ksplice 30 Tage testen

Ksplice

http://ksplice.oracle.com/try/trial

- Einfache Registrierung, danach 30 Tage testen
- Oracle Linux 5,6 und 7 und RHEL 5,6 und 7 werden unterstützt

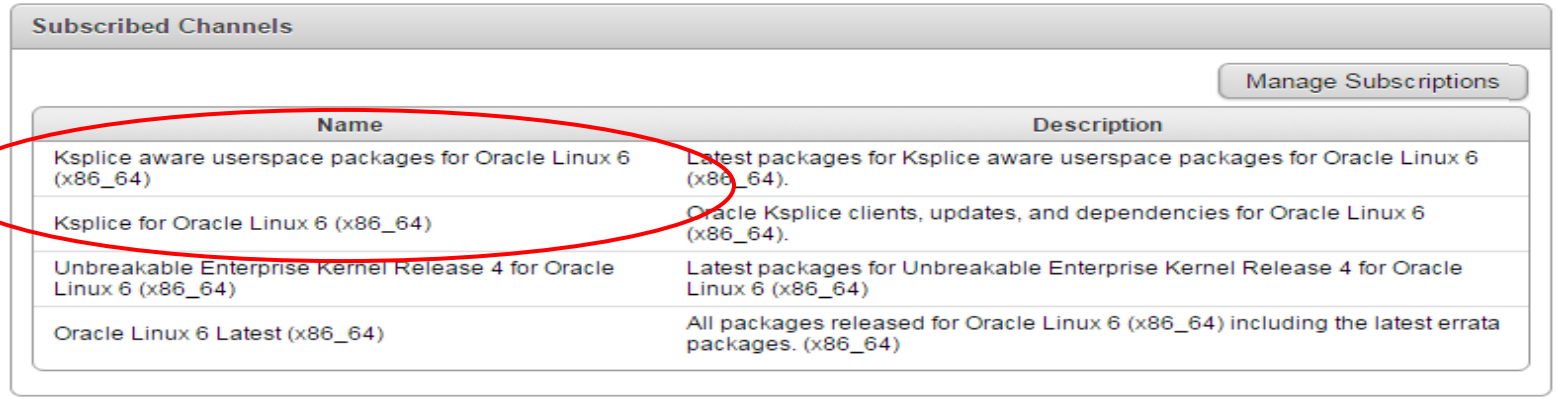


ORACLE

Einfache Installation

Ksplice

- Einen ULN Account registrieren (Premier Support bzw. Trial)
- Server im ULN registrieren
- Ksplice Channel zum Server hinzufügen (Auf der ULN Webseite)



- Install uptrack

```
# yum install -y uptrack
```

- Fertig. Kein Reboot notwendig.

ORACLE

Ksplice Command Line Tools (1/4)

uptrack-show Kommando

- Listet die Kernelpatches, die installiert sind

```
# uptrack-show
Installed updates:
[guclwyc2] CVE-2012-0957: Information leak in uname syscall.
[j4d07e02] Kernel panic in IPv4 ARP and IPv6 Neighbor Discovery.
[r8og1ec4] CVE-2013-1979: Privilege escalation with UNIX socket credentials.
#
```

Ksplice ID

- Mit der --available Option sieht man alle verfügbaren Patches.

```
# uptrack-show --available
Available updates:
[fiq04xbb] CVE-2013-2237: Information leak on IPSec key socket.
[9q4luou3] CVE-2014-3687: Remote denial-of-service in SCTP stack.
#
```

Ksplice Command Line Tools (2/4)

uptrack-upgrade Kommando

- Kommando zum Installieren aller verfügbaren Patches.

```
# uptrack-upgrade -y
The following steps will be taken:
Install [guclwyc2] CVE-2012-0957: Information leak in uname syscall.
Install [j4d07e02] Kernel panic in IPv4 ARP and IPv6 Neighbor Discovery.
Install [r8og1ec4] CVE-2013-1979: Privilege escalation with UNIX socket credentials.
Install [fiq04xbb] CVE-2013-2237: Information leak on IPSec key socket.
Install [9q4luou3] CVE-2014-3687: Remote denial-of-service in SCTP stack.
Installing [guclwyc2] CVE-2012-0957: Information leak in uname syscall.
Installing [j4d07e02] Kernel panic in IPv4 ARP and IPv6 Neighbor Discovery.
Installing [r8og1ec4] CVE-2013-1979: Privilege escalation with UNIX socket credentials.
Installing [fiq04xbb] CVE-2013-2237: Information leak on IPSec key socket.
Installing [9q4luou3] CVE-2014-3687: Remote denial-of-service in SCTP stack.
Your kernel is fully up to date.
Effective kernel version is 2.6.39-400.215.13.el6uek
#
```

- Mit uptrack-install <Ksplice ID> kann ein einzelner Patch installiert werden.

```
# uptrack-upgrade guclwyc2 -y
The following steps will be taken:
Install [guclwyc2] CVE-2012-0957: Information leak in uname syscall.
Installing [guclwyc2] CVE-2012-0957: Information leak in uname syscall.
Your kernel is fully up to date.
#
```

ORACLE

Ksplice Command Line Tools (3/4)

uptrack-remove Kommando

- Kommando zum Entfernen aller installierten Patches.

```
# uptrack-remove -y
The following steps will be taken:
Remove [guclwyc2] CVE-2012-0957: Information leak in uname syscall.
Remove [j4d07e02] Kernel panic in IPv4 ARP and IPv6 Neighbor Discovery.
Remove [r8og1ec4] CVE-2013-1979: Privilege escalation with UNIX socket credentials.
Remove [fiq04xbb] CVE-2013-2237: Information leak on IPSec key socket.
Remove [9q4luou3] CVE-2014-3687: Remote denial-of-service in SCTP stack.
#
# uptrack-show
Installed updates:
None
#
```

- Mit uptrack-remove <Ksplice ID> kann ein einzelner Patch entfernt werden (Abhängigkeiten werden berücksichtigt).

```
# uptrack-remove -y 9q4luou3
The following steps will be taken:
Remove [9q4luou3] CVE-2014-3687: Remote denial-of-service in SCTP stack.
#
```

Ksplice Command Line Tools (4/4)

uptrack-uname Kommando

- Das uname Kommando liefert die Kernelversion auf der Disk. Für die aktuell laufende Kernelversion benötigt man uptrack-uname.
  - Vor der Installation von Ksplice Patches:

```
# uptrack-show
Installed updates:
None
# uname -r
2.6.39-300.26.1.el6uek.x86_64
# uptrack-uname -r
2.6.39-300.26.1.el6uek.x86_64
```

  - Nach der Installation von Ksplice Patches:

```
# uptrack-upgrade -y
The following steps will be taken:
Install [guclwyc2] CVE-2012-0957: Information leak in uname syscall.
...
Installing [9q4luou3] CVE-2014-3687: Remote denial-of-service in SCTP stack.
Your kernel is fully up to date.
Effective kernel version is 2.6.39-400.215.13.el6uek
# uname -r
2.6.39-300.26.1.el6uek.x86_64
# uptrack-uname -r
2.6.39-400.215.13.el6uek.x86_64
```

Ksplice Konfigurationsdatei

/etc/uptrack/uptrack.conf

- Hier können diverse Parameter gesetzt werden:

```
https_proxy = https://proxy_URL:https_port

autoinstall = yes

install_on_reboot = yes

upgrade_on_reboot = yes
```

Uptrack API Tools

RESTful Web API

- Die Kommand Line API Tools sind im **python-ksplice-uptrack** Paket verfügbar.
- Details darüber auf unseren Webseiten:
  - http://ksplice.oracle.com/uptrack/api
  - https://docs.oracle.com/cd/E37670_01/E39380/html/ol_kspapi.html

Ksplice Enhanced Client (Userspace)

- Neue Funktion seit Q3/2015
- Ksplice Enhanced Client kann in-memory pages von shared Libraries patchen, die für Ksplice vorbereitet sind.
- Derzeit für **glibc** and **openssl** userspace Libraries verfügbar.
- Benötigt zusätzliches Paket, um den Ksplice Enhanced Client zu installieren:

```
# yum install -y ksplice
```

- Danach ist ein Update der beiden Libraries notwendig, um die Ksplice fähigen Versionen beider Libraries nutzen zu können:

```
# yum update *glibc *openssl*
```

ORACLE

Ksplice Enhanced Client Kommandos (1/3)

ksplice all list-targets Kommando

- Kommando zum Anzeigen der laufenden Userspace Prozesse, welche gepatcht werden können.

```
# ksplice all list-targets
User-space targets:

glibc-ISO8859-1-2.17.78.0.1.1.ksplice25.el7
  └─ gnome-shell (3783)

glibc-libutil-2.17.78.0.1.1.ksplice25.el7
  ├─ firewalld (680)
  ├─ tuned (695)
  ├─ libvirtd (1492)
  ├─ sshd (1497)
  ├─ httpd (1503)
  ├─ httpd (1706)
  ├─ httpd (1707)
```

⋮

```
  ├─ abrt-applet (3980)
  ├─ tracker-miner-f (4040)
  ├─ gvfsd-trash (4062)
  ├─ sshd (29328)
  ├─ packagekitd (29465)
  └─ python (29679)
...
Kernel version: Linux/x86_64/3.10.0-229.el7.x86_64/#1 SMP Fri Mar 6 04:05:24 PST 2015
```

ORACLE

Ksplice Enhanced Client Kommandos (2/3)

ksplice all show Kommando

- Kommando zum Anzeigen aller installierten Userspace und Kernel Updates.

```
# ksplice all show
httpd (1706)
httpd (1708)
httpd (1707)
rsyslogd (689)
chronyd (705)
httpd (1503)
  ├─ [h73qvumn]: CVE-2014-7817: Command execution in wordexp().
  └─ [ml55ngz4]: CVE-2015-1781: Privilege escalation in gethostbyname_r().

Ksplice kernel updates installed:

Installed updates:
[rfywob9d] Clear garbage data on the kernel stack when handling signals.
[6w5ho5e2] Provide an interface to freeze tasks.
```

⋮

```
[89yjgn50] CVE-2015-3636: Memory corruption when unhashing IPv4 ping sockets.
[g327jyvw] CVE-2015-2922: Denial-of-service of IPv6 networks when handling router advertisements.
```

Ksplice Enhanced Client Kommandos (3/3)

ksplice user show Kommando

- Kommando zum Anzeigen von Userspace Updates, die zu einer PID gehören.

```
# ksplice user show --pid=705
 chronyd (705)
 ├─ [h73qvumn]: CVE-2014-7817: Command execution in wordexp().
 └─ [ml55ngz4]: CVE-2015-1781: Privilege escalation in gethostbyname_r().
```

- Mit dem **remove** Subkommando können alle Updates eines Prozesses entfernt werden.

```
# ksplice user remove --all --pid=705]
```

- Um einen speziellen Patch zu entfernen, muß das Subkommando **undo** verwendet werden.

```
# ksplice user undo --pid=705 h73qvumn
```

ORACLE

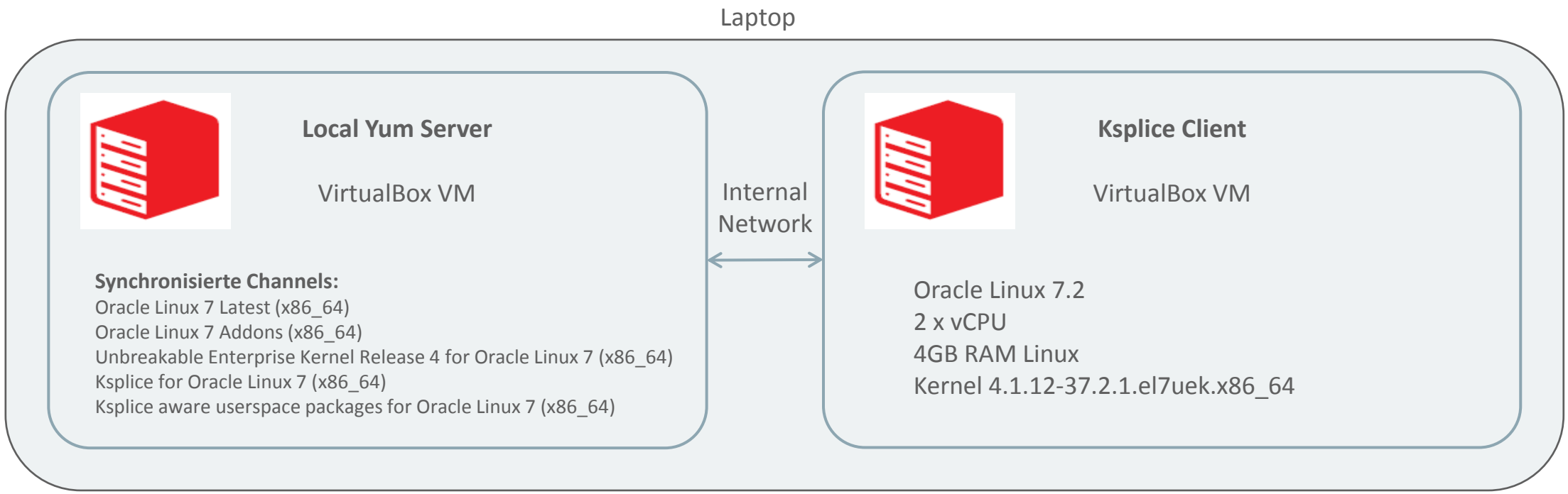
Agenda

- Oracle Linux / Oracle VM
- Ksplice
- Demo

Demo

Ksplice

- Demo Umgebung:



ORACLE

Integrated Cloud

Applications & Platform Services


ORACLE®