



Achieve a 0-downtime CERN Database infrastructure

Summer Student: Varsha Rao
Supervisor: Borja Aparicio Cotarelo
IT-DB-IMS

Why is it required?

- Security vulnerabilities
- Difficulty in scheduling downtime
- Hardware consolidation



What can be done?

What can be done?



Live Kernel Patching

“Hot patching, also known as live patching or dynamic software updating, is the application of patches without shutting down and restarting the system or the program concerned.”

- Wikipedia Definition

Comparison

Use Cases



Ksplice

- Runtime security vulnerabilities and stability bugs.

Kpatch

- Urgent security and stability fixes, CVEs, driver issues and kernel development.

Comparison

License



Ksplice

- It was originally GPLv2, after Oracle acquisition it is no longer.

Kpatch

- GPLv2

Comparison

Is it merged into Kernel Mainline?



Ksplice

- No

Kpatch

- Yes

Live Patching Technology



Comparison *Status*



Ksplice

- Production ready

Kpatch

- Not production ready

Comparison

Operating System



Ksplice

- Support available only for Oracle Linux.
- Community Edition is provided for Fedora and Ubuntu.

Kpatch

- Support is only available for RHEL.
- Available on major Linux distros.

Comparison Installation



For both of them, the installation process is

- Easy and quick
- Well documented

What did we do

- Understand both Kpatch and Ksplice

What did we do

- Understand both Kpatch and Ksplice
- Install both of them

What did we do

- Understand both Kpatch and Ksplice
- Install both of them
- Test and Verify the features

Features

	Ksplice	Kpatch
License	Initially GPLv2	GPLV2
Patch Provisioning	Lacks transparency	Patch can be built easily
Dependency	Yes, Oracle Updates	Optional, RedHat Updates

Ksplice

```
██████████ # uptrack-upgrade -y → { Install Command }
```

The following steps will be taken:

Install [fnk2i8lq] Workaround for alternative instruction inconsistencies.

Install [ij6564y4] Clear garbage data on the kernel stack when handling signals.

Install [hgdep9fv] Provide an interface to freeze tasks.

Install [k98laohw] Connection loss when forwarding between network namespaces.

Installing [fnk2i8lq] Workaround for alternative instruction inconsistencies.

Installing [ij6564y4] Clear garbage data on the kernel stack when handling signals.

Installing [hgdep9fv] Provide an interface to freeze tasks.

Installing [k98laohw] Connection loss when forwarding between network namespaces.

Your kernel is fully up to date.

Effective kernel version is 3.10.0-862.9.1.el7

Kpatch

```
# Build Patch Module
██████████ # kpatch-build -t vmlinux kpatch_version.patch
Using cache at /root/.kpatch/src
Testing patch file(s)
Reading special section data
Building original kernel
Building patched kernel
Extracting new and modified ELF sections
version.o: changed function: version_proc_show
Patched objects: vmlinux
Building patch module: livepatch-kpatch_version.ko
SUCCESS
# Load Module
██████████ # kpatch load → { Loads Patch Module }
loading patch module: livepatch-kpatch_version.ko
waiting (up to 15 seconds) for patch transition to complete...
transition complete (2 seconds)
```

{ Builds Patch Module }

Conclusion

- Live Kernel Patching Works
- Requires long term evaluation
- General Kernel Upgrade is not possible
- Depends on sysadmin requirements



Thanks!!

varsha.rao@cern.ch
rvarsha016@gmail.com

