



*“If it doesn’t fit,
try a bigger
hammer!”*

– Bob the builder

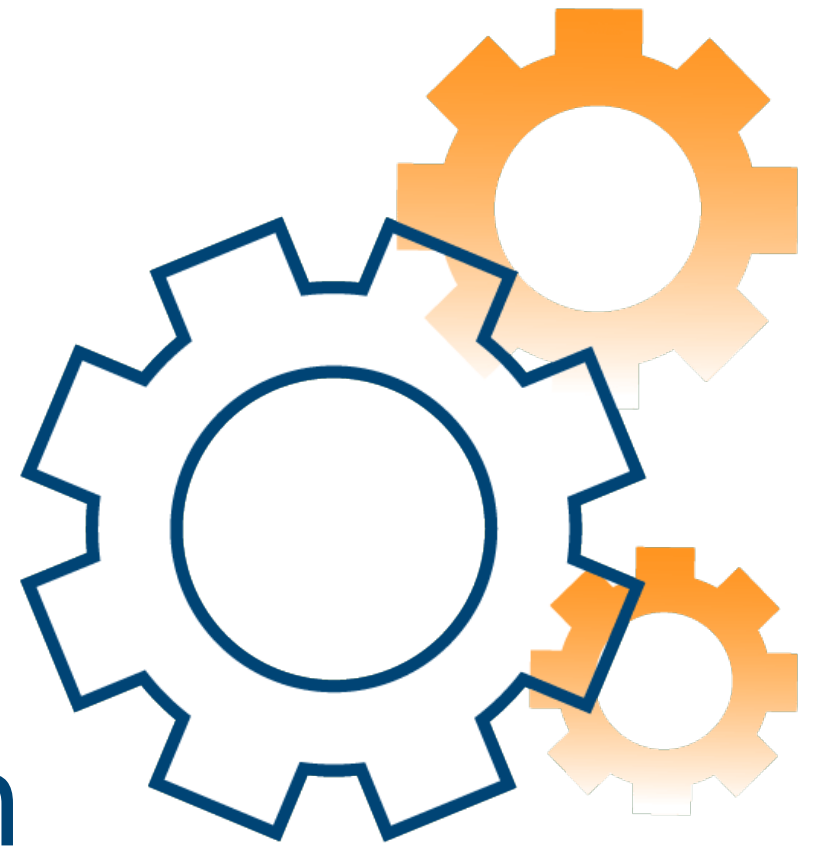




The Linux & Open Source Company

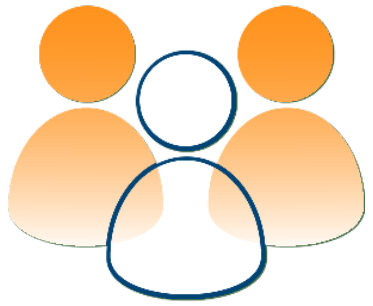
Live Patching & Foreman

How it fits together...

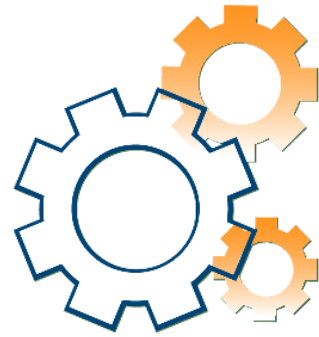


Bernhard Suttner

THE Linux & Open Source Company!



Consulting



Engineering



Support



Training





orcharhino 
🔄 DEPLOY ⚙️ RUN ✅ CONTROL SIMPLIFY YOUR DATACENTER

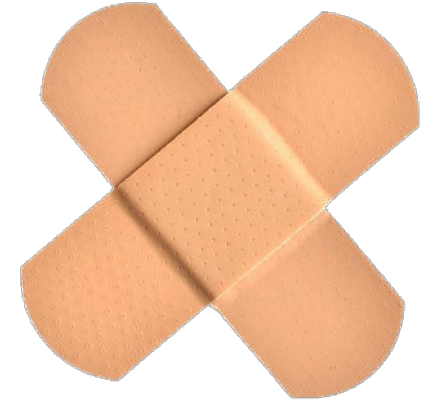
Why should I live-patch my Kernel?

- Security!
- Mission critical systems
- No scheduled maintenance
- No down-time
- It just works



... because your kernel is vulnerable!

Linux live patching tools



OS vendor solutions

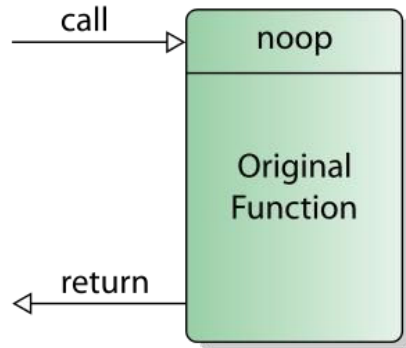
- Oracle: ksplice
- Red Hat: kpatch
- SUSE: kGraft
- Ubuntu: Livepatch service

OS-independent

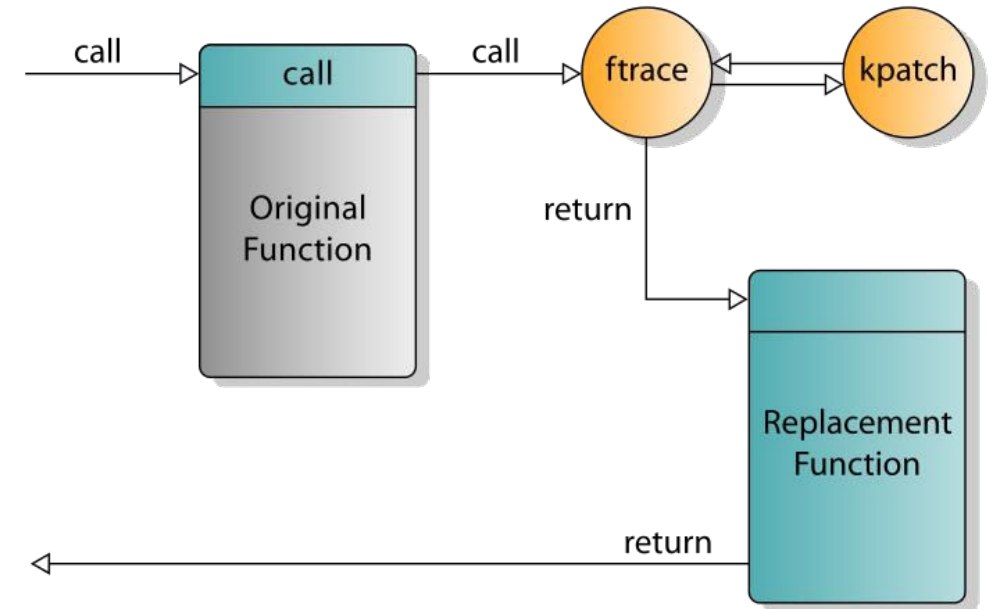
TuxCare KernelCare solution available for a lot of systems – but not SUSE

How it works?

**Before
patching**



**After
patching**



source: https://en.wikipedia.org/wiki/Kpatch#/media/File:Linux_kernel_live_patching_kpatch.svg

Example: live patch RHEL kpatch

```
root@redhat8-219:~  
[root@redhat8-219 ~]# uname -r  
4.18.0-305.el8.x86_64  
[root@redhat8-219 ~]# echo "kpatch-patch = $(uname -r)"  
kpatch-patch = 4.18.0-305.el8.x86_64  
[root@redhat8-219 ~]# dnf install -y "kpatch-patch = $(uname -r)"  
Failed to set locale, defaulting to C.UTF-8  
Updating Subscription Management repositories.  
Puppet 7 EL8  
RHEL Client 8  
Kernel Care EL8  
Saltstack EL8  
EPEL 8  
Dependencies resolved.  
=====
```

Package	Architecture	Version	Repository	Size
---------	--------------	---------	------------	------

```
=====
```

Installing:				
kpatch-patch-4_18_0-305	x86_64	1-6.el8	rhel-8-for-x86_64-baseos-rpms	49 k

```
=====
```

Transaction Summary

```
=====
```

Install 1 Package

Installed:

kpatch-patch-4_18_0-305-1-6.el8.x86_64

Complete!

FOREMAN

ATIX ▾ Any Location ▾

Admin User

Monitor

Content

Containers

Hosts

Configure

Infrastructure

Administer

Overview

Filter ... × 🔍 Search ▾

Generated at 23 Aug 12:36 Manage ▾ ↺ Documentation

Host Configuration Status for All ×

Hosts that had performed modifications without error

Hosts in error state

Good host reports in the last 30 minutes

Hosts that had pending changes

Out of sync hosts

Hosts with no reports

Hosts with alerts disabled

0

0

0

0

0

5

0

Total Hosts: 5

Host Configuration Chart for All ×

100%

No report

Host Configuration Status for Puppet ×

Hosts that had performed modifications without error

Hosts in error state

Good host reports in the last 35 minutes

Hosts that had pending changes

0

0

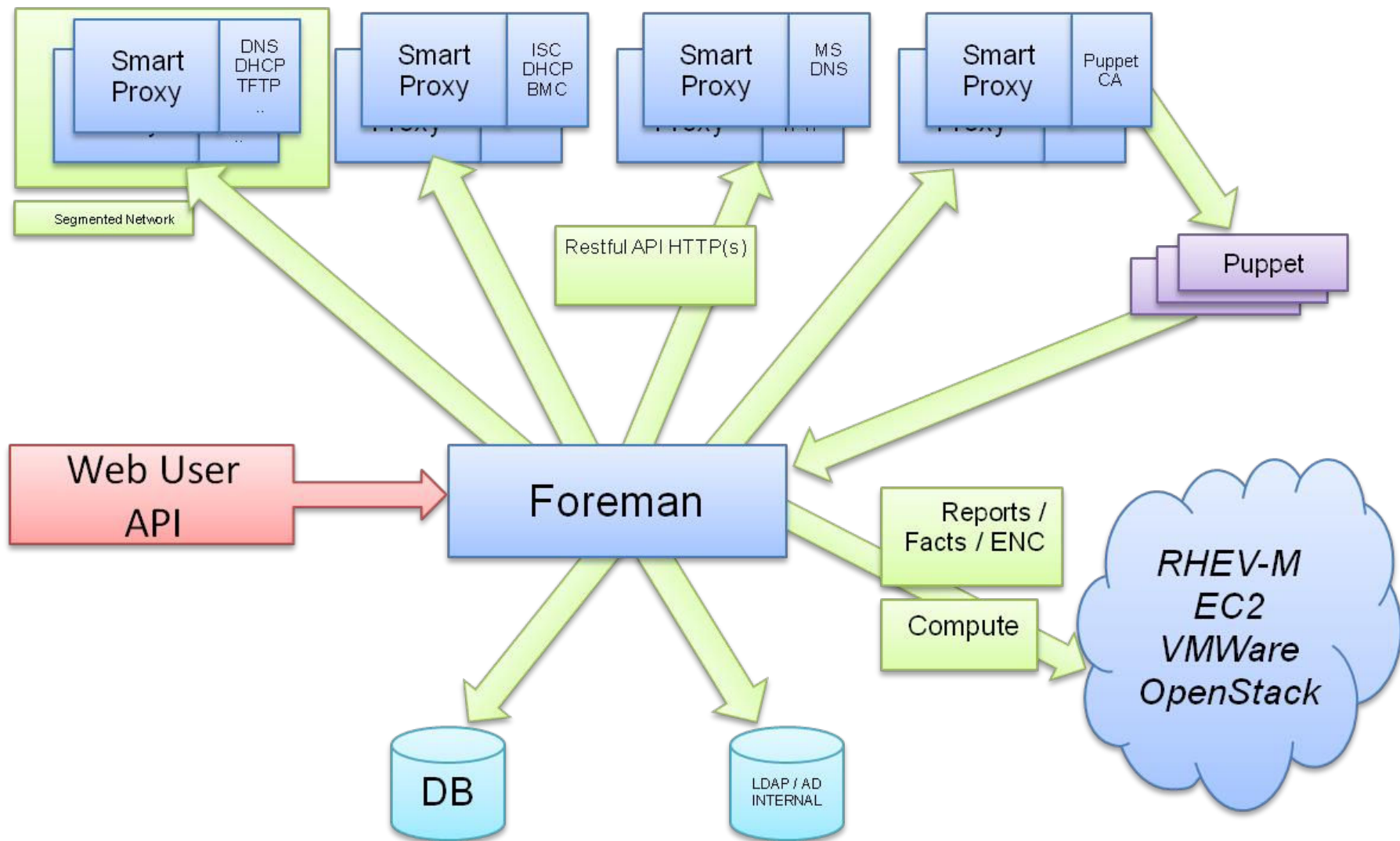
0

0

Host Configuration Chart for Puppet ×

No Data Available

atix.de



The Foreman / Katello world



- Lists installed packages on a host
- Manages installation / update of packages
- Lists services and if the host itself need to be restarted
- Supports to restart services / the host itself

See:

<https://github.com/theforeman>

<https://github.com/katello>

Package management



redhat8-219.nr.nine

Unregister Host

[Content Hosts](#) > [redhat8-219.nr.nine](#) > Installed Packages

[Details](#) [Provisioning Details](#) [Subscriptions](#) [Host Collections](#) [Tasks](#) [Packages ▼](#) [Errata](#)
[Module Streams](#) [Traces](#) [Repository Sets](#)

Installed Packages



Search



Remove Selected

0 of 2 Selected



Installed Package



kernel-4.18.0-425.10.1.el8_7.x86_64



kernel-4.18.0-305.el8.x86_64

200 ▼

per page

Showing 1 - 2 of 2



1

of 1



Foreman Remote Execution



- Run any command using SSH or Ansible
- Install kernel updates
- Install live patching tool
- Install kernel patches
- Receive and validate the live patching state

Install a Kernel patch with Foreman REX

Jobs > Job invocation

Job category *

Job template *

Bookmark

Search Query

Resolves to 1 hosts

command ⓘ *

> [Display advanced fields](#)

Type of query ⓘ ☒ Static Query
☐ Dynamic Query

Schedule ☒ Execute now ☐ Schedule future execution
☐ Set up recurring execution

Show kernel patch information with Foreman REX



Jobs > Job invocation

Job category *

Job template *

Bookmark

Search Query

Resolves to 1 hosts  

command ⓘ *

```
echo "List installed kernel patches"
kpatch list
echo
echo "Its a kernel module"
lsmod | grep kpatch
echo
echo "Show kpatch changes"
rpm -q --changelog kpatch-patch-4_18_0-305-1-6.el8.x86_64
```

> Display advanced fields

Type of query ⓘ ☒ Static Query ☐ Dynamic Query

Schedule ☒ Execute now ☐ Schedule future execution ☐ Set up recurring execution

Ooops!

Installed Packages

0 of 1 Selected

- | | |
|--------------------------|----------------------------------|
| <input type="checkbox"/> | Installed Package |
| <input type="checkbox"/> | kernel-4.18.0-425.3.1.el8.x86_64 |

20 per page

Showing 1 - 1 of 1



1 of 1



Traces

Tracer helps administrators identify applications that need to be restarted after a system is patched.

0 of 1 Selected

<input type="checkbox"/>	Application	Type	Helper
<input type="checkbox"/>	kernel	static	You will have to reboot your computer

20 per page

Showing 1 - 1 of 1



1 of 1



So, how does it fit?

- Wrong package lists
- Wrong traces / kernel state

=> No “nice” kernel live patch administration support



Do you know KernelCare?

- Delivers kernel patch through a cloud service / ePortal
- Management tool `kcarectl`
- Auto-Mode
- Patch after reboot



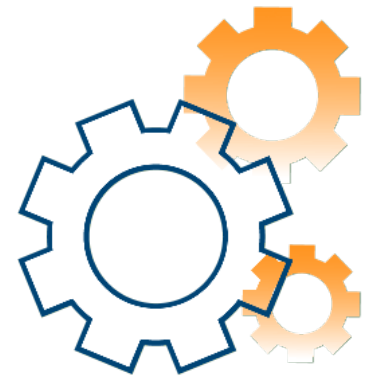
Improvement: foreman_kernel_care

- Currently supported for: dnf/yum based EL
- Keep kernel package list on Foreman/Katello up-to-date
- Removes trace to restart host
- WIP: Debian/Ubuntu support

It's an open source project.

Contributions are welcome.

See: https://github.com/maccelf/foreman_kernel_care



foreman_kernel_care: how it works

- Modifies Foreman / Katello traces
- Gets kernel care version
- Updates package list



Issue solved? Time to go home?



Integration expectations (1)

Kernel live patching

https://foreman.local

Kernel live patching

Name	OS	Auto patch	Installed kernel	Running kernel	Actions
centos.local	CentOS 9 Stream	<input checked="" type="checkbox"/>	4.18.10	4.18.13	<input type="button" value="Install Pkg"/>
ubuntu.local	Ubuntu 22.04	<input type="checkbox"/>	4.31.7	4.31.8	<input type="button" value="Patch"/> <input type="button" value="Install Pkg"/>
alma.local	Alma Linux 8	<input type="checkbox"/>	4.29.3	4.29.4	<input type="button" value="Patch"/> <input type="button" value="Install Pkg"/>
debian.local	Debian Bullseye	<input checked="" type="checkbox"/>	4.25.7	4.25.8	<input type="button" value="Install Pkg"/>
suse.local	SuSE 15 SP2	<input checked="" type="checkbox"/>	4.28.3.1	4.28.3.1	<input type="button" value="Install Pkg"/>

Integration expectations (2)

- Which host and which tool?
- Activate / deactivate live patching
- Independent (kpatch, kGraft, KernelCare)
- No reboot-warning
- Use build-in tools like REX



If you have any questions...



sbernhard @ #theforeman-dev



<https://github.com/sbernhard>



suttner@atix.de

