



Live Kernel Patching Using kGraft

SUSE Linux Enterprise Server 12

This document describes the basic principles of the kGraft live patching technology. kGraft is a live patching technology for run-time patching of the Linux kernel, without stopping the kernel. This maximizes system uptime, and thus system availability, which is important for mission critical systems. By allowing dynamic patching of the kernel, the technology also encourages users to install critical security updates without deferring them to a scheduled downtime.

A kGraft patch is a kernel module, limited to replacing whole functions and constants in the kernel. kGraft offers tools for creating the live patch modules.

Publication date: 07/02/2017

Contents

- 1 Advantages of kGraft 2
- 2 Installing kGraft Patches 2
- 3 Removing a kGraft Patch 3

1 Advantages of kGraft

Live kernel patching using kGraft is especially useful for quick response in emergencies (when serious vulnerabilities are known and should be fixed as soon as possible or when the systems are already actively exploited). It is not used for scheduled updates where time is not critical.

The main advantage of kGraft is that it never requires stopping the kernel, not even for a short time period like competing technologies.

A kGraft patch is a `.ko` kernel module in a KMP RPM package. It is inserted into the kernel using `insmod` command when the RPM package is installed or updated. kGraft replaces whole functions in the kernel, even if they are being executed. An updated kGraft module can replace an existing patch if necessary.

kGraft has also some technical limitations. It is designed for fixing critical bugs, that means primarily for simple changes. Changes in kernel data structure require special care and, if the change is too large, rebooting might be required.

2 Installing kGraft Patches

To apply a kGraft patch, follow these steps:

1. Using `zypper`, install the kGraft patch from kGraft channel. Choose the appropriate patch for your kernel version (`-default` or `-xen`).

When installing the first patch, the `kgraft` package with the necessary kGraft scripts is also installed.

2. The kernel is patched automatically after the package installation. However, the old kernel functions are not completely removed until all sleeping processes wake up and get out of the way. This can take a considerable amount of time. Sleeping processes using the old kernel functions are not considered a security issue, however, in the current version of kGraft, it is not possible to apply another kGraft patch until the previous patch is completely finished.

First, check the global flag in `/sys/kernel/kgraft/in_progress`. The value `1` signifies existing sleeping processes that still need an update, the value `0` signifies that the patch was completely finished.

To get a list of all sleeping processes, check the number in [/proc/process_number/kgr_in_progress](#) for each process. The value 1 signifies sleeping process that still needs an update.

3. It is up to the system administrator to decide how to deal with the sleeping processes. One possibility is to wait, another possibility is to send a SIGSTOP signal followed by a SIGCONT signal to all the sleeping processes.

3 Removing a kGraft Patch

It is not sufficient to simply remove a kGraft patch with zypper. Rebuilding initrd and rebooting is required:

1. First remove the patch itself using zypper:

```
zypper rm kgraft-patch-default
```

2. Rebuild the initrd:

```
mkinitrd
```

3. Reboot the machine.