One more essential step towards zero downtime: SUSE Linux Enterprise Live Patching

1. Introduction

In today’s service-oriented IT, zero downtime becomes more and more a must-have feature. This article will show you what SUSE Linux Enterprise can do for you to achieve this. One way is the use of high availability clusters.

A second approach is the idea to patch the running software without the need of stopping it. This what live patching does for you. Imagine that a security issue is found in the Linux kernel and you are forced to update your systems in order to stay compliant or simply because of staying secure. That means downtime to your service.

SUSE Linux Enterprise Live Patching (or just Live Patching) helps you to avoid these downtimes. This means also that you will save money at the end of the day, because your critical business applications can run without interruption due to software maintenance.

To make this happen you need the SUSE Linux Enterprise Live Patching subscription. As of today this enables you to patch your SUSE Linux Enterprise Server Linux kernels while running e.g. SAP HANA without the need to shut SAP HANA down and reboot your server, which can take a serious amount of time if you consider the length of the reboot cycle and the time until all data is loaded back into memory.

2. Activation of SLE Live Patching

If your system is not registered against SUSE Customer Center (SCC) or a local SMT server, please do so now.

1. You need also a valid subscription code for your SLES installation
2. as well as for Live Patching.

You then have to use YaST to add the SUSE Linux Live Patching module to your installation. Start YaST and select “Add-On Products”:

You see your already installed Add On products. In this case there are no Add Ons installed yet.
Choose "Add".

You are asked to define the source where the add on product should be installed from. We choose "Extensions and Modules from Registration server".

We pick the SLE Live Patching Module:
You have to accept the EULA.

If you have not registered SLE Life Patching in SCC or SMT, you will be asked now to enter the registration code, then click NEXT.

Now the installation of SLE Live Patching is prepared. Click ACCEPT to start the the installation. This will install the base SLE Live Patching components together with the most recent live patch.
Confirm that the selected software packages will be installed:

YaST shows you the progress of the installation:
Finally you see an installation report.

The Add-on product screen shows that you successfully installed the SLE Live Patching add-on product.

3. Updating your system

- SLE Live Patching updates are distributed in a form that allows using standard SLE update stack for patch application. The initial live patch can be updated using zypper patch, YaST2 Online Update or equivalent method.

- The kernel is patched automatically during the package installation. However, invocations of the old kernel functions are not completely eliminated until all sleeping processes wake up and get out of the way. This usually takes just a small amount of time. Sleeping processes that use the old kernel functions are not considered a security issue but are restarted nevertheless to finish the patching process.

- To see the global status of patching, check the flag in /sys/kernel/kgraft/in_progress. The value 1 signifies the existence of sleeping processes that still need to be woken (the patching is still in progress). The value 0 signifies that all processes are using solely the patched functions and patching has finished already. Alternatively, use the kgr status command to obtain the same information.

- The flag can be checked on a per-process basis too. Check the number in /proc/process_number/kgr_in_progress for each process individually. Again, the value 1 signifies sleeping process that still needs to be woken. Alternatively, use the kgr blocking command to output the list of sleeping processes.

- 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. It can be achieved easily using the kgr poke command. Running processes are not interrupted.

3.1. Example for SLE Live Patching with SAP HANA as workload

SLES 12 - Kernel version: 3.12.51-52.31-default

K graft patch: kgraft-patch-3_12_51-52_31-default-2-1.1.x86_64.rpm

To test this scenario, we created a new HANA database with 1 table and 7 columns and 3 entries. we then wrote a python script that would query for all the entries in the table on a continuous loop.

We also started a continuous ping to the server and left it running.
We then applied the kgraft patch by using the following command:

```bash
# zypper in kgraft-patch-3_12_51-52_31-default-2-1.1
```

During the patch there was no interruption of the query and no break of the access to the server and service.

As you may get aware, this is simple and similar to any other patch process with SUSE Linux Enterprise, so no new procedures to implement.

4. The tool kgr for managing Live Patching

The tool kgr helps in managing Live Patching.

- `kgr status` shows the status of Live Patching: either in_progress or ready
- `kgr patches` shows the installed Live Patching patches
- `kgr blocking` Lists the processids of the processes that are preventing kgraft from finishing.

For more information see the man page of kgr.

5. References:

SUSE Linux Enterprise Live Patching:
https://www.suse.com/products/live-patching/

SUSE Linux Enterprise Server Administration Guide, Chapter Live Patching

SAP Note 1984787 SLES 12 Installation