Hewlett Packard Enterprise

linuxKI

Q1: Is LinuxKI safe to run on a production server?

A1: As with any software that contains a kernel driver, any defects in the kernel driver (whether in ftrace or LiKI) can cause a system crash or hang. So there are some risks but every attempt has been made to limit the risks as much as possible, including testing on large SMP servers and testing on a variety of Linux releases. LinuxKI has been run in many large mission critical environments without incident.

Q2: How much overhead does LinuxKI add to the system?

A2: The amount of overhead depends on the number and frequency of events trace. A good rule of thumb for most systems is about 3%. Remember, that a KI dump obtained with the runki script only collects trace data for a default of 20 seconds, so most systems can withstand a 3% degradation over 20 seconds.

Also, remember that LinuxKI also needs CPU and memory to run, as well as disk space if the data is logged to disk instead, and memory if the data is logged to /dev/shm.

Q3: How large are the KI dumps?

A3: This also depends on the number and frequency of events traced. On a busy DL380, the LinuxKI dump may be 300 MB or less, but on a busy Superdome, it could be well over 1 GB. We have seen 20 second KI dumps as large as 5 GB.

Q4: I get the following error when I install LinuxKI:

```
/opt/linuxki/module_prep: line 45: make: command not found
                Unable to build compatible LiKI module - you may still be
able to use ftrace mode
```

A4: In order to compile the LiKI module from source, you need the GCC compiler and the make packages installed, as well as the kernel headers.

Q5: I get the following error when I install LinuxKI:

```
# rpm --install linuxki-7.4-1.noarch.rpm
        Finishing installation of the Linux KI Toolset ...
        Unable to find compatible module - attempting to build from
source ...
hostkernel=3.12.53-12.g1f7ba8b-default
hostdistro=sles
hostversion=12.1
EXTRA CFLAGS=-g -O3 -Wall -DSLES12 -DHARDCLOCK STACK SKIP=0 -
DOTHER_STACK_SKIP=3
make -C /lib/modules/3.12.53-12.g1f7ba8b-default/build
M=/tmp/tmp.sqG4SojNeN   modules
make[1]: *** /lib/modules/3.12.53-12.g1f7ba8b-default/build: No such file
or directory.  Stop.
Makefile:147: recipe for target 'build' failed
make: *** [build] Error 2
        Unable to build compatible LiKI module - you may still be able to
use ftrace mode
```

A5: In order to build the LiKI DLKM module (likit.ko), you will need the Linux kernel headers installed. Note that you can still use LinuxKI in ftrace mode. Please refer to the LinuxKI Masterclass documentation for more details on the prerequisites.

Q6: I get errors about missing dependencies when installing LinuxKI.

A6: You can simply ignore dependencies when installing the toolset:

```
$ rpm --install --nodeps linuxki-7.4-1.noarch.rpm
```

Q7: When I try to run *kiinfo* on a running system, I get the following error:

```
kiinfo error: load_liki_module():94 [likis.c]: Unable to load likit.ko
module
```

A7: It's possible the proper DLKM is not present. Check the /opt/linuxki/modules directory to see if the appropriate likit.ko file is there that matches the version of the LinuxOS you are using (uname -r). It's possible the system has been upgraded.

To resolve the issue, simply remove any old likit.ko modules and re-compile as follows:

```
$ cd /opt/linuxki/modules
$ rm -f likit.ko.*
$ ../module_prep
```

The module_prep script should create a new likit.ko module.

Q8: I get the following error when I execute *kiinfo* or the *runki* script:

```
/opt/linuxki/kiinfo: error while loading shared libraries: libtinfo.so.5:
cannot open shared object file: No such file or directory
```

A8: Be sure to link the appropriate libtinfo.so library located in /lib64. For example:

```
$ ln -s /lib64/libtinfo.so.5.9 /lib64/libtinfo.so.5
```

In some cases, you may need to build the kiinfo from the source in /opt/linuxki/src/kiinfo, or try to copy kiinfo.sles15 or kiinfo.rhel8 to /opt/linuxki/kiinfo.

Q9: I get the following error when I execute *kiinfo* to analyze data on a running system:

```
  Failed to open liki directory in debugfs.  Make sure debugfs is mounted
or use debug_dir option to specify the correct location.
kiinfo error: init_liki_tracing():160 [likis.c]: Failed to initialize liki
tracing module: errno 2 - No such file or directory
  Unloading likit.ko...
```

A9: Be sure the debugfs is mounted:

```
$ mount -t debugfs debugfs /sys/kernel/debug
```

Q10: Can I collected LinuxKI data on a VMware host:

A10: No. Some Linux kernels do not include the necessary tracing facilities provided by more mainstream kernels. However, you can collect LinuxKI data from a VMware guest, and you can also collect LinuxKI data from a KVM host and KVM guest.

Q11: Can I collected LinuxKI data on a RHEL 5 system:

A11: No. RHEL 5 kernels do not include the necessary tracing facilities provided by more mainstream kernels. You must have Linux kernel version 2.6.32 or later and CONFIG_FTRACE=y must be set for the kernel build.

Q12: When I execute the *runki* script, it collected data using ftrace instead of LiKI. Why?

A12: Be sure to check the resulting ki.err.<timestamp> file from the data collected for a possible cause. A couple of reasons that ftrace is used:

1. The LiKI DLKM file (likit.ko) was not built during installation. Check the /opt/linuxki/modules directory to be sure the appropriate version is present that matches your Linux kernel version. The `module_prep` script can be used to build the LiKI DLKM file after installation.
2. The likit.ko DLKM module was not unloaded in a previous run. Try executing "`rmmod likit`", and if it is successful, try executing the ***runki*** script gain.
3. The insmod command could not be located. Be sure to check the PATH environment various and ensure the appropriate path for insmod is included.

Q13: On RHEL 7 systems, I get a message about LiKI DLKM tainting the kernel:

```
likit: module verification failed: signature and/or required key missing
- tainting kernel
```

Will this impact my RHEL support?

A13: In RHEL 7 the tainted message has been made more generalized, which requires a deeper look into why the kernel was tainted to determine if there is an unexpected condition. Now, any loaded driver module that is built outside of a full Linux kernel build will taint the kernel.

The /proc/sys/kernel/tainted file contains additional information on the taint reasons. For more information, see:

https://access.redhat.com/solutions/800133

Q14: I received some compile errors when installing LinuxKI. For example:

```
Building with KERNELRELEASE = 4.14.4-dmwc+
  CC [M]  /tmp/tmp.3dqEX1WZTN/likit.o
/tmp/tmp.3dqEX1WZTN/likit.c: In function 'syscall_enter_trace':
/tmp/tmp.3dqEX1WZTN/likit.c:3140:9: error: implicit declaration of
function 'strlen_user'; did you mean 'strnlen_user'? [-Werror=implicit-
function-declaration]
   fnlen=strlen_user((const char __user *)*args_tmp);
         ^~~~~~~~~~~
         strnlen_user
...
make: *** [Makefile:147: build] Error 2
       Unable to build compatible LiKI module - you may still be able to
use ftrace mode
```

A14: The Linux kernel changes often, and the LiKI DLKM compile is sensitive to changes in the kernel. Be sure the version of LinuxKI is supported for the specific Linux OS you are using. Currently, LinuxKI version 7.4 supports Linux kernels through 5.14.21.

Q15: When I try to install the LinuxKI toolset, I get the following error:

```
insmod: Error: could not insert module /usr/lib/modules/3.10.0-
957.12.2.el7.x86_64/misc/likit.ko: Required key not available
```

A15: Beginning with Linux kernels 4.4.0-20 and later, the `EFI_SECURE_BOOT_SIG_ENFORCE` kernel parameter has been set in the kernel config file. This prevents loading any unsigned third party modules if UEFI Secure Boot is enabled. Currently, LinuxKI (as well as other 3rd party kernel modules) cannot be installed if SecureBoot is enabled. Try to disable SecureBoot and re-install LinuxKI.

Q16: Installing LinuxKI on RHEL 8.0 results in the following error:

```
make[1]: Entering directory '/usr/src/kernels/4.18.0-147.3.1.el8_1.x86_64'
Makefile:977: *** "Cannot generate ORC metadata for CONFIG_UNWINDER_ORC=y,
please install libelf-dev, libelf-devel or elfutils-libelf-devel".  Stop.
make[1]: Leaving directory '/usr/src/kernels/4.18.0-147.3.1.el8_1.x86_64'
make: *** [Makefile:167: build] Error 2
insmod: ERROR: could not load module likit.ko: No such file or directory
```

A16: This issue appears to be introduced in the Linux 4.14.12 kernel. Prior to that, the elfutils-libelf-devel package was not required. To resolve, please install the elfutils-libelf-devel package.

Q17: When installing LinuxKI, I get the following error after the likit.c

```
make[1]: Leaving directory '/usr/src/kernels/4.18.0-167.el8.x86 64'
cp likit.ko likit.ko.4.18.0-167.el8.x86_64
insmod: ERROR: could not insert module likit.ko: Permission denied

ERROR: Unable to build compatible LiKI module
```

A17: The Permission Denied error occurs when SELinux is enabled as the installation will attempt install the likit.ko module to see if it is successful. To resolve, either disable SELinux or set it to permissive mode, or simply following the instructions to manually build the LiKI DLKM that you see right after the Permission deinied" error:

```
cd /opt/linuxki
rm -f /opt/linuxki/modules/likit.ko*
/opt/linuxki/module_prep
```

Q18: When executing runki.cmd on a Windows server, I get the following error:

```
xperf: error: NT Kernel Logger: Cannot create a file when that file
already exists. (0xb7)
```

A18: The error indicates that there is already a consumer of the Windows ETW trace events, and the ETW tracing can only have one consumer at the time. Other known consumers include Process Explorer (version 14 and later), Process hacker, and other tools, so check to see if there is another consumer of the ETW trace events. Some tools only collect trace data periodically, so try collecting data again with runki.cmd.

If you previously executed runki.cmd and it did not terminate normally, make sure XPERF has been stopped and then execute runki.cmd again:

```
> xperf.exe -stop "NT Kernel Logger"
```