
## *Rocky Enterprise Linux 9.2 Manual Pages on command 'systemd-pcrphase.8'*

***$ man systemd-pcrphase.8***

SYSTEMD-PCRPHASE.SERVICE(8)systemd-pcrphase.serviceSYSTEMD-PCRPHASE.SERVICE(8)

NAME

systemd-pcrphase.service, systemd-pcrphase-sysinit.service, systemd-pcrphase-initrd.service, systemd-pcrphase - Measure boot phase into TPM2 PCR 11

SYNOPSIS

systemd-pcrphase.service

systemd-pcrphase-sysinit.service

systemd-pcrphase-initrd.service

/usr/lib/systemd/system-pcrphase STRING

DESCRIPTION

systemd-pcrphase.service, systemd-pcrphase-sysinit.service and systemd-pcrphase-initrd.service are system services that measure specific strings into TPM2 PCR 11 during boot at various milestones of the boot process.

These services require systemd-stub(7) to be used in a unified kernel image (UKI) setup. They execute no operation when invoked when the stub has not been used to invoke the kernel. The stub will measure the

invoked kernel and associated vendor resources into PCR 11 before handing control to it; once userspace is invoked these services then will extend certain literal strings indicating various phases of the boot process into TPM2 PCR 11. During a regular boot process the following strings are extended into PCR 11.

1. "enter-initrd" is extended into PCR 11 early when the initrd initializes, before activating system extension images for the initrd. It is supposed to act as barrier between the time where the kernel initializes, and where the initrd starts operating and enables system extension images, i.e. code shipped outside of the UKI. (This string is extended at start of systemd-pcrphase-initrd.service.)
2. "leave-initrd" is extended into PCR 11 when the initrd is about to transition into the host file system, i.e. when it achieved its purpose. It is supposed to act as barrier between kernel/initrd code and host OS code. (This string is extended at stop of systemd-pcrphase-initrd.service.)
3. "sysinit" is extended into PCR 11 when basic system initialization is complete (which includes local file systems have been mounted), and the system begins starting regular system services. (This string is extended at start of systemd-pcrphase-sysinit.service.)
4. "ready" is extended into PCR 11 during later boot-up, after remote file systems have been activated (i.e. after remote-fs.target), but before users are permitted to log in (i.e. before systemd-user-sessions.service). It is supposed to act as barrier between the time where unprivileged regular users are still prohibited to log in and where they are allowed to log in. (This string is extended at start of systemd-pcrphase.service.)
5. "shutdown" is extended into PCR 11 when system shutdown begins. It is supposed to act as barrier between the time the system is fully up and running and where it is about to shut down. (This string is extended at stop of systemd-pcrphase.service.)
6. "final" is extended into PCR 11 at the end of system shutdown. It

is supposed to act as barrier between the time the service manager still runs and when it transitions into the final boot phase where service management is not available anymore. (This string is extended at stop of systemd-pcrphase-sysinit.service.)

During a regular system lifecycle, the strings "enter-initrd" ? "leave-initrd" ? "sysinit" ? "ready" ? "shutdown" ? "final" are extended into PCR 11, one after the other.

Specific phases of the boot process may be referenced via the series of strings measured, separated by colons (the "boot path"). For example, the boot path for the regular system runtime is "enter-initrd:leave-initrd:sysinit:ready", while the one for the initrd is just "enter-initrd". The boot path for the the boot phase before the initrd, is an empty string; because that's hard to pass around a single colon (":") may be used instead. Note that the aforementioned six strings are just the default strings and individual systems might measure other strings at other times, and thus implement different and more fine-grained boot phases to bind policy to.

By binding policy of TPM2 objects to a specific boot path it is possible to restrict access to them to specific phases of the boot process, for example making it impossible to access the root file system's encryption key after the system transitioned from the initrd into the host root file system.

Use systemd-measure(1) to pre-calculate expected PCR 11 values for specific boot phases (via the --phase= switch).

OPTIONS

The /usr/lib/systemd/system-pcrphase executable may also be invoked from the command line, where it expects the word to extend into PCR 11, as well as the following switches:

--bank=

Takes the PCR banks to extend the specified word into. If not specified the tool automatically determines all enabled PCR banks and measures the word into all of them.

--tpm2-device=PATH

Controls which TPM2 device to use. Expects a device node path referring to the TPM2 chip (e.g. /dev/tpmrm0). Alternatively the special value "auto" may be specified, in order to automatically determine the device node of a suitable TPM2 device (of which there must be exactly one). The special value "list" may be used to enumerate all suitable TPM2 devices currently discovered.

-h, --help

Print a short help text and exit.

--version

Print a short version string and exit.

SEE ALSO

systemd(1), systemd-stub(7), systemd-measure(1)