

Known limitations of CPU virtualization

Whenever perfect emulation of a CPU feature is impossible or too hard, KVM has to choose between not implementing the feature at all or introducing behavioral differences between virtual machines and bare metal systems.

This file documents some of the known limitations that KVM has in virtualizing CPU features.

x86

KVM_GET_SUPPORTED_CPUID issues

x87 features

Unlike most other CPUID feature bits, CPUID[EAX=7,ECX=0]:EBX[6] (FDP_EXCPTN_ONLY) and CPUID[EAX=7,ECX=0]:EBX[13] (ZERO_FCS_FDS) are clear if the features are present and set if the features are not present.

Clearing these bits in CPUID has no effect on the operation of the guest; if these bits are set on hardware, the features will not be present on any virtual machine that runs on that hardware.

Workaround: It is recommended to always set these bits in guest CPUID. Note however that any software (e.g. `WIN87EM.DLL`) expecting these features to be present likely predates these CPUID feature bits, and therefore doesn't know to check for them anyway.

Nested virtualization features

TBD