SDSi and KVM

By Roy Schestowitz
Created 21/11/2021 - 3:07pm
Submitted by Roy Schestowitz on Sunday 21st of November 2021 03:07:40 PM Filed under Linux [1]

- Intel Posts Updated "Software Defined Silicon" Driver To Activate Licensed Hardware Features - Phoronix [2]

Back in September we were first to report on Intel developing "Software Defined Silicon" support for being able to activate extra licensed hardware features not otherwise exposed. Intel hasn’t talked about the controversial feature in terms of product plans but this weekend they posted a new revision of this Intel "SDSi" Linux driver.

Intel Software Defined Silicon "SDSi" is about being able to securely activate additional features of the processor's silicon that won't otherwise by exposed out-of-the-box. This is likely with Intel Xeon processors in mind where Intel could offer additional features as an up-charge for those wanting to opt-in to extra features like say theoretically AVX-512 or AMX but without that license the feature wouldn't be exposed even with being baked into the processor. A decade ago Intel tried a similar concept with the "Intel Upgrade Service" that if paying for an activation code could allow additional cache to be exposed, higher clock frequencies, and/or Hyper Threading for select processors.

- KVM: x86/mmu: Overhaul TDP MMU zapping and flushing [3]

- New x86/x86_64 KVM Patches Would Help Reduce Excess TLB Flushing - Phoronix [4]

A set of more than two dozen patches by Google engineer Sean Christopherson overhauls KVM's x86/x86_64 TDP MMU zapping and flushing code.

The focus of the work is to help reduce the number of TLB flushes while the code is cleaned
up in the process too.

Source URL: http://www.tuxmachines.org/node/158212

Links:
[3] https://lore.kernel.org/lkml/20211120045046.3940942-1-seanjc@google.com/