

# Debug Support for Confidential VMs

*Tuesday, 21 September 2021 08:35 (20 minutes)*

Debug Support for AMD SEV Encrypted VMs.

Discussion on QEMU debug support for memory encrypted guests like AMD SEV/Intel TDX. Debug requires access to the guest pages, which are encrypted when SEV/TDX is enabled.

Discussion on exploring common interfaces which can be re-used for both AMD SEV and Intel TDX platforms with regard to encrypted guest memory access for debug in Qemu.

Latest posted patches on qemu-devel list from the Intel TDX team:

[RFC][PATCH v1 00/10] Enable encrypted guest memory access in QEMU

<https://lore.kernel.org/qemu-devel/20210506014037.11982-1-yuan.yao@linux.intel.com/>

Link to the last posted patch-set from AMD:

<https://lore.kernel.org/qemu-devel/cover.1605316268.git.ashish.kalra@amd.com/>

Original discussion thread on qemu-devel list :

[https://lore.kernel.org/qemu-devel/20200922201124.GA6606@ashkalra\\_ubuntu\\_server/](https://lore.kernel.org/qemu-devel/20200922201124.GA6606@ashkalra_ubuntu_server/)

## I agree to abide by the anti-harassment policy

I agree

**Primary author:** KALRA, Ashish

**Presenter:** KALRA, Ashish

**Session Classification:** Confidential Computing MC

**Track Classification:** Confidential Computing MC