Contribution ID: **42** Type: **not specified**

Live Migration of TD Guest

Tuesday, 21 September 2021 07:05 (25 minutes)

The Intel Trust Domain Extension (TDX) technology extends VMX and MKTME to enhance guest data security by isolating guests from host software, including VMM/hypervisor. Live migration support for such isolated guests (i.e. TDs) facilitates the deployment of TD guests in the cloud.
This talk presents the QEMU/KVM design of TDX live migration and initial PoC results for the migration performance evaluation. A common framework is added to the QEMU migration to support TD guests and other similar technologies (e.g. SEV guests). For TD guest live migration, the guest shared memory pages are migrated in plaintexts. The guest private memory pages, vCPU states and TD scope states are encrypted via a migration key when they are exported by KVM from the TDX module. A migration stream in the workflow has a KVM device created and the device creates shared memory between KVM and the QEMU migration thread to transport the encrypted guest states.

I agree to abide by the anti-harassment policy

I agree

Primary author: WANG, Wei (Intel Corp.)

Presenter: WANG, Wei (Intel Corp.)

Session Classification: Confidential Computing MC

Track Classification: Confidential Computing MC