linaro™

Arm Solutions at Lightspeed

Core Collective

Confidential Computing

Update - September 13th

Mathieu Poirier - Linaro

Progress Updates

- QEMU - System Emulation
  - Patchset to introduce foundational support for DA has been published
    - Related to the prerequisite features devices and root port must support
    - IDE and TEE capabilities to PCIe root port
    - DOE + IDE + TEE for sata device
  - Work continues to integrate the TDISP state machine with QEMU devices
    - What TDISP state is a device in?
    - Properly set the ‘T’ bit on PCIe DMA transaction when a device is in locked state

- Shrinkwrap support for QEMU
  - QEMU-SBSA machine can be booted on Shrinkwrap master branch
  - Some stability details need to be addressed
  - Public patchset is expected in the coming days

Progress Update

- QEMU - VMM
  - [RFC v2]
    - Based cca/V15
    - Shrinkwrap integrated solution
  - [RFC v3]
    - Based cca/V16
    - Older QEMU branch, based on Michael Roth's in-place-conversion work
    - Shrinkwrap integrated solution
  - [RFC v4]
    - Based cca/V16
    - Michael Roth's in-place-conversion work rebased to QEMU master
    - Shrinkwrap integrated solution
  - Carefully read the cover letter for each release
  - Carefully read the release notes and build instructions
  - No support for Device Assignment

- Currently working on RFCv5 → V17

Progress Update

- Device Assignment
  - Support CCA DA version hosted here on QEMU-SBSA
  - Work is progressing as time allows
  - No time estimate available

Backlog

- QEMU support for Boot Sync
- Enhance QEMU Live Migration support to Realms
- Planes → coconut-svsm on Arm64
- Confidential Containers
- Integration with “Device Evidence and Trust for PCI Security Protocol (TDISP)”


linaro
Arm Solutions at Lightspeed