linaro™

Arm Solutions at Lightspeed

Core Collective

Confidential Computing

Update - November 9th

Mathieu Poirier - Linaro

QEMU - System Emulation

Patchsets from Jim MacArthur to follow

1. Add SMMUv3 Root registers
   - Root registers definition
   - Discoverability of DA capability

2. RME-DA capabilities for PCIe Root Port
   - TEE flag in legacy configuration space
   - 2 new extended capabilities → IDE & RME-DA DVSEC

3. IDE & TEE support for ICH9 SATA Driver
   - Adds IDE and TEE capability to ICH9 SATA device

Upstreaming of Secure SMMU Support

Linaro Contribution

- Linaro offered help to speed things along and advance SMMU work → it was well received

Current Patchset Development

- Linaro is actively working on a patchset to define Secure and Realm SMMU register banks

QEMU - VMM

[RFC v5]

- Based cca/V21
- Shrinkwrap integrated solution
- Mailing list changelog says V21, Build instructions say V20

[RFC v5-kvmv23]

- Same as V5 (above), but based cca/V23
- Shrinkwrap integrated solution

[RFC v6]

- Will be based on Steven Price's cca-host-mm/v1/integration
- Will include Michael Roth's latest convert-in-place guest-memfd (v3) work
- Currently addressing comment from RFCv4 and RFCv5
- Not all comments will be addressed though
- Hoping for a publication before the KVM forum (November 12th and 13th)

Shrinkwrap Support for QEMU

Current Status

No progress since last update

Pending Action

- Anthony Roberts publish this PR
- Need help from CC management to get it review by a human

Backlog

- Device Assignment
- 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