linaro™

Arm Solutions at Lightspeed

QEMU Support for Realms

2026-05-11

Current state of QEMU Features

1. Publicly Available
   a. System emulation support for basic Realm
   b. Support to start a Realm using QEMU-VMM (ongoing)
   c. Support to start a Realm using kvmtool (Arm branch)

2. Not Publicly Available
   a. System emulation support for SMMU (Device Assignment)
   b. Support to start a Realm with Device Assignment using kvmtool

QEMU System Emulation

1. Proper integration of QEMU and SPDM-emu (FUNDED)
   a. Handling of T-bit in transport layer packets (TLPs)
   b. TDISP interface report
   c. Support for multiple device

2. Support for Realm SMMU (FUNDED)
   a. Enabling support for Realm SMMU using existing mailing list patches
   b. Resolving discrepancies between QEMU and RMM translation table format

3. Additional CPU features for architectural compliance (FUNDED)
   a. FEAT_RNG_TRAP, FEAT_ECV_POFF

4. Shrinkwrap support for QEMU architecture (PARTLY FUNDED)
   a. Urgently needs to be addressed

QEMU System Emulation

1. Virt architecture support (NOT FUNDED)
   a. Broken and no current plans to address the issues

2. SBSA architecture support (NOT FUNDED)
   a. Fix upstream regressions (TF-A and RMM)
   b. Definition of SMMU devices (TF-A)
   c. Adaptation of TF-A SMMU driver to SBSA platform
   d. Adaptation of RMM SMMU driver to SBSA platform
   e. Proper functioning of the TDISP state machine on SBSA platform

QEMU VMM for Realms

1. Supports RMM 1.0, build instructions available publicly

2. Supports RMM 2.0 without DA (FUNDED)
   a. Recently completed
   b. Patches for upstream are being prepared (TF-A + QEMU)

3. Support for Device Assignment (NOT FUNDED)
   a. Will target RMM 2.0
   b. Done on a best effort basis
   c. Priority is given to customer requests

Planned Sequence Of Work To Come

1. Upstreaming of QEMU-VMM patches to support basic Realm (Ongoing)
2. Provide support for Device Assignment, i.e SMMU, using kvmtool
3. Upstreaming of QEMU System Emulation SMMU support
4. Provide support for Device Assignment, i.e SMMU, using QEMU-VMM
5. Upstreaming of QEMU-VMM SMMU support

* KVM patches upstreaming done by Arm

Potential Upcoming Work

1. QEMU support for Boot Sync
2. Support for Realm live migration
3. Support for Planes
4. Support for CXL → Serious Undertaking
   a. Standardization (Entity Attestation Token)
   b. Qemu System emulation (SPDM-emu)
   c. Linux system equivalent of the current TDISP framework


linaro
linaro
linaro