LINARO OPEN DISCUSSIONS: QEMU 6.1

ALEX BENNÉE

INTRODUCTION

MISSION STATEMENT

- **Ensure an active and well maintained upstream project**
- Upstream useful architectural features
- Support software reference platforms
- Improve QEMU as a development tool

QEMU WORK IN LINARO

- Core Team, 3 people
  - all upstream maintainers
  - Lead maintainer, ARM, core translator, testing, tools
- Work from other groups
  - Core: Toolchain, Kernel Working Group
  - Vertical Tech: MCU, Server
  - Member Engineers

QEMU RELEASE CYCLE

Steady 3 releases a year, roughly 4 months apart

6.0	April 29th 2021
6.1	Late August 2021
6.2	December

2022 will start with 7.0

QEMU STABLE RELEASES

- roll-ups of trivial and security fixes
- mostly useful for distros

If you want features just track **master** branch

QEMU 6.1 RELEASE

ARM CPU FEATURES IN 6.1

SVE2	Neon in SVE form
FEAT_I8MM	Integer Matrix Multiply Accumulate
FEAT_BF16	Bfloat16 Support
FEAT_MTE3	MTE async faults
FEAT_TLBIOS/TLBRANGE	TLB invalidation instructions

See https://qemu.readthedocs.io/en/latest/system/arm/emulati

NEW ARM MODELS IN 6.1

rainier-bmc	Cortex-A7
quanta-q7l1-bmc	ARM926EJ-S
quanta-gbs-bmc	Cortex-A9
stm32vldiscovery	Cortex-M3

INTERNALS

- consolidating meson changes
- AccelOpsClass
- SysemuCPUOps
- target/foo/[kvm|tcg] cleanups
- custom configs

LINARO ADMIN

- Cards migrated to Cloud JIRA
- ARMv8.x Feature Matrix
- Releases

NEAR TERM FOCUS (6.2/7.0)

CONCRETE CPU MODELS

- Cortex A76
- Neoverse N1/V1

VECTOR EXTENSIONS

- MVE (Helium) - for M-profile
- SME, Scalable Matrix Extensions

LONG TERM THOUGHTS

The following slides do not represent planned work but are for discussion which we hope members will engage with.

V9.X

- -cpu max leaves a lot of gaps
- maintain a piecemeal feature focused approach

CONFIDENTIAL COMPUTING ARCHITECTURE

- Next level architecture
- Broad and complex
- Testing is a key challenge

SECURITY CO-PROCESSOR

- needed to model more complex systems
- usually contain secret sauce

COUNTERS, TRACES, EVENTS

- PMU is a registers only approach
- TRF and friends require translator support
- WFxT will a NOP be OK?
- RAS requires fault injection to be useful?

TRANSACTIONAL MEMORY

- Would require deep surgery to translator
- Does anyone care?

QUESTIONS/DISCUSSION

SUMMARY

- Small team
- Help us to help you

USEFUL PAGES

- QEMU Team Page
- Upstream Issues (GitLab)