УДК 004.318

Варианты реализации аппаратной поддержки виртуализации архитектуры Эльбрус

Д. В. Знаменский

ЗАО “МЦСТ”

Национальный Исследовательский Ядерный Университет “МИФИ”

Возрастающее значение приобретают технологии консолидации нагрузки и резервирования, а также сфера облачных вычислений. Их быстрое развитие обуславливает эволюцию технологий виртуализации, причём требования к производительности виртуализованных систем неуклонно возрастают. Практика показывает, что существенный прирост быстродействия можно обеспечить путём введения в архитектуру платформы средств аппаратной поддержки виртуализации. Различные варианты такой поддержки реализованы для архитектур x86, IA-64, ARM и SPARC. Предлагается рассмотреть возможные варианты реализации аппаратной поддержки виртуализации архитектуры Эльбрус.

С программной точки зрения, виртуализацию в системы на основе архитектуры Эльбрус планируется первоначально внедрять в форме паравиртуализации, при которой используется модифицированная гостевая ОС, взаимодействующая с гипервизором через программно-аппаратный интерфейс. Поэтому в первую очередь необходимо обеспечить аппаратную поддержку, необходимую для ускорения паравиртуализованных вычислений. Кроме того, при проектировании описанных средств поддержки требуется предусмотреть возможность их расширения для дальнейшего ускорения паравиртуализации, а также для перехода к полной виртуализации (запуску немодифицированных гостевых ОС).

Анализируя существующий мировой опыт [1] [2] [3], можно выделить минимально необходимое «ядро» средств аппаратной поддержки виртуализации, а именно — наличие гиперпривилегированного и гостевого режимов работы ядра процессора. Предлагается ввести эти режимы в архитектуру Эльбрус в первую очередь. Вводимые режимы ортогональны существующим привилегированному и непривилегированному режимам. В гиперпривилегированном режиме (режиме гипервизора) доступны расширения, позволяющие управлять гостевыми ОС. В гостевом режиме для особых ситуаций, прерываний и команд предусмотрен перехват с выходом в режим гипервизора. Кроме того, предлагается реализовать гипервызов — команду выхода из гостевой ОС в гипервизор. Рассматриваются варианты

реализации переходов между режимами, использующие различные техники переключения архитектурного состояния (специальная область памяти, теневые регистры).

Следом за описанным «ядром» предлагается ввести средства поддержки виртуализации прерываний и двухуровневой трансляции адресов. Поддержка виртуализации прерываний включает возможность перехвата прерываний гостевой ОС с уровня APIC в гипервизоре и механизм инжекции виртуальных прерываний в гостевую ОС. Двухуровневая трансляция адресов позволяет существенно повысить быстродействие систем с полной виртуализацией путём аппаратной трансляции гостевого физического адреса с помощью специализированной таблицы страниц гипервизора. Приводится вариант реализации, аналогичный технологии AMD Rapid Virtualization Indexing [4] - линейная таблица страниц гипервизора, а также альтернативный вариант — хэшируемая таблица страниц гипервизора [5]. Кроме того, предлагается аппаратно поддержать укороченные гостевые физические адреса с «плоской» таблицей страниц гипервизора [6], что позволит дополнительно увеличить быстродействие при использовании «компактных» гостевых ОС, использующих до 4 ГБ физической памяти.

Литература:

1. *Neiger et al.* Intel Virtualization Technology: Hardware Support for Efficient Processor Virtualization. - Intel Technology Journal, Volume 10, Issue 03 — 2006.

2. AMD64 Virtualization Codenamed «Pacifica» Technology. Secure Virtual Machine Architecture Reference Manual — AMD - 2005

3. *Goodacre J.* Hardware accelerated Virtualization in the ARM Cortex processors — XenSummit Asia - 2011

4. *Bhargava R., Serebrin B., Spadini F., Manne S.* Accelerating Two-Dimensional Page Walks for Virtualized Systems. - Proceedings of the 13th International Conference on Architectural Support for Programming Languages and Operating Systems - 2008

5. *Hoang G. et al.* A Case for Alternative Nested Paging Models for Virtualized Systems - Computer Architecture Letters — 2010

6. *Ahn J., Jin S., Huh J.* Revisiting Hardware-Assisted Page Walks for Virtualized Systems — Proceedings of the International Symposium on Computer Architecture - 2012