Estudo das Técnicas de Suporte à Virtualização para Projeto de Instruções no Contexto Multi-Core*

Manuela K. Ferreira, Henrique C. Freitas, Philippe O. A. Navaux
Instituto de Informática - Universidade Federal do Rio Grande do Sul
{mkferreira, hcfreitas, navaux}@inf.ufrgs.br

Abstract

In this paper we analyze two main trends in the development of virtual systems – full virtualization and paravirtualization – and the recent Intel Virtualization Technology for IA-32 architecture. The goal of this paper is provide basement for development of an instruction set that offer support for virtualization in a multi-core environment.

1. Introduction

Virtualização pode ser vista como a capacidade de executar múltiplos sistemas operacionais (SOs) em uma única plataforma física, dividindo os recursos de hardware. Com a disponibilização de múltiplos núcleos físicos, a execução de cada SO convidado poderia ocorrer realmente em paralelo, pois cada Máquina Virtual (MV) disponibilizada para cada SO convidado é totalmente isolada de qualquer outra MV, não havendo dependência de dados. Isso possibilitaria um melhor aproveitamento dos sistemas de múltiplos núcleos. Assim parece natural fornecer suporte à virtualização em um contexto *multi-core*.

Foram analizadas as duas principais técnicas de virtualização – virtualização total (*full virtualization*) e paravirtualização [1] – e a tecnologia Intel VT-x (*Virtualization Technology*), que oferece suporte à virtualização voltado para *single-core*. Essa análise tem o intuito de gerar conhecimento para desenvolver um conjunto de instruções que oferça suporte à virtualização especificamente em um contexto *multi-core*.

Este artigo apresenta alguns conceitos sobre virtualização, seguidos de uma descrição das duas técnicas de virtualização acima citadas. Por fim, é feita uma análise da tecnologia Intel VT-x.

* Apoiado pela empresa Microsoft.

2. Proposta do Estudo

O desenvolvimento de um conjunto de instruções que ofereça suporte à virtualização em um contexto *multi-core* está sendo feito em três etapas: (1) estudo dos conceitos de virtualização e das arquiteturas existentes que oferecem suporte à virtualização em um contexto *single-core*, (2) análise de quais são as necessidades da virtualização em um contexto *multi-core*, (3) desenvolvimento e avaliação de um conjunto de instruções que atenda às necessidades detectadas na etapa 2.

2.1. Conceitos e vantagens da virtualização

O Monitor de Máquinas Virtuais (MMV) é um software que gerencia a distribuição dos recursos de hardware para cada SO convidado, criando um ambiente virtual isolado (Máquina Virtual) para cada um SO [1].

Um dos principais benefícios da virtualização é o melhor aproveitamento dos recursos de hardware, sendo possível, por exemplo, em um mesmo servidor possuir vários SOs executando simultaneamente com suas aplicações específicas ao invés de haver um servidor para cada SO [2]. Outro exemplo é a divisão dinâmica de recursos, permitindo a realocação de recursos para a MV que mais necessitar deles naquele momento. Outra vantagem é a maior confiabilidade, pois as MVs são totalmente isoladas, sendo possível reiniciar um SO que travou sem afetar os outros sistemas instalados nas de mais MVs [1].

2.2. Técnicas de Virtualização

A virtualização total permite virtualizar SOs não modificados, pois replica virtualmente toda a arquitetura do hardware [1]. O software VMWare é um

exemplo de MMV que implementa a virtualização total. A última versão do software Xen também é capaz de implementar virtualização total quando o suporte de hardware à virtualização está presente.

Na paravirtualização, o SO convidado é modificado para poder executar concorrentemente com outros SOs que também foram modificados para a paravirtualização [2]. O Xen é um MMV que originalmente suportava apenas paravirtualização [3].

A paravirtualização sempre demonstrou desempenho superior ao da virtualização total. Entretanto, com a utilização do atual suporte à virtualização fornecido pelas arquiteturas, ambas as técnicas têm apresentado desempenho equivalente. As últimas versões do VMWare ESX 3.0.1, com virtualização total, e do XenEnterprise 3.2., com paravirtualização, apresentam desempenho semelhante e ambas aproveitam o suporte de hardware à virtualização fornecido pelos processadores atuais [4].

2.3. Intel VT

O suporte à virtualização para arquiteturas IA-32 fornecido pela Intel VT-x inclui a oferta de dois novos modos de operação da CPU chamados VMX *root*, onde o MMV executa, e VMX *non-root*, onde os SOs convidados executam. Ambos suportam todos os quatro níveis de privilégio [2], como pode-se ver na figura 1, permitindo que os SOs convidados executem em um nível zero e acreditem que possuem o controle da CPU.

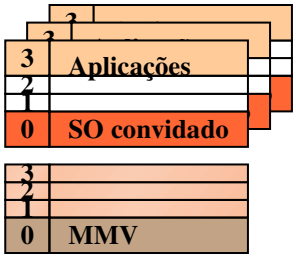

Figura 1 – Modo VMX *root* e VMX *non-root* [2].

Esta tecnologia define duas novas transições: **MV entrada** (*VM entry*), que é a transição do modo VMX *root* para o modo VMX *non-root*, e **MV saída** (*VM exit*) que faz a transição inversa [2], veja figura 2. Também é disponibilizada uma nova estrutura de dados, o VMCS, que guarda o estado da CPU em duas áreas: área de estado do convidado e área de estado do hospedeiro. Com a configuração do VMCS é possível definir quais instruções irão causar **MV saídas** [2].

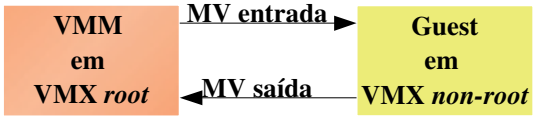

Figura 2 – MV entrada e MV saída.

Cada **MV entrada** irá salvar o estado da CPU na área de estado do hospedeiro no VMCS e carregar o novo estado da área de estados do convidado no VMCS. A **MV saída** irá salvar o estado do processador na área de estado do convidado no VMCS e carregar o estado da área de estado do hospedeiro no VMCS [2].

3. Conclusões

Neste trabalho, foi apresentada uma análise das duas principais técnicas de virtualização, onde pode-se concluir que com o atual suporte à virtualização oferecido pelos processadores modernos, a virtualização total possui desempenho cada vez mais semelhante ao da paravirtualização.

Também foi apresentada uma análise da Intel VT-x que oferece suporte à virtualização em arquiteturas IA-32, esse suporte se concentra na troca de contexto entre o MMV e os SOs convidados e na detecção de instruções executadas pelo SOs convidados que devem ser interceptadas pelo MMV.

Como trabalhos futuros pretende-se simular processadores com a tecnologia Intel VT-x em um contexto *multi-core* com a utilização das ferramentas ArchC e SystemC, e com isso identificar quais instruções poderiam ser acrescentadas ou modificadas para oferecer suporte à virtualização neste contexto.

4. Referências

[1] R. Rose, “Survey of System Virtualization Techniques”, CiteSeer.IST, http://citeseer.ist.psu.edu/720518.html, Março 2004.

[2] R. Uhlig, G. Neiger et all, “Intel Virtualization Technology”, Computer Journal, v. 38, p. 48-56, Maio de 2005.

[3] Y. Dong, S. Li et all, “Extending Xen* with Intel Virtualization Technology”, Intel Technology Journal, v. 10, Agosto de 2006.

[4] Xen Source, “A Performance Comparison of Commercial Hypervisors”, em julho de 2007 em http://www.xensource.com/files/hypervisor_performance_comparison_1_0_5_with_esx-data.pdf, 2007.